On Security of a Home Energy Management System

A. Saha, S. Rahman, M. Pipattanasomporn, and M. Kuzlu
Bradley Department of Electrical and Computer Engineering and Advanced Research Institute
Virginia Tech, Arlington, Virginia, USA
E-mail: avijit@vt.edu, srahman@vt.edu, mpipatta@vt.edu, mkuzlu@vt.edu

***Abstract*— Smart grid, constituting of numerous components and sub-systems, can be a target for security threats. Failure of any sub-system to properly defend itself against attacks poses a serious risk to the protection of smart grid as a whole. Therefore, securing residential demand response (DR) applications as part of the smart grid requires careful attention. This paper discusses security concerns of a specific DR implementation: the Home Energy Management (HEM) system developed at Virginia Tech (VT). The paper identifies possible security attacks against its various key components, and presents best practices for the counter-measure against those attacks. Privacy issues have also been addressed using access control methods. The paper serves as a use case example of assessing and mitigating security risks in residential DR programs.**

***Index Terms*— Home Energy Management System, Security.**

I. Introduction

Smart Grid, as opposed to the traditional power grid, is a very complex dynamic network of inter-connected devices for information exchange, decision-making, and actuation. Two key challenges of smart grid implementation are security and interoperability [1], which should be addressed as a part of the design problem instead of after-thought.

One of the benefits of the smart grid is its ability to curtail peak loads using demand response (DR) [2]. Automated DR programs are gaining attention due to their ability to automatically manage loads without direct customer intervention. Residential DR programs typically rely on smart appliances/load control devices within a home wireless/wired network, and make automated decisions of load reduction based on pricing/control signals provided by the utility [3]. This exposes areas of vulnerability that need to be addressed to protect the data and customer privacy. For example, residential wireless networks or communication channels between a utility and customer premises may become a possible target for security attacks. This opens up many concerns regarding the security of smart grid and privacy of customers participating in DR programs. Although work has been reported that identifies security vulnerabilities in wireless sensor networks for demand response applications [4-7], assessment of security risks in residential DR applications and their mitigation remain to be investigated.

This paper discusses the security and privacy concerns in a specific residential DR program: the Virginia Tech (VT) Home Energy Management (HEM) system [8]. It is an automated incentive-based DR algorithm. Hardware implementation of the HEM algorithm in a laboratory environment [9] was realized utilizing the ZigBee wireless network for communication with load monitoring and control devices, and a web-server based communication between HEM and other entities (i.e., electric utility, third party etc.). This paper identifies key system components and considers probable threats for each of them. It also discusses best practices for counter-measures that have been/can be implemented. Data privacy of customers is another issue in residential DR implementations. The paper also discusses an approach of access control for ensuring data privacy in the HEM system.

II. VT HEM System and its Components

Fig. 1 shows components of the VT HEM system. The HEM algorithm is hosted on a central PC/embedded system (referred as the 'HEM unit'). The HEM unit takes into account customer priority and preference settings for appliances. Control signals from a utility consist of a demand limit and duration of the DR event. Based on these, the HEM unit takes automated decisions to control four power-intensive loads in a household (i.e., water heater, air conditioner, clothes dryer, and electric vehicle) to keep the total household consumption within the specified demand limit. Control decisions are actuated by smart plugs/load controllers, which communicate with the HEM unit over a ZigBee network. This communication enables smart plugs to provide their data to the HEM unit, and the HEM unit to provide control signals to smart plugs.

