Security Threats in Advanced Metering Infrastructure

He-Ming Ruan[1], Yu-Sheng Yang[1], I-An Fan[1], Christine Peijinn Chai[1], Chun-Ying Huang[2], and Chin-Laung Lei[1]

[1] Department of Electrical Engineering, National Taiwan University
[2] Department of Computer Science and Engineering, National Taiwan Ocean University

Abstract. Advanced metering infrastructure (AMI) is drawing more and more attention due to various benefits which it brings. Compared to traditional power grid systems or advanced meter reading (AMR) systems, AMI systems possess capabilities to provide improved management and predictability of power utilization, to monitor and detect fault occurrences, and to conserve energy.
However, behind the various benefits brought by AMI, there still exist plenty of security threats. The open network used by AMIs is an extremely convenient interface for malicious attackers or network hackers to damage the AMI systems; on the other hand, the immature hardware design for AMI devices might cause physical breach points.

Keywords: Advanced metering infrastructure, smart grid, security, vulnerability

1 Introduction

The advanced metering infrastructure (AMI) deployed globally nowadays will change our viewpoints on energy utilization forever. It provides precise, efficient, and low cost energy management via various services such as dynamic pricing, automatic meter reading, on demand energy delivery, and quality of services (QoS) control. All these services and benefits are enabled by the necessary communication and control functionalities provided by this new infrastructure.

In the meantime, the AMI also introduces new security threats due to semi-open networks, improper security mechanisms and immature hardware design for AMI devices. The essence of AMI is a vast and distributed sensor system which is tethered by the open Internet and some neighborhood networks (NANs) which can be open networks or close ones. It implies that anyone on the Internet might find their way to interfere the AMI, especially the Internet service providers (ISPs) who can possibly control partial or all of the connections in an AMI system. Besides, the computationally weak meters can be easily accessed by anyone who can stand before the meter, and this makes them vulnerable to compromise. Furthermore, even the internal threats which traditional power grid suffers still threaten the security of AMI.

There are already some works which address potential threats in AMI systems. [7], [12], and [14] provide an overview of AMI-related threats; [13] uses attack tree to analysis possible attacks for some particular goals; [11] describes rich attacking methodologies along with recommends of design to smart meter vendor; [4] proposes a blueprint for an AMI-specific IDS.

In this work, we will not only review potential threats exist in AMI environments which [7], [12], and [14] have done, but also discuss about possible impacts and solutions for each of the common vulnerabilities. This paper is organized as follows. We will describe an overview of AMI systems in Section 2 and present related security requirements in Section 3. The common vulnerabilities along with some real world cases and possible solutions are introduced in Section 4. And finally we conclude the security threats in Section 5.

2 AMI Overview

Figure 1 shows an overview of an AMI environment. An AMI system consists of at least smart meters, collectors, neighborhood area network (NAN), backhaul network, and AMI head-end.

2.1 Smart Meter

Smart meters are used to monitor, record, and report back on energy consumption and other related events. Besides, they are also responsible for receiving commands and reporting results.

2.2 Collector

A collector acts as a network gateway of NAN. It collects data from smart meters and forward messages for smart meters and AMI head-ends.

2.3 Neighborhood Area Network (NAN)

An NAN connects smart meters and collectors. It provides routes for smart meters and collectors to transmit messages.

2.4 Backhaul Network

This network provides routes for information to be transmitted between collectors and AMI head-ends.

2.5 AMI Head-end

This system acts as an I/O interface of an AMI system. It mainly deals with the information exchange between the AMI system and other systems, such as Meter Data Management System (MDMS), which manages all the meter data in a centralized or distributed fashion.

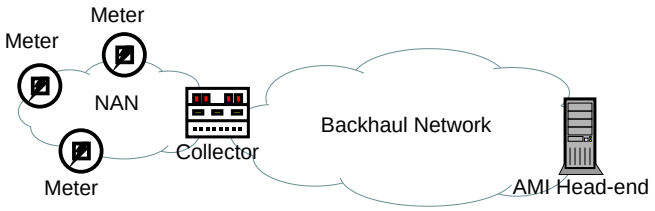

Fig. 1. The overview of AMI system

3 AMI Security Requirement

Generically, the basic security requirements of an IT system are confidentiality, integrity, availability, and non-repudiation. In this section, we will discuss the four security requirements for each of the AMI components.

3.1 Confidentiality

The major concern of confidentiality in an AMI system is the privacy of customers. The reason is that most data transferred between each components of an AMI system are related to customers' behavior. For example, the energy consumption of some particular time intervals of a day will provide a rough sketch of a specific customer's daily schedule.

