NETWORK SECURITY ARCHITECTURE FOR DEMAND RESPONSE/SENSOR NETWORKS

CONSULTANT REPORT
(DRAFT)

Prepared for:

California Energy Commission
Public Interest Energy Research Group

Prepared by:

CyberKnowledge
& University of California at Berkeley

October, 2005.

(Revised June 2006)

10.2005.1

Prepared By:
CyberKnowledge
(45110 Pawnee Drive, Fremont, CA 94539)
P.A.Subrahmanyam (Principal Investigator)

&

University of California at Berkeley
David Wagner (Principal Investigator)
Deirdre Mulligan (Co-Principal Investigator)
Erin Jones
Umesh Shankar
Jack Lerner

Contract Number 500-01-043

Prepared For:
California Energy Commission

David Michel
Contract Manager

Gaymond Yee
Project Manager

Martha Krebs, Ph.D.
Deputy Director
Energy Research and Development Division

Scott W. Matthews
Action Executive Director

DISCLAIMER

ACKNOWLEDGEMENTS

The authors wish to thank Gaymond Yee for his guidance, support, responsiveness, and timely introductions. We wish to thank Ron Hofmann for helping us define the goals and scope of the project, and for sharing valuable insights about California's demand response strategy.

The authors would like to express our grateful thanks to the stakeholders who consented to be interviewed for this project, and helped us try to develop a picture of the possible future implementations of demand response systems and their legal ramifications. Finally, we would like to acknowledge and thank our industrial collaborators and colleagues for sharing their insights and inputs.

PREFACE

The Public Interest Energy Research (PIER) Program supports public interest energy research and development that will help improve the quality of life in California by bringing environmentally safe, affordable, and reliable energy services and products to the marketplace.

The PIER Program, managed by the California Energy Commission (Energy Commission), annually awards up to $62 million to conduct the most promising public interest energy research by partnering with Research, Development, and Demonstration (RD&D) organizations, including individuals, businesses, utilities, and public or private research institutions.

PIER funding efforts are focused on the following six RD&D program areas:

- Buildings End-Use Energy Efficiency
- Industrial/Agricultural/Water End-Use Energy Efficiency
- Renewable Energy
- Environmentally Preferred Advanced Generation
- Energy-Related Environmental Research
- Strategic Energy Research

What follows is the final report for the **Network Security Architecture for Demand Response/Sensor Networks project**, CIEE Award No. DR-04-03A, B, WA No. DR-005, under CEC/CIEE Prime **Contract No. 500-01-043**, conducted by **CyberKnowledge** and the **University of California at Berkeley**. The report is entitled **Network Security Architecture for Demand Response/Sensor Networks**. This project contributes to the PIER **Demand Response Enabling Technology Development** (DRETD) program.

For more information on the PIER Program, please visit the Energy Commission's Web site at: http://energy.ca.gov/research/index.html or contact the Energy Commission's Publications Unit at 916-654-5200.

TABLE OF CONTENTS

TABLE OF FIGURES

ABSTRACT

The goal of this project was to explore the privacy and security concerns that arise in the context of advanced metering and demand response infrastructures and propose general options for addressing them. We have studied likely implementations of advanced metering and demand response, investigated the privacy and security issues that will become important as the technology is deployed, and suggested both legal and technological solutions. Our technological solutions have focused in particular on security and privacy in sensor networks and agile radio nodes, and the likely role of these technologies in a future demand response infrastructure.

The major accomplishment of this project was to develop an overall picture of the likely short, medium and long term deployment scenarios for demand response, delineate the central design elements of each, identify the privacy and security issues of each, and recommend possible technical and legal solutions. By identifying opportunities to build privacy and security solutions into the demand response architecture, in addition to legal and regulatory solutions, this approach will aid developers and policy makers alike. Directions for future work are also suggested.

EXECUTIVE SUMMARY

In the wake of the California energy crisis of 2000-2001, the California Energy Commission (CEC) and California Public Utilities Commission (CPUC) are aggressively pursuing "demand response" energy programs aimed at reducing peak energy demand. Ongoing efforts aimed at developing technologies that will enable demand response benefits include advanced metering, sensors, and control technologies research and development. It is envisioned that these will eventually be coupled with a communication and network infrastructure that supports the multicast of real-time pricing information, as well as the aggregation of energy usage and billing information.

It is the goal of this project to provide background information, frameworks, and recommendations that will promote increased discussion of the important and somewhat overlooked security and privacy concerns raised by the introduction of this technology. We focus special attention on security and privacy issues that may develop in future demand response networks that employ sensors and wireless communication networks in conjunction with advanced metering technologies.

Our research objective was to identify the specific security and privacy issues associated with demand response energy systems and use this as a basis for developing an overall framework—technical architecture and policy controls—for delivering security and privacy. We have developed a short/medium/long-term framework for looking at likely demand response architectural features, understanding the attendant privacy and security issues, and suggesting recommended solutions.

The areas of study and the outcomes in these areas are summarized below.

- Study of privacy concerns in the demand response context
  - A legal survey was performed to identify legal rules that affect privacy, public utility business practices, use of utility records by law enforcement, and unauthorized access to computing resources and communications.
  - Interviews were conducted with relevant stakeholders to learn about advanced metering and demand response system requirements, data handling practices and use of utility data, and future plans for infrastructure development.
- Study of security issues in demand response/wireless/sensor networks
  - Security challenges, including likely attack methods, have been catalogued and studied for sensor networks that are representative of those that likely to be used in future demand response deployments.
  - Security measures for protecting data in the specific types of wireless sensor networks expected in demand response deployment are developed and explained.

- Potential security threats associated with the use of agile radio nodes in demand response networks have been assessed; techniques for addressing selected classes of these threats have also been investigated.

- A Network Security Architecture/framework has been delineated, and provides a basis for developing detailed security implementations in heterogeneous networks.[a]

Some of the results and recommendations of the study are summarized below.

Sensor Network Security

Wireless sensor networks afford a natural and potentially cost-effective mechanism for the monitoring and control of appliances and energy management systems. However, sensor networks may suffer from many layers of potential vulnerabilities: they are subject to the problems of computer networks in general; ordinary wireless networks; ad-hoc networks; and additional physical attacks that take advantage of the sensor nodes' new form factor. Sensor nodes have limited resources, including slow CPUs, short battery life, and small memories. These limitations both open up additional attack avenues for adversaries and make it difficult to use existing cryptographic techniques as defenses. The security implications of these criteria have been studied in detail, and lead to the following recommendations for designing and implementing sensor networks designed for demand response applications:

- Encryption is recommended over a manufacturers' proprietary format for securing data over the entire transmission path, from the meter to the utility.

- We recommend that designers adhere to published, well studied, and where possible, provably secure standards.

- We recommend the use of authentication for all data.

- We recommend that spread-spectrum radios be used if feasible.

- We recommend that a single-hop network be used if possible for sensor networks.

- As it is expected that customer usage and demand response data are likely to be held, either temporarily or long-term, by both utilities and third party systems, current and updated rules covering data privacy and business record handling need to apply to both utilities and third-parties who hold the data.

- Access to hourly customer usage data should be limited within the utility, to systems that have a justifiable requirement for it.

- Guidelines for how much data is necessary and should be stored for the purposes of customer service and other functions should be set by the appropriate regulatory body.

- Separate data pathways (communication channels) for systems that do and do not require identifiable data should be built into the system. In other words, data that is tagged with information relating to the consumer that is private

should be transmitted over a different (more "secure") channel compared to data that is anonymous.

- The data mining of hourly usage data (or fine-grained usage data in general) should be carefully monitored and regulated.
- When significant computing capability exists inside the home, that processing capability should be developed to enable the customer or his smart equipment to perform necessary energy-related functions – energy monitoring, demand response control, self-education, and billing – at the home site.

Agile Radio Node Security

Agile or Software Defined Radios (SDRs) provide an efficient and cost-effective solution to the problem of building multi-mode, multi-band, multi-functional wireless devices that can be enhanced using software upgrades. Agile Radio Nodes can play an important role at several levels of the hierarchy in the context of Demand-response networks. Specifically, SDRs can be profitably leveraged in sensor cluster gateway nodes and neighborhood gateway nodes, as well as in the wireless infrastructure.

We have examined the security issues that can arise in Demand-response networks that employ agile radio nodes. Some of the issues related to software download security are unique to the use of agile radio nodes. More generally, hackers can use blended attacks against both the radio and computer layers of agile radio nodes. To defend against the blended attack requires a multi-layered defense-in-depth which protects both the agile nodes and infrastructure servers.

A high confidence security architecture must

- Ensure integrity of the software applications and downloads including download, storage, installation and instantiation;
- Ensure integrity of the reconfigurable platform against blended attacks by employing defensive layers (firewalls, intrusion detection, virus protection);
- Integrate a set of complementary strategies where available and appropriate, for example, it may be beneficial to incorporate biometric (e.g., fingerprint) and radiometric assurance techniques;[b]
- Employ trusted architecture, high assurance operating systems and middleware[c]
- Preserve the integrity of the analog signal or data, and protect it from exploitation and/or compromise.

An important open problem in this context relates to the security challenges arising from the need to accommodate third party software to be downloaded onto agile radio nodes.[d]

Network Security Architecture

The network security architecture/framework delineated here draws from evolving networking standards, and captures the perspectives and security challenges of service

providers, enterprises, and consumers and is applicable to a variety of transport media, such as wireless, optical and wire-line networks. In particular, the architecture addresses security concerns for the management, control, and use of network infrastructure, services and applications.

The security architecture divides end-to-end network security-related features into separate architectural components. The goal is to allow for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks.

The security architecture provides a framework that addresses the following key questions with regard to the end-to-end security:

- What kind of protection is needed and against what threats?
- What are the distinct types of network equipment and facility groupings that need to be protected?
- What are the distinct types of network activities that need to be protected?

These questions are addressed by three architectural components: sets of security measures (also referred to as security dimensions), security layers and security planes. The principles described by the security architecture can be applied to a wide variety of networks independently of the network's technology or location in the protocol stack.

We suggest that demand response systems should have an associated security program that consists of policies and procedures in addition to technology, and that progresses through three phases over the course of its lifetime: the Definition and Planning phase; the Implementation phase; and the Maintenance phase. The security architecture can be applied to security policies and procedures, as well as technology, across all three phases of a security program.

Privacy Concerns: Legal/regulatory issues

Our study of the legal/regulatory issues related to privacy concerns in demand response systems lead to the following recommendations:

- Laws controlling law enforcement access to utility records should be updated to ensure that detailed and real-time consumption data held by or accessible to the utility is only available to law enforcement with a warrant.
- If utilities begin to provide other services, such as Internet service, over a wholly owned medium, such as broadband over powerline (BPL), stricter telecommunications privacy laws and regulations should be applied or extended to apply to these services and other communications sent via BPL. [e] Smart appliances systems for the home should be designed to protect a customer's reasonable expectation of privacy in his activities and preferences, and appropriate regulations/regulatory bodies should enforce this principle to the extent possible.
- If data from in-home smart appliances, in-home sensors or smart meters is available to be collected, we recommend that state laws or regulations be updated to address the

handling of this data; such rules should protect privacy by limiting the utility's and other business processors' use of the data, and limiting access and use by government and private parties.

Benefits to California

One of the goals of this project was to foster an increased awareness and deeper understanding of the security and privacy issues that exist in advanced metering and demand response systems among the technical designers who build the elements and infrastructures, and among the regulators and legislators who oversee or drive that process.

We anticipate that this report will be useful to the energy industry, for helping identify areas where security and privacy issues may be important for both commercial or consumer protection. We hope that our recommendations may provide a starting point and framework for the development of solutions to network security, in particular in demand response networks that may employ emerging sensor and wireless technology.

Attention to these problems benefits California utilities, as their networks are strengthened against attack, and their customers retain confidence in the companies' handling of their personal information. Attention to these problems benefits California's consumers, both in protection of their California Constitutional rights to privacy, and in the safety of their personal information from exploitation or theft. We hope this report may also provide information useful to regulators and lawmakers that may need to enact new rules to enforce sound privacy and security choices.

1.0 Introduction

1.1 Background

In the wake of the California energy crisis of 2000-2001, the California Energy Commission (CEC) and California Public Utilities Commission (CPUC) are aggressively pursuing "demand response" (DR) energy programs aimed at reducing peak energy demand. It is hoped and expected that both residential and commercial customers will reduce energy usage and/or shift their usage to non-peak hours once subject to time-varying energy pricing plans, such as time-of-use or real-time pricing. Demand response is essentially a means for conveying market conditions through pricing or reliability signals that influence customers to exert choice regarding their time-varying use of electricity. Ongoing efforts aimed at developing technologies that will enable demand response benefits include advanced metering research and development [OpenAMI], and sensor and control technologies development [DRETD]. These will be coupled with a communication and network infrastructure that supports the multicast of real-time pricing information, as well as the aggregation of energy usage and billing information.[a]

Demand response programs were studied in the residential context in a California Statewide Pricing Pilot program mandated by the state legislature,[b] and developed, monitored and studied by working groups reporting to the CPUC and CEC.[c] This project studied a variety of time-varying rates and customers' reactions to them, and allowed utilities an opportunity to try out various technologies that might be used to implement advanced metering and demand response in a widespread residential deployment. Subsequent to the pilot, California's main investor-owned utilities (hereinafter, IOUs or "utilities") have submitted plans to the CPUC proposing various strategies for widespread deployment of advanced metering infrastructures and proposed dynamic pricing tariffs.

In response to these utility plans, the CPUC proposed a framework of six functionality criteria to use for evaluating proposed advanced metering and demand response deployments.[d] In addition to being able to support the desired dynamic tariffs,

---

[a] It is intended that the associated infrastructure support other operations, such as diagnosis and maintenance, but a discussion of this is beyond the scope of this paper.

[b] The pilot study was enacted in Cal. Pub. Util. Code § 393 (West 2005), effective January 1, 2001.

[c] Reports on the Statewide Pricing Pilot are available at http://energy.ca.gov/demandresponse/documents/index.html.

[d] Order Instituting Rulemaking on policies and practices for advanced metering, demand response, and dynamic pricing, R. 02-06-001, (Cal. Pub. Util. Comm'n Feb. 19, 2004) (Joint Assigned Comm'r & Admin. Law Judge's Ruling Providing Guidance for the Advanced Metering Infrastructure Bus. Case Analysis). The ruling suggested that proposed AMI systems should support the following six functions: (a). Implementation of a variety of variable tariffs for residential, and small, large, and very large commercial customers on an opt out basis. (b). Collection of usage data at a level of detail (interval data) that supports customer understanding of hourly usage patterns and how those usage patterns relate to energy costs. (c). Customer access to personal

these functional criteria suggest that advanced metering and demand response technologies should provide a customer with the ability to access his data, learn about his usage, and understand his energy costs. An appropriate infrastructure should enable energy management, customized services, and improved customer service. In the appendix of this ruling, it is also suggested that the technology choices implemented should be "respectful of potential privacy concerns" of the customer.

It is the goal of this project to provide background information, frameworks, and recommendations that will promote increased discussion of the important and somewhat overlooked security and privacy concerns posed by advanced metering and the demand response infrastructure. This goal has been shared among three groups of researchers: researchers in the Department of Electrical Engineering and Computer Sciences at U.C. Berkeley and at CyberKnowledge who studied security and privacy issues in sensor networks; researchers at CyberKnowledge, who studied frameworks for network security architectures and security issues in agile radio nodes; and faculty and law students at the Samuelson Law, Technology & Public Policy Clinic at the Boalt Hall School of Law at U.C. Berkeley, who studied the legal, regulatory and business practice issues that effect privacy and security in planned demand response architectures and advanced metering initiatives, including sensor networks, data communication, data warehousing, and data processing.

1.2 Overview

This research focuses on security and privacy issues in the context of demand response (DR) networks, especially DR networks employing sensors and wireless sensor networks in conjunction with advanced metering technologies [DRETD]. The security of critical national infrastructures, such as electric utilities and distribution infrastructure, was identified as an area of key importance in a Presidential commission report in 1998 [PCAST CIP 1998]. The importance of security and cybersecurity in this context has since been highlighted as a consequence of the exceptional outages in power grids in the northeast, and a general increase in the number of hostile attacks on cyber infrastructure.

Security in wireless networks is a topic that has received considerable attention in the press recently, particularly in the context of the growing popularity and increase in the number of IEEE 802.11x based "WiFi" networks. This has resulted in an increased awareness on the part of both individuals and enterprises of the importance of security in wireless networks, and equally importantly, served to underline the subtleties and difficulties of dealing with the overall security problem. Wireless sensor networks and other emerging wireless technologies represent new components being injected into a

---

energy usage data with sufficient flexibility to ensure that changes in customer preference of access frequency do not result in additional AMI system hardware costs. (d). Compatible with applications that utilize collected data to provide customer education and energy management information, customized billing, and support improved complaint resolution. (e). Compatible with utility system applications that promote and enhance system operating efficiency and improve service reliability, such as remote meter reading, outage management, reduction of theft and diversion, improved forecasting, workforce management, etc. (f). Capable of interfacing with load control communication technology.

legacy system. It is therefore important to pay particular attention to the security issues that relate to these technologies.

Privacy is a growing concern of California's citizens and policy makers. From California's Constitution to its recent leadership in requiring companies to acknowledge and alert citizen's to breaches effecting personal information, California has consistently sought to preserve citizen's privacy through legal and regulatory mechanisms that improve data handling practices and encourage sound investments in privacy and security architectures. Addressing citizens' privacy and security concerns, California will pave the way for a smooth transition to DR and AMI, as they are approved. The failure to fully vet and address privacy issues relating to technical developments can lead to the rejection, and in extreme circumstances demonization, of useful technology. Considering policy goals during the process of technical design and implementation provides fruitful opportunities to maximize the benefits and minimize the risks posed by new technologies.

Demand response systems are expected to eventually serve most of California's residential and commercial energy customers, whose privacy and security interests must be considered up front. It is especially important that relevant security and privacy issues are considered at an early stage, and potential solutions engineered into the design of the DR network, as it has historically proven to be much more difficult and expensive, if not impossible, to retrofit privacy and security solutions. Further, security and privacy issues must be addressed at *several levels*: at the system level (spanning multiple networks, business practices, regulatory and legal constraints), at the algorithmic level, and in the context of specific deployments. Examples of these levels are dispersed in the subsequent sections of this report.

1.3 Project Objectives

Our research objective is to develop a basis for developing an overall privacy-security framework—technical architecture and policy controls—in the context of demand response (DR) systems. The overall goals of the research are to:

- Identify and categorize privacy and security concerns that arise in the context of demand response systems and advanced metering infrastructure, including, specifically, privacy and security concerns and threats arising in the context of:
    - Sensor networks which consist of nodes with limited power and computation capacity, and their application in the DR context;
    - Communication gateways and channels; a communication channel typically consists of a medium (e.g., cable, phone lines, optical fiber, wireless) and a communication mechanism/protocol.
    - Alternative business models presented by DR adoption; an example of an alternative business model is the use of third party service providers to provide services such as transmission of energy curtailment signals and data archival services.

- Define the nodes in the architecture where agile radio technology e.g., Software Defined Radios (SDRs) can be advantageous; Investigate the security issues relating to such nodes.
- Develop a Network Privacy and Security Architecture that accommodates communication between the field of sensors and the back-end network/management nodes at the utilities, Independent System Operators (ISOs), and energy utilities.

The project will study the following elements so their effect on an overall architecture can be addressed:

- Security and privacy issues,
- Sensor specific constraints, e.g., energy and power constrained nodes
- Attack modes (of different categories)
- Evolving technology trends e.g., Software Defined Radios and Cognitive Radios.
- Existing & evolving standards in industry (e.g., in the networking and wireless domains)

The specific tasks pursued by our experts were the following:

1. Privacy concerns in the demand response context (UC Berkeley Samuelson Law Technology & Public Policy Clinic):

    - Analyze Constitutional and other privacy concerns raised by collection of information about the interior of residences. Develop recommendations for addressing heightened privacy concerns consistent with United States and California Constitutions and consumer expectations and consistent with other needs (regulatory, criminal, private).
    - Generate a list of relevant stakeholders.
    - Meet with technologists to understand system requirements.
    - Interview users of current Energy Service Provider (ESP) data (ESPs, law enforcement, regulators) to understand current use of utility data and rules about internal use and disclosure to third parties.
    - Consolidate collected data to develop a list of privacy related concerns. Define the broad agenda related to privacy and security in the DR context.
    - Identify possible architectural features that would support privacy and explore feasibility of adoption.

2. Security and privacy issues in Wireless/Sensor Networks (U.C. Berkeley Computer Sciences Dept., and CyberKnowledge):

- Identify and categorize attack modes in sensor networks
- Identify known vulnerabilities in existing protocols
- Identify appropriate security goals for DR/sensor networks

3. Network Security Architecture and Agile Radio Node Security (CyberKnowledge):

- Understand and assess the security challenges in demand response networks from the perspectives of different disciplines and stakeholders, including
    - Network-related security and privacy concerns
    - Security issues in Sensor networks
    - Security in Agile Radios
    - Privacy concerns in the DR context
- Develop a framework for a network security architecture that can serve as basis for Phase II research and development, and that
    - Accommodates security & privacy in leaf/sensor/cluster nodes, gateway nodes, transit networks, wide area networks and enterprise networks;
    - Respects the energy and power constraints of the sensor nodes (and consequently associated computation and communication constraints in the context of security and privacy algorithms);
    - Anticipates the use of Software Defined Radio (SDR) technology in some of the gateway nodes.

1.4 Report Organization

This report is organized as follows:

Section 1.0 Introduction

Section 2.0 Project Approach

Section 2.0 presents the approach and methodology used in each of the three main investigations that took place under the auspices of this contract: the study of legal framework and likely evolution of security and privacy elements of demand response systems, the study of sensor and wireless system vulnerabilities and solutions, and the study of agile communication systems security and their promise in demand response systems.

Section 3.0 Project Outcomes: Identification of Regulatory Framework for Demand Response

In this section, we present the data and research results for the legal survey (section 3.1), and the data collected from stakeholder interviews and other study on current and future trends in demand response infrastructure development.

Section 4.0 Project Outcomes: Identification of Technologies and Potential Solutions

This section presents research results in the areas of security in sensor networks (section 4.2), security in agile radio nodes (sections 4.3-4.5), and a framework for network security architecture.

Section 5.0 Conclusions and Recommendations

Section 5.1 summarizes our overall conclusions. In section 5.2, we integrate the results of the investigations detailed in sections 3.0 and 4.0 into sets of key issues and recommendations for the future development of secure and private demand response systems. The demand response timeline is broken down into short, medium and long term scenarios, and likely issues and recommended solutions are suggested for each time period. In this section, we also summarize the benefits to California and make recommendations for future research.

There are 2 appendices:

Appendix A: Supplemental Elaboration of California Statutory Law

Appendix B: List of Interviewees and Compiled Interview Questions

In addition, explanatory notes are contained in an extensive set of footnotes and endnotes.

2.0 Project Approach

2.1. Overview and Methodology

This network security and privacy analysis project was structured as a collaborative, multi-disciplinary effort, and was conducted jointly by three groups: researchers at the Samuelson Law, Technology & Public Policy Clinic at the Boalt Hall School of Law at U.C. Berkeley, who focused on identifying the regulatory framework, developing a picture of the likely evolution of demand response infrastructures, and investigating the legal aspects of security and privacy issues that arise therein; researchers in the Computer Science department at U.C. Berkeley and CyberKnowledge, who focused on data security issues in sensor networks; and researchers at CyberKnowledge that focused on security issues of agile communications systems and their likely implementation in a demand response framework. Researchers at CyberKnowledge also explored an overall architectural framework for demand response/Sensor networks that could serve as a basis for the exploration of relevant security and privacy issues. CyberKnowledge was further responsible for overall project management and coordination.

- The regulatory and legal framework that demand response programs will encounter was studied by reviewing the California state laws pertaining to investor-owned utilities, privacy and handling of business records, and

unauthorized computer access. Federal law on privacy of utility records and unauthorized computer access were surveyed as well. California Public Utilities Commission and California Energy Commission regulations were also surveyed, and ratesetting cases currently pending before the CPUC, pertaining to advanced metering and demand response, were monitored. We have also interviewed representatives of law enforcement to determine their role. We have set forth this legal framework as an outcome of this project.

We have investigated the likely evolution of demand response infrastructures in a number of ways. To develop a picture of what advanced metering and demand response might look like in the short term, we have studied the California Statewide Pricing Pilot, developed by the California Legislature, CPUC and CEC to test demand response concepts, and have interviewed some of the people who monitored and studied the Pilot about their findings. We also have monitored current utility filings with the CPUC on this topic. To develop a picture of what longer term plans for demand response might entail, we have interviewed representatives of the three major utilities about their plans, interviewed industry consultants and infrastructure sub-contractors about their views, monitored the OpenAMI project, and attended talks on the future of demand response enabling technologies. [e]

- We studied data and security issues in sensors and other demand response network elements by surveying the literature to collate several classes of attacks, then analyzing those in light of the demand response context developed in other parts of this project, arriving at several concrete recommendations for implementation.
- Security issues in agile communications systems were studied by investigating the perspectives of the different stakeholders involved, identification of the kinds of threats possible, and potential methods to address such threats.
- The Network Security Architecture framework builds on existing standards, and anticipates an evolution to accommodate emerging technology related to sensor networks, agile radios, as well as security mechanisms for legacy networks, including SCADA networks.

3.0 Project Outcome : Identification of Legal and Regulatory Framework for Future Demand Response Projects

Key tasks and objectives of this section of the project were:

[e] See section 3.3.3 for information on OpenAMI and other forward-looking projects.

- Analyze Constitutional and other privacy concerns raised by collection of information about the interior of residences. Develop recommendations for addressing heightened privacy concerns consistent with Constitution (both of the United States and California) and consumer expectations and consistent with other needs (regulatory, criminal, and private).
    - See section 3.2 for these results.
- Generate a list of relevant stakeholders.
    - See Appendix B for a list of interviewees, and section 3.3.2 for discussion and analysis of interviews.
- Meet with technologists to understand system requirements AND
- Interview users of current ESP data (ESPs, law enforcement, regulators) to understand current use of utility data and rules about internal use and disclosure to third parties.
    - See Appendix B for a detailed discussion of interviews that were performed June – October 2005.
    - See section 3.2.4 for data from law enforcement interviews.
    - See sections 3.2.5 and 3.3.2 for data from energy industry stakeholders' interviews.
- Consolidate collected data to develop a list of privacy related concerns. Define the broad agenda related to privacy and security in the DR context.
    - See section 5.2 for discussion of issues identified in short, medium, long term demand response deployments.
- Identify possible architectural features that would support privacy and explore feasibility of adoption.
    - See section 5.2 for discussion of recommendations developed for short, medium, long-term demand response deployments.

3.1. Background and Overview

The current political climate is encouraging for the development of advanced metering and demand response infrastructure. The federal Energy Policy Act of 2005,[f] not only suggests the development of advanced metering and demand response programs, but directs the Department of Energy to identify target levels of demand response benefits that can be achieved by January of 2007.[g] The statute directs "each electric utility" to begin offering time-varying energy rates, and a meter capable of supporting those rates, to

---

[f] Energy Policy Act of 2005, Pub. L. 109-58, § 1252, 119 Stat 594, (2005), which amended § 111(d) of the Public Utility Regulatory Policies Act of 1978 (16 U.S.C. § 2621(d)).

[g] Id § 1252(d).

consumers within 18 months of August 8, 2005.[h] The Department of Energy is charged with beginning to educate consumers on the benefits of advanced metering and demand response; both state and federal agencies are charged with investigating the potential of, and making plans for, demand response adoption.[i] Proposed California state legislation that would have postponed the adoption of advanced metering and dynamic tariffs is no longer active.[j]

Current advanced metering and demand response adoption activity in California centers around a number of rulemaking and rate-setting cases being considered by the CPUC. Since June 2002, the CPUC has been engaged in a joint rulemaking with the California Energy Commission "to develop demand response as a resource to enhance electric system reliability, reduce power purchase and individual consumer costs, and protect the environment."[k] Under the auspices of this joint rulemaking were the Statewide Pricing Pilot, implementation of demand response for large industrial customers, and development of a framework for the study of residential demand response implementation.

Proceedings at the CPUC have included requests by investor-owned utilities PG&E and SDG&E to begin pre-deployment and full deployment of advanced metering infrastructures (AMI), and a request by SCE to develop an advanced integrated meter to support a future AMI deployment. [l] To date, the CPUC has approved PG&E and SDG&E's pre-deployment activities, [m]and PG&E's full deployment application.[n] The CPUC is now reviewing SDG&E's full deployment application.[o]

---

[h] Id. § 1252(a).