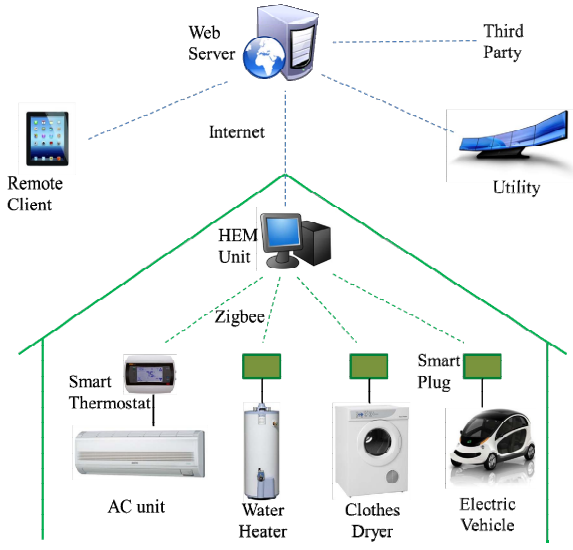

Fig. 1. VT HEM Architecture.

978-1-4799-7720-8/14/$31.00 ©2014 IEEE

The HEM unit is also a part of a web-based service, which utilizes the Internet to provide communications among the electric utility, the HEM unit, third party providers, and customers accessing from remote devices (i.e., smart phone, or remote PC). Through web services, the HEM unit provides the household consumption data to the utility, shares data with remote clients, and receives DR event signals from the utility. A web server is used to host web interfaces and databases to provide access control for shared resources, and to address web-related security issues. Each customer premises has its own HEM unit, and therefore, the web server is a shared resource among all HEM units served by the utility.

The sequence diagram as shown in Fig. 2 illustrates the interaction among different entities in the VT HEM system. It shows how a utility may send a demand limit to the HEM unit inside a house through a web server, and how the HEM unit can impose the demand limit by controlling the operation of the target loads. Household power consumption data can be recorded in the HEM unit in 1-minute intervals. The minimum of 1-minute duration is needed to allow the HEM algorithm to calculate and implement control decisions on the target loads.

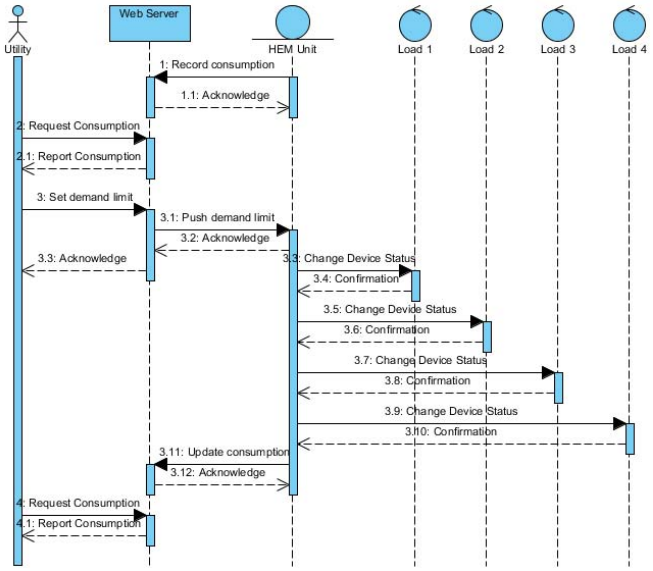

Fig. 2. Sample sequence diagram showing interactions between VT HEM components for implementing demand response.

III. Major Security Aspects in HEM

Before identifying security vulnerabilities, major HEM security objectives are identified, as follows:

Confidentiality: All information transferred to/from HEM related to customers, a utility or third parties needs to be kept confidential. A breach in confidentiality may mean leak of sensitive information, like customer usage profile, administrative information of utility, customer geographical location and identity etc.

Integrity: All data communication should be impervious to data manipulation. If integrity is not ensured, attackers may provide incorrect customer data to utility or spurious control signals to customers.

Authentication: All participants should properly authenticate themselves before starting any communication. This prevents impersonation and allows access to authorized entities only.

Availability: Shared resources should be available to authorized entities at all times. Failure to provide availability may cause failure in DR implementation at crucial periods.

Control: Control devices should be accessible to authorized entities only, and should be guarded against malicious control attempts.