Smart Meter. The major concern for a smart meter is privacy. Customers may not feel happy if their patterns of energy usage or other information can be accessed by unauthorized entities. Thus, there should be adequate protections adopted to protect smart meters from unauthorized accesses such as reading data from internal memory by compromising the smart meter. For example, smart meters should be installed in hidden locations and show no privacy-related information. Besides, if data backup is a routine of the backend MDMS, destroy all stored data is a possible solution to preserve confidentiality for smart meters when they are going to be compromised physically.

Collector. The situation of collectors is similar to smart meters. Besides, the collector should never allow unauthorized accesses to the data stored in the collectors.

NAN. The information transmitted in NAN might be wiretapped by malicious adversaries or curious neighbors easily. Thus, those pieces of information should be protected by proper mechanisms such as encryption with sound key management.

Backhaul Network. The backhaul network suffers similar problems as NAN from the aspect of confidentiality.

AMI Head-end. As an interface between the AMI system and other external systems, the AMI head-end should assure the confidentiality of customer

information. It should adopt proper access control and authentication mechanism to enforce that every single access to customer information is authorized, wherever the access request comes from.

3.2 Integrity

The integrity requirements of AMI mainly aim at the integrity of data and commands. There should be no unauthorized modification of meter data to occur and no unauthorized control command to be executed.

Smart Meter. The smart meters should possess capabilities to verify the integrity of received commands to prevent themselves from executing unauthorized control command. Ideally, a smart meter should protect its data against any unauthorized modification to preserve the integrity of energy-consumption data or other related information. However, smart meters are located in somewhere outside the energy provider's control; it is hard to guarantee the safety of smart meters. Thus, the main target here is to detect any unauthorized change of meter data. Once unauthorized changes of meter data can be detected, the energy provider can take their action to deal with these problems.

Collector. Similar to smart meters, collectors may be located in unsafe places. Thus, the capability to detect unauthorized changes of collector data is the most important issue from the aspect of integrity.

NAN. The connective network between smart meters and collectors might be open and suffer from various attacks which occur in traditional network environments. Thus, all data and commands transmitted over NAN should be properly protected by some mechanisms such as digital signature to provide each ends of a connection the ability to detect any unauthorized change of the transmitted information.

Backhaul Network. The collectors and the AMI head-ends are tethered by open backhaul networks. This nature makes it almost impossible to prevent unauthorized change of transmitted data. Again, the most important issue here is the way to detect unauthorized changes of data.

AMI Head-end. The environment which AMI head-ends are located in is relatively safer than other components of AMI. However, the major threats come from insiders instead of malicious attackers outside. The insiders may possess skill and knowledge to modify various data such as pricing information or issue control command such as meter connect and disconnect. The threats caused by insiders may be much more serious than any other threats, because the insiders know exactly what they are doing and how to deal most damage before being detected. Moreover, the insiders may be able to corrupt security certificate in order to launch attacks from any point in the AMI system.

3.3 Availability

In the past power grid, the availability of data is not a critical issue due to the predictability and monotonic type of data. Since all data needed by past power

grid are energy-consumption records alone, and they can easily be predicted by past behavior of energy usage, the energy provider can estimate the amount of energy used when the data needed are temporally unavailable. However, the situation is totally different in AMI environment because of the diversity of data which flow across every single component in AMI. In the AMI system, the lack of availability might cause fatal result.

Smart Meter. Smart meters will inevitably undergo some hardware failure, software fault, and even malicious command tempering. All these problems are difficult to prevent because the locations of smart meters may not be safe. We can certainly perform regular maintenance of hardware and software to reduce the frequency and effect of failure, but there is still some other possibility such as contrived damage on smart meters to bring the availability down. Thus, the focus here should be how to reduce the effect and how to detect the loss of availability. Redundancy of is always a method to increase availability. However, the redundancy of smart meter should be carefully designed to keep both synchronization and independence. Besides, periodical reporting is a naïve but effective method to monitoring availability.

Collector. Similar to smart meters, but the unavailability of a collector might cause more critical problems than a smart meter. Thus, the collectors should possess backup hardware devices and reserved bandwidth to maintain the functionality when they are temporally unavailable. Moreover, methodologies used in load-balancing of network traffic may also be possible solutions.

NAN. The unavailability of an NAN will make multiple smart meters unreachable via network. The reasons which paralyze an NAN might be the overload of traffics, the interference of radio waves, the damaged circuit, and etc. Among these reasons, the overload of traffics is the most important because the easiness of launch an attack to stuff the NAN with useless packets. Thus, a well-designed quality of service (QoS) management should be applied to the NAN to manage the availability. Besides, the NAN should provide multiple routes or media between the collector and any of the smart meters to reduce the impact of media failure.