[i] Id § 1252(a)-(g). The language of the statute appears to say that states may perform a complete analysis in 18 months – 2 years and then come to the conclusion that implementing advanced metering and demand response at that time is "inappropriate," § 1252(a), but the statute clearly encourages adoption of demand response programs, and pledges Department of Energy assistance to help states develop their programs. § 1252(e).

[j] Cal. S.B. 441, became inactive September 1, 2005.

[k] Order Instituting Rulemaking on policies and practices for advanced metering, demand response, and dynamic pricing, R. 02-06-001, (Cal. Pub. Util. Comm'n Oct. 19, 2005) (Draft Decision Closing this Rulemaking and Identifying Future Activities Related to Demand Response), available at http://www.cpuc.ca.gov/word_pdf/COMMENT_DECISION/50428.pdf.

[l] The advanced metering pre-deployment and deployment cases filed with the CPUC include A. 05-03-016 and A. 05-06-028 (PG&E), A. 05-03-015 and A. 05-06-017 (SDG&E), and A. 05-03-026 (SCE).

[m] A decision in the PG&E ratesetting case was issued September 22, 2005. The draft decision is available at http://www.cpuc.ca.gov/word_pdf/COMMENT_DECISION/48707.pdf. A decision on the SDG&E pre-deployment filing was filed August 25, 2005. The draft decision is available at http://www.cpuc.ca.gov/word_pdf/COMMENT_DECISION/48180.pdf.

[n] A proposed decision on PG&E's Advanced Metering Infrastructure is available at http://www.cpuc.ca.gov/EFILE/PD/57156.pdf

[o] "An Advanced Metering Update" is provided by the CPUC at: http://www.cpuc.ca.gov/static/hottopics/1energy/ami_update+june+2006.pdf.. .

Utilities are proceeding with planning and deployment activities: evaluating meters and other technological elements, determining how to integrate them into new communications systems and existing software systems, and thinking ahead about how to implement demand response. In the following two sections, we have studied some elements of the framework within which this new technology will be deployed, with an eye to rules and practices that may affect customer privacy. Section 3.2 summarizes legal and regulatory rules that may affect either technological choices or information practices in demand response systems. In section 3.3, we have tried to discover which technological choices and information practices may be more likely in the development of demand response in California, by interviewing a number of stakeholders, including representatives from the three major investor-owned utilities.

3.2. Legal and Regulatory Framework

Law and social norms together draw a boundary, although sometimes a fuzzy one, between permissible and impermissible ways to use a technology – permissible and impermissible being defined according to what law, markets, and individuals do and don't accept. Privacy and security concerns in the widespread deployment of demand response infrastructure will intersect with a large number of different pre-existing federal and state rules regarding the privacy of activities occurring within the home, handling of business records and identifiable customer information, privacy of electronic communications, and other regulations. Understanding these concerns and rules is important because likely demand response implementations will impact privacy and security in ways that are qualitatively different from the existing energy infrastructure and information collection practices. We also review recommended privacy principles that provide guidance as to ways that information privacy may be promoted or maximized by information systems.

3.2.1. Legal protections for privacy in the home

A person's home receives special treatment under the law. The Fourth Amendment of the U.S. Constitution and the California Constitution both provide protections against unwanted government intrusions into the home. Property and tort laws also protect against other unwanted intrusions into the home. Supreme Court jurisprudence under the Fourth Amendment to the Constitution has long held that activities within the four walls of the home, even illicit activities, warrant special protection from intrusion by law enforcement. In many instances, California law is more protective than federal law.

In 2001, the Supreme Court decided *Kyllo v. United States*, 533 U.S. 27 (2001), which illustrates the high level of privacy and freedom from surveillance people may reasonably expect in their homes. The Court held that law enforcement agents may not use sense-enhancing technology that is capable of revealing both illegal and legal activity, technology that is not readily available to the public, to reveal activity within the home, regardless of whether the information discovered is incriminating. In its discussion, the Court focused on two details of the sense-enhancing technology employed. First, the Court asked, was the technology in common use at the time, such that residents of the house might have expected the technology to be used against them? The thermal-imaging device in this case was uncommon and not publicly available, so the surveillance was improper without a

warrant. Second, would the information gathered be otherwise accessible without entering the home? The information gained by the imaging device in this case would not otherwise be available from outside, and so again, the surveillance was improper.

It is useful to think about privacy in a demand response setting by considering the two key questions from *Kyllo*. New technologies that make information on in-home activity available to other persons outside the home, information such as occupancy, movement, or any other behavior that otherwise would not be visible from outside, may cross this line set by the Supreme Court and may violate a person's rightful expectation of privacy inside his home. It is possible that very sophisticated data mining of energy data might be able to discover enough about in-home behavior to cross this line. On the other hand, the expectation of privacy is dynamic, tied to the novelty of the technology used to invade it, and so that expectation of privacy may change over time as new technologies become commonplace.

To lawfully obtain information about activity inside a home, law enforcement agents generally must obtain a warrant or receive permission to "enter" the home, even if "entry" does not entail setting foot inside the threshold. Private parties wishing to access and use information stored in the home must obtain the data from the owner, subpoena it, and obtain a court order requiring production; otherwise, they must trespass upon private property to obtain it. In all instances, the law provides strong protections against access to personal information and other items maintained in the home. Any data on personal behavior, habits, or energy usage that is maintained inside the home is afforded the same high level of privacy protection against both private party and government intrusions. Therefore the individual is able to exercise the highest level of control over the reuse and disclosure of personal information maintained inside the home.

3.2.2. Legal Protections for Privacy of Personal Information Held by Third Parties

Legal protections for personal information (generally described as "any information relating to an identified or identifiable individual")[p] are varied, fragmented, and incomplete. Personal information maintained in the home will be protected by the general rules, stated above, that protect papers and effects within the home. However, personal information revealed to and maintained by third parties has generally been considered outside the scope of the Fourth Amendment protection and therefore accessible to law enforcement without a warrant. The California Constitution has been interpreted to create a zone of privacy around individuals' bank records despite the fact they are held by the bank and not the individual. It is uncertain what the scope of personal information afforded Fourth Amendment-like protection is under the California Constitution; however it is clearly broader than the protection afforded by the U.S. Constitution. Under federal and state statutes, and the backdrop of federal and state constitutional law, personal information held by third parties is subject to a variety of substantive and procedural

---

[p] *See* Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980, available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

privacy protections depending upon whether state or federal law applies, who maintains it, the substance of the personal information, and the circumstances in which it was obtained.

3.2.2.1. California Statutory Law[q]

Under the California Code, public utility consumer confidentiality protections tend to vary with the type of data at issue: either personal information or utility records. Personal or customer information is generally well protected throughout the Code. For example, the Government Code § 6254.16 specifies that while public records must be made available for public inspection, public utilities and other agencies are not required to disclose information such as a consumer's "name, credit history, utility usage data, home address or telephone number." Exceptions to this rule include court orders or requests by law enforcement officers to view the data; such requests may be granted subject to certain conditions. For example, under Public Utilities Code § 588(a), district attorneys and their agents may only request information from public utilities such as "the full name, date of birth, social security number," and other demographic information of a given consumer, for the purposes of a child abduction investigation. However, utility records which do not contain personal information are generally accessible to law enforcement agents, and do not carry the same privacy protections as personal records.

Under California law, law enforcement agents generally may obtain an individual's utility records in two ways. First they may subpoena records held by a public utility during an "ongoing criminal investigation."[r] Under California Penal Code § 1326.1, law enforcement agents may receive a utility records subpoena from a judge, upon "a written ex parte application by a peace officer showing specific and articulable facts that there are reasonable grounds to believe that the records or information sought are relevant and material to an ongoing investigation of a felony violation." The utility may notify the consumer that records are being sought unless otherwise directed by the court, in which case this notice would occur after disclosure. Case law suggests that law enforcement access to utility records may be routine for detecting excessive energy usage as an indication of marijuana growing operations.[s] Part (e) of § 1326.1 specifies that "nothing in this section shall preclude the holder of the utility records from voluntarily disclosing information or providing records to law enforcement on request." Thus, subpoenas may not be required for law enforcement agents to access utility records.[t]

---

[q] A more complete listing of the state statutes which apply may be found in Appendix A.

[r] The Code suggests that an ongoing criminal investigation is one in which nothing more may have occurred than identification of the suspects.

[s] *United States v. Payner*, 447 U.S. 727 (1980); *United States v. Porco*, 842 F. Supp. 1393 (D. Wyo. 1994); *United States v. Cole*, 983 F.2d 1078 (9th Cir. 1992); *People v. Stanley*, 72 Cal. App. 4th 1547 (1999); *People v. O'Leary*, 70 Cal. App. 3d 323 (Cal. Ct. App. 1977); *People v. Thuss*, 107 Cal. App. 4th 221 (2003). Interviews with law enforcement practitioners suggest it is even more common to obtain energy records to confirm residence of a suspect at an address. See section 3.2.4, infra.

[t] Interviews with law enforcement practitioners suggest that they prefer to obtain a subpoena in most situations, as utilities may and often do refuse to release the records without a subpoena. See section 3.2.4, infra.

The standard procedure for obtaining business records in civil suits is found in California Code of Civil Procedure § 2020. Records, including those held by an electric utility provider, can be subpoenaed without notice to the consumer whose records are sought. After the subpoenaing party serves the custodian of records with the subpoena, the custodian has at least 20 days to produce from the time of issuance of the subpoena. Currently, no special exception from this standard procedure exists for subpoenas of consumer electric utility records. Section 1985.3 provides special procedures for the subpoena of "personal records" held by entities like doctors, hospitals, schools, banks or telephone corporations. This exceptional procedure requires notice to the consumer and provides an independent right to object to the subpoena where personal records are to be released. A subpoena for personal records held by a "telephone corporation which is a public utility" is not valid unless a form consenting to release is signed by the consumer.[u]

3.2.2.2. Case Law

Federal and state cases that discuss the use of utility records against criminal defendants mainly deal with the growth of marijuana in home laboratories. The collection of utility records by state actors requires, in some jurisdictions, a warrant issued by a judge. In other jurisdictions it requires much less (e.g. reasonable suspicion).

The essential difference in how courts have interpreted the Fourth Amendment derives from what "reasonable expectation of privacy" a court believes an individual has in his utility consumption records. Although electricity is a necessary component of modern life, disclosure of power consumption to a utility company for billing or other limited business purposes should not relinquish the entirety of an individual's interest in the privacy of those records. The U.S. 9th Circuit Court of Appeals has defined a less generous right to privacy, in a marijuana production case,[v] citing other cases to say that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties … in the ordinary course of business."[w]

The California Court of Appeals elaborated an identical position dealing with information deemed as "business records," in a case where police used data collected from a specially-installed surveillance electricity meter to obtain a search warrant to look for marijuana plants: "Where activities, statements, or objects are exposed to public view, the protection of the amendment does not apply."[x] With respect to electricity metering equipment, the Court determined that because the metering information did not reveal information about activities within the home, there is no constitutional protection:

> "The surveillance meter neither measures nor reveals anything about the intimate details of activities within the house. The technology employed does not tell those monitoring it what electrical devices are inside the house or what activities the

---

[u] Cal. Civ. Proc. Code § 1985.3(f).

[v] *United States v. Starkweather*, 1992 U.S. App. LEXIS 20207.

[w] *Id*. at 3.

[x] *People v. Stanley*, 72 Cal. App. 4th 1547, 1552 (1999).

> power supports. The meter does not discriminate between electricity used to fire pottery and power used to grow orchids, tomatoes or marijuana. It only tells officers how much electricity is being delivered by the utility and, by comparison to billing records, whether it is being diverted or stolen."[y]

Similar conclusions denying reasonable expectations of privacy in utility records have been drawn in other state and federal courts.[z] This reasoning seems to suggest that metering information that discloses relatively more detailed information from the interior of a home may be more likely to fall within a reasonable expectation of privacy than traditional monthly collection of *aggregate* utility data. If the California courts were to determine that customers do have a reasonable expectation of privacy in utility records containing demand response or advanced metering data, that would mean such records could not be released without a warrant under California law. [aa]

3.2.3. Legal rules regarding unauthorized access to computing and communications

We have included in our survey of legal rules a look at federal and state rules pertaining to unauthorized or malicious access to computer systems. Since legal rules regarding unauthorized access to computer systems are typically very broadly construed, it is possible that these rules may in time be applied to intrusions into demand response and in-home network systems, especially if those systems include the networking of smart meters, smart thermostats, wireless sensors, smart appliances, and a consumer's home computing system.

Since the unauthorized access rules are so very broad, whether or how they are applied in a demand response context may depend on fine details of how the systems are designed, how they function, and how they are perceived. Key questions that will be asked when deciding how to prosecute unauthorized access to elements of a demand response system may include the following: does the transmittal or storage of data in an element constitute interstate commerce (and might federal laws therefore apply)? Would the provision of data management services by a third party contractor implicate interstate commerce? Might an interloper obtain legal access to the system if the consumer does not utilize security measures such as using encryption and password restrictions? Would intercepting energy

---

[y] *Id*. at 1153-54.

[z] *See Samson v. Alaska*, 919 P.2d 171 (1996); *see also Colorado v. Dunkin*, 888 P.2d 305 (1994); *United States v. Boger*, 755 F. Supp. 333 (E.D. Wash. 1990); *United States v. Delgado*, 121 F. Supp. 2d 631 (E.D. Mich. 2000).

[aa] California Courts have determined that consumers do have a reasonable expectation of privacy in some records held by telecommunications public utilities. *See People v. Chapman*, 36 Cal.. 3d 98 (1984) (holding that a customer who paid to keep her name, phone number, and address unlisted in telephone directories had a reasonable expectation of privacy in that data, and so a warrant was required to obtain that data from the telephone company).; *see also In Re Pacific Bell*, 44 C.P.U.C.2d 694 , 1992 WL 613306 (Cal. Publ. Util. Comm'n 1992).

usage data constitute "obtaining information," in the same way as the interception of a wireless phone call or pager message?

Since it is impossible to predict with very much accuracy how courts may treat a future demand response infrastructure with unknown features, we will here discuss the relevant sections of current law, and highlight the kinds of questions that might be asked when demand response systems begin to be considered by the law.

3.2.3.1. Federal Law

Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA)[bb] makes it a federal offense to intentionally access a computer without authorization or to exceed the authorized level of access, if a party uses that access to obtain information from or cause damage to a protected computer involved in interstate commerce. The word "computer" in the statute has been interpreted expansively, covering ipods, devices w/embedded processors and software, and other gadgets.[cc] The definition of what constitutes "interstate commerce" may be equally broad: for example, any wireless electronic communication sent via the federally regulated electromagnetic spectrum would qualify.[dd] This broad interpretation of interstate commerce would likely make the law applicable to most energy appliances and sensor networks.

There is some question as to what makes access "unauthorized." Some courts classify any access made without express or implied permission given beforehand to be unauthorized.[ee] Setting up even a simple barrier to access, such as password protection, may be viewed as "limit[ing] authorization by implication (and technology), even without express terms."[ff] Access may be considered unauthorized if it violates the terms of the accountholder's terms of service,[gg] even though an interloper might not know of those terms. Which test is chosen may matter, because most home networks are not well secured, home users often being unable to perform the complicated steps necessary to enable security measures on their home computer equipment, especially wireless access points.

Despite the broadness of this law, and the fact it may be used as a civil cause of action, it may not be very useful in the demand response context because the law may not be invoked unless the interloper has caused aggregated damages of at least $5,000 in value during any one-year period to one or more persons. The law may be useful only for prosecuting large or widespread thefts of energy services or damages to energy systems.

[bb] 18 U.S.C. § 1030 (2005).

[cc] *United States v. Mitra*, 405 F.3d 492, 494-96 (7th Cir. 2005).

[dd] *Id*. at 496.

[ee] *EF Cultural Travel v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003).

[ff] *Id*. at 63.

[gg] *America Online, Inc. v. LCGM, Inc*., 46 F. Supp. 2d 444 (E.D. Va.).

The same law may be used to prosecute for "war-driving" offenses, by which is meant gaining access to computer networks through unauthorized access to wireless LANs. As wireless access points become ubiquitous, this kind of unauthorized access may become more common. Again, because $5000 in damages must be incurred for the statute to be invoked, it is likely that most prosecutions will pursue unauthorized wireless access made to rob or damage corporate networks.[hh]

Electronic Communications Privacy Act

Under the Electronic Communications Privacy Act (ECPA),[ii] liability ensues when an individual (1) intentionally (2) intercepts, endeavors to intercept, or procures another person to intercept (3) the contents of an (4) electronic communication (5) using a device. "Electronic communication" includes any transfer of signals, images, data, or intelligence by wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce. The law has been applied to a broad range of communications systems. Sections of the law also cover electronic storage of electronic communications and transaction records.[jj]

The ECPA provides additional limitations on any person or entity that provides electronic communication service to the public, forbidding those from knowingly divulging the contents of any communications kept in electronic storage by that entity. The definition of electronic service provider may not include entities that provide some communication services as only a minor portion of their business.[kk] A utility that provides electronic communication services for meters or smart thermostats may be in an uncertain position with regard to this law, whereas a third party who provided those same services as their main business would likely be subject to ECPA.

California Penal Code

California laws regarding unauthorized access to computer systems and communications are similar to the federal rules in many ways, but mention privacy more explicitly and in somewhat stronger language. The California Computer Crime Act[ll] is a privacy measure that bars unauthorized access by any person to lawfully-created computer data and computer systems. The "High Technology Theft Apprehension and Prosecution Program" identifies as crimes unauthorized access or entry into private and public computers and networks, and unauthorized use or manipulation of data found therein. [mm] Separate unauthorized eavesdropping rules make it a felony for any person to make "any

---

[hh] *See, e.g., United States v. Salcedo* (defendants gained wireless access to computer network of Lowe's store in Michigan, and attempted to steal customer credit card information thereby), information available at http://www.usdoj.gov/criminal/salcedoSent.htm.

[ii] Electronic Communications Privacy Act of 1986, Pub. L. 99-508, § 1, 100 Stat. 1848, codified at 18 U.S.C. § 2050 et seq. (2005).

[jj] 18 U.S.C. § 2701 et seq. (2005).

[kk] D*yer v. Northwest Airlines Corps*., 334 F Supp 2d 1196 (D.N.D. 2004). (finding that the airline was not an electronic service provider because it sells products and services instead of providing internet services).

[ll] Cal. Penal Code § 502.

[mm] Cal. Penal Code § 13848(b).

unauthorized connection . . . with any telegraph or telephone wire, line, cable or instrument;" to read, attempt to read, "or learn the contents or meaning of any message, report or communication while the same is in transit or passing over any wire, line or cable;" or to use, or attempt to use, "in any manner, or for any purpose, or to communicate in any way, any information so obtained . . .". [nn] However, this section does not apply to any communications that are a part of public utility services.

3.2.3.2. Trespass to Chattels

Trespass to chattels arises when intentional interference with a party's possession of personal property causes injury. This doctrine may be of limited use in the demand response context, as recent decisions in California have held that trespass to chattels "does not encompass … an electronic communication that neither damages the recipient computer nor impairs its functioning."[oo] A party merely gaining access to a sensor network and causing no damage to it may not be covered by this doctrine, although damages might be recovered if an attacker actually overburdened or interfered with the efficient functioning of a computer system and threatened harm in the potential for others to imitate the defendant's activity.

3.2.4. Law Enforcement Practices

It is clear that demand response information needs to be kept from would-be criminals. We are only beginning to understand what information could be gleaned from demand response data. For example, data could show whether occupants are away. Data might also show the type of appliance and the number of appliances in the house.

In addition, because access to utility records by the government raises very important privacy issues in the context of demand response, and because many of the laws and regulations we reviewed for this project dealt with access to utility records by law enforcement, we spoke with current and former U.S. Attorneys. We inquired about the current use of energy records by law enforcement, and how those practices might change once advanced metering and demand response become widespread.[pp] This section highlights issues that were raised by, and discussed with, these interviewees.

The most common use of energy records in a criminal case is to establish or confirm residency at an address.[qq] Using the records as evidence that a residence is using extraordinary amounts of energy, as corroborating evidence of a home marijuana growing operation, is the next most likely use, but is more rare. Records may be sought at many stages of a case. Usage records may be sought early in a marijuana home-growth case to support a tip or preliminary evidence, and build a case for a search warrant. Records of

---

[nn] Cal. Penal Code § 631. Sections 630 - 637.9 comprise Chapter 1.5 of the Code, entitled "Invasion of Privacy."

[oo] *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003).

[pp] The questions used as a basis for discussion are listed in Appendix A.

[qq] The fact that a suspect pays the electric bill at an address may be used to infer that he had some knowledge or control of events that take place or contraband that is found in the residence.

usage and billing may be sought later, when more evidence is in hand, to show that the person paying the energy bill must have had knowledge of the illegal activity.

Records are generally sought using a grand jury subpoena in any non-emergency situation,[rr] as utilities rarely exercise their option to release customer data to law enforcement voluntarily. Also, there is a perception that subpoenaed records may appear stronger in court. Obtaining a grand jury subpoena is a simple thing, and in some cases can be done in as little as ten minutes. The records sought are usually copies of energy bills, records of payment, and internal records that identify the subscriber. Although it would likely be permitted for law enforcement to request customer data for a neighborhood or larger area, and either sift through it looking for a suspiciously high usage, to target a suspect in a neighborhood where marijuana growth is suspected, or use the neighborhood data to show that a suspect's usage is high compared to neighbors, in most cases the only records that are needed, requested and used are those for a suspect's individual residence.

It is speculated that advanced metering data might become valuable to law enforcement if it turns out that hourly usage data can be employed in establishing the timing of a crime. Perhaps, in some cases, the energy usage profile might help establish that a residence was or was not occupied at a certain critical time. This could be useful in a broad range of cases. It might be possible to use hourly data to help or cast doubt on an alibi, or suggest when a person came home or left. If meters were being polled or messages sent to the utility when a meter went offline, records on these events might be useful for establishing the time a home fire started, for example.

Hourly data might not make energy records more useful in marijuana litigation, as in those cases, the excessive usage divulged by the single monthly data point may be all that is needed. However, access to historical and real-time data might allow law enforcement to learn about a suspect's marijuana growing cycles, so that a search of the suspect's home might be scheduled when the plants are in full growth, instead of a week after harvest. Interviewees report skepticism that data which is even more revealing, such as in-home sensor, smart thermostat, or other data which can expose significant detail on in-home behavior, should be made available to law enforcement without a warrant, due to 4th Amendment concerns.[ss]

It has been reported that with the increasing saturation of wireless systems, crimes of unauthorized access to such systems are increasing. Since large losses must occur for an intrusion to be prosecuted under federal statutes, it is unlikely that federal law enforcement will pursue crimes of unauthorized access to electronic meters or home wireless systems unless such violations became widespread. The key to preventing electronic intrusion crimes is maintaining vigilance, constantly upgrading security measures as intruders learn to crack the old ones, as intrusion rates drop when new security measures are put in place, but always pick up again with time.

[rr] Some agencies have their own administrative subpoena power, and obtain records through a different process.

[ss] See discussion of 4th Amendment issues and the *Kyllo* case in section 3.2.1, above.

3.2.5. Utility Best Practices

Two important areas of data handling practices are controlled primarily by internally set utility standards: retention of customer usage data, and control of data handling practices of third party contractors who may perform certain data collection, storage, or processing services under contract to the utilities. Both of these areas of data handling can critically affect the privacy and security of customer information, and as both of these areas have already been identified as incompletely covered by legal rules, it is worth taking a closer look at utility practices.

The length of time that a public utility may or must retain customer usage data or other customer records is not specified in California statutes or CPUC general orders,[tt] but has been set at seven years as an internal company policy choice. The storage period of seven years has been approved and affirmed as reasonable in a recent case before the CPUC.[uu] The utility customer in this case argued that utility records should be kept longer, to provide needed information for utility billing disputes, but the CPUC considered seven years sufficient, as requiring longer storage "would require the utilities to expend huge sums of money for record retention."[vv] As mentioned in the data from our interviews with utility representatives, below, seven year storage of utility records has become an industry standard practice. This practice and its purpose are important to keep in mind when one considers that even with a shift to advanced metering, and later, demand response, utilities are likely to continue the current industry practice. Whatever data may be collected is likely to be collected and stored for seven years. Whether the storage of this much data is truly necessary to fulfill the purpose of having enough information on hand to properly resolve customer usage disputes is a matter that will require debate.

Another matter that is controlled by utility standard practice is the control of data handling practices of third party contractors who perform certain data collection, storage, or processing services under contract to the utilities. The utility holds third party contractors to the same legal and regulatory data handling requirements the utility is subject to. These requirements are passed along to the third party through contract, ensured by audit, and may enforced through formal breach-of-contract actions or informal measures. One utility expressed a preference for contractors who use, or even better, are certified practitioners of, industry standard information security practices,[ww] such as ISO 17799, which includes recommended policies for secure storage of data and hardware,

---

[tt] It is unclear whether the investor-owned utilities are subject to 4 Cal. Admin. Code § 4090, promulgated by the Division of Measurement Standards, Department of Food and Agriculture. This section provides invoicing guidelines to any "operator" that provides utility services through "commercial weighing or measuring devices." The section requires that operators of a "metered utility service system" must retain records of "all pertinent rate schedules, and individual customer billings" for at least 12 months, and must make those records shall be made available for viewing and copying by the customer.

[uu] *Utility Audit Co. v. Southern Calif. Gas Co.*, Decision 98-09-061, Case 97-02-015, 1998 Cal. PUC LEXIS 1097 (Cal. Pub. Util. Comm'n 1998),.

[vv] Id. at *15.

[ww] NIST and ISO 17799 standards were mentioned. ISO 17799 standards are available at http://www.iso-17799.com/.

controlling access to data, and managing, archiving and securing data. Recommendations include using encryption whenever transmitting confidential or sensitive information, preventing cybercrime by maintaining the highest possible levels of security on networks, and many other information security practices.

3.2.6. Privacy Principles in Demand Response Systems

Fair Information Practice Principles are a standard tool that institutions may use to develop internal information privacy practices and standards.[xx] The core principles important to consider in the context of energy data and the design of demand response are that a data collection entity should: 1) limit the collection of data to that minimum amount which is necessary to support the purpose for which the data is being provided, from the

---

[xx] *See* Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980, available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION.

Collection Limitation Principle 7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle 8. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle 9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle 10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle 11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle 12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle 13. An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle 14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

data subject's perspective; 2) establish appropriate technical and procedural mechanisms to protect the personal data collected from unauthorized access and use, internal and external. It is also essential that individuals should be able to: 1) control the reuse of personal information and 2) control the disclosure of personal information. In practice these principles typically require that data controllers establish the data necessary to support a given interaction or transaction with the data subject (in this instance consumer), obtain the permission of the individual prior to using the personal information for a new purpose internally or disclosing the data to a third party, and establish appropriate mechanisms to implement and enforce privacy and security rules.

Given the disparate rules protecting personal information maintained by third parties, the location of customer data storage and processing can affect the level of privacy protection of that data. This design choice, along with other related decisions, can alter the control individuals have over the reuse and disclosure of personal information to private parties and the standards controlling government access to personal information. The personal information subject to these varied sets of rules may go far beyond the coarse monthly consumption data currently collected and maintained by public utilities and include information about the individual consumer's presence in, absence from, and activities within the home, whether this is collected directly or deducted by data mining customer usage data.

The availability of detailed consumer energy usage profiles, potentially without the notice and consent of the consumer, raises novel privacy concerns. Private data management corporations, separate from public utilities, could profit from access to and sale of these usage records. Law enforcement agents, who currently may subpoena consumer utility records (although nothing prevents utility companies from voluntarily turning over such profiles to law enforcement[yy]), could potentially have access to real-time information about energy usage or extremely detailed and revealing longitudinal energy consumption profiles that provide a virtual window into the home and the activities of its inhabitants under the same subpoena provision. The increasingly detailed quality of the data enhances its potential to reveal information about activities in the home, which are legally and practically considered highly private. The potential for law enforcement to access detailed energy consumption profiles or real-time information about energy use and the potential for market actors to buy, trade and sell such data may force courts and policy-makers to consider the questions of whether and where to draw the line defining the curtilage of the technically mediated home and how much control consumers should have over such data.

This overview highlights the important but sometimes overlooked fact that security measures may not fully protect personal privacy. Regardless of the security provided, the disparate legal rules governing reuse and access to personal information are limited in the privacy protection they afford. Even lawful access, where it is unauthorized by the individual, compromises individual privacy. Ensuring that such lawful access occurs in a secure manner is a positive step but on its own does not mitigate the incursion on privacy that many policymakers and/or consumers may consider objectionable. Such access at

---

[yy] See sections 3.2.2.1 and 3.2.4.

times reflects a deliberate choice by the legislature to impinge on privacy to meet another social goal. In other instances, the lack of rules governing reuse or access to personal information does not necessarily reflect a social consensus about the privacy one ought to expect, but rather the lack of a policy process to determine the answer to this question. In any event, "lawful" access to personal information that is not authorized by the individual limits his ability to maintain his privacy. Given that security structures cannot entirely address this privacy issue, it is exceedingly important to consider all applicable legal rules.