IV. Security Concerns in HEM Components

Security threats and best practice counter-measures for key components of the VT HEM system are discussed below.

A. Security Concerns in ZigBee Network and Devices

1) ZigBee Terminal Devices

In the VT HEM implementation ZigBee terminal devices (also known as ZigBee End Device in ZigBee terminology) are smart plugs/load controllers used to monitor and communicate power data and implement control decisions through relays. Sensors like smart thermostats can also be considered as ZigBee terminal devices. These devices - along with the ZigBee coordinator connected to the HEM host - form a ZigBee mesh network according to IEEE 802.15.4 standards [10]. To understand possible security threats for these devices, it is necessary to understand their components and interactions.

Load monitoring and control operation can be implemented in the VT HEM system by using either off-the-shelf commercial ZigBee smart plugs or load controllers developed at VT ARI. These devices include low-power and low-resource embedded systems with ADC (Analog to Digital Converter) to sample load data, actuator relays to turn loads ON/OFF and ZigBee modules to communicate with the HEM unit. These components are hard-wired/PCB (Printed Circuit Board) fabricated and packaged compactly. One of the possible threats is direct physical tampering of these devices. Most commercial off-the-shelf products offer some form of tampering protection as well as data/code protection in the embedded controller. Hence, it is difficult in most cases for an adversary to take control of terminal devices. Since, these controllers are inside the house, physical tampering is only possible from an insider attack. Possible threats associated with insider attacks are listed in Table I.

2) ZigBee Network Between HEM Coordinator and Terminal Devices

This is the mesh network within the home that connects all ZigBee devices and makes HEM implementation possible through coordination. Even if none of the devices in the HEM system has been compromised, there are other threat models that may be attempted by an outsider attacker having sufficient computational resources and radio access within the

ZigBee network. Possible threats to a ZigBee network are summarized in Table II.

TABLE I.
POSSIBLE SECURITY THREATS TO ZIGBEE TERMINAL DEVICE

Security Aspect	Possible Threats
Control	The compromised terminal device can be remotely controlled to turn ON/OFF loads by the adversary, thereby causing potential expensive power usage or customer annoyance.
Authentication	The adversary taking control of the terminal device can authenticate within the mesh network, and can launch various other forms of attack in the network.
Confidentiality	The compromised terminal device can be used to eavesdrop packets between other nodes being forwarded through it.
Data integrity	- The compromised terminal device can be used to provide false load data to the HEM, causing it to make incorrect decisions. - The terminal device may be manipulated to cause jamming and/or insertion of packets. This can be done on data packets between other nodes in the network, which are only being routed through the compromised end device. - It can also be used to impose routing attack, by generating incorrect routing trees and forwarding packets incorrectly/selectively. It can also cause wormhole attacks by decreasing latency and can be used to exploit routing race conditions.
Availability	The compromised end device can provide a huge number of data packets transmission to the HEM unit, thereby causing availability issues for the HEM coordinator with limited resources.

TABLE II.
POSSIBLE SECURITY THREATS TO ZIGBEE NETWORK

Security Aspect	Possible Threats
Confidentiality	An attacker may eavesdrop to messages transmitted within a ZigBee network. If not protected by good cryptographic methods, this may mean possession of key information about the communication protocol within the network.
Integrity	An attacker may cause inter-leaving or man-in-the-middle attacks causing jamming or insertion of packets. Successful attacks can cause severe problems in DR implementation including wrong data and local actuation.
Privacy	Eavesdropping may give away private customer information like: appliance usage profiles and life-style, when customer is inside or outside house etc.