Backhaul Network. Although the open backhaul network such as Internet extends the interface which attackers can access to, the open backhaul network indeed provides a more reliable and available channel between the AMI head-ends and collectors. However, this open network might also partially fails due to mistakes inside some Internet service providers (ISPs). To keep sufficient availability, one should have some kinds of QoS guarantee in his service level agreement (SLA) with the ISP he uses.

AMI Head-end. The availability issue at the AMI head-end depends on the role it plays in the AMI system. If the AMI head-end takes charge of control command forwarding, on demand request forwarding, or even more, issuing control command, then the unavailability of the AMI head-end will be a disaster. Once again, at the AMI head-end, the most important issue is to enforce fine grained access control policies and mechanisms to restrain insiders from accessing any resource without authorization and going a step further to spoil the availability.

3.4 Non-repudiation

Non-repudiation is a critical issue in almost all kinds of transactions, and the AMI system is not one of the exceptions. Generically, the non-repudiation should cover data content, control command, on demand request, and precise time which are sourced from all participants of an AMI system. However, those data themselves also suffer the issues of integrity and availability.

Smart Meter. The charge for energy usage is based on data from smart meters. Thus, all modifications to meter parameters including time, energy-usage record, control commands, and result of command execution should never be denied. Although the non-repudiation is usually achieved by digital signature in traditional IT environment, it might be a big problem for smart meters to sign a digital signature due to the lack of computing power. Some lightweight signatures such as BLS signature [5] may ease the computing load, though they may also be impractical.

Besides, combining digital signature and message authentication code (MAC) is also a possible solution which minimize the computation needed to be performed by smart meters. A smart meter can use a signature on a pre-defined message, such as date, as its MAC-key to generate MAC of generated data as follows:

$$MAC_K(data), K = sig_{sk}(date),$$

where sk is the secret key of the meter,and sign on the previously generated MACs when needed:

$$sig_{sk}(MAC_K(data_1) \oplus MAC_K(data_2) \oplus \ldots \oplus MAC_K(data_n))$$

Thus, one can check the non-repudiation by verifying the signature on the pre-defined message, the correctness of the MACs, and the signature on the MACs.

Collector. Similar to smart meters, all control commands issued by collectors should never be denied. Besides, all responses to control commands should also be stored for future audit. Again, the issue of computing power might also exist in collectors.

NAN. One in an AMI system may claim that he had sent out certain messages which he never sent and blame the unreached messages on the failure of the network. On the other hand, one might claim that he did not receive certain messages even if he actually received it. To prevent these situations, the nodes on the network path may randomly store some packets as evidence of transmission. Moreover, the two ends of any single connection which carries critical message should also take the responsibility to enforce the non-repudiation of transmission.

Backhaul Network. Packet loss is always a problem in all kinds of open networks. The same problems in NAN also exist in backhaul network with a much larger scale. By using services which provide digital receipts for certain kinds of connections which carry critical messages with higher charge

of service, this problem might be eased. Besides, not only the both sides of any single network connection, but the network itself, should also take the responsibility to enforce the non-repudiation of transmission. Again, for applications such as AMI systems in which the reliability of networks is a major concern, one should ensure that there are QoS guarantees in his SLA with the ISP he uses.

AMI Head-end. The AMI head-end is responsible for summarizing all stored data in the AMI system, including time-synchronized event records such as energy consumption data or control commands. Thus, the AMI head-end should take the responsibility to verify the non-repudiation of every single record. Besides, if the AMI also issues or forwards control commands to collectors or smart meters, all the control commands should also satisfies the non-repudiation requirement.

4 Vulnerabilities

The weakest points for AMI systems should be smart meters and collectors along with the NAN which they are located inside. The reason is that devices in this part of AMI system are directly exposed to attackers and can physically be accessed with lesser effort compared to devices in AMI head-ends. Thus, in this section, we will mainly focus on some common vulnerabilities which exist between devices inside NAN.

4.1 Plaintext Traffics inside NAN

Some meters may possess no encryption capability to reduce the cost of meter. Under this condition, an attacker can just wiretap the NAN to get the information he needs. The degree of privacy leakage depends on the type of information leaked. The most straightforward solution to this vulnerability is to choose smart meters which possess adequate capability to process encryptions with sufficient key-length.