3.3. Review of Current and Future Plans for Demand Response

3.3.1. Study of Advanced Metering and Demand Response Plans filed with CPUC

An overview of utility business plans submitted to the CPUC in support of advanced metering and demand response suggests some general conclusions that might be drawn about the capabilities of advanced metering systems that may be deployed in the short term.[zz] The kind of advanced metering capability that may be implemented most rapidly, i.e. in 2006, is expected to consist of refurbished meters supplemented with a data collection module that will enable hourly readings and transmittal of raw data to the utility. Advanced metering installations that are projected to begin in 2007 or later contemplate somewhat more sophisticated meters that contain more internal processing and data storage capability.

Utility business plans contemplate the installation or use of a mobile communications network of intermediate data concentration nodes, or use of the meters themselves as a relay network to relay raw usage data. All utility plans expect the raw meter data to be routed to and centrally collected at the utility site.

Advanced metering data is expected to enable savings in operating costs, when integrated into and used by utility sub-systems such as remote meter reading, outage management, load forecasting, workforce management, billing, planning, field automation, asset management, and others. Additional benefits will accrue when time-variable demand response tariffs become available. Utilities' current plans for AMI display significantly different targets for meter processing capability and requirements for cost-effective deployment. Utilities that would rather delay deployment of advanced metering appear to prefer integrated meters with more process capability, and their calculations seem to require that some amount of demand response benefits be available for deployment to be cost-effective.

3.3.2. Interview Data from Energy Industry Stakeholders

To learn more about the deployment plans and likely technology preferences in an AMI deployment in California, we conducted a number of interviews with stakeholders in July to September of 2005. We interviewed consultants, energy data collection services sub-

[zz] Materials studied include testimony and other materials filed in support of AMI pre-deployment requests A. 05-03-016 (PG&E), A. 05-03-015 (SDG&E), and A. 05-03-026 (SCE).

contractors, and representatives from the three major investor-owned utility companies. A master list of the questions asked can be found in Appendix B. In the following section, we will highlight areas of agreement and disparity among the participants' views of plans for large scale deployment of advanced metering and demand response infrastructure.

Type of meter being considered for widespread deployment.

Many kinds of meters were used and tested in the statewide pilot program, with varying ranges of internal processing and storage capabilities. Some in industry believe that sophisticated meters with the ability to store a month's worth of data might not be cost-effective for widespread deployment today. They argue that cost-effective deployment today would require a relatively dumb meter, or meter upgraded with a small communications module with relatively minor processing capability and only a few days' worth of storage. Others in industry believe a more sophisticated meter can be cost effective and better for the network. Those officials that would prefer to deploy a more sophisticated meter that has the capability of receiving and responding to signals from the utility, communicating with other appliances or smart thermostats, are driving research or requesting proposals from meter manufacturers as to how such a meter may be made cheaply enough for deployment. It is desired that a smart meter might be able to notify a customer when energy rates change, so that the customer can elect to shut down appliances or air conditioning. Even better would be a meter that allowed a customer to input preferences so the meter could automatically shut down appliances when the energy rates changed.

Meters being contemplated will collect data on usage every 15 minutes to one hour. The data set the meter will send to the utility is expected to contain a unique meter identifier, timestamp, usage data and some kind of time synchronization information. Outage information, voltage, phase, and frequency data are desired, but not expected. The data is expected to be formatted in a proprietary format unique to the manufacturer, although some participants are looking forward to the availability of open standards and architecture for meters, as may be available from the OpenAMI project. [aaa]

There is little agreement on how often data may be sent to the utility or intermediate nodes, or how long the meter may be expected to store data. It appears universally desired that the meter can store at least a few days' worth of data, even if only as an emergency backup. The meter may send usage data hourly, daily, or a few times a day, but other data

---

[aaa] See section 3.3.3. The American National Standards Institute (ANSI) also provides some standards for electric and other meters. ANSI C12.19 standardizes data formats for the storage, alteration, and transmission of metering information. This includes a language used to dynamically resize data tables to include and exclude certain categories of information for transmission. It also includes standard formats for the users to define their own tables for reading, their own audit logs of metering events such as communications, executions of procedures, and alterations to data or the system clock. C12.19 includes requirements for authentication using a non-hierarchical password (one password for open access) scheme and encryption with meter reading. It provides a read interval (the period of time in between automatic reads) in the range of 1 minute to every 45 days. It includes space for up to 15 distinct seasonal settings (categories of pricing). It is not clear what proportion of meters being considered for widespread deployment actually meet this standard.

may be sent less frequently. All data collection plans appear to contemplate main storage of usage and other data at the utility. Current utility practices include saving many years worth of customer usage data to enable customer disputes, and these data storage practices are expected to continue.[bbb]

Data transmission pathway from meter to utility

There are a number of different visions for data transmission from meter to utility. Data may be collected by a node at a substation or meters may relay data to an intermediate node. A substation node might collect data from about 100-10,000 meters, depending on local fan-out. It is expected that little data processing will occur at intermediate nodes, though there may be some re-arrangement or scheduling of data at that level. If a reading is missed or lost, the head end will be able to poll an individual meter again.

All utilities express an interest in broadband over power line (BPL). BPL fits with the utility preference for owning all the components of their business. BPL is not required to make advanced metering or demand-response infrastructure work, but utilities would switch to it if it were available. Current research is focused on determining whether BPL will be cost-effective at some point. As a BPL communication node in an electrical substation would be able to talk to any device plugged into any electrical socket that received power from that substation, BPL may introduce unique security and privacy issues.[ccc]

Cost-effective encryption of data transmissions is currently under study. Interviewees suggest that it is not certain that the whole data path requires encryption, but only segments where risk is high and the cost of adding encryption-decryption processing on both ends is low enough. Interviewees suggest that proprietary meter data formats provide some measure of security for the data.[ddd]

Advanced metering data requirements of utility subsystems

The availability of fine-grained, hourly advanced-metering usage data will be a big change for utilities. It is a current issue of discussion how this data should be used and distributed to utility subsystems. Raw usage data is desired for billing, customer service, and automatic meter activation. Customer service needs access to usage data and profiles to provide real-time counseling to customers on how to reduce their bill. It was also suggested that customer service and field automation should have the ability to query the meter in real time to take a reading on demand. Billing systems need fine-grained data to be able to calculate a bill given time-variant tariffs ("Dynamic Pricing"). If any individualized services or products are developed for offer to customers, fine-grain data may be needed to support

---

[bbb] One interviewee explained that data is stored for 7 years. Customers can dispute a bill for 3 years, and if they do so, may dispute another 4 years previous. See *Utility Audit Co. v. Southern Calif. Gas Co.*, Decision 98-09-061, Case 97-02-015, 1998 Cal. PUC LEXIS 1097 (Cal. Pub. Util. Comm'n 1998),.

[ccc] Messages might be able to be sent to and from the utility or substation to any appliance or computing system plugged into any socket. Capture of a node in a substation would mean the ability to control messages flowing to smart appliances or computing systems in customer homes. These possibilities are unique to BPL.

[ddd] This is a misconception that will be discussed at length in sections 5.2.2.2 and 5.2.2.3.

those programs. There may also be services that require communication to individual meters.

Outage management is likely to be somewhat different. Some systems anticipate polling meters on short 3- to 15-minute cycles, collecting small data packets containing only an on-off flag, to monitor meter health. Other systems may utilize meters with some battery back up that allow meters to send a 'last gasp' signal to notify the utility when the meter goes down. It is valuable to the utility to be able to poll meters to assure that they have come back online after a power outage.

Another valuable use for advanced metering data is monitoring peak load or voltage variation at transformers, allowing customization of transformer size, detection of load imbalance, rerouting, and rebalancing. All utilities look forward to using advanced metering data for research tasks like load profiling, rate design, and program evaluation, but these systems will likely not have access to real-time usage data. Some utilities expect research tasks can be accomplished using only subsets or samples of the usage data. Others look forward to data mining the entire set. Since data is not routed to researchers in real time, there is the ability to preprocess the data that is released.

Outsourcing of information service tasks to third party contractors

In the state-wide pilot program, some utilities developed their own capabilities to collect and process advanced metering data, where others outsourced most of the operation. In widespread deployment, there was general agreement among our interviewees that utilities prefer to own as much of the infrastructure as possible. As outsourcing contracts from the pilot are starting to end, it has been seen that utilities are starting to bring those functionalities in-house. Utilities will certainly want to own all the hardware, but some interviewees suggest that services like billing, web-services, data collection, and customer service might be outsourced at some point.

Third party subcontractors are held to the same data-privacy and security standards as the utility by contract. We understand that utilities aim to ensure that privacy and security standards are met by evaluating third-party servers and security practices, and through periodic audits. Third party contracts will also limit what uses the third party can make of collected and stored data.[eee]

Data feedback to customers

Customers must have access to information about their energy usage so they may learn how to control and reduce their energy cost. This is an important goal of any demand-response project. In the statewide pilot program, usage data was available to customers via the Internet, but it was found that customers did not use data on the Internet very much. Customers tend only to check the detailed information available on the web at the beginning of the project or when a major change in their premises or usage occurs. When customers get monthly feedback on usage versus time in graphical form on their bill, they are better able to make the decisions to control their usage. The most important tool to

---

[eee] One interviewee recommends ISO 17799 industry standards for data security, available at http://www.iso-17799.com/.

make it easier for customers to understand the relation between their usage and cost is good rate design. Time-of-use rates appear to be easier to understand than the current inverted-tier rates, and this alone may make it easier for customers to change usage behavior.

It is rare for residential customers to look at the meter, and so getting them to actually query a smart meter for data and respond to it is not considered feasible by all utilities. Utilities are looking for new kinds of feedback and communication mechanisms that will motivate consumer response to future demand-response energy signals. Web-based communication may not be effective at this, but still it is the main avenue being pursued, since customers are already familiar with web-based online billing.

Just like online billing, customers will have to sign up and sign a release to get access to their own usage information via the web, whether it is provided by the utility or a third-party information services provider.

System changes expected in the long term

Some utilities have discussed the idea of having a meter with enough processing and storage capability to be able to compute the customer's bill on customer premises, but this does not seem cost-effective to any utility at this time. The consensus among utilities is that a meter with this kind of processing capability would be much more expensive than feasible for residential deployment, and would require higher security and a more robust encryption than are currently planned. Further, calculation within the meter when time-variable rates are used requires a clock in the meter, and this in turn usually means a battery back-up is required. Battery back-up inside the meter is another high-cost item, as batteries would have to be replaced every ten to fifteen years. Another option is wireless synchronization of meters after outages, which would require more processing capability than is currently available.

Another-long term change might be the development of a standardized open-architecture demand-response data routing system. Such a standardized system might allow easier communication among different segments of the energy market and allow the entry of new service providers and promote outsourcing of many of the functions described above.

3.3.3. Study of long term demand response plans

To learn about possible longer-term advancements in energy-related in-home technologies and system infrastructure, we attended lectures, working group meetings, and talked with researchers involved in developing these technologies. Three projects that have been interesting and useful in provoking thought about the kind of privacy issues that may be expected in future energy networks include the OpenAMI project,[fff] the DRBizNet project,[ggg] and the studies of advanced wireless sensors and controls needed to create a wired house which are being pursued in the Mechanical Engineering, Electrical

[fff] www.OpenAMI .org. Also see http://ciee.ucop.edu/dretd/PIERDemandResponseSummaryReport.pdf.

[ggg] Presentation on DRBizNet available at http://ciee.ucop.edu/dretd/DRBizNet_06-02-2005.pdf.

Engineering and Computer Sciences, and Architecture departments at U.C. Berkeley.[hhh] As these projects are still in the prospective stage, instead of analyzing their technological details, which are certain to change over time, we look at the systems at a higher level, remarking on constituent components that may have particular privacy issues that should be taken into account when making eventual technological choices.

The OpenAMI and DRBizNet projects share the goal of developing standardized, open architecture systems. OpenAMI aims to develop a reference design for an advanced meter, which will encourage the production of interoperable, secure, low cost meters, which are flexible enough to adapt to tariff or other regulatory policy changes.[iii] The reference design anticipates a more highly functional meter than today, that may monitor voltage and frequency, and other parameters that the utilities would like to monitor. Another goal of this project is to develop toward standard interfaces inside the AMI infrastructure, so that equipment from different manufacturers may be easier to integrate and network together in the future.

DRBizNet is envisioned as an open, scalable, modular, standardized architecture for communications among energy market participants. Behaving something like an internet registry for the energy industry, the DRBizNet system might allow decentralized control, collection, storage, and processing of energy data and communications, making it easier for third parties to enter the energy market to provide services like meter reading, customer relations management and billing, energy provision to selected groups of customers, and other business processes. It is expected that an open architecture, very different from the utility controlled communications infrastructures of today, would enable new market entrants to enter the market with only marginal incremental cost.

The projects on demand response enabling technologies being pursued at U.C. Berkeley envision a home peppered with low-cost, batteryless sensors that communicate wirelessly with a smart thermostat or some other kind of controller that collects sensor data, processes it, and responds automatically.[jjj] Instead of acting on pre-programmed customer preferences, the envisioned smart thermostat will instead learn the customer's

---

[hhh] Presentation on UC Berkeley projects available at http://ciee.ucop.edu/dretd/UCB_Project_06-02-2005.pdf.

[iii] The guiding design principles of the OpenAMI project include the following, available at http://www.openami.org/twiki/bin/view/Main/RDPrinciples:

IV. Ease of use: There are logical and consistent (preferably intuitive) rules and procedures for the infrastructure's use and management.

VI. Standards: The elements of the infrastructure and the ways in which they interrelate are clearly defined, published, useful, open and stable over time.

VII. Openness: The infrastructure is available to all qualified entities on a nondiscriminatory basis.

VIII. Security: The infrastructure is protected against unauthorized access, interference with normal operation; it consistently implements information privacy and other security policies.

[jjj] This paragraph contains information from talks given at the CIEE/UCOP Demand Response Enabling Technologies Workshop, June 2, 2005, presentation available at http://ciee.ucop.edu/dretd/UCB_Project_06-02-2005.pdf.

preferences and habits by monitoring sensors in every room, including occupancy sensors. The controller will learn about the heating and cooling requirements of the home by monitoring temperature sensors throughout the house and outside, including weather, wind, and radiation sensors. The smart thermostat might communicate with sensors on light switches and doorstops, and be capable of turning lights off and closing doors. Sensors might be installed on each outlet or power cord in the house, monitoring the power being drawn, and transmitting that information to the smart thermostat for processing.[kkk] It is also possible that sensor nodes might in time contain some processing capability and be able to compile or process data themselves. Research challenges in this project include developing low cost sensors, figuring out how to power the sensors without battery, developing the smart thermostat control system, developing the communications protocols for these elements, and figuring out how to make this whole system user friendly enough for the average energy consumer to employ.

These visions of what a long-range advanced metering, demand response infrastructure may look like inform many of our discussions in the following sections.

4.0 Project Outcome: Review of Technologies and Identification of Potential Solutions

In this section, we elaborate on the technological aspects of our research into security and privacy in demand response systems. Section 4.1 establishes the overall context for our discussion by identifying the representative subsystems and networks in demand response/sensor networks. Section 4.2 reviews the objectives of this aspect of the current project. Section 4.3 introduces some of the general security concerns in communication networks. Section 4.4 discusses security issues and recommendations specific to wireless sensor networks in a DR system. Section 4.5 introduces the notion of agile radio nodes, identifies where they may be useful in a demand response system, and then elaborates on related security issues.

4.1. Subsystems and networks in Demand Response/Sensor Networks

Figure 1 depicts at a high level some of the subsystems and networks comprising the demand response/Sensor Network Architecture that we will use as a basis for our discussion. These are briefly described below.

- *Sensors, Sensor Clusters and Sensor Networks.* To begin with, there is a collection of sensors and actuators at the user premises; such user premises may be either a residence, or a commercial enterprise/industrial building. Examples of sensors include temperature and lighting sensors; examples of actuators include a thermostat/control system that regulates the airflow in heating/cooling ducts

[kkk] Sensors at power outlets might contain on/off switches the smart thermostat could control, but sensors on power cords can only monitor the power drawn. It was suggested that power cords might someday contain such imbedded sensors as a standard feature.

via registers and that controls various appliances such air conditioners, water heaters and lighting.

Increasingly, such sensors are being integrated with computational and communication capabilities. In particular, emerging classes of sensors are capable of wireless communications (this combination is sometimes referred to as "motes"). The computational capabilities can be used to perform a limited set of computational tasks, including local data aggregation and encoding. The communication capabilities in such nodes can be used to receive data comprising DR pricing information and sensor/actuator query and control information, and to transmit relevant sensor data, energy usage, status, etc.

Depending on the size of the installation, the number and types of sensors deployed, their geographic distribution, and other relevant factors, it can be useful to group together some of these sensors/actuators to form a number of *sensor clusters* (and perhaps even a hierarchy of sensor clusters).

- *Cluster gateway node(s).* Each sensor cluster can have a cluster gateway node that acts as the proxy for that cluster. Analogously, the entire sensor network at the building level can have a network gateway node. In a residential context, a "neighborhood gateway node" may serve a group of homes in a neighborhood.
- *Building gateway node(s).* The Home/building control subsystem may be comprised of one or more building gateway nodes, sensors for different attributes (such as temperature, light, humidity, etc), and enterprise monitoring & control subsystems. Further, the building network gateway node will typically have scaleable LAN/WAN connectivity, usually via an appropriate access network, either wireless or wired. Examples of typical access networks include (1) Wired networks such as DSL, Cable, Leased line, Passive Optical Networks (PONs), and (2) Wireless networks, such as various generations of cellular networks (2/2.5/3/4G) operating in licensed frequency bands IEEE 802.11x networks, as well as Mesh and other kinds of networks in the licensed and unlicensed bands.
- *Backhaul Networks.* The access networks provide connectivity to backhaul networks. Examples of Backhaul networks include: (1) Private Enterprise Networks, e.g., leased lines/Wide Area Networks, and (2) Public Internet.
- *Other Networks.* Eventually, the backhaul networks provide a link to the enterprise networks owned and operated by other participants in the Demand-Response ecosystem, such as Investor Owned Utilities (IOUs) e.g., PG&E, Power generators and Independent System Operators (ISOs). These customers need to be able to deploy, provision, manage, and control the network services, broadcast or multicast pricing information, monitor load characteristics, etc., and (selectively) obtain data from various end users for local processing on enterprise back end systems.

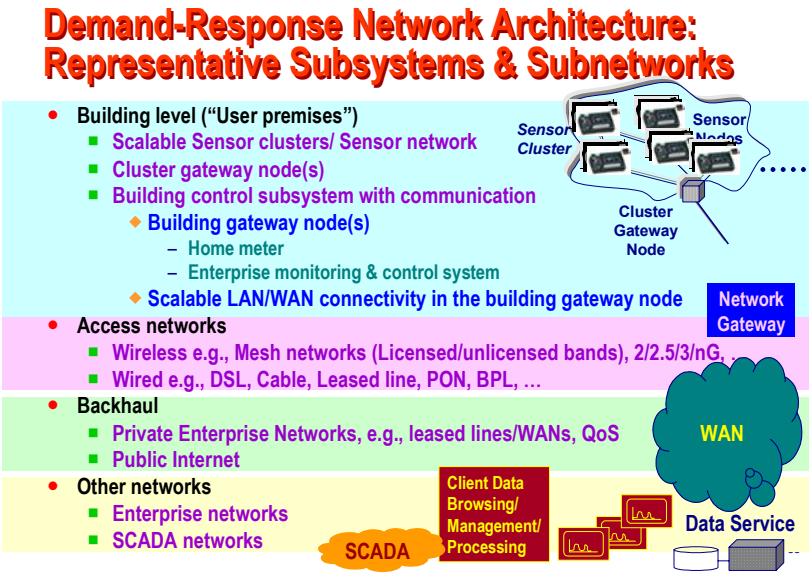

Figure 1. Examples of Subsystems & Networks in a Sensor-Network Based DR Architecture

4.1.1. Advanced Metering Infrastructure (AMI)

Several ongoing efforts are aimed at developing and deploying technologies related to an Advanced Metering Infrastructure e.g., [OpenAMI]. Some other efforts are explicitly targeted at implementing demand response e.g., [DRETD], whereas others consider a wider variety of objectives. For example, a gateway can be designed to provide a superset of the basic communication facility needed for demand response implementations. In some contexts, a home gateway with energy management related functionality is referred to as a "Consumer portal" e.g., [Intelligrid]. Such a portal is typically a combination of hardware and software that enables two-way communication between energy service organizations and equipment within the consumers' premises. Consumer portals have the potential to enable a variety of advanced utility applications; such as demand response, energy management services, improved outage management, automation functions, advanced metering and reporting, power quality management, and many other functions.

One of the key issues that concern "information" flow relates to where the data gathered by various sensors and meters is stored and processed. At one extreme, data gathered can be largely localized to stay within the customer premises (i.e., a consumer home or office complex), transmitting only the abstractions of relevance, e.g., the monthly bill. At the other extreme, all of the data generated can be transmitted to a central facility, for example under control of the energy service provider, and processed at a subsequent point in time. Architectural designs that correspond to any point between these extremes are also possible, and indeed, under consideration.

Security and Privacy issues arise when considering how this information can be protected, both from a technological perspective, and from a legal perspective.

4.2. Objectives

The objectives of this aspect of the project were to:

- Understand and assess the security challenges from the perspectives of different disciplines and stakeholders, including:
  - Security issues in Sensor networks
  - Privacy concerns in the demand response context
  - Network related security and privacy concerns
  - Software Radio and terminal device vendors; a terminal device here refers to a device that s used by a consumer, e.g., a cellular handset (mobile phone) or a Personal Digital Assistant (PDA).
  - Regulatory agencies; examples of regulators in this context include the Federal Communications Commission (FCC).
  - Network security standards
- Identify and Categorize attack modes in sensor networks
- Identify known vulnerabilities in existing protocols
- Identify appropriate security goals for DR/sensor networks
- Propose an architecture/framework for considering security in demand response/sensor networks.

To establish context, we begin by describing the basic categories of security concerns in a network context (Section 4.3). Subsequent sections then discuss in greater detail security issues that relate to wireless sensor networks (Section 4.4) and wireless networks that have agile radio nodes (Section 4.5). We then describe a framework for network security architecture aimed at providing end-to-end network security (Section 0). This framework defines some of the general security-related architectural elements that are needed for providing end-to-end security, and can be used as a basis for developing the detailed recommendations for the end-to-end network security in specific implementation and deployment contexts.

4.3. Security concerns in a network context

The aspects of security that are traditionally of concern in the context of conventional computer networks are the following:

- Access control;
- Authentication;
- Non-repudiation;
- Data confidentiality;

- Communication security;
- Data integrity;
- Availability; and
- Privacy.

These security aspects are briefly elaborated upon below. A set of security measures that are designed to address a particular aspect of network security is referred to as a security "dimension". Properly designed and implemented security dimensions support security policy that is defined for a particular network and facilitate the rules set by the security management. The security dimensions are not limited to the network, but extend to applications and end user information as well; additionally, they apply to service providers or enterprises offering security services to their customers.

Access control

The access control security dimension protects against the threat of unauthorized use of network resources. Access control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. In addition, Role-Based Access Control provides different access levels to guarantee that individuals and devices can only gain access to, and perform operations on, network elements, stored information, and information flows that they are authorized for.

Authentication

The authentication security dimension serves to confirm the identities of communicating entities, and is designed to guard against threats arising out of entities that can adopt forged identities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or an unauthorized replay of a previous communication.

Non-repudiation

The non-repudiation security dimension provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place.

Data confidentiality

The data confidentiality security dimension protects data from unauthorized disclosure. Data confidentiality ensures that the data content cannot be understood by unauthorized entities. Encryption, access control lists and file permissions are methods often used to provide data confidentiality.

Communication
The communication security dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points).

Data integrity
The data integrity security dimension ensures the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.

Availability
The availability security dimension ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category.

Privacy
The privacy security dimension provides for the protection of information that might be derived from the observation of network activities. Examples of this information include web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS (Domain Name Service) names of devices in a service provider network.

Some of the privacy issues specific to demand response networks are discussed in detail elsewhere in this report.

4.4. Security in Sensor Networks

In this section, we describe our research related to security in wireless sensor networks. Following a brief overview of wireless sensor network technology, we summarize the security attacks and countermeasures that have been investigated in this context.

4.4.1. Overview

Sensors offer a promising mechanism for monitoring relevant information such as temperature, lighting and humidity that are relevant in formulating the response to an energy management system. Wireless sensor networks afford a natural and potentially cost-effective mechanism for the monitoring and control of appliances and energy management systems. Sensors may be deployed to take fine-grained readings and affect fine-grained control; for example, the air conditioning may be turned down only in areas where the temperature is deemed to be in the comfort range.

To implement this function, the sensor nodes need to take appropriate readings and forward them to a base station, which will likely also serve as a control center. The base station can retrieve real-time or time-of-use prices, then, based on all the sensor data, make decisions about how to control each area at the site. The decisions are disseminated back through the sensor network and the control effected.

This model can expose the network to security vulnerabilities. An attacker that can change, eliminate, or insert some sensor readings can provide the base station with a distorted view of the site's status and cause it to make incorrect decisions. Conversely, since sensor nodes may be used for control, an attacker that can cause nodes to accept his commands instead of the base station's can cause problems with the site's environmental control, to say nothing of the potentially expensive power usage that may result.

Sensor networks have the disadvantage in this regard of suffering many layers of potential vulnerabilities: they are subject to the problems of computer networks in general; ordinary wireless networks; ad-hoc networks; and additional physical attacks that take advantage of the fact that sensor nodes are small in size, and may be placed in open accessible locations from which they can be removed (or easily destroyed in place). Sensor nodes have limited resources, including slow CPUs, short battery life, and small memories. These limitations both open up additional attack avenues for adversaries and make it difficult to use existing cryptographic techniques as defenses.

This is not to say that using sensor networks necessarily means a lack of security. A critical element of security analysis is analyzing a system with respect both to its configuration and to a particular *threat model*, i.e., the capabilities and objectives of the adversary. For example, some attacks assume high-powered adversaries in an outdoor, military setting, which are not necessarily applicable to a DR application. Further, by limiting the configuration of the sensor network, we can limit the space of possible attacks dramatically.

In the process of minimizing security risks, we often reap additional gains in reliability and lower maintenance costs. For example, most demand response applications will use sensor nodes in a fairly "dumb" way. They are basically sending and receiving simple messages from the base station. In particular, they will typically not need to perform much computation on the data they collect, and they do not need to move around. Advances in cryptography on these limited devices in fact allow us to make the implementations simpler, by reusing known techniques.

Accordingly, we will first provide a brief survey of the space of known attacks on sensor networks and some countermeasures. Next, we will make a set of recommendations for the deployment of sensor networks in a DR context, with a view towards security against these attacks and general robustness and reliability. In making some recommendations, we take note of the fact that nodes may be used not just for sensing but also for local actuation, perhaps turning on or off HVAC elements in response to commands from the control system. This means that attackers might be able to directly *influence* the target environment rather than simply learning information about it. We propose solutions for this threat as well.

4.4.2. Survey of Existing Attacks and Countermeasures

Attacks on sensor networks may be classified by the layer or service they affect. We will use these categories to provide recommendations for DR deployment that meet DR's requirements while minimizing the security risks. There is a wealth of existing literature on

security in sensor networks. This section provides a brief summary of the various kinds of attacks; more detail can be found in the references.

Routing attacks constitute the bulk of the types of attacks we discuss here, as many of them apply to wireless or ad-hoc networks generally and are well understood. Ad-hoc network formation is a relatively fragile process (though ongoing work seeks to change that), and in the case of sensors, the adversary may have much greater capabilities than the legitimate nodes. The other reason is that many physical, network-layer, and application-layer attacks are specific to the hardware and particular application being run.[lll] We address DR-specific recommendations in the next section.

4.4.2.1. Physical attacks

A new threat compared with most traditional networks is that the sensor network nodes themselves may be physically captured. If a captured node is not sufficiently tamper-resistant, any data on it may be obtained, including secret keys. The node itself may be reprogrammed as an agent of the adversary. Advances in tamper-resistant technology and a trend toward single-chip solutions suggest that cloning of nodes by an adversary make soon become much more difficult. Disabling nodes will, of course, still be feasible due to their small size.

4.4.2.2. Network / Link Layer

There are two obvious attacks: jamming (deletion) and insertion of packets. These can be addressed in part with spread spectrum techniques, although in practice this requires time synchronization among the nodes. Attacks based on insertion of packets can be mitigated by including a verifiable authenticator early in the packet so that the rest can be rejected. Nonetheless, it is not very difficult to drain the power of one or more sensor nodes once messages may be sent to them, especially if the attacker has a large computation and power-source advantage.