3) Countermeasures Against Threats to ZigBee Network and Devices

a) Threats to Physical Layer

Physical capturing of end nodes can only be prevented by advances in tamper-resistant technologies. Current trends toward tamper-resistant smart plugs and single chip solutions can make it difficult for adversaries to take control of end nodes physically. It will still be feasible for an insider to disable terminal devices, but that can easily be detected by the HEM unit and a warning can be issued to the homeowner to check the deactivated terminal device.

b) Threats to Network Layer

These threats include outsider attacks to the network that rely on eavesdropping and packet jamming/insertion. The best defense against these kinds of attacks is the use of cryptography and proper authentication protocols. The ZigBee specification by ZigBee alliance [11] assumes the 'open trust' model where the protocol stack layers trust each other and the cryptographic encryption/decryption occurs only between devices. The ZigBee coordinator is designated as the 'trust center', which stores cryptographic keys for the network and is used to provide keys to other devices and authorize devices into the network. ZigBee security typically uses symmetric key cryptography and the keys can be pre-installed or transported between devices. Use of the same key for all devices in the network can make the network vulnerable if one of the terminal devices is compromised. Hence, a separate key may be used for each pair of nodes to protect frames at APS layer (Application Support Sub-layer). The secure distribution of these keys may be costly in terms of resources available at ZigBee terminal devices, hence alternate schemes may be adopted, as discussed in [12]. ZigBee security suites use AES-CCM, as discussed in NIST special publication 800-38C [13], which ensures both encryption to defend against eave-dropping and Message Integrity Code (MIC) signing to provide authentication as well as message integrity.

Recent research [14] has shown that public-key cryptography, like elliptic-curve cryptography, is feasible on sensor networks. It can also be used to provide protection in ZigBee networks. Having private and public keys for each node in the network also protects other nodes in case one of the nodes has been compromised.

B. Security Concerns in HEM Unit

1) Possible Threats

The physical HEM host PC/embedded system may also be compromised by an adversary, which can initiate either an insider attack (direct physical capture of the HEM host) or an outsider attack (using web network). A successful captured HEM host unit can be used by an adversary to do all sorts of possible attacks through web services. Some possible threats are listed in Table III.

TABLE III.
POSSIBLE SECURITY THREATS TO HEM HOST

Security Aspect	Possible Threats
Control	The adversary can implement their own commands for the controlled appliances in the household. Potential appliance damage, excessive power consumption, customer discomfort/ annoyance: a wide variety of nuisances can be done using a compromised HEM unit.
Confidentiality and privacy	Data and identity theft can be done by a compromised HEM unit. This kind of attack does not raise suspicion in the customer, and the adversary can keep collecting private customer data for days.
Integrity	The compromised HEM unit can be used to provide wrong data to web server and hence to utility. Multiple compromised HEM units may cause misrepresentation of actual demand scenario within an area.
Availability	Denial of service attacks on web server may be conducted using a compromised HEM unit.
Communication security	The compromised PC can be used to initiate attacks on other HEM host PCs in the network.

2) Counter Measures Against Threats to an HEM Unit

The same security guidelines for protecting personal computers can be applied to protect an HEM host, as it is a computers/embedded system hosting the HEM software. Customers should follow preventive guidelines for protecting the host PC from an insider attack. This includes using strong username password combinations, and, making sure the host is locked when a customer is not around (auto lock-out timers may be implemented). While any tablet or android device (with ZigBee router functionality and ability to process simple computing functions) is sufficient for use as an HEM host, a dedicated computing system that only runs HEM algorithms may be recommended to minimize possibilities of compromised security from other software. Proper security firewalls and threat detection suites should be implemented to provide security from outsider attacks (attack through the Internet). Required software/firmware upgrades for HEM software or security suites can be automated with dedicated system resources, so that HEM operation will not be interfered. A homeowner should only be allowed to view consumption data and change priority/preference settings or ON/OFF commands through the HEM unit, but not be granted administrative access to the HEM software. This can prevent possibilities of manipulating the system through misrepresentation of data or denial of reception of DR signals from a utility.