4.2 Bus Wiretapping

Many embedded systems leverage external communication modules to deal with communication problem. Besides, many communication modules implements hardware cryptographic module to encrypt or decrypt data transmitted for the sake of efficiency. However, it will be under the risk of wiretapping if the smart meter leaves the tasks of encryption and decryption to the communication module. The reason is very simple; the data flow on the bus which connects a processor and a communication module will exist in a plaintext fashion. Thus, one can possibly wiretap the bus directly to gain whatever information he want. Therefore, either physical box-open detection should be enabled or all sensitive data to be transmitted should be encrypted before they leave the processor if necessary.

4.3 Insecure I/O Interface

Optical communications such as infrared often require both ends of a communication to be close and may be regarded as secure channels. Thus, the hardware vendor might pay less attention to the optical interfaces. However, this could cause the leakage of meter data due to the lack of protection for the optical interfaces or leak information about authorized staff by a compromised smart meter. Even for physical I/O interfaces such as optical port, the authentication of identity and access control of data should be carried out.

4.4 Weak Key Derivation and Flawed Pseudo-random Generator

Many cryptographic protocols and their implementations rely on the randomness of pseudo-random generator. For example, OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based systems uses flawed random number generator, which leads to the predictability of cryptographic keys [3]. Thus, one should choose his pseudo-random generator very carefully while implement any practical system.

4.5 Improper Re-use of Key

Improper re-use of key-streams will make it possible for any attackers who observed a plaintext-ciphertext pair to decrypt another ciphertext, especially in stream cipher. An example occurred on Windows NT 4.0, which enabled the offline dictionary attack against the Windows NT password database [1]. One should avoid the re-use of keys. In the case of stream cipher, one should choose sufficient initial vectors (IVs) with sufficient bit-length and keep changing the IVs.

4.6 Lack of Protection against Replay Attack

Some implementations of cryptographic tools only check the correctness of decryption to verify the validation of authentication. However, without checking time-related information such as sequence number or timestamp, the tools will be vulnerable to replay attack. Attackers will have their chance to pass authentication by replaying previously captured authentication data. One example of this kind of vulnerabilities happened on FreeBSD. The IPsec originally prevents replay attack by verifying sequence numbers. However, a programming error in the fast_ipsec(4) implementation [2] allows packets to unconditionally pass sequence number verification checks [8]. The implementation of any mechanism which is possibly under the threat of replay attack should also implement the check on time-related information or use challenge-response mechanism with unique challenge for every single session.

4.7 Insecure Encryption Mode

Some encryption modes are relatively weak, such as ECB mode of AES. The ECB mode will encrypt the same plaintexts into exactly the same cipher with the same encryption key. Thus, one can infer that the corresponding plaintexts of two ciphers are the same if he observed two identical ciphers. One should avoid these encryption modes when implementing a practical system.

4.8 Weak Protection of Integrity

Some encryption algorithm use extra integrity check vector (ICV) to validate the integrity of encrypted data. However, attackers can possibly arbitrarily modify encrypted data or even decrypt cipher successfully by preserving valid ICVs. A real-world example is the Temporal Key Integrity Protocol (TKIP) used by IEEE 802.11i [15]. A short rekeying time might reduce the impact of this vulnerability.

4.9 Insufficient Key Length

Insufficient key length is always vulnerable in any implementation of encryption algorithms. For example, DES can be cracked in 12 hours [10], and the modulus of RSA 512-bit can be successfully factored in seven months using Number Field Sieve (NFS) [6]. We suggest using elliptic curve cryptography (ECC) instead of finite field cryptography (FFC) such as Digital Signature Algorithm (DSA) and integer factorization cryptography (IFC) such as RSA to reduce necessary key-length for smart meters. If ECC is adopted, the key-length should be at least 224-bit nowadays instead of 2048-bit in FFC and IFC [9].

4.10 Passwords and Keys Stored in Meter

It is a common way to pre-distribute some keys on sensor nodes in wireless sensor network (WSN). As a similar scenario, the smart meters in AMI systems also possess some pre-distributed keys or passwords to perform cryptographic operations such as authentication or encryption. However, those pre-distributed keys or passwords will cause potential threats once some smart meters are compromised. Attackers can use those pieces of information to corrupt some part of the AMI system. Besides, depending on the key update mechanism used, it is possible for attackers to get the up to date keys and passwords of a corrupted smart meter. We suggest multi-factor authentication for logical access control and some physical protections which can destroy pre-distributed keys and passwords when a physical attack is detected.