4.4.2.3. Routing Layer

The discussion in this section is based largely on a condensation of the survey by [Karlof & Wagner 2003]. We consider the routing layer to consist of two functions: building a routing tree that specifies where each node sends its packets, and actually routing packets. Adversaries may simulate one or more nodes, have out-of-band channels, and modify data they forward or generate arbitrarily. This can lead to incorrect routing trees being generated and packets being forwarded incorrectly.

Threat Model and Goals

We assume that an attacker may have a laptop-class machine with a more powerful radio that can listen to, and broadcast to, all nodes in the network. Some attacks may rely on the attacker having broadband, high-power transmission capability for jamming. Jamming may be used to delete messages from the network; modified messages may be

[lll] Appendix C provides a brief definition of these networking terms drawn from the OSI reference model..

sent instead. Attack nodes are also assumed to be able to communicate amongst each other on an out-of-band channel. Note that some defenses are able to detect attackers, so an attacker that actively inserts or modifies messages runs the risk of being detected and rejected.

We will consider *insider attacks* where an attacker has compromised a legitimate node and any data on it, and *outsider attacks* where the attacker only has radio access. Essentially, we want reliable delivery of each genuine node's unaltered messages in the presence of an adversary. If we only consider outsider attacks, then the problem is simpler, since by using a shared key, nodes can ensure that messages are genuine (authentic) and unaltered (their integrity maintained). However, an adversary can still drop packets instead of forwarding them. In the presence of insider attacks, some number of messages will likely be corrupted, depending on the number of compromised nodes. Since it is in general impossible to preclude or be resistant to all attacks, we would ideally like the reliability of message delivery to degrade gracefully as the number and power of attackers increases.

Selective forwarding

An attacker can simply decided not to forward every packet it is supposed to. If it does so too often and is thus judged unreliable, the route may be changed so as not to include it. By selectively dropping packets, the attacking node can preserve its status while causing problems for particular victim nodes. Obviously, the more traffic the attacker routes, the more effective selective forwarding is. The next two attacks, sinkhole attacks and the Sybil attack, are ways for an attacker to attract more traffic.

Sinkhole attacks

A sinkhole attack is when an attacker advertises a good route to the base station or other destinations, causing many nodes to forward their packets through it. If the adversary has a powerful radio, it may be able to provide this route when needed to pass route consistency checks by other nodes. In this manner it may corrupt the routing tables even of nodes that are far away. Then it can apply selective forwarding or any packet-modification attack easily.

The Sybil attack

In a Sybil attack, a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, dispersity and multipath routing, and topology maintenance. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities. Sybil attacks also pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. It is only reasonable to expect a node to accept but a single set of coordinates from each of its neighbors, but by using the Sybil attack an adversary can "be in more than one place at once".

Wormholes

In the wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. More specifically,

packets transmitted through the wormhole should have lower latency than those packets sent between the same pair of nodes over normal multi-hop routing. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes that would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. This will most likely always be the case when the endpoint of the wormhole is relatively far from a base station.

More generally, wormholes can be used to exploit routing race conditions. A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. In this case, an adversary may be able to exert some influence on the resulting topology if it can cause a nodes to receive certain routing information before it would normally reach them though multi-hop routing. Wormholes are a way to do this, and are effective even if routing information is authenticated or encrypted. Wormholes can also be used simply to convince two distant nodes that they are neighbors by relaying packets between the two of them. Wormhole attacks would likely be used in combination with selective forwarding or eavesdropping. Detection is potentially difficult when used in conjunction with the Sybil attack.

HELLO flood attack

Many route formation protocols use "HELLO" packets for neighbor discovery. Nodes listen for HELLO packets and assume that all such packets come from nearby nodes. If an attacker re-broadcasts a HELLO packet with high power, even far-off nodes will think the original sender of the packet is close by. This will result in an incorrect routing tree. Note that the attacker can simply replay an earlier packet: he does not have to be able to construct new authenticated packets.

Acknowledgement spoofing

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. An adversary can spoof link layer acknowledgments for overheard packets. By doing this, the attacker can convince a sender that a weak link is strong or that a dead or disabled node is alive. For example, a routing protocol may select the next hop in a path using link reliability. Artificially reinforcing a weak or dead link is a subtle way of manipulating such a scheme. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links.

Rushing attack

Hu et al. identified a *rushing attack* [Hu et al 2003b] on route formation that works as follows. Many ad-hoc routing protocols have mechanisms to prevent message explosions during tree formation. Consequently, they often use the first message they receive of a

particular type and ignore the rest. If an attacker can forward messages faster than legitimate nodes, then he can cause a lot of traffic to be routed through his nodes (since they will be included in many nodes' forwarding paths). There are several methods, including optimized network stacks, which can be used to implement the attack.

Defenses

Broadly speaking, there are two kinds of defenses: those that use cryptography and those that use timing or geographical information. Cryptography lets us authenticate packets: each node can tell which node generated the packet, preventing an outsider from injecting packets into the network. Naturally, if an attacker has captured one or more nodes, he can impersonate them successfully. Therefore, we would like to know the threat from capture of some subset of nodes. If all the nodes communicate using a single shared key, then even one compromised node can lead to impersonation of any node. The ideal is to have separate keys for each pair of nodes, so that one compromised node does not allow impersonation of any others. This can be costly, since it requires secure distribution of $O(n^2)$ keys, if n denotes the number of nodes.[mmm] There have been many proposed schemes for symmetric-key management and distribution: a survey by Chan et al. discusses many of these [Chan et al 2004]. Most such schemes rely on predistribution of keys so that each node has shared keys with some subset of its neighbors; this allows reasonably good connectivity, while mitigating the effects of node capture. Another option is to have the base station (with which each node can have a secret key) negotiate pairwise keys as in Kerberos [Neuman & Ts'o 1994]. Unfortunately these options tend to have high communication and implementation costs. This leads to shorter battery life and a higher incidence of bugs.

A significant recent development has been the arrival of public-key cryptography on sensor-class nodes, in particular elliptic-curve cryptography[f] [Blass & Zitterbart 2005], [Wander et al 2005] This allows us to perform much simpler key setup and management, since each node can have its own public/private key pair. These public keys can be used to set up symmetric keys for ordinary message-sending. Pairwise keys may be negotiated directly using public-key crypto (the base station having signed each node's public key along with the node's ID). Having per-node keys also means that compromised nodes do not reveal anything about messages from the remaining nodes. Anomalous readings or those suspected to be falsified can pinpoint the compromised node.

Certain attacks rely on timing or powerful radios; these attacks can be countered with timing or geographic-based defenses. Wormhole attacks can be mitigated with *packet leashes* [Hu et al 2003]. A variant of packet leashes have been used to counter rushing attacks [Hu et al 2003b]. Recent work by Parno et al. [Parno et al 2005] has nodes cross-check geographic information to prevent an adversary from replicating a compromised node at different places in the network.

[mmm] The term $O(n^2)$, read "Order of n-squared" indicates that this expression grows as the square of the number n.

4.4.2.4. Security Measures

Use of cryptography

Cryptography is not simply a "feature" of a secure network. It is important to use cryptographic techniques judiciously to achieve particular goals. Many cryptographic protocols have significant computation or communication requirements, so existing techniques must be modified; the good news is that more and more traditional approaches are being made feasible on sensor-class nodes.

Two good security goals for data-gathering sensor networks are *semantic security* [Goldwasser and Micali 84] and *nonmalleability*. Informally, semantic security means that, given an encrypted message, an adversary cannot compute any function of the plaintext[g] better than choosing at random. Obviously, learning the plaintext itself is forbidden, but so is predicting the value of the first bit with greater than a 0.5 chance of being correct. For a temperature sensor, this would be mean that the attacker could not deduce from an encrypted message the temperature reading it contained, say, whether the temperature was above or below a certain value, or if the reading was an even or odd value.

Non-malleability means that an adversary cannot alter a ciphertext in such a way that the plaintext corresponding to the modified message is related to the original (versus being random) and appears unmodified to the recipient. This condition is actually the same as being secure against chosen ciphertext attacks (CCA1) and adaptive chosen ciphertext attacks (CCA2) [Bellare et al 98]. Basically, the attacker can learn the decryptions of any messages but the one under consideration, but should not be able to learn any interesting information about it. Returning to our example, an attacker would not be able to take a reading and make it appear to be two degrees higher or, significantly, the same as some prior reading. Typically this is achieved by using a message authentication code (MAC) over the message.

We strongly recommend using accepted public standards for cryptography. It is all too easy to make mistakes by implementing cryptography in an ad hoc manner. Using proprietary ciphers, using block ciphers in the wrong modes and implementing the wrong sequence of encryption and authentication are very common errors. Designers should be careful to adhere to published, well-studied, and where possible, provably secure standards. Common radio standards including encryption are 802.15.4 [IEEE 802.15.4] and 802.11i CCMP [IEEE 802.11i] (not WEP, which is broken). The AES block cipher [FIPS] has undergone rigorous peer review and is designed to be efficient on 8-bit platforms. Recently, Elliptic-Curve public-key cryptography has been shown to be feasible on sensor networks [Blass & Zitterbart 2005], [Wander et al 2005]. Standard elliptic curves have been established and should be used.

Use encryption.

All sensor data should be encrypted. First, randomness must be employed in encryption. Without an element of randomness, an attacker can likely correlate messages to earlier ones. For example, if the attacker knows the temperature at some point and the message sent at that point, then he will know that all future messages that are identical indicate the same temperature. With randomness, the encrypted messages should never

repeat, even if their plaintexts are the same. Second, some form of time stamping should be used to prevent replays: an attacker should not be able to store and resend a previous message. (While all nodes may no have a clock, a logically equivalent notion of time stamping is possible.) Lastly, messages should not differ in obvious meta information such as length.

Use authentication for all data.

Simply encrypting (providing secrecy) is not enough. We must also provide for the integrity of the message by using a Message Authentication Code (See Endnote j).

4.4.2.5. Application Protocol / Data Processing

Adversaries that have access to the network, either by physical node capture or breaking any crypto used, may insert false sensor readings or jam or alter legitimate ones that are being sent. They may also be able to influence sensor readings: imagine holding a candle to a temperature sensor. The problem is that many functions that we would like to compute on the sensor readings can be completely corrupted by even a single attacker-controlled value. For example, say we want to find the maximum reading. If an attacker controls even one node, he can provide an arbitrarily high value that would be interpreted as the maximum. That is, many useful functions are not *resilient* to attacker-controlled values or even random faults. We discuss solutions to this in the Recommendations section.

4.5. Security in Agile Radio Nodes

4.5.1. Outline

In this section, we discuss security issues in the context of demand response Networks that employ *agile radio nodes* –network nodes that can be agile/flexible in their wireless communication interface. The term "agile radio nodes" is used here as a generic term that subsumes both Software Defined Radios [SDR] and Cognitive Radios [CR].[nnn] Both of these areas have been the subjects of much research, discussion and debate in recent years, and Software Defined Radios in various incarnations are anticipated to have a significant impact in the commercial arena over the next few years. For this reason, our discussion is phrased in terms of security issues in Software Defined Radios.

We begin by briefly reviewing the notion of Agile Radio nodes and Demand response networks, focusing specifically on Software Defined Radio (SDR) nodes. We introduce the various flavors of Agile Radio Nodes; comment on why and where they are useful, and specifically on where they may play a role in demand response Networks. We then introduce the security issues that can arise in the context of Software Defined Radios, and in the context of Demand-response networks that contain such radio nodes. Following this, we discuss a security framework for exploring investigating SDR related security

---

[nnn] "Software Defined Radios" are radios whose communication characteristics are defined and/or controlled via software (see Section 4.5.2), "Cognitive Radios" are radios designed to enable opportunistic use of spectrum that might be unused at any instant in time, although it might be pre-allocated to a primary user other than the current one.

issues, potential sources of threat, as well as attack modes, in particular relating to Software Download Security. Finally, we summarize the key points, and list some open research issues.

4.5.2. What is a Software Defined Radio (SDR)?

Some of the basic components of a radio, as depicted in Figure 2, consist of analog radio and human interfaces, along with an assembly of hardware (analog and digital) and software components that perform various signal processing and general-purpose computation tasks. A Software (Defined) Radio is a radio system whose functionality is partially implemented in software.[ooo] Examples where this technology is used include cellular basestations and access points, mobile terminals (cellular phones), as well as many other emerging applications.

[ooo] As a historical footnote, it is worth recalling that early radio systems were implemented entirely in hardware with analog components. The Analog-Digital and Hardware-Software Boundary continues to evolve over time, and as semiconductor CMOS technology evolves; the general trend is to reduce the number of analog components (versus digital components), and to increase the software components (compared to hardware components). It should be noted that no functional radio system can be implemented without hardware, and that analog functionality is necessary at both the RF and the human interface.

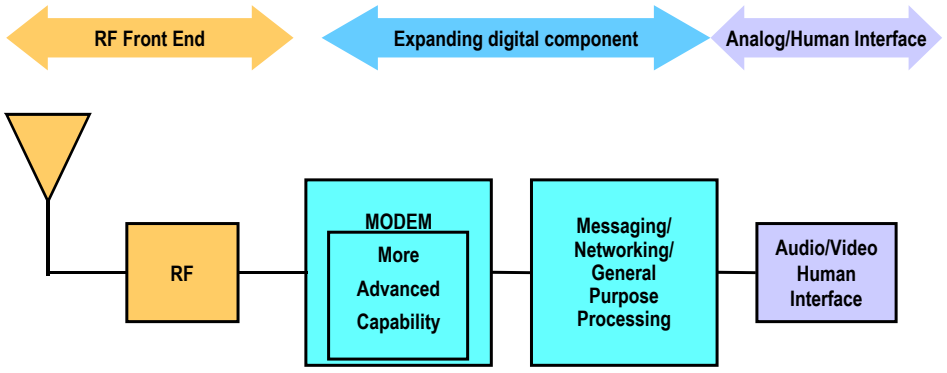

Figure 2 Radio Components: Evolution of the Analog-Digital and Hardware-Software Boundaries

4.5.2.1. Flavors of Software Defined Radios

In an attempt to categorize the spectrum of implementations of the general notion of Software (Defined) Radios, the Software Defined Radio Forum[PPP] (a consortium of groups interested in Software Defined Radio technology) has defined five tiers of "Software Radios", spanning the spectrum from implementations that employ exclusively hardware components to systems that employ hardware components only at the edges, with software being used for the rest.

[PPP] www.sdrforum.org

Tier 0: Hardware Radio (HR). The radio is implemented using hardware components only and cannot be modified except through physical intervention.

Tier 1: Software Controlled Radio (SCR). Only the control functions of an SCR are implemented in software - thus only limited functions are changeable using software. Typically this extends to inter-connects, power levels etc. but not to frequency bands and/or modulation types etc.

Tier 2: Software Defined Radio (SDR). SDRs provide software control of a variety of modulation techniques, wide-band or narrow-band operation, communications security functions (such as hopping), and waveform requirements of current and evolving standards over a broad frequency range. The frequency bands covered may still be constrained at the front-end requiring a switch in the antenna system.

Tier 3: Ideal Software Radio (ISR). ISRs provide dramatic improvement over an SDR by eliminating the analog amplification or heterodyne mixing[qqq] prior to digital-analog conversion. Programmability extends to the entire system with analog conversion only at the antenna, speaker and microphones.

Tier 4: Ultimate Software Radio (USR). USRs are defined for comparison purposes only. A USR accepts fully programmable traffic and control information and supports a broad range of frequencies, air-interfaces & applications software. It can switch from one air interface format to another in milliseconds, use GPS to track the users' location, store money using smartcard technology, or provide video so that the user can watch a local broadcast station or receive a satellite transmission

The interesting developments from a pragmatic point of view are in "Tier 2 Software Radios" as described above; such radios are referred to as Software Defined Radios, henceforth abbreviated SDRs.

4.5.2.2. Benefits of Software Defined Radios

In essence, Software Defined Radio (SDR) technology is a collection of hardware and software technologies that enable reconfigurable system architectures for wireless networks and user terminals. Software Defined Radios (SDRs) provide an efficient and comparatively inexpensive solution to the problem of building multi-mode, multi-band, multi-functional wireless devices that can be enhanced using software upgrades.[rrr] As such,

---

[qqq] Heterodyning is the process of "beating together" or *mixing* two different frequencies to obtain an output at some other, related frequency. The mixing of two frequencies f1 and f2 results in the creation of two new frequencies, one at the sum of the two frequencies mixed (f1 + f2), and the other at their difference (f1 -f2). A superheterodyne receiver converts any selected incoming frequency by heterodyne action to a preselected common intermediate frequency, for example, 455 kilohertz (AM receivers) or 10.7 megahertz (FM receivers), and provides amplification and selectivity, or filtering.

[rrr] Multi-band operation refers to the ability to operate in multiple frequency bands. Multi-mode operation refers to the ability to communicate using more than one protocol, e.g., Bluetooth and IEEE 802.11. Multi-

SDRs can really be considered an enabling technology that is applicable across a wide range of areas within the wireless domain. SDR-enabled devices (e.g., handhelds) and equipment (e.g., wireless network infrastructure) can be dynamically programmed in software to reconfigure the characteristics of equipment. In other words, the same piece of "hardware" can be modified to perform different functions at different times. This allows manufacturers to concentrate development efforts on a common hardware platform. Similarly, it permits network service providers (also called “operators”) to differentiate their service offerings without having to support a myriad number of terminal devices. Finally, users of SDR enabled devices have a piece of scalable hardware that is at once compatible at a global scale and robust enough to deliver a "pay as you go" feature set.

4.5.3. Software Defined Radios in Demand Response Networks

Figure 3 highlights some locations in a demand response network where Software Defined Radios can be deployed. In particular, as suggested in the illustration, SDRs can be profitably leveraged in sensor cluster gateway nodes and neighborhood gateway nodes, as well as in the infrastructure. They are currently unlikely to be used in the leaf level sensor nodes because of the extremely stringent constraints on cost and power that are imposed on such nodes, and because of the absence of a predominant need for RF agility in the end sensor nodes deployed within a home.

For example, a Software Defined Radio node that supports *multi-mode* operation can support IEEE 802.15.4 [IEEE802.15.4] (and Zigbee Radios [Zigbee]), IEEE 802.11b (WiFi) [IEEE 802.11] or Bluetooth all of which operate in the 2.4 gigahertz band. Multi-band operations can also be useful, and may be used to support commonly used frequency bands such as 2.4 GHz, 5 GHz, and 800/900 MHz. These capabilities can be leveraged by the gateway node for local area communications (using IEEE 802.11), sensor networks (e.g., using IEEE 802.15.4 and Zigbee devices), as well as backhaul communications using wide area networks.

---

functional devices are capable of supporting more than one function, such as a combination of the functions associated with a phone, camera and PDA.

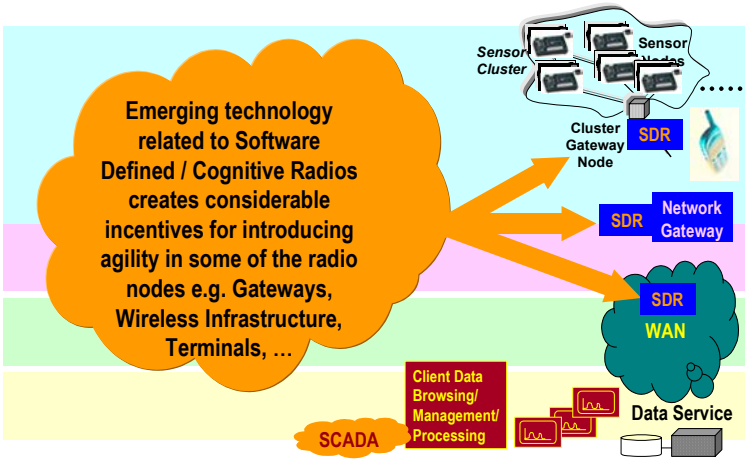

Figure 3 Potential Roles for Software Defined Radios in Demand Response Networks

4.5.3.1. Security Issues

As is the case with most software or hardware components, potential security issues associated with Software Defined Radios can arise in any of the deployment contexts suggested above. Security concerns associated with Software Defined Radios and the wireless communication enabled by them include:

- Conventional security issues, such as protection needed for content confidentiality, privacy and integrity, authentication, non-repudiation, etc.
- Security issues arising from the use of wireless RF links in mobile wireless networks and sensor networks. The use of wireless links introduces security considerations beyond those of wireline telephony and communications because interception of the signal cannot be prevented.
- Novel security concerns arising from the new capabilities introduced by the use of software-defined radios in the system. In particular, SDRs enable access over the air to parts of a system, such as the radio component, that hitherto have required *physical* access to the radio hardware components. The security issues concerned with this new level of access to the system need to be well understood and addressed. In particular, the full cycle of download, storage, installation, and instantiation (DSII) for software over wireless links must be considered.

In essence, the implementation of radio links with software defined radio technology requires security measures to preclude introduction of software that can compromise existing security measures and existing security systems. At the present there is no single solution to the problems associated with wireless systems/SDR security. However, in light of the growing importance of agile radios, and of security, many of the issues are under study by the technical community. Researchers and system designers

working in this area need to make the needed trade-offs, and select approaches and components that are best suited to the specific issues at hand.

The overall goal of our effort is to amalgamate some of key considerations related to agile node security, including work in the SDR community, and to develop the rudiments of a security model for wireless communication using SDR technology. This provides a basis for considering the architectural implications of SDR security issues in demand response networks.

4.5.4. Security Issues in Demand Response Networks using Agile Radio Nodes

4.5.4.1. An analogy: Vulnerabilities in WiFi Networks

Deployments of various versions of IEEE 802.11 (also known as Wireless Fidelity or WiFi) to establish a wireless local area network (WLAN) are becoming increasingly prevalent. Because WiFi enabled laptop computers and personal digital assistants (PDA) combine a radio and computing interface, they provide a useful analog for examining potential dangers posed by hackers to networks of software defined radio terminals. The initial security design (WEP) associated with IEEE 802.11 was flawed [WEP], and led to a number of significant attacks on public and corporate networks; some of these attacks have been widely publicized, and unfortunately some of them have resulted in substantial losses. While the more recent versions of IEEE 802.11 systems, such as IEEE 802.11i, have a more comprehensive approach to security [IEEE 802.11i], many of these systems deployed at homes and enterprises are still prone to various forms of attack. In essence, such networks are subject to "blended attack" methods combining coordinated attacks on the radio and computer. Such blended attacks can be used to threaten the integrity of a system that employs software-defined radios.

We briefly list some of the basic tools and blended attack methods used by hackers to attack and exploit WiFi equipped mobile terminals. We then examine parallels between the WiFi scenario and similar threats to software defined radio terminals and networks by wireless hackers. This leads up to an initial proposal for requirements and architectures for high assurance SDR.

4.5.4.2. Blended Attacks on Systems with Radio Nodes

"Blended" attacks combine various attack methods (unauthorized access to data, threats to integrity, denial of service, unauthorized access to services, repudiation, …) against both the radio and computing interfaces of a wireless mobile terminal. For example, special techniques allow the hacker to jam encrypted WiFi networks, making normal access points "invisible" to WiFi terminals and allowing hackers to use their own access points to seize control of networks.

A number of well designed wireless hacking tools and equipment are now available. Some of these tools are freely distributed software that can be downloaded from the Internet. Other tools, including enterprise-grade hardware and systems, can be purchased online. Examples of such tools that enable blended attacks on the radio and computer software/hardware include:

- "Stumblers" that allow wireless hackers to explore the network characteristics of wireless base stations and mobile terminals.
- "Sniffers" that intercept, display, and store data being transmitted over the network
- "Crackers" that break encryption codes, such as Wired Equivalent Protection (WEP) and network access codes for GSM.

SDR: Radio Vulnerabilities

In the context of SDRs (and in particular, deployment of SDRs that employ the Software Communication architecture (SCA) mandated by the US Department of Defense) the term "Radio platform" is used to refer to the set of hardware and software components that are used as building blocks to instantiate a specific "radio implementation".[h] Such a radio implementation is obtained by writing a "Radio Application" that programs the details of an application specific wireless protocol (synonymously, *air interface* or *waveform*) using the hardware and software components and interfaces provided by the Radio platform.

In the Radio implementation, vulnerabilities affect the stability and integrity of both the Radio Platform hardware and software, and the Radio Applications. Using blended attack methods, hackers can exploit both hardware and software vulnerabilities within the Radio Set.

The components of a radio system can be annotated with vulnerabilities, as shown in Figure 4. The vulnerabilities affect both hardware and software in the basic hardware and software components (alluded to as the "Radio Set") and the components of the system that are used to manage and deploy field units (referred to as the "Administration System" components). Hackers can exploit security vulnerabilities by blending the various attack methods against both the radio and computer interfaces.

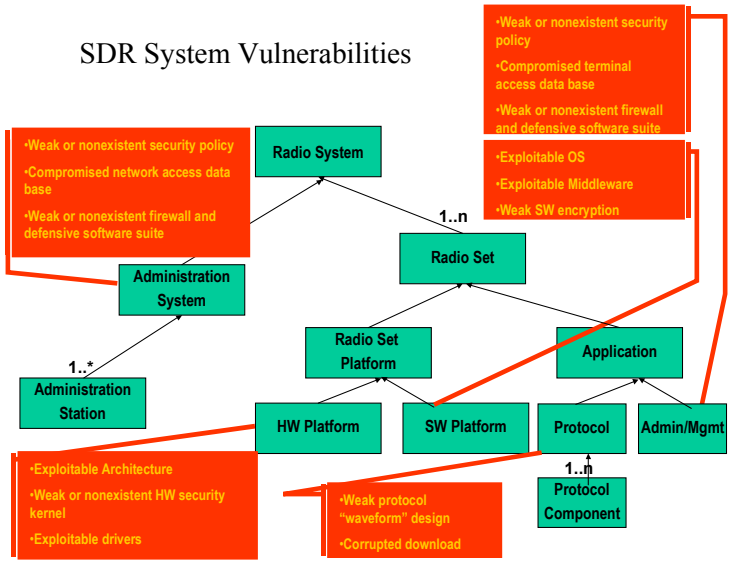

Figure 4 Examples of SDR System Vulnerabilities

Vulnerabilities related to hardware may result from a variety of factors, including: lack of a hardware based security kernel (such as an encryption engine); lack of a hardware firewall; and exploitable hardware device architectures with corresponding exploits in the device drivers.

Software vulnerabilities may include exploitable operating environments including: vulnerable operating system (OS) and middleware; weak software based encryption engine; use of protocols waveform(s) with weak security design; corrupted waveform or application download; weak or nonexistent anti-virus and firewall software; and weak or nonexistent security policy.

SDR System Vulnerabilities

A successful attack usually has the following (undesired) effect on the terminal device (e.g., DR cluster gateways and neighborhood gateways, mobile handsets) and access point, highlighting the importance of protecting the platform, and not just the data:

- The upload and download data being passed between mobile terminal and access point are compromised.
- The radio and network configuration software in the SDR are corrupted.
- A keystroke or packet repeater (a type of "Trojan Horse" software) is successfully planted on the host or client platform.

4.5.4.3. Assurance Architecture

A good approach to a blended attack is a "multilayered" defense, sometime referred to as a defense in depth. That is, a combination of methods, instantiated in both hardware and software, is implemented in both the end sensor, and the Agile Radio equipped gateway device or access point in the demand response network.

In the most secure high assurance systems, a hierarchical architecture is employed, where multiple layers provide specific, well-defined security mechanisms that can be used by higher levels. A high assurance security mechanism must be: (i) always invoked, (ii) non-bypassable, (iii) tamperproof, and (iv) verifiable.

4.5.4.4. Software Download Security

The ability to download software into terminals introduces several new security issues; furthermore, the aspects of concern can vary with the role of the stakeholders. From a regulatory perspective, the downloading of new software has the potential to change radio transmission characteristics, in particular, the frequency and power radiated. From a user's perspective, content of various forms is important to protect in the context of downloads. From a service provider's perspective, it is important to be able to consistently account for all billable time. From the point of view of a device manufacturer, a key concern is that the software download is appropriate for the target terminal and is unaltered.

In the context of demand-response networks, the ability to do software downloads is one of the main attractions of deploying agile radios nodes. The security of downloads is important in order to ensure the integrity of the radio function, compliance with

regulations, integrity and security of the billing process and/or the billing data, and to prevent the loss of valuable user and energy usage data. Furthermore, there is a desire to ensure that no programs are installed that essentially takes over the subsequent interface to the back end, thereby serving as proxy for, (or in this case, masquerading as) the home meter, thermostat, and the sensor field.