C. Security Concerns in Web-based Communications

1) Possible Threats

All security threats and measures discussed so far address security issues for components within the home wireless network. But, the other crucial part of this HEM implementation is the web-based solution to provide communications among a utility, the HEM unit, remote customers and third party service providers. This whole network is essentially based on the existing Internet framework, and hence the security of this network is also of paramount concern. All of the security concerns applicable to Internet-connected computers are also applicable here. Various forms of attacks are possible exploiting vulnerabilities in the web services design, like Impersonation attacks, Man-in-the middle attacks, Denial of Service attacks, Replay attacks etc.

2) Best Practices in Securing Web-based Communication

Communications between the web server and all other clients (HEM, remote customer, utility, third party providers) can be secured using HTTPS protocol, i.e., HTTP (Hypertext Transfer Protocol) over TLS (Transport Layer Security) [15]. The authentication and non-repudiation can be provided using certificate based mutual authentication protocols. Well-known certificate authority (CA) signed certificates can be used to ensure verification and thwart impersonation. Intrusion Detection System can be included to secure the server. Access control lists can also be used to filter illegitimate requests, as discussed in next section.

V. Access Control for Data Privacy

As a web server processes and stores various types of data, strict access controls over these data are required to ensure privacy and confidentiality. A role-based access control model is the most appropriate in this case, as different entities in HEM implementation can have different permissions to use different sub-sets of data. These may be defined in access control lists, which, after proper authentication of an entity in the server, will govern which data it has permission to see or use. To ensure customer privacy, the web server can be managed by a trusted third party provider other than utility or customers. Based on Fig. 1, roles that may have different access permissions are:

A. Customer Clients

There are two types of customer HEM clients that can be authenticated with the server. The first one is the HEM client at the customer premises (HEM unit). The second one is the remote client (smart phone/ remote PC, etc.) from which the customer may access their data.

The HEM client at the premises has access to its individual power consumption and sensor data, priority and preference settings, and DR event data provided by the utility. The HEM client will be able to write the latest consumption and sensor data to the server, and hence, will be able to provide up-to-the-minute data, which can be accessed by the customer from remote clients. The HEM client also can read/write the priority and preference settings. This enables two conveniences for the customer: firstly, if the customer changes these settings directly at the HEM host at their home, then changes will be reflected in the server by write access. Secondly, if these settings are changed by the customer from a remote client, the changes will be reflected at the HEM host through call-back. The HEM client will have read-only access to the DR event data provided by the utility, so that it can implement DR decisions based on these data. The read-only access prohibits the HEM client to change DR event data and hence preventing attacks if a customer HEM client has been compromised. An assumption made here is that DR limit and duration can only be set by the utility by its own algorithm, and if negotiations are needed between the customer's HEM unit and a utility to decide demand limit or duration, then it may be achieved by some other means.

The remote customer client has read-only access to consumption and sensor data. This prevents data alterations by an attacker even if the remote client is compromised. The remote client has write access to preference and priority settings, so that customers may change settings from outside their homes. These changes may be confined to acceptable ranges (i.e., room temperature set-point changes may be restricted to acceptable upper and lower limits), so that associated threats can be minimized if a remote client has been compromised. The remote client has read-only access to DR event data.

Data from different customers are separately stored and processed in the server, and customer clients are only allowed access to their own data after proper authentication. This ensures privacy of individual customers.

B. Utility

The electric utility has read-only access to total household consumption data from each customer. This helps the utility to decide DR event parameters for each customer, and also to verify if household demand has been appropriately reduced by a customer HEM. Consumption and sensor data for individual appliances in the customer household may give away private customer information (i.e., life-style, appliance usage, customer presence/absence at home, etc.) and hence this data is not accessible to utility to ensure customer privacy. Finally, the utility has write access to DR event parameters for each customer in order to be able to impose DR events.

C. Administrative Access

This role is reserved for system administrators, who can make changes to web server properties and settings. This role has authority over all other roles, and hence highest security measures should be taken to prevent attacks on administrative access.