4.11 Key Distribution and Management

Because the scale is extremely huge for an AMI system, the key distribution and key management become troublesome problems. It is nearly possible to maintain a unique pairwise key between each components of an AMI system. Thus, an old

problem occurs in WSNs is coming back again in AMI systems. The problem is that an attack can corrupt some part of the entire system by compromise a single smart meter (or a sensor node in WSN). The reason is that there exist shared keys between certain numbers of smart meters. The worst case might be that a group of smart meters, which are geographically nearby, share the same symmetric key for rekeying. Thus, attackers can possibly impersonate whichever nearby smart meter he wants by compromising a single smart meter. The entire AMI system should be divided into smaller areas geographically and the keys shared by any pair of components in the same small area should be unique in the area.

4.12 Weakness of Time Service

Time synchronization is an important task for distributed systems such as AMI systems. The most common ways to synchronize distributed devices may be network time protocol (NTP). However, it is subject to man-in-the-middle attack and time server impersonation. We recommend that smart meters should verify the sources of all time-related configurations.

4.13 Attacks or Omissions inside the AMI Head-end

Insiders are always a problem in any organization. The attacks launched by insiders or insiders' omissions may cause enormous damage to the AMI system. To reduce the impact of these conditions, separation of duty, authentication, and fine grained access control should be enforced.

5 Conclusion

In this paper, we summarize the security requirements and common vulnerabilities to address security threats in AMI systems. Besides, we also discuss possible solutions to the vulnerabilities.

There is still a long way to go for the AMI systems, while the functionalities, standards, and security threats are still worked out. Our suggestion to smart meter vendors, designers, and manufacturers is to avoid at least all the mistaken assumptions and design flaws mentioned in Section 4. Besides, the deployment of smart meters and related devices such as collectors should be very careful to reduce possible physical threats. We also suggest that power providers should exam that if their AMI solution provider provides an in-depth implementation including but not limited to the cryptographic issues discussed in Section 4. Still, there is a long way to go for us to perfect the security of AMI systems, but every discussion and every piece of effort will gradually enhance them.

Acknowledgements. This study is conducted under the "Advanced Metering Infrastructure (AMI) Enhancement Project" of the Institute for Information Industry which is subsidized by the Ministry of Economy Affairs of the Republic of China.

References

[1] Microsoft security bulletin (ms99-056) (December 1999), http://www.microsoft.com/technet/security/bulletin/ms99-056.mspx

[2] Manual reference pages - fast_ipsec (4) (January 2003), http://www.gsp.com/cgi-bin/man.cgi?section=4&topic=fast_ipsec

[3] Vulnerability summary for cve-2008-0166 (May 2008), http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0166

[4] Berthier, R., Sanders, W., Khurana, H.: Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. In: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on. pp. 350 –355 (oct 2010)

[5] Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. J. Cryptol. 17, 297–319 (September 2004)

[6] Cavallar, S., Dodson, B., Lenstra, A.K., Lioen, W., Montgomery, P.L., Murphy, B., Riele, H.T., Aardal, K., Gilchrist, J., Guillerm, G., Leyland, P., Marchand, J., Morain, F., Muffett, A., Putnam, C., Putnam, C., Zimmermann, P.: Factorization of a 512-bit rsa modulus. In: Proceedings of the 19th international conference on Theory and application of cryptographic techniques. pp. 1–18. EUROCRYPT'00, Springer-Verlag, Berlin, Heidelberg (2000)

[7] Cleveland, F.: Cyber security issues for advanced metering infrasttructure (ami). In: Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE. pp. 1 –5 (july 2008)

[8] Dawidek, P.J.: Ipsec replay attack vulnerability (March 2006), http://security.freebsd.org/advisories/FreeBSD-SA-06:11.ipsec.asc

[9] Elaine Barker, William Barker, W.B.W.P., Smid, M.: Recommendation for key management part 1: General (revision 3). Tech. rep., National Institute of Standards and Technology (2011)

[10] Kelly, S.: Security implications of using the data encryption standard (des) (December 2006), http://www.ietf.org/rfc/rfc4772.txt

[11] Matthew Carpenter, Travis Goodspeed, B.S.E.S.J.W.: Advanced metering infrastructure attack methodology. Tech. rep., InGuadians (2009)

[12] McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. IEEE Security and Privacy 7, 75–77 (2009)

[13] McLaughlin, S., Podkuiko, D., McDaniel, P.: Energy theft in the advanced metering infrastructure. In: Proceedings of the 4th international conference on Critical information infrastructures security. pp. 176–187. CRITIS'09, Springer-Verlag, Berlin, Heidelberg (2010)

[14] Parks, R.C.: Advanced metering infrastructure security considerations. Tech. rep., Sandia National Laboratories (2007)

[15] Tews, E., Beck, M.: Practical attacks against wep and wpa. In: Proceedings of the second ACM conference on Wireless network security. pp. 79–86. WiSec '09, ACM, New York, NY, USA (2009)