Security Related to Software Download: Areas of Concern

The uniqueness of the media and the hardware and software flexibility in reconfigurable, software defined radio devices present some unique potential security threats and requirements including:

- Security threats during the software creation process
- Reconfiguration of hardware and software
- Unique authentication, authorization, and accountability requirements
- Trust relationship based on the type of software being downloaded
- Resource constraints — limitations of processing power and memory
- International interoperability considerations[sss]
- Device management aspects
- Controlled access
- Existing security download mechanisms (e.g., SSL) typically not flexible or not efficient enough to accommodate the wide range of devices

4.5.5. Agile Radio Nodes: Security Framework

The Agile Radio node/SDR security framework discussed here draws from a number of related efforts. The objective of this framework is to provide a template for discussing specific issues and for comparing different topics and approaches.

The model consists of three levels, representing

- the wireless link,
- security threats, and
- the intervening security provisions for protecting the link from the threats.

In each of the levels issues relating to the information source, central network and radio infrastructure, the wireless link, and the remote destination are considered individually. For simplicity, this version of the model considers a path that is a one-way transfer of information from a central source to a remote location over a wireless link. Most

[sss] International interoperability is deemed very important in the context of radio-equipped devices such as handsets in commercial and military use that can be deployed or roam worldwide. A much more limited deployment scenarios may relax this interoperability constraint.

of the security concerns are the same for outbound, inbound, or full duplex operation. Where any differences exist, they can easily be illustrated with variations of the basic model.

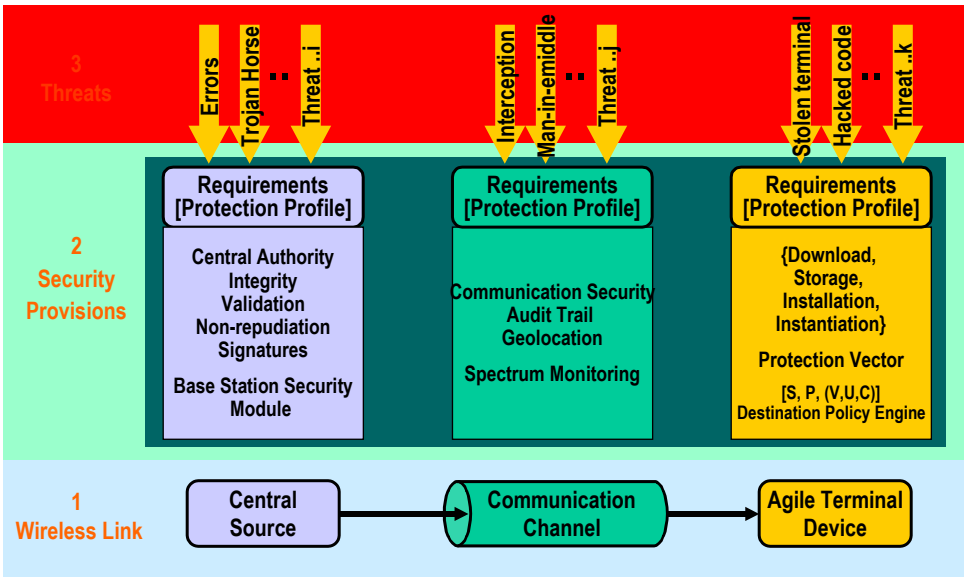

Figure 5 Initial SDR Security Framework

4.5.5.1. Wireless Link: The Communication Layer

Central Information Source

In the context of demand response networks, the "central source" depicted in the model includes the energy management/utility infrastructure that originates decisions about real-time pricing to be communicated to the rest of the network, destined eventually to the neighborhood/sensor cluster gateways and the terminal devices/appliances in the customer premises/homes e.g., smart thermostats and smart meters. The equipment and data sources used in any intervening communication service providers are also included as part of this source.

This block includes all of the wireline facilities as well as the wireless infrastructure, down to the base station antenna. Traffic carried in this network is at (relatively) lower risk compared to the wireless infrastructure, because system nodes can be made physically secure and most of the transmission links can be implemented with more secure fiber technology.

It is worth noting that Agile radio (SDR) technology allows software to change the RF characteristics of the base stations that are included in this block.

Wireless Link/Channel

The physical layer employed when communicating using a software-defined radio (or any radio) is vulnerable because of the wireless communication channel. This channel is shown in the figure as being one way for simplicity, but half duplex and full duplex modes are extensions. The security implications of attacks on this channel vary with content. For example, there are varying consequences incurred by the loss or corruption—intentional or accidental—of Software Downloads, Funds (Electronic funds transfer, Billing, etc), voice and data.

In the transition from wireline service to the first generation of cellular phones there was a significant impact due to lack of security. Not only were conversations overheard and made public, but also substantial revenue was lost from hackers stealing phone numbers over the air. That experience led to architectural provisions for greatly increased security in the second generation of telephones. In addition provisions for digital protocols, directional sectors, antenna beam steering, and low power operation have improved security in the radio link.

In the context of DR systems, the link carries information related to DR pricing signals, energy usage, and billing, amongst others. Additionally, as elaborated elsewhere, the link also carries critical information that relates to provisioning and radio software on the agile radio node. Security of these communication links is therefore of relatively high priority.

Terminal Device

The terminal device, in the context of Demand-response systems, is the neighborhood or home/building gateway that employs an agile radio node. In the cellular domain, the terminal device is typically a mobile handset, PDA or analogous device. In contrast to a cellular mobile phone application, where the receiving terminal device is a battery powered consumer device with fairly stringent constraints on power and form factor, the constraints on the gateways nodes are *a priori* not that stringent, since such a device can typically be powered from the main electric supply, using batteries only as a backup if at all. On the other hand, the cost and power constraints on the leaf sensor nodes are so stringent that SDR technology is inappropriate for these nodes give the current state of implementations for SDRs.

In the commercial wireless world, wireless service providers sell access to a wireless infrastructure. They may own that infrastructure or lease capacity on it. They specify what terminal models will operate in their service, and either sell them directly to customers or through a third party vendor.

In the demand-response context, the (electricity/…) utility service providers (e.g., PG&E) provide utility services (electricity/…) to the end customer. The utility service providers may use wireless services as a mechanism for communicating control/pricing signals to the consumer, obtaining data related to energy usage, billing related information, etc., and potentially also provide final billing information back to the end user (consumer at home) via a web portal. The utility service providers would normally tend to specify the capabilities of the gateway nodes/devices. Many variations of business models are possible

for who makes, owns, and operates the various components of the devices and services in such a context.

4.5.6. Terminal Device Security: What is appropriate for Demand Response

Since the terminal device of interest in the DR context is nominally a gateway that may be located in a publicly accessible location (such as in the neighborhood lamppost, or outside the house in an open area), it is important to have a way of verifying the identity of the device (and to potentially carry a secret key), and the data obtained data from this device, in order to ensure that it is the original device that was provisioned. Further, the device must be tamper resistant/tamper proof, such that any attempt to tamper with the device can be easily detected.

From this perspective, there is a deviation between the requirements of traditional mobile phones, base stations, and agile radio nodes used in the DR context. Many phones now incorporate a user identity module (UIM) that is identified with a specific user. This technique permits the user's personal information can be moved to a different unit; in order to deter theft, the UIM can carry a password. At first blush, there is no need for *physical mobility* of the agile gateway node in the DR context.

4.5.7. Threats

Any occurrence that detracts from perfect operation of the system is a threat. Threats generate requirements for security protection. The "threat layer" depicted in Figure 5 is concerned with sources of possible intrusion, disruption, or interception. In general, threats to a system can come from anywhere, and cannot be fully anticipated. The motivations of the attackers can vary significantly. The type of threats can also range significantly across the board.

The threats can come from negligent, careless, or untrained employees; from unauthorized manipulation of system controls, exceeding delegated authority; or they can be malicious in intent. The types of violations may include disallowed access to content (in the case of DR networks, this may be access to private billing information or energy usage information, for example); impersonation, spoofing (for example, to forge dynamic price reductions or increases); unauthorized use of system, to avoid payment, etc. The threats may also result in denial of access, system overload, disruption of service, reduced Quality of Service (QoS),[ttt] violation of power control protocol.

Individual threats can strike at any part of the system at any time, and they can be new or ones previously seen. There is no way to develop an exhaustive list of threats, because ingenuous individuals will always find new ways to attempt to crack the system.

In addition to malicious threats, users of a wireless system can cause disruption of normal operation inadvertently, although good system design should mitigate most such potential problems. In particular, the system should handle failures gracefully.

[ttt] See glossary of terms for QoS

The threat space in Demand-response networks is complex because it is very large and sparsely populated. The threat space is large because an attacker can attack any one of a large number (potentially millions) of utility meters, and the even larger number of sensors. Further the attack can take place at any point in the system (other than the gateways and sensors), so there are several more possible threat points or places that an attack could conceivably occur. It is sparsely populated because attacks are rarely seen in the normal course of events; thus the number of DR-network transactions that come under attack may be a miniscule fraction of the overall transactions completed without incident.

The threats in the security framework illustrated in Figure 5 are shown as arrows attacking individual parts of the system, and deterred by the security provisions protecting those components. The framework provides a template for "mapping" the very complex space of wireless download security. In areas where the threat structure can be identified, systems may benefit from an approach that considers threats first, and then build the appropriate constructs to mitigate those threats. Other systems will start with a proposed communication layer architecture, build security provisions as a second layer, and then test these provisions against a threat taxonomy to explore for possible weaknesses.

4.5.7.1. Threats: Information Source

Threats in the network may come from personnel who have been given access to facilities as part of their work. Such an individual can be a threat if they violate their trust. System design must identify the source of all actions within the system, and segment allowable procedures by job function. Staff that is careless or under-trained may also be part of the threat space.

All of the security provisions applicable to any computer system on the Internet also must be provided here. If an intruder can cause damage by accessing an internal IP address, that is a point of vulnerability.

4.5.7.2. Threats: Channel

The RF link is a major source of threat. An individual (and/or device) can access a base station (inside the DR source network) by masquerading as a legitimate user (or source of information), such as a Demand-response neighborhood gateway, or a cluster gateway, or even a leaf sensor node.uuu Alternately, a fake base station can attempt to attract legitimate terminals (e.g., DR gateway nodes) to connect to them, and attempt to extract information from them.

A more sophisticated attack is the "man-in-the-middle", in which a perpetrator communicates to a DR gateway (terminal device) by posing as a legitimate base station. The fraudulent station then logs on/connects to a real base station, and relays the information. By monitoring the exchange between the terminal and base station the fraudulent station can acquire critical information.

[uuu] The discussion related to security issues is outside the scope of this report, but is contained in a companion paper.

4.5.7.3. Threats: Destination/Terminal Device

Threats in this block arise from misuse of a gateway node or agile terminal device. A thief can steal a unit, and attempt to use it for fraudulent purposes. As experience with attacks on personal computers has demonstrated, an exhaustive determination of threats is not possible.

4.5.8. Security Provisions

The overlay of security mechanisms protects information traveling through the communication channel. While not essential for information transfer, security provisions are required to deter threatened attacks, and a trade-off between cost, efficiency, and protection is needed.

A "Protection Profile" is a system design tool to specify protection requirements, and is derived from threats. Protection that is not declared cannot be assumed to be present.

4.5.8.1. Security Provisions at the Source

Security provisions at the source refer to the set of mechanisms needed to provide assurance that the source of the information to be transferred is reliable, trusted, and authorized to undertake the transaction. This may involve adding information to establish that the source is bona fide, and may include ancillary information such as the results of software testing. Certificates may be used to ensure that there has been no perturbation in the information during transmission. Signatures may be used to authenticate that an individual or office is who they say they are. A Central Authority is needed to endorse both parties to the transactions. Exactly who such a Central Authority might be is usually the domain of appropriate industry organizations, in much the same way as is accepted practice in the regular security industry. (See End note [i].)

4.5.8.2. Security Provisions in the Channel

Security Provisions in the Channel refer to the set of techniques that are used to protect the transmitted information, and includes encryption, transmission security, or low probability of detection/interpretation techniques. It is not possible to prevent interception on a wireless link, but interpretation can be made very difficult. Security is rarely absolute, but measured in terms of the effort required to access content. An audit trail of the path transited by the download package en route to the destination can be used to establish that the package was not diverted and manipulated en route. Geolocation and spectrum monitoring can develop information to identify anomalies in terminal behavior from attempts to penetrate the system. (For example, if a mobile client is detected to be at a geographical location not "typical" or expected, based on its prior roaming patterns, this can be classified as an anomaly.)

4.5.8.3. Software Download: Security Provisions at the Destination

A Protection Vector (PV) is a series of numeric values for various system security aspects. Those vector elements are provided to a rule-based Destination Policy Engine that renders a verdict as to whether a given software downloaded should be accepted or not.

The Source (S) parameter is an assessment of the reliability of code that is a candidate for download, and is related to the module that is concerned with Security Provisions at the Source. Example levels of assurance are

- a statement by the code originator that it is acceptable,
- identification of the author(s),
- development by trusted authors,
- independent trusted third party test, and
- formal proof of correctness.

The Path Vulnerability (P) parameter is an evaluation of the intermediate path between the developer and the target terminal. Path protection mechanisms are digital signatures, public key infrastructure, audit trail and path histories, and trusted intermediate repositories.

Three parameters provide local context for policy evaluation and decision-making. First is the Inherent Value (V) of the content, with a priority structure of "worth" such as mission critical control/data, money, executable code, data, and audio or visual material. The second parameter for this module is Urgency (U), rated from high to low. Under some circumstances it might be appropriate to accept information that is extremely urgent even though some risk is involved because its other parameters were lower than desired. The final parameter is Criticality (C). That is concerned with the impact on system operations if the received information is faulty. Low criticality would be assigned to a correction for a function such as a spelling error, minor feature addition, or improvement in the user interface. High criticality would be assigned to software downloads that affect radio and other sensitive system functionality.

When all of the PV elements are collected together, a Destination Policy Engine uses policy rules to determine whether the code should be installed or not. The philosophy here is similar in concept to the Protection Profile (PP) described in common criteria portal (www.commoncriteria.org).

The Protection Profile is a set of requirements cast in the form of prevention before system design or during system evaluation. It also involves policy instantiation and execution during run time. The Protection Vector is a go-no go decision after a specific instance of information transfer.

Security Provisions will vary from system to system. The military goes to considerable effort and expense to provide secure tactical radios, but makes extensive use of commercial mobile radios and wireless PCS communications for administrative traffic.

Wireless telephony discovered with systems such as AMPS[vvv] that inadequate security leads to loss of revenue from stolen service and customer dissatisfaction from lack of privacy.

4.5.9. Summary: Agile Radio Node Security Recommendations

Agile or Software Defined Radios (SDRs) provide an efficient and cost-effective solution to the problem of building multi-mode, multi-band, multi-functional wireless devices that can be enhanced using software upgrades. Agile Radio Nodes can play an important role at several levels of the hierarchy in the context of Demand-response networks. Specifically, SDRs can be profitably leveraged in sensor cluster gateway nodes and neighborhood gateway nodes, as well as in the wireless infrastructure.

We have examined in this section some of the security issues that can arise in Demand-response networks that employ agile radio nodes.

Security in a demand response system employing agile nodes is a system level problem. In order to design a system with appropriate defenses, one must first understand the system threat and defense requirements. We have described some of the issues related to software download security that are unique to the use of agile radio nodes. More generally, hackers can use blended attacks against both the radio and computer layers of agile radio nodes. To defend against the blended attack requires a multi-layered defense-in-depth which protects both the agile nodes and infrastructure servers.

The security architecture must

- Ensure integrity of the software applications and downloads including download, storage, installation and instantiation;
- Ensure integrity of the reconfigurable platform against blended attacks by employing defensive layers (firewalls, intrusion detection, virus protection);
- Integrate biometric and radiometric assurance techniques; (See Endnote b for a brief elaboration of these terms.)
- Employ trusted architecture, high assurance operating systems and middleware
- Preserve the integrity of the analog signal or data, and protect it from exploitation and/or compromise.

The SDR security framework is intended to serve as a model to describe relation between system elements, components, and functions. It provides a basis for an exploration of the very complex space of wireless download security. By the nature of the security problem space, preventative measures are a response to threats that have been observed in the past. It is impossible to predict and thwart all future threats, and there are always trade-off between the cost of protection, operating convenience, and the probability of

---

[vvv] **Advanced Mobile Phone System** or **AMPS** is the analog mobile phone system standard developed by Bell Labs, and officially introduced in1984. It had a poor security system that allowed people to steal a phone's serial code to use for making illegal calls.

penetration. In areas where the threat structure can be identified, systems may benefit from an approach that considers threats first, and then build the "Security Provisions" constructs to mitigate those threats. Other systems will start with a proposed transmission channel/link structure, build a layer of security provisions on top of this channel, and then test the Security provisions against a threat taxonomy to explore possible weaknesses.

In summary, we have identified some of the key security issues related to the use of Software Defined Radios. Future research is needed to explore a holistic way to accommodate the different dimensions of security and privacy for agile radio nodes into a legacy network security framework. An important open problem in this context relates to the security challenges arising from the need to accommodate third party software to be downloaded onto agile radio nodes. This issue is being researched in the community.

4.6. SCADA Networks

Supervisory Control And Data Acquisition (SCADA) networks are prevalent in many process control systems used in industry; SCADA systems are also used by electric utilities for distribution automation and substation automation. The scope of research in this project did not include a detailed study of security and privacy related to SCADA networks; however, we include a few brief observations here in the interest of completeness.

Process control systems were not built with security in mind, and as a result many existing process control systems remain vulnerable to physical and cyber attacks. Factors include the following:

- Companies use a complex mix of hardware and software systems, often without any basic security (authentication, intrusion detection, encryption, logging).
- The prevalence of old technology and the real-time environment limit security options – shutting down process control systems upon suspicion of an attack is often not possible.

Since potential threats directed at process control systems are quite real, it behooves the operators of such critical infrastructure systems to consider threats like professional hackers and organized cyber-terrorism. A coordinated attack along several threat vectors is a serious long-term threat. A thorough analysis of the real risks (vulnerabilities, threats and probability of occurrence) and consequences (damage restoration time and costs) is therefore quite important. Access to information about control systems and software tools to compromise them is readily available, often on the web.

Historically, security issues have not been a dominant consideration in the design of SCADA networks and systems. Dependability, reliability and redundancy were the main priority for legacy SCADA systems, typically designed to be stand alone, and system availability was the most important metric.

Increasingly however, control systems are often remotely accessible and increasingly connected via the Internet or through wireless networks. In many cases attackers can access critical control systems through non-critical corporate networks. Insider attacks from disgruntled employees with detailed system knowledge are one of the most serious

security challenges. Hence it is important to note that in today's networked context, an attack on the security of systems can easily make the entire system unavailable, and hence this is an issue of serious concern in an environment wherein many of the systems are connected, indirectly or directly, to the internet.

The high cost of patching and constant software security fixes puts a strain on the industry and reduces security. The increasing use of commercial software and networking technologies introduces known vulnerabilities. Inadequate information sharing within the industry and with government may contribute to an apparent dearth of incident and threat information.

Solutions require close collaboration between infrastructure operators, vendors, the research community and the government. Widely accepted security standards, best practices and metrics for the industry are urgently required. Further, it is useful to explore the development of inherently secure SCADA systems and technologies.

4.7. A Network Security Architecture Framework

4.7.1. Security architecture

In this section, we delineate a network security architecture framework for Demand-Response Networks. Deriving from some of the evolving networking standards, it aims to capture the perspectives and security challenges of service providers, enterprises, and consumers and is applicable to a variety of transport media, such as wireless, optical and wire-line networks (www.itu.org). In particular, the architecture addresses security concerns for the management, control, and use of network infrastructure, services and applications. The security architecture provides a top-down, end-to-end perspective of network security and can be applied to network elements, services, and applications in order to detect, predict, and correct security vulnerabilities.

The security architecture divides end-to-end network security-related features into separate architectural components. This allows for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks.

The security architecture addresses the following key questions with regard to the end-to-end security:

- What kind of protection is needed and against what threats?
- What are the distinct types of network equipment and facility groupings that need to be protected?
- What are the distinct types of network activities that need to be protected?

These questions are addressed by three architectural components: security measures (sets of security measures are sometimes referred to as security dimensions), security layers and security planes. The principles described by the security architecture can be applied to a wide variety of networks independently of the network's technology or location in the

protocol stack. We next elaborate on the architectural elements and their functions with respect to the major security threats.

4.7.2. Security layers

In order to provide an end-to-end security solution, the sets of security measures designed to address the potential security threats, i.e., the security dimensions, must be applied to the network elements and systems that comprise the end-to-end network.

The basic network security architecture described here is defined in terms of two major concepts: security layers and security planes. *Security Layers* address requirements that are applicable to the network elements and systems that constitute the end-to-end network. There are three layers that are important in this context, namely the Infrastructure layer, Services layer and Applications layer. The vulnerabilities at each layer are different, and countermeasures must be defined to meet the needs of each layer.

- The *Infrastructure layer* consists of the network transmission facilities as well as individual network elements. Examples of components in conventional networks that belong to the Infrastructure layer are individual routers, switches and servers as well as the communication links between them.

- The *Services layer* addresses security of network services that are offered to customers. These services range from basic connectivity offerings such as leased line services to value added services. In conventional networks, an example of value added service might be VPN, location services, instant messaging, Quality of Service (QoS), etc. In demand response networks, a value added service might be the ability to choose the most cost efficient backhaul network. The services security layer is used to protect the service providers and their customers, both of which are potential targets of security threats. For example, the attackers may attempt to deny the service provider's ability to offer the services, or they may attempt to disrupt service for an individual customer of the service provider (e.g., a utility).

- The *Application layer* addresses requirements of the network-based applications used by the customers. These applications are enabled by network services. Examples include basic file transport (such as FTP) and web browsing applications (HTTP), fundamental applications such as network based voice messaging and email, as well as high-end applications such as customer relationship management, electronic/mobile-commerce, etc. Other examples in the demand response context include the ability to access billing and energy usage on line.

  Network-based applications may be provided by third-party Application Service Providers (ASPs), service providers acting also as ASPs, or by enterprises hosting them in their own (or leased) data centers. At this layer there are four potential targets for security attacks: the application user, the application provider, the middleware provided by third-party integrators (e.g., web-hosting services), and the service provider.

The security architecture addresses the fact that each layer has different security vulnerabilities and offers the flexibility of countering the potential threats in a way most suited for a particular security layer. It should be noted that all three security layers can be applied to each layer of the OSI reference model [OSI].

The security layers identify where security must be addressed in products and solutions by providing a sequential perspective of network security. For example, first security vulnerabilities are addressed for the infrastructure layer, then for the services layer and, finally, security vulnerabilities are addressed for the applications layer.

Figure 6 depicts how the security dimensions are applied to security layers in order to diminish vulnerabilities that exist at each layer and thus mitigate security attacks.

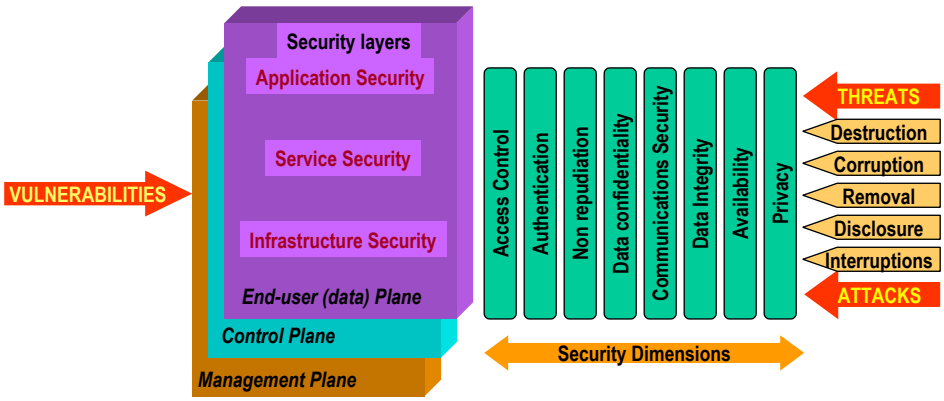

Figure 6. Network Elements and systems in the Network Security Architecture Recommendation. The security dimensions mitigate attacks, and are applied to each plane

4.7.3. Security Planes

The *security planes* address the security of different categories of activities performed in a network. The basic network security architecture consists of three Security Planes to address the three types of protected activities that take place on a network. The Security Planes are: (1) the Management plane, (2) the Control plane, and (3) the End-User plane. These Security Planes address specific security needs associated with network management activities, network control or signaling activities, and end-user activities correspondingly.

The Management plane is concerned with Operations, Administration, Maintenance and Provisioning (OAM&P) activities such as provisioning a user or a network, etc. The Control plane is associated with the signaling aspects for setting up (and modifying) the end-to-end communication through the network irrespective of the medium and technology used in the network. The End-User plane addresses security of access and use of the network by customers. This plane also deals with protecting end-user data flows.

Networks should be designed in such a way that events on one security plane are kept totally isolated from the other security planes. For example, in a regular network, a flood of DNS (Domain Name Service) lookups on the end-user plane, initiated by end-user requests, should not lock out the OAM&P interface in the management plane that would allow an administrator to correct the problem. In a hypothetical demand response scenario, a burst of user level requests for energy related data should not disable the ability to manage and update the basic meter.

Each type of network activity typically has its own specific security needs. The concept of security planes allows the differentiation of the specific security concerns associated with those activities and the ability to address them independently.

Consider, for example, the security of a DR service (e.g., the ability to transmit real time pricing signals), which is addressed by the services security layer. Securing the management of the DR service (e.g., provisioning users) is independent of securing the control of the service (e.g., initiating a service session) and also independent of securing the end-user data being transported by the service (e.g., the energy usage and billing information). A communication service analogy is, for example, a VoIP service, which is addressed by the services security layer. Securing the management of the VoIP service (e.g., provisioning users) has to be independent of securing the control of the service (e.g., protocols such as SIP) and also has to be independent of securing the end-user data being transported by the service (e.g., the user's voice).

4.7.4. Security threats

The network security architecture framework suggests a plan and set of principles that describes a security structure for designing the end-to-end security solution. The architecture identifies security issues that need to be addressed in order to prevent both intentional threats as well as accidental threats. Examples of threats in traditional networks include: destruction of information and/or other resources; corruption or modification of information; theft, removal or loss of information and/or other resources; disclosure of information; and interruption of services.

The intersection of each security layer with each security plane represents a security perspective where security dimensions are applied to counteract the threats. This yields to a matrix in which security dimensions can be mapped to the potential security threats.

4.7.5. Recommendations: Objectives achieved by application of security dimensions to security layers

We suggest that demand response systems have an associated security program that consists of policies and procedures in addition to technology, and that progresses

through three phases over the course of its lifetime: the Definition and Planning phase; the Implementation phase; and the Maintenance phase. The security architecture can be applied to security policies and procedures, as well as technology, across all three phases of a security program.

The security architecture can guide the development of comprehensive security policy definitions, incident response and recovery plans, and technology architectures by taking into account each security dimension at each security layer and plane during the definition and planning phase. The security architecture can also be used as the basis of a security assessment that would examine how the implementation of the security program addresses the security dimensions, layers and planes as policies and procedures are rolled out and technology is deployed. Once a security program has been deployed, it must be maintained in order to keep current in the constantly evolving security environment. The security architecture can assist in the management of security policies and procedures, incident response and recovery plans, and technology architectures by ensuring that modifications to the security program address each security dimension at each security layer and plane.

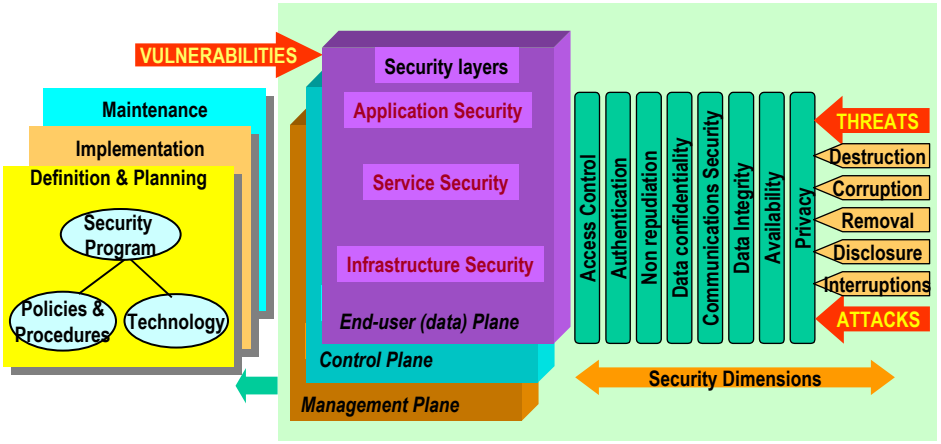

Figure 7 Security Design and Roll out phases

5.0 Conclusions and Recommendations

5.1. Summary of Conclusions and Recommendations

Section 5.2 presents a thorough analysis of the issues likely to be seen in short, medium and long-term deployments of advanced metering and demand response infrastructures, and provides detailed recommendations for each of these timescales and their unique problems. This section provides only a very short summary listing of the recommendations and conclusions discussed in greater depth and detail in section 5.2.