D. Third Party Service Providers

This role is reserved for a third party web services provider, where specific access control lists can be maintained based on specific services of each provider. Table IV shows data access permissions for different roles for the VT HEM use case.

TABLE IV.
DATA ACCESS PERMISSIONS FOR DIFFERENT ROLES

Type of Data	HEM Client	Remote Customer Client	Utility
Individual appliance consumption and sensor data for each customer	Read/write	Read-only	No access
Total household consumption	Read/write	Read-only	Read-only
Priority and preference settings	Read/write	Read/write	No access
DR event signal (demand limit and duration)	Read-only	Read-only	Read/write

VI. CONCLUSION

The cyber security concerns are now integral part of any smart grid system design. Assessment of security vulnerabilities and implementation of proper counter-measures should be considered from the very initial stages of design of any smart grid sub-system. As such, residential DR implementation through an HEM system should be secured and protected through best practices available against all known threat models. This paper discusses security issues concerning a specific use case of DR implementation: the VT HEM. The VT HEM system is analyzed from the security point of view, through assessment of probable security threats to different components of the system and presents best practices of counter-measures against the assessed vulnerabilities. Though the discussion here addresses security concerns in the VT HEM system, most of the discussed vulnerabilities and counter-measures pertain to any typical HEM system.

VII. REFERENCES

[1] S. M. Amin, “Smart grid security, privacy, and resilient architectures: Opportunities and challenges,” *IEEE PES General Meeting, 2012*, pp. 1-2, San Diego, CA, July 2012.

[2] M. H. Albadi and E. F. El-Saadany, "Demand response in electricity markets: An overview," in *Proc. of 2007 IEEE PES Gen. Meeting,* pp. 1-5, June 2007.

[3] J. Li, J. Y. Chuang, J. Xiao, J. W. Hong, and R. Boutaba, “On the design and implementation of a home energy management system,” in *Proc. the 6th International Symposium on Wireless and Pervasive Computing (ISWPC)*, pp. 1-6, Feb 2011.

[4] C. Karlof, and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” *Proc. of 2003 IEEE Intl. Workshop on Sensor Network Protocols and Applications*, May 2003.

[5] P. A. Subrahmanyam, D. Wagner, D. Mulligan, E. Jones, U. Shankar, and J. Lerner, “Network Security Architecture for Demand Response/Sensor Networks,” Consultant Report to California Energy Commission, October 2005.

[6] M. Paranjpe, “Security and Privacy in Demand Response Systems in Smart Grid,” M.S. Report to California State U., Sacramento, 2010.

[7] M. Zillgith, D. Nestle, and M. Wagner, “Security Architecture of the OGEMA 2.0 Home Energy Management System,” *Proc. of 2013 Intl. ETG-Congress: Symposium 1: Security in critical infrastructures today*, pp. 1-6, Nov 2013.

[8] M. Pipattanasomporn, M. Kuzlu, and S. Rahman, "An algorithm for intelligent home energy management and demand response analysis," in IEEE Trans. on Smart Grid, vol. 3, no. 4, pp. 2166-2173, 2012.

[9] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Hardware demonstration of a home energy management system for demand response applications," IEEE Trans. on Smart Grid, vol. 3, no. 4, 2012.

[10] IEEE 802.15.4: Standards for Wireless Personal Area Networks, 2011-2012. Available: http://standards.ieee.org/about/get/802/802.15.html.

[11] ZigBee Alliance, “ZigBee Smart Energy Profile Specification V1.1,” 2011.

[12] H. Chan, A. Perrig, and D. Song, “Key distribution techniques for sensor networks,” pp. 277-303, in Wireless Sensor Networks, Kluwer Academic Publishers, 2004.

[13] M. Dworkin, “Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality,” NIST Special Publication 800-38C, May 2004 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf.

[14] 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).

[15] E. Rescorla, “HTTP over TLS,” RFC 2818, Informational, May 2000. Available: http://tools.ietf.org/html/rfc2818 [Online].