5.1.1. Short and Medium Term Summary Recommendations

5.1.1.1. Sensor and Network Security Recommendations in the Short- and Medium-Term

- ***We recommend that all sensor data should be encrypted***
- Encryption is recommended over manufacturers' proprietary formats for securing data over the entire transmission path, from meter to utility. Only well-studied, time-tested, standard algorithms provide adequate security for sensitive data. Even public key cryptography has been shown to be feasible on resource-constrained 8-bit microprocessors that appear commonplace.
- We recommend that designers adhere to published, well studied, and where possible, provably secure standards: 802.15.4 [IEEE 802.15.4], 802.11i CCMP [IEEE 802.11i] (not WEP, which is broken), AES block cipher [FIPS]. Recently, Elliptic-Curve public-key cryptography has been shown to be feasible on sensor networks [Blass & Zitterbart 2005], [Wander et al 2005]. Standard elliptic curves have been established and should be used.
- Randomness must be employed in encryption. Without an element of randomness, an attacker can likely correlate messages to earlier ones. With random elements incorporated into the protocol, the encrypted messages should never repeat, even if their plaintexts are the same.
- Some form of time stamping should be used to prevent replays of messages sent: an attacker should not be able to store and resend a previous message.
- Messages should not differ in obvious meta information such as length.
- Use authentication for all data. Simply encrypting (providing secrecy) is not enough. We recommend that using a MAC (Message Authentication Code) to enhance the integrity of messages.[j]

5.1.1.2. Advanced Metering and Demand Response Privacy Recommendations in the Short- and Medium-Term

- Rules covering data privacy and business record handling in the utilities should be extended to cover access to such data regardless of whether it resides, temporarily or long-term, within the utility or on third-party premises. Consistent rules should

be developed so there is no question that the requirements for access to data are just as stringent if the data is located off site.

- Guidelines for how much data is necessary and should be stored for the purposes of customer service, and how much information may be shared among utility sub-systems should be set by the appropriate regulatory body, and only that data which is essential for performing mandatory functions should be saved or shared.
- Access to hourly customer usage data should be limited within the utility itself. Utility sub-systems should be required to identify precise data requirements for their research and business needs, justify the granularity of usage data that they request, and should be provided with no more data than necessary to accomplish stated goals. Systems that do not require identifiable data should not have access to it.
- Separate data access mechanisms should be provided for systems that do and do not require identifiable data.
- The data mining of hourly usage data by utilities should be carefully monitored and regulated. As data-mining practices develop, information in which consumers have a reasonable expectation of privacy may be exposed. At this point, utilities should be subject to more stringent rules on release and re-use of personal data.

5.1.2. Longer-Term Summary Recommendations

5.1.2.1. Sensor and Network Security Recommendations in the Longer-Term

- We recommend that spread-spectrum radios be used if feasible, e.g., those used in standards such as 802.11a/b/g (Wireless Ethernet) and 802.15.4 (Zigbee) standards. The use of spread spectrum signaling also makes the system more resistant to narrowband noise. Standards based radios additionally provide a considerable advantage in that they can leverage large volumes of well-tested hardware and software.
- We recommend that a single-hop network be used if possible. By eliminating the need for tree formation, dynamic routing updates, and packet forwarding by potentially malicious or missing nodes, we realize significant increases in reliability of the system.
- If for placement or cost reasons, a single-hop network is not possible, then a network with fixed routing should be set up. Fixed routing makes sense in a DR context, since there is no need for node mobility. Fixed routing defeats touting attacks that disrupt the tree formation phase or dynamic route changes. Routing overhead is reduced to a constant amount of space and there is little to no temporal variability. DR sensor networks also will likely have a constant, and low, bandwidth requirement, making route changes unnecessary.

- Only resilient aggregation functions should be used.[www] If any aggregate functions on the sensor readings are computed, only functions that are resilient to incorrect or malicious readings should be used.
- We recommend that an overall assessment be done to ascertain that the network security architecture addresses relevant threats, using, for example, the principles outlines in Section 4.7. We further recommend considering SCADA security in this context.

5.1.2.2. Advanced Metering and Demand Response Privacy Recommendations in the Longer-Term

- Laws controlling law enforcement access to utility records should be updated to ensure that personal information gained through data-mining, smart meter, sensor, or smart appliance data is not available to law enforcement without a warrant.
- If utilities begin to provide other services over BPL, such as internet service, stricter principles found in telecommunications privacy laws and regulations will likely apply. It may be worthwhile to extend these rules to apply to DR services and other communications sent via BPL, as well.
- Smart appliances for the home should be designed to protect the privacy of customer/owner activities and preferences, and appropriate regulatory bodies should enforce this principle.
- If data from in-home smart appliances, in-home sensors or smart meters is available to be collected, we recommend that state laws or regulations be updated to address the handling of this data.
- When significant computing capability exists inside the home, that processing capability should be developed to enable the customer or his smart equipment to perform necessary energy-related functions – energy monitoring, demand response control, self-education, and billing – at the home site. Keeping this data inside the home is the best way to protect the consumer's privacy interest.

5.2. Analysis and Recommendations

In the following section, we combine the results of our studies of current and future plans for demand response architectures (divided into short, medium and long term implementations) with our studies of applicable legal structures and available and prospective technology solutions. Combining these studies, we identify issues of concern in the privacy and security of demand response architectures, and propose both technological and regulatory solutions; we also suggest opportunities for future research

---

[www] *Resilient functions* are a formal class of functions on n-dimensional vectors, the detailed discussion of which is beyond the scope of this document. Further information can be found in [Zhang and Zheng 1997].

5.2.1. Introduction

The major California investor-owned utilities are currently seeking CPUC approval for residential advanced metering deployment, and for approval of time-variable, demand response tariffs. Full approval of these plans appears to hinge on cost-effectiveness and functionality evaluations.[xxx] The CPUC is expected to decide the matter of full AMI deployment in mid-2006. Whether the utilities may begin employing variable demand response tariffs for residential customers is also expected to be decided in 2006. Advanced metering is necessary to enable time-varying, demand response tariffs, and must precede them. As this report is being written, no advanced metering infrastructure proposals have been approved, and the utilities are in the requests-for-proposals stage in their process of choosing technologies. Thus, our proposals are based on generic short, medium, and long term scenarios for advanced metering and demand response deployments. These scenarios are based on the outcome of our interviews, study of the CPUC proceedings, and other data as summarized in previous sections.

The three major utilities in California are pursuing advanced metering and demand response deployment with differing levels of urgency. Where advanced metering is being pursued aggressively, especially in the short-term scenarios described below, there are issues that may need to be addressed in the immediate future, as these infrastructures are deployed. In the following, we highlight the issues, and suggest both technological and regulatory strategies for dealing with them.

5.2.2. Short Term Deployment

The short-term deployment category encompasses advanced metering activities for which CPUC approval is already being sought, mainly advanced metering deployments that are proposed to be pursued even without the benefits of demand response tariffs. Such deployments are expected to take place in less than 1-2 years. Aggressive timetables for deployment of advanced metering equipment propose to use finer grained advanced metering data (as compared to the single monthly data point on energy usage that is collected today) to make possible a wide range of operational benefits, including improved energy load profiling, improved research, better customer service, and improved rate designs, among many others. In business plans where advanced metering is not being pursued so aggressively, the reasons given include: the utility considers itself to have enough fine-grained data available to allow the kind of load profiling and demand planning that it needs for the present; the kind of higher intelligence meter they desire is not yet available at a reasonable cost; sufficient benefits cannot be achieved to justify the cost of meters until such time as variable demand response tariffs are available, or a combination of these. The short-term scenario we will analyze considers the likely contours and features of an aggressive advanced metering deployment which is pursued without demand response.

[xxx] For example, see the functionality criteria proposed by the CPUC, supra footnote c.

5.2.2.1. Elements and Properties of Short Term Deployment relevant to Security and Privacy

Meters and In-home elements:

To begin widespread installation of advanced meters for residential customers on a short-term timescale, within a year or two, means that meters or upgrades for existing meters must be chosen now. The most likely choices will be meters with limited storage and processing capability, or meters that are retrofitted with processing modules that can store and send to the utility limited amounts of data.[yyy] Since these meters have minimal processing capability for encryption mechanisms, it is not known whether they will encrypt usage data before that data transmitted away from the meter.[zzz]

Data collected and sent by the meter is expected to include at the minimum a meter identification number and usage data for the time period (kWh).[aaaa] If possible, some kind of timestamp or time-synchronization signal is likely to be included. Additional data that is desired and that a meter might collect, although it may not be possible or cost-effective to do so immediately, include measurements of voltage, phase and frequency (power quality) measured at the meter.

Data is sent hourly by the meter (potentially via a wireless communication system) to some sort of backhaul network that routes the data to the utility. Intermediate nodes in this backhaul network may have the capability of scheduling meter data transmissions, re-querying a meter for a new read if a data reading is lost or miscollected, and querying meters on an accelerated schedule (every few minutes) to check that the meter is operational. Despite this minor processing capability at intermediate nodes, the main processing of the data is expected to take place within the utility.

Data transmission:

In the short term, it is expected that advanced meter data will be transmitted to the utility using a combination of public and private wired/wireless communications systems, according to ease of use and cost-benefit analysis. Many kinds of communications media and mechanisms may be used, including wireless, wired Ethernet, powerline, cable, optical fiber, and other methods. Segments of this transmission path from the meter to the utility

---

[yyy] Our description of this issue is based on information gathered in our interviews. Meter choice for widespread residential deployment depends heavily on meter cost. The CEC desires that meters for residential deployment should cost less that $50 [DRETD-Meter RON]. Data from interviews suggests likely meters may store 6-7 days of data as backup, but otherwise will transmit hourly data, 4 times per day or more. Intermediate nodes may collect data from about 100-10,000 meters. Some rearrangement or scheduling of data may occur at the substation level, but main data processing expected to take place at utility.

[zzz] Meters typically format data according to manufacturer's proprietary formats. It has been suggested, incorrectly, that encryption may not be necessary in such a case, because the proprietary format can prevent decoding of the data.

[aaaa] Some meters may follow data collection and storage standards from the American National Standards Institute (ANSI), but the formatting and arrangement of data are expected to be proprietary, unique to each manufacturer.

may be outsourced, to single or multiple third-party vendors. It has been suggested that data encryption may not be used along this entire data path, but only along segments where the benefit exceeds the cost of doing so.

Although intermediate nodes may contain enough processing capability to schedule data collection or perform other functions described above, the main purpose of the data transmission path will be to route data to the utility for aggregation and processing.

Data Storage and Processing:

As described above, in the short term, it is expected that hourly usage data from advanced meters will be collected, processed, and stored centrally on servers at the utility, or perhaps at a third party information services partner. Once available for processing, it is expected that the compiled hourly usage data may be routed to other utility subsystems that may make use of it. In the short term, it is not expected that the raw hourly meter data will be routed to utility sub-systems, instead, data is likely to need some pre-processing so it may be used by existing (legacy) software systems. High probability uses of the data include aggregation of the data for billing, real time access to data by customer service for customer advising or resolution of customer disputes, or provision of real-time or compiled feedback to customers for education purposes. It is expected that this data mining will be performed on the hourly usage data to discover what other value it may provide to the utility. Currently, 7 years of customer usage data is stored, as backup and to inform customer billing disputes. This practice is expected to continue.

5.2.2.2. Privacy and Security Issues in Short Term Deployment

Meters and In-home elements:

The key meter issues in the short-term deployment include the security of the device, security of the data, and privacy issues surrounding the data collected. Security of the device and data can only be appropriately gauged relative to threats they are subjected to. In the current environment, it appears that energy theft and meter tampering are minor issues, but it may be that these become more prevalent problems if tampering becomes a lower-risk, remote electronic process as compared to a matter of physical meter alteration.

Relevant security questions we ask are whether the meter itself is sufficiently secure such that the backup data stored in it cannot be obtained by hacking. Regarding the security of the data, the question must be asked whether the manufacturer's proprietary data format is secure enough to protect the data through its entire transmission path. Privacy concerns encompass questions about what kinds of data are collected, transmitted, and stored, and whether these make more personal information about a customer available to an interceptor than was available without advanced metering.

Data Transmission:

Issues in data transmission can be divided into two categories: security of the data and security of the transmission "pipe" that the data travels through. Security of the pipe encompasses issues related to every element of the transmission pipe: is transmission from

the meter secure, is transmission to and from every node secure, is data storage at every node secure, is every node physically secure?

It may become a particularly complex problem to identify locations where data is vulnerable if data is passed among multiple third party vendors along the transmission path. Transferring data among parties may also make legal data handling standards less clear, as privacy and data handling rules may vary among utilities and third parties. Many of these pipeline security issues are less critical if the data itself is properly secured.

Data security encompasses issues of what data is sent, and in how secure a format the data is sent. It is important whether the data leaving the meter is raw data or processed in some way, and how easily the data packets may be correlated to the meters or customers.

Long-term data storage at intermediate transmission nodes adds another level of vulnerability, as the more data that is stored there, the more attractive it may become to hack into that data for purposes of energy theft, privacy intrusion, or surveillance.

Data Storage and Processing:

Although it is clear that hourly meter data will likely be collected, transmitted and stored by the utility, and that most of the data processing will occur centrally, either at the utility or third party site where the data is stored, not much else is clear about how the data will be handled or used, and this makes it difficult to assess the magnitude of security and privacy issues that will result.

The most serious privacy issues arise when a new and not generally available technology is used to gather information that would not otherwise be available without entering the home. In the case of hourly energy data, it is not clear how much personal information might be gleaned from the data mining of hourly energy data, and so it is not clear how much of a privacy intrusion may exist. Nor is it clear what the collected data will be used for, what other customer data it may be combined with, or to whom that data may be made available. Certainly, both billing and customer service areas wish to have access to both the hourly data and customer personal information, but it is not known what other utility sub-systems may be given access or why.

Sale or disclosure of the stored data to third parties is another issue, as an increased amount of information about customer habits may make the data more attractive for marketing partners or law enforcement. One may expect parties beyond the utilities to think about and propose possible uses for finer-grained utility information. Perhaps a business can find value in the knowledge that some customers use a lot of energy mainly early in the morning, or mainly late at night, or perhaps law enforcement can correlate a certain usage profile with a certain illegal behavior. When the data is stored at and within a utility, data disclosure and release rules are at least clear, but if the data is stored by a third party information services vendor, the rules are not so transparent. As a result, there is some concern that the records might be more vulnerable to disclosure, either because of different legal treatment for third parties, or because third parties might be less likely to take appropriate security measures to protect the data.

Our interviews suggest that hourly energy usage data, even without data mining, will make energy usage records much more interesting to law enforcement. Hourly data may expand the usefulness of energy records far beyond home marijuana cases.

5.2.2.3. Security and Privacy Recommendations for Short Term Deployment

Meters and In-home Elements:

It is unlikely that meters deployed at this stage would possess enough processing power to compute the bill; thereby keeping detailed information on customer usage within the home. Given that technology will be unable to protect privacy, we must look to law to establish rules limiting the collection, storage, and use of information about energy consumption.[bbbb]

Although it is important that steps be taken to protect meters against break-in, it is assumed that physical tamper-resistance techniques will be employed to prevent customers from modifying or otherwise compromising their meters. From a privacy perspective, it is not the in-home elements that present the most serious risks, as adversaries are unlikely to perform large-scale or remote collection of data directly from the physical meters. Rather, it is the interconnection network (the "grid") linking the meters and the data warehouses that are likely to be targets for wholesale data theft, leading to substantial security and privacy attacks

In the short-term scenario described here, the most serious security problem is the assumption that sending data in a manufacturer's proprietary format automatically provides for security of that data. In fact, quite the opposite is likely to be the case: the concept of "security through obscurity"—the idea that if it is hard to interpret the data, then it is secure—has been thoroughly debunked. Not only must there be explicit provisions for data encryption and integrity in the transmission protocol (as well as any other desired properties, such as privacy protection), the techniques employed should be well-studied, time-tested algorithms in order to have any faith in their security.

Once proprietary formats become compromised, there is little to prevent the meters from being hacked into or compromised, enabling new mechanisms for energy theft, privacy compromise, or surveillance.

Concerns have been expressed that encryption may make meters too expensive for widespread deployment. This need not be the case as long as minimal processing power is available in the meter. The specifics of cost analysis obviously depend on the particular algorithms being employed and the hardware-software mix in the implementation, but

---

[bbbb] It has been suggested (by Gaymond Yee) that even if the meter is capable of locally computing the customer's bill, there might be potential operational problems because of the need for the utility to make audits of every meter on a routine basis to ensure that the bill is computed accurately and if not, to make adjust for prior potentially erroneous bad bill calculations.

even public key cryptography has been shown to be feasible on resource-constrained 8-bit microprocessors that appear commonplace.[cccc]

Data transmission:

Network security architects generally assume that a network is insecure as a starting point in assessing a network security plan. This is a reasonable assumption to make about the complex, multi-segment, multi-vendor transmission pipe likely in a short-term advanced metering deployment. In well-designed systems, the security of this transmission path is less critical because the data is secured properly. This is the well-known "end-to-end" security concept. If the data is properly encrypted, there will be no ability to manipulate data anywhere along its transmission path. This should work fine in the short term model where no data manipulation is expected to take place along the data path. The ability of intermediate nodes to query meters and replace missing data sets would be preserved. If intermediate nodes need to have the ability to check the timestamps of the data coming from the meters, it is possible to encrypt the usage data alone, and allow the meter identifier and timestamp to be readable by intermediate nodes.

Data Storage and Processing:

Given that the legal protections for business records and personally identifiable customer information are varying and often ill-defined, the release of detailed energy usage data from the home and the subsequent transformation of that data into business records, can potentially permit substantially increased access to, distribution, and sale of private information compared to current energy infrastructures. Currently the privacy protections for customer information are stronger for data kept by banks and telecommunications providers than for energy utilities, although they are higher for energy utilities than most other businesses. When a utility outsources information services to a third party, it appears the industry practice is to impose the utility's data handling and security requirements on the third party through contract, audit, and by requesting and recommending a set of best business practices for the third party to use. This should limit the third party's ability to disclose or sell the data to another business. However, it is not clear whether this would affect the ability of law enforcement to access the data. It is recommended that, at the very least, the rules that cover data privacy and business record handling in the utilities be extended to cover access to such data regardless of whether it resides, temporarily or long-term, within the utility or on a third-party network. It is important that consistent rules should be developed so there is no question that the requirements for access to an individual's energy consumption data is just as stringent if the data is located off site or on another party's network.

We also recommend limiting access to customer data within the utility itself. Certainly sub-systems such as billing and customer service will need access to both usage data and personally identifiable customer data, but systems that do not require identifiable data should not have access to it. Utility sub-systems that request usage data should be required to identify precise requirements for their research and business needs, should be required to justify the granularity of usage data that they request, and should be provided

---

[cccc] See section 4.2.2.4, "Use of cryptography."

with no more data than necessary to accomplish their stated goals. As the utilities replace their legacy systems and build new software systems to collect and process the advanced metering data, protections against unwarranted release of personally identifiable information to sub-systems that don't really need it should be built in to the system. These same protections should apply to the use of data by third parties.

We further recommend that separate data channels for systems that do and do not require identifiable data be built-in to the system. This facilitates partitioning the data channels that may or may not be available to third parties, including law enforcement, depending upon the privacy guidelines that might prevail.

We recommend that the data mining of hourly usage data by utilities be carefully monitored and regulated. It is not known how much information on personal habits or in-home activity may be gained at present from the data mining of hourly data, but as data-mining practices develop, information for which consumers have a reasonable expectation of privacy may begin to be exposed. At this point, utilities should be subject to more stringent rules on release and re-use of personal data, like those that are applied to telephone corporations and banks.

We recommend that laws controlling law enforcement access to utility records be updated to ensure that personal information gained through data-mining should not be available to law enforcement without a warrant. One way this might be done is to spell out, in legislation or regulation, which data or information the consumer may reasonably expect a utility to keep private. Since the usage of energy records is likely to become more common due to the usefulness of hourly data in checking alibis, establishing timing of a case, and other ways, the current rule that utilities may release customer data without a warrant needs to be reconsidered.

5.2.3. Medium Term Deployment

What we call the medium term scenario is what might be envisioned to occur when changes in state and CPUC policy make time-variable demand response tariffs available to all residential customers. Pressure for widespread deployment of advanced metering and demand response tariffs is continually increasing, and it is expected that widespread deployment will become cost-effective, and pursued across the board at some point, within two to five years. This is a vision shared by the federal Energy Policy Act of 2005, which requires that "each electric utility" must make available time-variable energy rates and meters capable of supporting those rates, and supply those to customers that request them, within 18 months of August 8, 2005.[dddd] Once demand response tariffs are approved and are desired by or required for all residential customers, advanced meters will become mandatory, and widespread deployment inevitable. Once this infrastructure deployment reaches a certain level of maturity, we expect the following changes to occur.

[dddd] ENERGY POLICY ACT OF 2005, PL 109-58, August 8, 2005, 119 Stat 594, section 1252, which amends section 111(d) of the Public Utility Regulatory Policies Act of 1978 (16 U.S.C. 2621(d)).

5.2.3.1. Elements and Properties of Medium Term Deployment relevant to Security and Privacy

Meters and In-home elements:

There is a lot of activity in advanced meter development today, and the technology can be expected to advance rapidly. Open standards initiatives such as OpenAMI may be expected to have an impact on the kind of meters available for installation in widespread deployments two or more years down the road. Meters installed or upgraded at that time may be expected to contain greater storage and processing capability, and more sophisticated security and encryption measures.

To take best advantage of time-varying demand response tariffs, it is expected that some kind of two-way communication between the utility and customer will be sought. New meters installed at this time may have some ability to receive dynamic rate change information from a utility and either alert the consumer or somehow automatically respond to demand response conditions, perhaps by sending a signal to a smart thermostat and other smart appliances inside the home. As meter costs and the labor costs to replace them may be prohibitively high, it may mean that for customers whose meters were already upgraded to allow hourly data collection, the same ability to receive rate information and respond automatically may instead reside in a smart thermostat enabled for two-way communication.

Data Transmission:

Options for the transmission of smart meter or smart thermostat data, as described in the short-term scenario, are expected to remain numerous, and the technology can be expected to continue advancing rapidly. The choices that will be made in the medium term scenario will be based on what is most cost-effective at that time, and so are difficult to predict with any accuracy now. Therefore, instead of predicting a likely mode of transmission for the medium term, we will comment here on some trends and technologies that were mentioned in our interviews as desired in the medium term for data transmission.

Our interviewees mentioned that utilities tend to prefer to own their hardware and infrastructure, so there may be movement toward transmission systems that utilities might have more control over compared to public networks. (We remark that this desire seems counter the general technological trend towards disaggregation and horizontalization, which would suggest that items such as communication infrastructure and services would tend to be more efficiently provided by parties specializing in those domains. Also, outside of the utility industry, the current consensus appears to be that there is inadequate momentum to propel Broadband over Powerline into leadership as a preferred method of communication, given substantial research and industry backing of several alternative mechanisms.) Possible technologies that might enable this include the broadband over powerline protocol, developing the meters themselves as a relay network, implementing a private wireless network owned by the utility alone, or encouraging an open architecture, user group owned private communication infrastructure that might be used both by utilities and other service providers in a demand response market.

Data Storage and Processing:

As advanced metering, time-variable tariffs, and demand response become widespread, legacy data processing systems (where add-ons and fixes were used to allow use of advanced metering data) will be upgraded to newer software to allow better processing and increased integration of demand response data into utility systems and sub-systems. It is expected that advanced metering and demand response data will be desired for automating systems and improving planning. It is expected that there will be significant research performed as to how hourly data and access to it can optimize and automate systems, improve load planning, and otherwise seek out operational savings.

With the addition of information on customer responsiveness to price signals and other information on customer behavior that may be gleaned once time-variable tariffs and demand response monitoring become widespread, there may be additional pressure to mine the collected customer data to develop new energy products or to target customers for new energy plans. This additional information may make the data even more valuable and useful to the utility and pressure for its disclosure to external businesses and law enforcement may again increase. The storage of 7 years worth of this data (according to the current industry standard) means a great deal of information of past customer practices will available for data mining.

5.2.3.2. Issues in Medium Term Deployment

Meters and In-home Elements:

By the time that smart meters and smart thermostats are widely deployed, they will contain more processing and data storage capability than is available today, and data collection practices may have changed. With the ability to do more computation in the meter, it may be possible to explore using the meter to compute the customer's bill, or perform some types of data aggregation or anonymization on the data before it leaves the home. Usage of some techniques might result in coarser-grained data leaving the home, and a potential for less exposure of customer behaviors and information. An increase in data storage capability might also lead to more data storage in the meter, which in turn, might make those meters more attractive targets to hackers or energy thieves, especially if the meter contains billing computations and other data.

Another issue in this context that arises is that a move to standardized, open architecture meters with non-proprietary data formats, might make energy theft or meter tampering more attractive. Our interviews with law enforcement suggest that such tampering is more likely to take place on the transmission network (where data from many meters may be compromised at once) than by tampering with individual meters.

Data Transmission:

As observed earlier, the momentum in the communication industry suggests that broadband over powerline (BPL) technology is not a frontrunner for widespread adoption outside of the utility industry at the time of this writing. However, our interviews indicate that the utility industry is still keen to consider BPL, a fact that is obviously motivated by the advantage the utilities have of owning their power lines. If there is indeed a move to broadband over powerline, a number of issues arise. It has earlier been suggested that BPL

may not have enough bandwidth to allow sophisticated encryption, although this is not the case with more recent advanced modulation schemes. Nevertheless, if encryption is not used, a party gaining control of a substation communication module might be able to read any messages being transmitted by any ports below that substation. Data security in such a system is a critical issue if BPL is to be used. Most forms of BPL give rise to significant radio interference, and it is a concern whether a BPL transmission system will make interception or surveillance of energy usage data easier to accomplish.

On the other hand, there may be fewer problems due to lack of clarity of data privacy rules if utilities move to a utility proprietary transmission system.

Data Storage and Processing:

Once advanced metering systems are deployed or demand response becomes a mandatory program, large amounts of data on customer usage behaviors will be available from customers, and our interviews suggest that utilities are eager to mine this data to develop better rate designs, customized energy products that can be marketed to different customer segments, and other uses that have not yet been conceived of. It is not known which utility sub-systems or research projects will have access to advanced metering or demand response data, for what purposes and at what level of granularity.

It is not known how much information on in-home activity or personal customer behaviors may be exposed to a utility through the data mining of advanced metering or demand response data, or what information might be made available to hackers or eavesdroppers listening in on in-home network activity. It is in the consumer's interest to keep as little of the fine-grained data from leaving the home.

Utilities currently store 7 years worth of customer data to allow customers to dispute their bills going back that far. When raw, unaggregated demand response data becomes available, storing 7 years worth of this data will require a large increase in utilities' data storage capacity. Utilities are likely to look for ways to create value from this stored data storage, mining this data may make its storage more cost-effective.

5.2.3.3. Recommendations in Medium Term Deployment

Meters and In-home Elements:

Use of cryptography[k]

Cryptography is not simply a "feature" of a secure network, but must be used judiciously to achieve particular goals. Many cryptographic protocols have significant computation or communication requirements, so existing techniques must be modified; the good news is that more and more traditional approaches are being made feasible on even sensor-class nodes.

It is all too easy to make mistakes by implementing cryptography in an ad hoc manner. Using proprietary ciphers, using block ciphers in the wrong modes and implementing the wrong sequence of encryption and authentication are very common errors.

We recommend that designers adhere to published, well studied, and where possible, provably secure standards. Common radio standards including encryption are 802.15.4 [IEEE 802.15.4] and 802.11i CCMP [IEEE 802.11i] (not WEP, which is broken). The AES block cipher [FIPS] has undergone rigorous peer review and is designed to be efficient on 8-bit platforms. Recently, Elliptic-Curve public-key cryptography has been shown to be feasible on sensor networks [Blass & Zitterbart 2005], [Wander et al 2005]. Standard elliptic curves have been established and should be used.

Use encryption.

We recommend that all sensor data should be encrypted. First, randomness must be employed in encryption. Without an element of randomness, an attacker can likely correlate messages to earlier ones. With random elements incorporated into the protocol, the encrypted messages should never repeat, even if their plaintexts are the same.

Second, some form of time stamping should be used to prevent replays: an attacker should not be able to store and resend a previous message.

Lastly, messages should not differ in obvious meta information such as length.

Use authentication for all data.

Simply encrypting (providing secrecy) is not enough. We recommend using a MAC (Message Authentication Code) enhance the integrity of messages.

Data Transmission:

Techniques for protecting messages through robust encryption, as described for sensors, above, and more generally, as applicable to broadband communication and security standards, should be mandated. Stricter privacy laws and regulations should be applied or extended to apply to these services and other communications.

Data Storage and Processing:

Given the low cost of data storage today, the cost to store hourly advanced metering data, even for residential customers, will not be prohibitive. On the other hand, there may be no reason beyond the prospects for data mining to justify the storage of seven years' worth of this fine-grained information on customer usage. Guidelines for how much data is necessary and should be stored for the purposes of customer service and other functions should be set by the appropriate regulatory body, and only that data which is essential for performing mandatory functions should be saved. It should be investigated what combination of ordinary or extraordinary usage profiles and average usage numbers need to be stored for customer billing purposes. Such regulations would reduce the temptation to share and mine this data.

It is recommended that protocols be developed to govern which energy sub-systems receive access to advanced metering and demand response data, and only data which is required for well-identified, well-justified, and necessary functions should be approved and allowed.

5.2.4. Long Term Deployment

The long-term scenario we discuss below would be triggered by market forces, as some sort or combination of networked-house concepts become common in homes, as mote enhanced appliances and lighting systems become available, and as intercommunicating sensors, smart appliances, or smart thermostats achieve some level of market saturation and become common in homes. Whereas smart appliances appear to be taking off in some foreign markets where energy prices are exceptionally high, the timeline for their widespread adoption in the United States is speculative at this time.

5.2.4.1. Elements and Properties of Long Term Deployment relevant to Security and Privacy

Meter and In-home elements

As we progress into a mature demand response deployment, few meter changes are expected, since meters have very long lifetime, and the labor cost of swapping them out is prohibitive. Meters are expected to be chosen and fully deployed in the medium term scenario, and subsequent changes in home energy control will likely occur through upgrades to other appliances and smart thermostats. Over time, many home appliances are expected to gain processing capability and the ability to talk to each other and to a smart thermostat or other device. A smart thermostat, home computer, or other control device may be enabled to send and receive 2-way communications including price signals from the utility, and automatically respond to those signals by changing air conditioning settings, changing appliances into power setting modes, or turning them off. In-home sensor networks, including temperature, occupancy, and other sensors, may also be controlled through a smart thermostat, and provide additional data for the controlling algorithms.

Data transmission

The long-term makeup of demand response data transmission systems is the difficult to predict, as this is the area of technology where the largest technological advances are expected. Technologies that are on the distant horizon today are likely to become available in the long term, and the choices made will depend on what is cost-effective at that time. Possibilities include agile communication nodes and systems that enable flexibility and adaptability with respect to the communication channel and technique (based on various considerations, including variable communications cost, availability, and redundancy).

Data storage and processing

In the long term, we expect that utilities will continue to upgrade internal systems and enterprise software so as to integrate and take best advantage of operational savings and research advances possible with advanced metering and demand response data. This is similar to the case in the medium term scenario, except that increasingly sophisticated data mining techniques may be used, more may be learned from the data, and the pressure to use this data for business advantage are likely to increase. Additionally, open architecture communication protocols may be implemented that are aimed at streamlining business processes, such as DRBizNet.

Over time, data from in-home smart appliances, in-home sensors, smart meter or controller may become available to the utility, and added to the volume of data being data mined, and make available to the utility incredibly personal information on customer behavior and habits. This kind of information on customer private activity within the home has never been available to the utility, and would constitute a major erosion of customer privacy.

5.2.4.2. Issues in Long Term Deployment

Meters and In-home Elements:

In the long-term scenario, there will be significant computing capability inside the home, in a smart thermostat, connected computer, or other controllers, even if not in the electric meter. There will be opportunity for much calculation and analysis of energy usage inside the home, much opportunity for consumer self-education and monitoring of their energy needs, and it will be much less necessary for such data to be collected by the utility, analyzed, and fed back to the consumer. In principle, it should be easy for enough information to be collected at the home that all necessary computation regarding customer's energy usage and billing could be computed inside the home. As observed earlier, however, such an in-home computation of utility bills may be fraught with some operational issues relating to audit requirements for utilities.

If data from and communication to every appliance, or similar data from sensors, is being wirelessly transmitted and collected, that sensor/smart appliance data may become of increased interest to hackers for purposes of energy theft, energy diversion, impersonation, causing harm (ex-boyfriend, messy divorce) or surveillance (neighbor, thief, stalker). The data may become of increased interest to law enforcement (for example, occupancy sensor information might be sought by immigration services, or as surveillance).

Smart appliances that may be connected to the internet may open up new access paths for the theft of computing services as well.

Data transmission:

The introduction of sensor networks into the home and transmission of data among these raises the likelihood of increasing frequency of attacks on those elements, as described in section 4.2.1.

An open architecture, distributed communications network like DRBizNet may open up new issues in privacy and security. Of key importance to privacy of consumer data and records is understanding where data is stored, even for short periods of time. If an open architecture is meant to, and succeeds in bringing new providers of energy-related services into the market, and allows a more complex network of relationships among energy services and energy-related services, it may be very difficult to keep track of customer data and ensure that it is available only to those who actually require it, and to ensure that those parties store and protect data properly.

Data Storage and Processing:

If data from in-home smart appliances, in-home sensors or smart meters were available to utilities, this would provide an entirely new kind of information that utilities have never had. With this volume and variety of data on customer activities, even simple data mining could provide a wealth of data on customer preferences and likely commercial behavior. It is entirely foreseeable that many would be tempted to share and sell this information, or to use it for extremely targeted marketing.

We have discussed how the availability of hourly usage data alone, and then hourly usage data plus data mining may make energy records of greater interest to law enforcement. The collection and storage of any amount of sensor data at the utility would likely increase law enforcement interest by another order of magnitude. It is easy to imagine how sensor data, occupancy data especially, might be invaluable in establishing the parameters of a crime that took place in a person's home. However, sensor data on in-home activity may cross the line drawn in Kyllo, and be considered exposure of in-home activity by a not-generally available technological device. If so, use of sensor data by law enforcement would not be allowed under the 4th Amendment of the U.S. Constitution, even if California law said the utilities might volunteer it. On the other hand, if the data is regularly compiled as a part of a customer's energy records, the courts could conclude that by letting this data leave the home, customers forfeit the right to claim a privacy interest. It is therefore clearly in the customer's interest to keep this information, and any other information that may give clues to in-home activities, from leaving the home.

5.2.4.3. Recommendations for Long Term Deployment

Meters and In-home Elements:

Recommendations for Sensor Network Security in Demand Response Networks

In this section, we make recommendations about how sensor networks should be deployed for a demand response application. We consider the threats outlined in section 4.2.1 along with the requirements of DR in generating these guidelines. Ultimately we need a network that can implement all the DR functionality while avoiding known threats. Our goal is not to prescribe or design a very general purpose sensor network; indeed such a network would likely be less efficient and less secure.

Physical Form Factor

Our recommendation here depends strongly on the threat model and the desired data-processing capabilities. In a home setting or other environment where such attacks are unlikely, ordinary wireless nodes are sufficient. Many commercial wireless sensors promise battery life on the order of years, which seems reasonable for a small deployment where manual battery replacement every few years is acceptable. If power-draining attacks or jamming attacks are a plausible threat, then we recommend that nodes be plugged into a wall socket. This has several benefits. First, it avoids power-draining attacks. Second, it makes practical the use of more reliable but less power-efficient network protocols. Third, it eliminates the considerable maintenance challenge of replacing sensor nodes' batteries. We feel this usage model may be appropriate for large industrial DR, since the nodes will be deployed where outlets are readily available, but the stakes (and thus attackers' incentives) as well as maintenance costs are higher. However, there are some valid arguments that

counter the use of power outlets, particularly in contexts where such wiring is expensive, or in contexts such as public safety scenarios where power may be unavailable.

Network hardware.

We recommend that spread-spectrum radios be used if feasible. Good examples of these are the 802.11b (Wireless Ethernet) and 802.15.4 (Zigbee) standards. The former provides a considerable advantage in that it can leverage volumes of well-tested hardware and software. In fact, existing 802.11 base stations may be reused for gathering and relaying the sensor data at considerable cost savings; 802.11 chips' cost has also plummeted due to the ubiquity of the standard. Its use of spread spectrum signaling also makes it resistant to narrowband noise. The downside of 802.11 is that it contains more functionality than is needed in the DR context, which may result in higher cost and power usage. By contrast, 802.15.4 radios may be cheaper and smaller, but have a shorter range and less robustness. Both radios provide link-layer encryption in hardware, lowering implementation complexity. Proprietary radios that have spread-spectrum ability, such as those marketed by Johnson Controls [Johnson Controls] and Trs [Trs Systems] (among others) may support the required functionality, but may sacrifice interoperability.

Routing.

We recommend that a single-hop network be used if possible. A large number of attacks, especially routing attacks, on sensor networks occur on ad-hoc, multihop networks. By eliminating the need for tree formation, dynamic routing updates, and packet forwarding by potentially malicious or missing nodes, we realize significant increases in reliability of the system.

If for placement or cost reasons, a single-hop network is not possible, then a network with fixed routing should be set up. A fixed routing topology may be formed using any route formation algorithm whereby the network is set up, then locked in. Fixed routing makes sense in a DR context, since there is no need for node mobility. Fixed routing defeats touting attacks that disrupt the tree formation phase or dynamic route changes. Routing overhead is reduced to a constant amount of space and there is little to no temporal variability. DR sensor networks also will likely have a constant, and low, bandwidth requirement, making route changes unnecessary.

Application-layer protocols.

When significant computing capability exists inside the home, that processing capability should be developed to enable the customer or his smart equipment to perform all the necessary energy-related functions – energy monitoring, demand response control, self-education, and billing – at the home site. While energy utilities certainly need and should be able to collect the information they need for load control and planning – total usage at a customer site, a computed bill, voltages, phase, frequency, outage monitoring data – to maximize security, utilities should minimize the collection of fine-grained data from sensors, smart meters or any other smart appliances that may expose activities or personal choices made by the consumer inside his home.

Only resilient aggregation functions should be used. If any aggregate functions on the sensor readings are computed, only functions that are resilient to incorrect or malicious readings should be used. For example *max, min,* and *mean* can all be shown to be not

resilient owing to their mathematical properties. *Median*, by contrast, can be made resilient to a certain number of erroneous readings, as can the *count* function. A trimmed average function, which discards the highest and lowest 5% (for example), can provide a measure of resiliency. That is, the error of the computed aggregate can be bounded as a function of the number and capability of the adversary (of course, if the adversary can supply more than 5% of the samples in this case, then he has arbitrary influence). Note that the price we pay for this is that the result has more error in it in the non-adversarial case since we are discarding data.

Smart Appliances should be designed to protect privacy.

Smart appliances for the home should be designed to protect the privacy of customer/owner activities and preferences, and appropriate regulations should enforce this principle. If technology is developed that allows a utility to poll or communicate with smart appliances (or any appliance or plugged-in item, for that matter), those appliances must be designed so that customers have the option to release no information on the appliance or its use to the utility. Such appliances, as purchased, should be set in a default state where they will not broadcasting messages, and will be anonymous black boxes when polled by unauthorized or unauthenticated entities.

Smart appliances that can be internet connected or networked to a computer need to contain state of the art security measures, such as encryption and password protection, and those measures should be enabled in the product as purchased. Consumers may not understand the difference between a smart appliance and old-fashioned one, may not know how to engage security measures effectively, whereas the equipment manufacturer might often be able to leverage greater expertise in this context. This is the lesson to be learned from the fact that the vast majority of home wireless systems are unsecured. Security against wardriving[l], unauthorized access, spying, should in principle be present in every internet-connected appliance, sensor, smart element; however, because of the plethora of such appliances, and various cost and market considerations, it seems unlikely that any regulations in the near term can enforce such a requirement at a pragmatic level.

Data Transmission:

Security recommendations made for sensor networks in medium term deployment (section 5.2.3.3) will apply in the long term equally well.

By this point in time, if the utilities have gotten to the point that they do own and/or control the telecommunications infrastructure that they use, state law or regulation should require, as it is currently required of telecommunications providers, that the utility be held responsible by the appropriate regulatory body for the privacy of messages sent through their systems.[eeee] This particularly applies, as was discussed in the medium term scenario, for broadband over powerline mechanisms used by a utility that owns the communication (powerline) infrastructure. Additionally, the security features supported by a BPL channel needs to be as good as other available methods, and robust encryption must be a pre-requisite of its use.

[eeee] *See* Cal. Pub. Util. Code § 7906.

Data Storage and Processing:

Most data storage and processing and solutions will carry-over from the medium-term solution, except that if data from in-home smart appliances, in-home sensors or smart meters is available to be collected, we recommend that state laws or regulations be updated to address the handling of this data. A good starting point would be to emulate the stricter telecommunications regulations that place disclosure restrictions on personal calling patterns, service program choices, and individual or aggregated demographic information.[ffff] Even better would be a privacy law or regulation that only permitted collection of multiple-household aggregated data or anonymized data, from which good research, planning, and marketing can be done without jeopardizing the privacy of individual customers. At the very least, some appropriate legal and technical safeguards need to be in place to ensure that the ways in which utilities and third parties use the data reflect and uphold generally accepted privacy expectations.

As hourly energy usage data, smart meter data, sensor data, and smart appliance data, if collected and data-mined, may reveal much about private in-home activity, such data should not be released without a warrant. We recommend that legal rules should be updated to reflect this.

5.3. Suggestions for Future Work

Our work in this project suggests a number of avenues for future work. We categorize these below into legal and regulatory aspects, and technological aspects.

5.3.1. Legal and regulatory aspects

- One possible extension of this project is to draft proposed legislation covering new data privacy and business record handling rules for the energy utilities and their evolving business practices. Ideally flexible rules might cover current outsourcing practices, the role of third parties in handling data, future practices such as data-mining, and the customer's expectation of privacy in data from smart thermostats, smart appliances and in-home sensors.
- Data handling and usage guidelines or regulations should be drafted to cover utility internal access and usage of data.

5.3.2. Technology aspects

- Continuing research into cost-effective encryption methods for elements with limited processing power should be aggressively pursued. Encryption techniques for low-cost meters, sensor nodes, and BPL all require attention.
- Analysis of security and privacy related issues in the context of emerging standards, such as IEEE 802.15.4 and Zigbee.

[ffff] Cal. Pub. Util. Code § 2891.

- Study of security issues that relate to segments of the DR network not fully addressed in this research (due to the limited nature of its scope), e.g., SCADA networks.
- Development of security technologies for agile radio nodes, and in particular those supporting third party hardware and software components, is very valuable.
- The design of secure, scalable meters, that support processing capability to enable the customer or his smart equipment to perform necessary energy-related functions – energy monitoring, demand response control, self-education, and billing – at the home site.
- Guidelines might also be developed to deal with the storage of advanced metering and demand response data, and how that data might best be aggregated so that only that data which is essential for performing mandatory functions is saved.
- Technologies that assist in supporting security and privacy, bearing in mind the evolving trends in advanced metering infrastructure, organizational structures, policy considerations, and associated business processes.

5.4. Benefits to California

One overall goal of this project was to increase the awareness of security and privacy issues in advanced metering and demand response systems among the technical designers who build the elements and infrastructures, and among the regulators and legislators who oversee or drive that process. This work has been presented at a number of forums, at the Demand Response Enabling Technologies Development Workshop in Berkeley on June 2, 2005, before representatives from the state senate and house budget committees at a workshop held at the California Lighting Technology Center, in Davis on September 19, 2005; and in November 10 to the U.C. Berkeley Team for Research in Ubiquitous Secure Technology (TRUST), a multi-institution center funded by the National Science Foundation to protect the nation's computer infrastructure from cyber attacks. We look forward to presenting this research to other interested groups and parties.

We hope that this report will be useful to the energy industry, for helping identify areas where security and privacy issues may be important for both commercial or consumer protection. We hope that our recommendations may provide a starting point and framework for the development of solutions to network security, in particular in demand response networks that may employ emerging sensor and wireless technology. Attention to these problems benefits California utilities, as their networks are strengthened against attack, and their customers retain confidence in the companies' handling of their personal information. Attention to these problems benefits California's consumers, both in protection of their California Constitutional rights to privacy, and in the safety of their personal information from exploitation or theft. We hope this report may also provide information useful to regulators and lawmakers that may need to enact new rules to enforce sound privacy and security choices.

6.0 Glossary

AAA	Authentication, Authorization, and Accounting
A/D	Analog to Digital
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
ANSI	America National Standards Institute
BPL	Broadband over powerline
CATV	Cable TV
CCMP	Counter-Mode/CBC-MAC Protocol
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CEC	California Energy Commission
CFAA	Computer Fraud and Abuse Act
CIEE UCOP	California Institute for Energy and Environment, Office of the President, University of California
CPUC	California Public Utilities Commission
DR	Demand Response
DSL	Digital Subscriber Line
ECPA	Electronic Communications Privacy Act
EM	Electromechanical
EPRI	Electric Power Research Institute
ESP	Energy Service Provider
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HVAC	Heating, Ventilation, and Air Conditioning
iDEN	Integrated Digital Enhanced Network
IECSA	Integrated Energy and Communications Systems Architecture
IEEE	Institute of Electrical and Electronics Engineers

IPSec	IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet.
ISO	International Organization for Standardization
ISOs	Independent Service Operators
LAN	Local-Area Network
LEO	Low Earth Orbit
MAC	Message Authentication Code (Also used as an abbreviation for *Medium Access Protocol* in the context of networking.)
NG	Next Generation
NIST	National Institute of Standards and Technology
NOC	Network Operating Center
PG&E	Pacific Gas & Electric
PON	Passive Optical Networks
SCE	Southern California Edison
SDG&E	San Diego Gas & Electric
SDR	Software Defined Radio
SPP	Statewide Pricing Pilot
U.C.	University of California
VPN	Virtual Private Network
WEP	Wired Equivalent Protection
WiFi	Wireless Fidelity, IEEE 802.11 standard
WLAN	wireless local area network

7.0 References

[Arens-Wright] Ed Arens, Paul Wright, et al. New Thermostat and Meter DRETD Project, UC Berkeley, 2004.

[Bellare et al 98] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. .Relations Among Notions of Security for Public-Key Encryption Schemes. In Proceedings of CRYPTO '98.

[Blass & Zitterbart 2005] E.-O. Blass and M. Zitterbart. .Efficient Implementation of Elliptic Curve Cryptography for Wireless Sensor Networks. Technischer Bericht, Telematics Technical Reports TM-2005-1, Mar 2005 (ISSN 1613-849X).

[CommonCriteria] Common Criteria, http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf.

[Chan et al 2004] H. Chan, A. Perrig, and D. Song. .Key distribution techniques for sensor networks. In *Wireless sensor networks*, 2004, pp. 277.303. Kluwer Academic Publishers, Norwell, MA, USA.

[DRETD] Demand Response Enabling Technology Development Project, http://ciee.ucop.edu/dretd/

[CR]
[FCC NPRM 2003] FCC, *Notice of Proposed Rule Making and Order*, ET Docket No. 03-322, Dec 30, 2003

[FCC SPTF 2002] FCC Spectrum Policy Task Force, "Report of the Spectrum Efficiency Working Group," November 15, 2002

[FIPS] Federal Information Processing Standard (FIPS) 197: Advanced Encryption Standard. (See also http://csrc.nist.gov/cryptval/140-2.htm)

[Goldwasser and Micali 84] S. Goldwasser and S. Micali. .Probabilistic Encryption. Journal of Computer and System Sciences 28:270.299, April 1984.

[Hu & Perrig 2004] Y. Hu and A. Perrig. .A Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy, special issue on Making Wireless Work, 2(3):28-39, IEEE, May/June 2004.

[Hu et al 2003] Y. Hu, A. Perrig, and D. Johnson. .Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. In *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies* (INFOCOM 2003), vol. 3, pp. 1976-1986, IEEE, San Francisco, CA, April 2003.

[Hu et al 2003b] Y. Hu, A. Perrig, and D. Johnson. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. Proceedings of the 2003 ACM Workshop on Wireless Security (WiSe 2003), pp. 30-40, ACM, San Diego, CA, September 2003.

[Hughes 2003] Joe Hughes, The Integrated Energy and Communications Systems Architecture (IECSA) Project, Electric Power Research Institute June 4, 2003, http://ciee.ucop.edu/dretd/

[ICP] http: //www.epri-intelligrid.com/ intelligrid/docs/intelligrid_Consumer_Portal_Project_Plan_November_2004.pdf

[ICP-CPS] Intelligrid Consumer Portal FAQ_and_Survey, April 4, 2005. From http: //www.epri-intelligrid.com/

[IECSA 2003] Integrated Energy and Communications Systems Architecture. Initial Applications Scope and Stakeholder Identification, Task 1 Final Report, 2003.

[IEEE 802.11i] IEEE 802.11i Std 802.11i, July 2004

[IEEE 802.1X] IEEE 802.1X-Rev Draft 10.0, June 2004

[IEEE 802.11i] IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE Std 802.11i- 2004, Vol., Iss., 2004 pp. 1.175.

[IEEE 802.15.4] IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks specific requirements part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs). IEEE Std 802.15.4-2003, Vol., Iss., 2003 pp.1.670.

[ITU] http://www.itu.org

[Johnson Controls] Johnson Controls. Wireless Temperature Sensing System. Lit. Code No. LIT-1171100. Available at http://cgproducts.johnsoncontrols.com/metfipdf/1171100.pdf

[Karlof & Wagner 2003] C. Karlof and D. Wagner. .Secure Routing in Sensor Networks: Attacks and Countermeasures. Ad Hoc Networks, vol 1, issues 2.3 (Special Issue on Sensor Network Applications and Protocols), pp. 293-315, Elsevier, September 2003.

[Mitola 2001] Joseph Mitola III, "Cognitive Radio for Flexible Mobile Multimedia Communications," Mobile Networks and Applications, Volume 6, Number 5, Sept. 2001

[Network Management RON] Demand Response Enabling Technology Development Project: Network Management Research Opportunity Notice, June 4, 2003, http://ciee.ucop.edu/dretd/

[Neuman & Ts'o 1994] B.C. Neuman and T. Ts'o. .Kerberos: An Authentication Service for Computer Networks. In *IEEE Communications*, 32(9):33-38. September 1994.

[Newsome et al. 2004] J. Newsome, E. Shi, D. Song and A. Perrig. .The Sybil Attack in Sensor Networks: Analysis and Defenses. In Proc, of IPSN 2004, Berkeley, CA, April 2004.

[NSA] http://www.nsa.gov/

[OpenAMI] Advanced Metering Infrastructure. http://www.OpenAMI.org

[Parno et al 2005] B. Parno, A. Perrig and V. Gligor. .Distributed Detection of Node Replication Attacks in Sensor Networks. In Proceedings of the 2005 IEEE Symposium on Security and Privacy, May 2005.

[PCAST CIP 1998]

PCAST Letter on Critical Infrastructure Protection, President's Committee of Advisors on Science and Technology, 10 December 1998, http://www.ostp.gov/html/pcastcip.html

A National R&D Institute for Information Infrastructure Protection (I3P), Institute for Defense Analyses, April 2000, IDA Paper P-3511

White Paper on the Institute for Information Infrastructure Protection, Office of Science and Technology Policy, 11 July 2000

[Poon, Brodersen & Tse 2003]. Ada S. Y. Poon, Robert W. Brodersen and David N. C. Tse, "Degrees of Freedom in Spatial Channels: A Signal Space Approach", submitted to *IEEE Trans. on Information Theory*, August 2003.

[Sastry & Wagner 2004] N. Sastry and D. Wagner. Security Considerations for IEEE 802.15.4 Networks. ACM Workshop on Wireless Security (WiSE 2004). October 1, 2004.

[Semantic Web] The W3C Semantic Web, http://www.w3.org/.

[SDR Forum] Software Defined Radio Forum, http://www.sdrforum.org

[Trs Systems] Trs Systems Inc. WT1630A, B, C WirelessWall Temperature Sensors., Rev. 6. Available at http://www.trssys.com/specifications/WT1630%20rev6.PDF

[TCG] Trusted Computing Group, https://www.**trustedcomputinggroup**.org.

[Wagner 2004] D. Wagner. Resilient Aggregation in Sensor Networks. 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04), October 25, 2004.

[Wander et al 2005] A. Wander, N. Gura, H. Eberle, V. Gupta, S. Shantz. Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks. In *Third IEEE International Conference on Pervasive Computing and Communication (PerCom 2005).*, March 2005.

[Zhang and Zheng 1997] X.M. Zhang and Y. Zheng. *Cryptographically resilient functions*. In IEEE Transactions on Information Theory, 43(5):1740--1747, September 1997.

Appendix A: Supplemental Elaboration of California Statutory Law

This section contains an elaborated list of the California laws regarding privacy of personal information in the hands of third parties, and the California laws regarding unauthorized computer access.

California Statutes regarding personal information held by third parties

California Civil Code

Chapter 1 of Title 1.8 of the Code is entitled the Information Practices Act of 1977, and establishes that "the right to privacy is a personal and fundamental right [that is] being threatened by the indiscriminate collection, maintenance, and dissemination of personal information . . . [especially given] the increasing use of computers and other sophisticated information technology." As defined in section 1798.3, personal information means "any information that is maintained by an agency that identifies or describes an individual, including . . . name, social security number, physical description, home address, home telephone number, [and] statements made by, or attributed to, the individual." Section 1798.81.5(d) defines personal information to include "social security number . . . driver's license number . . . account number . . . [and] medical information." The chapter goes on to enumerate rules governing the maintenance and disclosure of personal information, and remedies for violations of these rules. This chapter may not be especially relevant to privacy issues concerning consumer electricity usage data, since it is concerned with demographic information relating to consumers.

However, the rules may influence the ways in which that data can be disseminated in the market, for example, or may play a role in protecting consumers from the de-anonymization of information. Section 1798.60 forbids "an individual's name and address [from] being distributed for commercial purposes, sold, or rented by an agency" unless permitted by law. Section 1798.81 requires that businesses destroy customer records "containing personal information which is no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying" the personal information. Section 1798.81.5(b) requires businesses that manage personal information about California residents to "implement and maintain reasonable security procedures" to protect the information from unauthorized disclosure. Section 1798.82 requires businesses to disclose "any breach in the security of a system" to consumers whose personal information may have been unlawfully disclosed as a result of that breach.

Several rules deal with information exchange between businesses and third parties. Section 1798.81.5(c) requires that businesses and nonaffiliated third parties contract to ensure reasonable security of information when businesses disclose customers' personal information to these third parties. Later, section 1798.83(a)(1) requires that businesses inform consumers of disclosures of personal information to third parties when consumers request that information and when the business knows or should know that the third party "used the personal information for [its] direct marketing purposes." Under subsection (e)(6), personal information, the disclosure of which to third parties requires notification to

the consumer, includes "the kind of product the customer purchased . . . [and] the kind of service provided," among several other demographic categories.

However, at subsection (d), the regulations enumerate certain disclosures which do not qualify as disclosures of personal information, including "disclosures between a business and a third party pursuant to contracts pertaining to . . . the processing, storage, management or organization of personal information, if the third party . . . does not use the information for a third party's direct marketing purposes;" "maintaining or servicing accounts;" "jointly offering a product or service . . . with the third party;" and several others.

California Public Utilities Code

The Public Utilities Code creates generalized protections against unfair dealings between electric service providers and consumers. For example, electric service providers may also have their registrations revoked for a number of violations, including "dishonesty, fraud or deceit with the intent to substantially benefit the electric service provider" under section 394.25.

Under section 451, rates for services provided by public utilities are required to be "just and reasonable." Rates may lawfully vary according to established customer classifications, as allowed under Business and Professions Code section 17042[gggg] and as demonstrated by PG&E's rate schedule dividing consumers into a multitude of different classes based on consumer usage trends, types of facilities, and other variables.[hhhh] Section 739.6 of the Public Utilities Code requires the CPUC to "establish rates using cost allocation principles that fairly and reasonably assign to different customer classes the costs of providing service to those customer classes." A subsequent question arises as to the extent to which public utilities may lawfully price discriminate, and the ways in which increasingly detailed consumer information might encourage further price differentiation not anticipated under the current regulatory structure.

Customer information is afforded basic protections under this Code. The CPUC is required by section 394.4 to adopt a confidentiality rule governing electric service providers.[iiii] This rule[jjjj] must ensure that customer information, including "customer specific billing, credit, or usage information," will remain confidential unless the customer

---

[gggg] This section provides that "nothing in this chapter prohibits . . . a differential in price for any article or product as between any customers in different functional classifications."

[hhhh] See http://www.pge.com/tariffs/ERS.SHTML#ERS.

[iiii] The difference between an electric corporation and an electric service provider is not entirely clear. According to Public Utilities Code section 294, an "electric service provider" is "an entity that offers electrical service to customers within the service territory of an electrical corporation, but does not include an electrical corporation, [and] includes the unregulated affiliates and subsidiaries of an electrical corporation." Under section 218, an electric corporation is a public utility that owns, manages, or provides electricity for compensation in California. However, it appears that an electric service provider may be construed as an electric corporation for purposes of administrative prosecutions, under section 394.25.

[jjjj] Note that the regulations themselves do not adopt this rule.

consents in writing to disclosure. Sections 2891-2894.10, entitled "Customer Right of Privacy," create extensive consumer protections against disclosure of personal and usage data without consent.[kkkk] However, these sections fall under the section of the Code pertaining to telephone corporations, and all customer rights under this section apply only to consumers of telephone and telegraph corporation services. Under section 2891, a telecommunications provider must obtain written approval from a customer to divulge to any other person or corporation any of the following: personal calling patterns, credit or other personal financial information, information on the services the customer receives from the company or any company providing service via the same lines, demographic information about the customer, or "aggregate information from which individual identities and characteristics have not been removed." These privacy protections are higher than those the energy utilities are held to.

On the whole, the law seems geared towards protecting the investor-owned utilities' data collections, including but not wholly composed of customer information, from adverse market consequences. Several regulations protect data in the possession of public utilities, especially when utilities transfer data to the CPUC. Section 583 specifies that, with few exceptions, "no information furnished to the commission by a public utility . . . shall be open to public inspection or made public except by order of the commission." Section 454.5(g) requires the CPUC, when soliciting long term procurement plans from the public utilities, to ensure confidentiality of "market sensitive information" including, but not limited to, "proposed or executed power purchase agreements, data request responses, or consultant reports."

The Public Utility Code's only mention of demand response infrastructure occurs at section 393(a) which set up the Statewide Pricing Pilot, meant to measure the benefits of making increased energy usage and pricing data available to ratepayers through advanced metering technology, and study how much load shifting results from time-variable energy tariffs.

California Code of Civil Procedure

Section 1985.3 discusses the procedures by which personal records may be sought by subpoenas duces tecum. The section defines "personal records" to include "electronic data pertaining to a consumer . . . which are maintained by any 'witness.'" The list of witnesses includes only a "telephone corporation which is a public utility, as defined in Section 216 of the Public Utilities Code." That section defines a "public utility" to include "every . . . electrical corporation [and] telephone corporation . . . where the service is performed for, or the commodity is delivered to, the public or any portion thereof." It is thus unclear whether electronic data maintained by an electrical corporation would constitute a public record for the purposes of this section.

[kkkk] Under section 2891, telephone and telegraph corporations are forbidden to reveal, without consumer consent, such information as "the subscriber's personal calling patterns," "the residential subscriber's credit or other personal financial information," "the services which the residential subscriber purchases from the corporation or independent suppliers," and "demographic information about individual residential subscribers."

Under section 1985.3, a subpoena duces tecum for personal records "maintained by a telephone corporation which is a public utility, as defined in Section 216 of the Public Utilities Code," is invalid without consumer consent as required by section 2891 of the Public Utilities Code.[llll]

Sections 2016-2036 comprise the Civil Discovery Act, which permits parties to obtain through discovery any information "that is relevant to the subject matter involved in the pending action or to the determination of any motion made in that action" according to section 2017(a). Under section 2017.020, the court may limit discovery if it is determined that "the burden, expense, or intrusiveness of that discovery clearly outweighs the likelihood that information sought will lead to the discovery of admissible evidence."

Section 2017(e) permits courts to "enter orders for the use of technology in conducting cases designated as complex . . . or to exceptional cases exempt from case disposition time goals . . . or cases assigned to Plan 3 pursuant to paragraph (3) of subdivision (b) or Section 2105 of the California Rules of Court."[mmmm] Section 2017.730 further specifies that a court may issue an order authorizing the use of technology in discovery, in a "case ordered to be coordinated under Chapter 3 . . . of Title 4 of Part 2."[nnnn] Under the same section, parties may also stipulate to an order authorizing the use of technology in discovery. Upon issuance of the court order, "discovery may be conducted and maintained in an electronic media and by electronic communication." This section later defines technology as including, but not limited to, "e-mail, . . . Internet websites, . . . electronic document depositories, and other electronic technology." Service providers may be "used and compensated" in discovery proceedings utilizing technology, under section 2017.740.

Section 2020 of the Civil Discovery Act addresses deposition subpoenas for acquiring business records from nonparties to an action. Such subpoenas do not require "an affidavit or declaration showing good cause for the production of the business records," under part (d)(1). Of interest may be part (d)(2), which states that when a witness holds business records which are "personal records pertaining to a consumer," the subpoenaing party must either also serve the subpoena upon the consumer and provide

---

[llll] See prior discussion of Public Utilities Code.

[mmmm] Section 2105 was renumbered section 212, and it is not clear that the three-tier Plan described in this section of the Code remains in effect.

[nnnn] Cases appropriate for coordination orders under section 404.1 of the Code of Civil Procedure include "civil actions sharing a common question of law or fact [where] one judge hearing all of the actions for all purposes in a selected site or sites will promote the ends of justice taking into account whether the common question of fact or law is predominating and significant to the litigation; the convenience of parties, witnesses, and counsel; the relative development of the actions and the work product of counsel; the

efficient utilization of judicial facilities and manpower; the calendar of the courts; the disadvantages of duplicative and inconsistent rulings, orders, or judgments; and, the likelihood of settlement of the actions without further litigation should coordination be denied."

proof of service in the subpoena served upon the witness, or obtain and demonstrate written consent of the consumer. However, this section applies the definition of "witness" articulated in section 1985.3 of this Code, so it remains unclear whether these procedures apply to an electricity corporation.

Legal Protections against Unauthorized Access to Computing or Communications

California Penal Code

The California Computer Crime Act, section 502 of this Code, is a privacy measure which bars unauthorized access by any person to lawfully-created computer data and computer systems. Crimes under the Act include several types of entry onto computer systems, done "knowingly and without permission," and with effects such as the alteration and destruction of data or computer systems, and disruption or illegal use of computer services. The Act also details penalties assessed for commission of any of these crimes, including fines of up to $10,000 or two years in prison. Part (h) of the Act specifies that the enumerated crimes do not automatically apply to any person acting within the scope of his or her lawful employment.

Section 629.50 et al. of the Penal Code specifies the procedures by which law enforcement agents may apply for an order "authorizing the interception of a wire, electronic pager, or electronic cellular telephone communication." For the purposes of this chapter, 'wire communication' means "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection . . . and the term includes any electronic storage of these communications." An 'aural transfer' is one which contains the sound of the human voice. While this chapter would thus not govern the interception of electronic energy usage information transferred between consumers and electric corporations, the format and approach of these regulations may later prove to be illuminating if lawmakers choose to take an analogous approach when regulating the new usage data transfers.

Under section 629.52, the judge may issue the interception order if there is probable cause to believe that the individual has engaged or may engage in one of several enumerated felonies. Section 629.20 requires that "a public utility engaged in the business of providing communications services and facilities . . . furnish the [law enforcement agent] all information, facilities and technical assistance necessary to accomplish the intervention unobtrusively. . .". This section provides for compensation to the utility in exchange for its assistance.

Sections 630 - 637.9 comprise Chapter 1.5 of the Code, entitled "Invasion of Privacy," which is intended by legislators to protect private communications from unlawful or unauthorized eavesdropping. Section 631 of this chapter makes it a felony for any person to make "any unauthorized connection . . . with any telegraph or telephone wire, line, cable or instrument;" to read, attempt to read, "or learn the contents or meaning of any message, report or communication while the same is in transit or passing over any wire, line or cable;" or to use, or attempt to use, "in any manner, or for any purpose, or to communicate in any way, any information so obtained . . .".

This Chapter uses broad language to forbid nearly any unauthorized entrance onto wire-based communication, and appears to apply to communications beyond the

telephonic. However, important exemptions exist. 631(b) specifies that "this section shall not apply (1) to any public utility engaged in the business of providing communications services and facilities . . . where the acts otherwise prohibited herein are for the purposes of construction, maintenance, conduct or operation of the services and facilities of the public utility, or (2) to the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility . . .". Section 633 provides that nothing in the preceding sections "prohibits [any law enforcement officer] from overhearing or recording any communication that they could lawfully overhear or record prior to the effective date of this chapter."

Sections 1326 - 1332 of the Penal Code delineate procedures for requesting production orders and witness subpoenas during an ongoing felony investigation. 1326.1(a) requires that "an order for the production of utility records in whatever form and however stored" may issue only upon a showing of specific and articulable facts, which demonstrate reasonable grounds to believe that the records will be relevant to the investigation. Under part (b) of this section, utility records include "call detail records, billing statements, [and] payment records" but do not include "the installation of, or the data collected from the installation of pen registers or trap-tracers, nor the contents of a wire or electronic communication." Part (e) specifies that "nothing in this section shall preclude the holder of the utility records from voluntarily disclosing information or providing records to law enforcement upon request." Thus, it appears that production orders may not be necessary for law enforcement agents to access utility records.

Sections 1523 - 1542 deal with search warrants. 1524.3(a) requires a "provider of electronic communication service or remote computing service [as defined in the Electronic Communications Privacy Act]," upon receipt of a warrant, to "disclose to a governmental prosecuting or investigating agency the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and . . . the types of services the subscriber . . . utilized." The governmental agency is not required to provide notice to the subscriber of the search.

Section 1536.5 specifies measures with which law enforcement agents must comply when carrying out search warrants for business records, generally prescribing that law enforcement agents must not compromise access to the records for an unreasonable amount of time. The section defines 'business records' as "computer data, data compilations, accounts, books, reports, contracts, correspondence, inventories, lists, personnel files, payrolls, vendor and client lists, documents, or papers of the person or business normally used in the regular course of business, or any other material item of business recordkeeping that may become technologically feasible in the future."

Chapter 5.7 of the Code is entitled the "High Technology Theft Apprehension and Prosecution Program." Section 13848(b) identifies as crimes unauthorized access or entry into private and public computers and networks, and unauthorized use or manipulation of data found therein. The Chapter goes on to describe methods of enforcing the enumerated laws and punishments for violations.

Appendix B: List of Interviewees and Compiled Interview Questions

Interviewed for this project:

George Cardona[oooo], U.S. Department of Justice

Greg Carstensen, PG&E

Steven Clymer, Cornell Law School (formerly U.S. Department of Justice)

Ahmad Faruqui, CRAI

Steve George, CRAI

Chris King, e-meter

Roger Levy, Levy Associates

Sharon Li, PG&E

Belvin Louie, PG&E

Mark Martinez, SCE

Terry Mohn, SDG&E

Ali Vojdani, UISOL

Gaymond Yee, UCOP CIEE

Interview Questions about Pricing Pilot:

Statewide Pricing Pilot Program

- How were participants chosen
- What kind of meter used –
- What kind of transmission –
    a. Meter to meter relay? Cell phone system?
- What kind of pricing
    a. Time-of-use (TOU) only or TOU + 50 price spikes/year
    b. Seasonal changes in price?
    c. How were price changes communicated? Did that work?
- Participants still have meters, still data being collected
    a. What research still ongoing?

[oooo] Comments made by Mr. Cardona represent his personal opinion, and not that of the U.S. Department of Justice.

Data Collection in Pilot Program

- What information was collected to analyze pilot?
    a. Hourly usage collected daily
    b. Demographic data?
- Was all information linked to customer name or other identifying info?
- How was data analyzed / used
    a. By economists
    b. By utility
    c. What was learned by economists/utilities?
- What additional data would have been useful
    a. to economists
    b. to utility
- Any studies done as to what hourly data could infer about customer?

Interview Questions about future AMI and demand response

Current AMI Operations

1. What kind of meter being installed?
2. What data is being generated / collected by meter?
3. How much data being stored in meter & how long?

Current AMI Data Collection (Pilot Program & Holdovers)

4. What is data path of collected data?
5. What is ideal data path in widespread deployment?
6. What kind of meter communication system is preferred?

Data requirements of utility subsystems for AMI data

7. Data and data granularity needed for particular operations subsystems (like Billing, Outage Monitoring, Field Automation, etc)
8. Data and data granularity needed for research tasks (like Load Profiling, Rate Design, Program Evaluation, etc)
9. Questions on data use by subsystems :
    a. What data required by subsystems & is data pre-processed?
    b. What data do sub-systems store & for how long?
    c. What data would allow subsystems to work better?
    d. How much would subsystem goals suffer if data were:
        i. anonymized, pseudonymized
        ii. aggregated at some level
    e. Are there ways customer could benefit if more data available?

10. Are there new, special, or customized services that could be provided to customers as a result of AMI data or AMI enabled research?

Data at 3d party

11. In widespread deployment, what data/services will be stored/enabled/participated in by 3d party?

12. How is utility privacy policy extended to 3d party and enforced?

13. What will Privacy Policy / Release say to customers?

Data at Customer

14. What data is fed back to customer about their usage and how?

15. What are protection mechanisms for this information?

What changes are expected in widespread implementation of AMI/Demand Response?

16. Any comments on a DRBizNet-like vision of open energy infrastructure architecture?

17. Any comments on other proposals:

- **a.** Meter computing bill
- **b.** Aggregation / Anonymization
- **c.** What problems would these cause?

Interview questions for Law Enforcement

1. Requests for Utility Data
    a. How frequently are utility records sought?
    b. At what point in a case are utility records sought – early in the case, as a basis for a warrant, or later, as supplementary evidence?
    c. In drug cases, are energy records sought in most cases where a home laboratory or home-growing are suspected? Or is energy data only requested in unusual circumstances?
    d. Aside from drug-related cases, do you know of other areas where utility records are of probative value in the development of a case?
    e. It is our understanding that energy utility records may be subpoenaed, but also that utilities have the power to release the data voluntarily.
        i. How frequently is data released by the utility without subpoena?
        ii. Do utilities ever bring information to law enforcement on their own initiative?

2. Internal regulations for getting/requesting utility data
    a. What are normal procedures for requesting utility data?
    b. Is there field manual guidance on this process?
    c. What data is usually received?
3. How is the data customarily used? What is its value?
4. If hourly energy data were available on residential customers…
    a. Might the data be more useful? How?
    b. Might the data become useful in different kinds of cases?
    c. Might real-time access to energy data ever be desirable?
        i. Are there any regulations that might constrain real-time access?
    d. Do you think subpoena requests for energy usage records would increase if hourly data became available?
5. In California, there was a demand response statewide pilot program in 2003-2004, where a few thousand customers were given system upgrades, and their energy usage was monitored hourly for 18 months.
    a. Might you know if any subpoena requests were made for hourly data during the pilot?
    b. If so, we're interested in how the data may have been used differently, or proved more valuable in any way.
6. How much concern is there in your division about energy theft (is this a problem even on the radar)?
7. Long-term energy utility plans envision smart meters, smart thermostats, and other in-home devices containing significant electronic processing capability, wireless communications, and perhaps even internet access. So, we are also studying the developing law of unauthorized computer access, and how it may relate to future smart appliances.
    a. To your knowledge, has there been any investigation or discussion about investigation of unauthorized access to wireless computer networks in the residential context in your division?
    b. Is this becoming an increasing area of concern?

If any, are these cases usually about theft of service, or have there been any cases where access was gained to networks for the purpose of spying on the owner or identity theft (more interesting to our work).

Appendix C: A review of some OSI-related networking terms

For completeness, this Appendix briefly reviews the seven-layer *Open System Interconnection (OSI) reference model.*

The *Open System Interconnection (OSI) reference model* describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. The model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered the primary architectural model for intercomputer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers. The following list details the seven layers of the Open System Interconnection (OSI) reference model:

- Layer 7—Application Layer

  This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level.

- Layer 6—Presentation Layer

  This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the *syntax layer*.

- Layer 5—Session Layer

  This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

- Layer 4—Transport

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

- Layer 3—Network

  This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

- Layer 2—Data link

  At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

- Layer 1—Physical

  This layer conveys a logical bit stream over a physical medium -- e.g., electrical impulse (over a wire), light (over an optical fiber) or radio signal (for wireless transmission) -- through the network at the electrical and mechanical level.

  The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems. Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors.

The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers.

The *upper layers* of the OSI model deal with application issues and generally are implemented in software. The highest layer, the application layer, is closest to the end user. Both users and application layer processes interact with software applications that contain a communications component. The term upper layer is sometimes used to refer to any layer above another layer in the OSI model.

The *lower layer*s of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical

layer, is closest to the physical network medium (the network cabling, for example) and is responsible for actually placing information on the medium.

End Notes

[a] The term *heterogeneous networks* is used to refer to networks that contain subnetworks with differing characteristics, such as wired IP networks and wireless sensor networks. A heterogeneous network can also consist of, for example, a collection of wireless networks using differing wireless technologies, such as 400-900 MHz sensor networks, IEEE 802.15.4 "Zigbee" networks [ZigBee], IEEE 802.11 a/b/g "WiFi" networks [IEEE802.11], and wide area wireless networks e.g., GSM or CDMA networks. In a broader sense, the term is used to allude to networks having subnetworks with differing administrative policies or administrative domains, as well as differing technological underpinnings and characteristics.

[b] A *Biometric assurance* technique is based on the measurement of a physical ("biological") characteristic of a human being (e.g., fingerprint, palmprint, retinal scan, voice, …) and the use of such measurements as the basis of an authentication mechanism. Similarly, a *radiometric assurance* technique uses measurements related to radio signals as the basis for authentication; this is analogous to using power and current measurements to suggest the activity inside of circuits and systems.

The term biometrics applies to a broad range of electronic techniques that employ the physical characteristics of human beings as a means of authentication. In a sense, human beings already routinely authenticate one another biometrically: confirming the identity of a friend on the telephone by the sound of his or her voice is a simple instance of this. A number of biometric techniques have been proposed for use with computer systems. These include (among a wide variety of others) fingerprint readers, iris scanners, face imaging devices, hand geometry readers, and voice readers. Usage of biometric authentication techniques is often recommended in conjunction with other user authentication methods, rather than as a single, exclusive method.

Fingerprint readers are likely to become a common form of biometric authentication device in the coming years. To identify herself to a server using a fingerprint reader, a user places her finger on a small reading device. This device measures various characteristics of the patterns associated with the fingerprint of the user, and typically transmits these measurements to a server. The server compares the measurements taken by the reader against a registered set of measurements for the user. The server authenticates the user only if the two sets of measurements correspond closely to one another. One significant characteristic of this and other biometric technologies is that matching must generally be determined on an approximate basis, with parameters tuned appropriately to make the occurrence of false positive matches or false negative rejections acceptably infrequent.

[c] The term *Trusted Architecture* is being used in this document in a generic sense to refer to a computer system architecture that has been explicitly designed to be "safe", or to at least significantly decrease the probability of being cracked (or physically broken into). In security engineering, a trusted system is a system that you have *no choice but to trust*. The failure of a trusted system will compromise security. In general, the number of trusted components in a system should be minimized.

Trusted Computing (TC) also sometimes refers to a technology developed and promoted by the Trusted Computing Group (TCG) [TCG] (https://www.trustedcomputinggroup.org). The term is taken from the field of trusted systems and has a specialized meaning. In this technical sense, "trusted" does not necessarily mean the same as "trustworthy" from a user's perspective. Rather, it means that it can be trusted more fully to follow its intended programming with a lower possibility of inappropriate activities occurring that are forbidden by its designers and other software writers.

[d] There is general agreement in the software defined radio community that "third party software" in the context of agile radios will evolve in availability and sophistication over time. An analogy for this can be found by looking at the evolution of the personal computer (PC) industry: in the very early stages, a PC manufacturer bundled all of the hardware and software components, including applications, into the product sold to the customer (i.e., there was typically no third party software or hardware). Over time, it has become commonplace for users to assemble their "customized" personal computer by buying multiple hardware components from multiple vendors (e.g., plug in cards for networking, video, gaming, etc.), and buying third party software (both applications and drivers) from an entirely different set of vendors.

[e] In this discussion, we specifically distinguish Broadband over Powerline (BPL) because the communication channel and physical medium (the powerline) is wholly owned by the (electric/ energy) utility, unlike alternative media such as cable or wireless, wherein the medium is shared and/or owned by an entity *other* than the utility.

[f] *Elliptic curve cryptography (ECC)* is an approach to public-key cryptography based on the mathematics of elliptic curves over finite (Galois) fields.

Public-key algorithms create a mechanism for sharing keys among large numbers of participants or entities in a complex information system. Unlike other popular algorithms such as RSA that are based on the difficulty of factoring the product of two large primes, ECC is based on discrete logarithms that are much more difficult to challenge at equivalent key lengths. While ECC offered a potential for improved security, the early implementations were relatively slow. Subsequent research has resulted in more efficient algorithms and implementations that make ECC practical for use in a variety of applications. (The following discussion cites extensively from a white paper published by the National Security Agency [NSA].)

Over the past 30 years, public key cryptography has become a mainstay for secure communications over the Internet and throughout many other forms of communications. It provides the foundation for both key management and digital signatures. In key management, public key cryptography is used to distribute the secret keys used in other cryptographic algorithms (e.g. The Digital Encryption Standard DES). For digital signatures, public key cryptography is used to authenticate the origin of data and protect the integrity of that data. For the past 20 years, Internet communications have been secured by the first generation of public key cryptographic algorithms developed in the mid-1970's.

Notably, they form the basis for key management and authentication for IP encryption (IKE/IPSEC), web traffic (SSL/TLS) and secure electronic mail.

Since the initial introduction and success of public key cryptography, new techniques have been developed which offer both better performance and higher security than these first generation public key techniques. The best assured group of new public key techniques is built on the arithmetic of elliptic curves. Arguments have been made for moving to elliptic curves as a foundation for future (Internet) security. These arguments are based on both the relative security offered by elliptic curves when compared to first generation public key systems and the relative performance of these algorithms. "While at current security levels elliptic curves do not offer significant benefits over existing public key algorithms, as one scales security upwards over time to meet the evolving threat posed by eavesdroppers and hackers with access to greater computing resources, elliptic curves begin to offer dramatic savings over the older, first generation techniques.

The two noteworthy first generation public key algorithms used to secure the Internet today are known as RSA and Diffie-Hellman (DH). The security of the first is based on the difficulty of factoring the product of two large primes. The second is related to a problem known as the discrete logarithm problem for finite groups. Both are based on the use of elementary number theory. Interestingly, the security of the two schemes, though formulated differently, is closely related.

Elliptic Curve Security and Efficiency

The majority of public key systems in use today use 1024-bit parameters for RSA and Diffie-Hellman. The US National Institute for Standards and Technology has recommended that these 1024-bit systems are sufficient for use until 2010. After that, NIST recommends that they be upgraded to something providing more security. The question is what should these systems be changed to? One option is to simply increase the public key parameter size to a level appropriate for another decade of use. Another option is to take advantage of the past 30 years of public key research and analysis and move from first generation public key algorithms and on to elliptic curves.

One way judgments are made about the correct key size for a public key system is to look at the strength of the conventional (symmetric) encryption algorithms that the public key algorithm will be used to key or authenticate. Examples of these conventional algorithms are the Data Encryption Standard (DES) created in 1975 and the Advanced Encryption Standard (AES) now a new standard. The length of a key, in bits, for a conventional encryption algorithm is a common measure of security. To attack an algorithm with a k-bit key it will generally require roughly 2^k-1 operations. Hence, to secure a public key system one would generally want to use parameters that require at least 2^k-1 operations to attack. The following table gives the key sizes recommended by the National Institute of Standards and Technology to protect keys used in conventional encryption algorithms like the (DES) and (AES) together with the key sizes for RSA, Diffie-Hellman and elliptic curves that are needed to provide equivalent security.

Symmetric Key Size (bits)	**RSA and Diffie-Hellman Key Size (bits)**	**Elliptic Curve Key Size (bits)**
80	1024	160

112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

To use RSA or Diffie-Hellman to protect 128-bit AES keys one should use 3072-bit parameters: three times the size in use throughout the Internet today. The equivalent key size for elliptic curves is only 256 bits. One can see that as symmetric key sizes increase the required key sizes for RSA and Diffie-Hellman increase at a much faster rate than the required key sizes for elliptic curve cryptosystems. Hence, elliptic curve systems offer more security per bit increase in key size than either RSA or Diffie-Hellman public key systems.

Security is not the only attractive feature of elliptic curve cryptography. Elliptic curve cryptosystems also are more computationally efficient than the first generation public key systems, RSA and Diffie-Hellman. Although elliptic curve arithmetic is slightly more complex per bit than either RSA or DH arithmetic, the added strength per bit more than makes up for any extra compute time. The following table shows the ratio of DH computation versus EC computation for each of the key sizes listed in Table 1.

Security Level (bits)	**Ratio of DH Cost : EC Cost**
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

Table 2: Relative Computation Costs of Diffie-Hellman and Elliptic Curves[1]

Closely related to the key size of different public key systems is the channel overhead required to perform key exchanges and digital signatures on a communications link. The key sizes for public key in Table 1 (above) is also roughly the number of bits that need to be transmitted each way over a communications channel for a key exchange[2]. In channel-constrained environments, elliptic curves offer a much better solution than first generation public key systems like Diffie-Hellman.

In choosing an elliptic curve as the foundation of a public key system there are a variety of different choices. The National Institute of Standards and Technology (NIST) has standardized on a list of 15 elliptic curves of varying sizes. Ten of these curves are for what are known as binary fields and 5 are

for prime fields. Those curves listed provide cryptography equivalent to symmetric encryption algorithms (e.g. AES, DES or SKIPJACK) with keys of length 80, 112, 128, 192, and 256 bits and beyond.

For protecting both classified and unclassified National Security information, the National Security Agency has decided to move to elliptic curve based public key cryptography. Where appropriate, NSA plans to use the elliptic curves over finite fields with large prime moduli (256, 384, and 521 bits) published by NIST."

As mentioned elsewhere in the report, algorithms have been invented over the past few years that facilitate efficient implementation of ECC on sensor nodes.

---

[1]These estimates are based on the theoretic costing of an n-bit multiply modulo a large prime as costing roughly n^2 operations. It is also based on an estimate that computing an inverse modulo a large prime is roughly 8 multiplies. Actual implementations could be radically different based on computer architecture.

[2]In the elliptic curve case, there is actually one additional bit that needs to be transmitted in each direction which allows the recovery of both the x and y coordinates of an elliptic curve point.

[g] *Plaintext* is used to refer to the "original" message that has not been encrypted.

[h] The US Department of Defense is one of the leading users of Software Defined Radio technology. The Software Communications Architecture (SCA) mandated by the Joint Tactical Radio System Program Office (JPO) of the Department of Defense provides a software framework for the implementation of software defined radio (SDR) platforms. This framework provides many features to increase the portability of wireless protocols or *air interfaces* (referred to as "waveforms" in the SCA context) including a common operating environment and a set of common services as well as standard application component interfaces. An SCA-compliant *software defined radio platform* provides a way to dynamically configure and reconfigure communication processing resources to meet differing requirements such as multi-mission support.

[i] In cryptography, a *certificate authority* or *certification authority* (CA) is an entity that issues digital certificates for use by other parties. It is an example of a trusted third party. CA's are characteristic of many *Public Key Infrastructure* (PKI) schemes.

There are many commercial CAs that charge for their services. Institutions and governments may have their own CAs, and there are free CAs.

A CA will issue a *Public Key Certificate* that states that the CA attests that the *public key* contained in the certificate belongs to the person, organization, server, or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users (the "relying parties") can trust the information in the CA's certificates. The usual idea is that if the user trusts the CA and can verify the CA's signature, then they can also verify that a certain public key does indeed belong to whoever is identified in the certificate.

[j] *Message Authentication*. A hash or *message digest* is a mathematical transformation that takes an arbitrary length message, and derives a small, fixed length value with the following unique property: if someone alters your message, it is computationally unlikely that it would hash into the same value you computed on the original message. A hash does not assure message integrity; however, a signed hash (or hashed message authentication code) does. When using pre-shared keys, each IKE party computes a hash on its Identity information and includes that hash in an encrypted message to its remote peer. The key used for authentication is derived from the shared key and keying material created during the Diffie-Hellman exchange. When the IKE peer receives this message, it decrypts the message, then computes its own value of the hash, using the same shared key; if the value proves to be "mutually obtainable," the integrity of the message serves to authenticate the exchange. Thereafter, all management messages exchanged during Phase 2 are protected by a hashed message authentication code. Of the choices available, Secure Hash Algorithm (SHA1) is considered more secure than Message Digest (MD5) because SHA1 uses a longer key (160 bit, compared to MD5's 128-bit key).

[k] *Cryptography* or *cryptology* is a field of mathematics and computer science concerned with information security and related issues, particularly encryption.

[l] "Wardriving" refers to the act of driving around in a vehicle with a laptop computer, an antenna, and an 802.11 wireless local area network adapter to exploit existing wireless networks. Set on "promiscuous mode", the wireless adapter, typically a network interface card or chip, will receive packets within its range (as opposed to packet addressed specifically to the card). Wardriving exploits wireless networks that have ranges that extend outside the perimeter of buildings in order to gain free Internet access or illegal access to an organization's data. One safeguard against wardriving is to use an effective encryption standard.