A Qualitative Risk Analysis of Smart Grid Security Protocols

Mustafa Saed
Electrical and Computer Engineering
University of Detroit Mercy
Detroit, USA
email: saedma@udmercy.edu

Kevin Daimi and Nizar Al Holou
College of Engineering and Science
University of Detroit Mercy
Detroit, USA
email: {daimikj, alholoun}@udmercy.edu

***Abstract*— Recently, smart grids have been attracting enormous interest as the Internet continues to rapidly expand. A smart grid embeds Information Technology (IT) in its transmission networks to become two way communications. This was achieved by installing dedicated devices, such as a smart meters and related software. A smart grid provides efficient usage of electric power and energy-saving that is passed down to the consumer. Furthermore, in a smart meter, which is an essential component of a smart grid, an individual's behavior can be indirectly understood, for example, by examining the utilization status of electric power at homes. However, such handling of a smart meter is problematic in terms of privacy protection and other security concerns. To this end, this paper performs a risk analysis of a number of proposed security protocols for smart meters in smart grid networks. In this analysis, four different vulnerability types are identified. These vulnerabilities are augmented by four types of attackers and seven types of attacks that exploit those them. After assessing the likelihood and impact levels for all the different combinations of vulnerabilities, attacks and attackers, a risk matrix for various risk levels is exploited. Overall findings include nine low risks, six medium risks, and three high risks in some of the proposed security protocols for smart meters in smart grid networks. Finally, appropriate mitigation techniques for different risks are suggested.**

Keywords*— *Risk Analysis; Communication Protocols; Smart Meters; Smart Grid; Risk Matrix

I. INTRODUCTION

In order to operate efficiently, power generation and distribution companies need to predict future energy consumption. This prediction is typically based on historical household energy consumption patterns [1][2]. Accurate prediction is essential to reduce unnecessary power generation, leading to financial savings and reduced carbon dioxide emissions. Different time periods for collecting energy data result in different electricity costs. The tendency of consumers to reduce their power demand in response to high electricity prices [3] is a useful tool for demand side managers. In addition, the bidirectional communication capability of smart meters enables the monitoring and control of all household appliances to reduce energy consumption at the customer site [1]. The analysis and prediction of energy consumption involves processing large amount of data from networks of smart meters. A smart grid network is a special type of an ad hoc network where smart meters are needed. Such a network is very appealing in the modern era since it allows for many amazing applications, such as event correlation (network and substation level of the power distribution of smart grid) and scheduled load shedding [4]. For this new type of networks, classical secure communication protocols over the Internet infrastructures, such as Transport Layer Security (TLS) [5] and IPsec [6], may not be sufficient due to the dynamic topology of these networks. There are a number of contributions to protect the two-way direct and indirect communication of smart meters with collectors in smart grid through the introduction of two cryptographic protocols based on PKI. Nonetheless, introducing new protocols always increases the attacking surfaces.

In network security, risk analysis is a process of defining and analyzing the threats to the security protocols, as well as the infrastructures and the entities that these protocols operate on [8]. It is a combination of identifying potential vulnerabilities and attacker, and accessing impacts of the attacks. The goal of such an analysis is to produce a qualitative risk analysis document and optionally a mitigation plan that offers guidance to security architects and related business decision makers. The National Institute of Standards and Technology (NIST) provide guidelines on how to perform a risk analysis [9]. This will be followed in this paper.

Risk analysis and management is an important field of research in network security. There are mainly two ways to conduct such analysis, namely qualitative and quantitative.

The approach taken in this work is of the qualitative type. Some work on quantitative analysis is presented in [10][11]. As emphasized in [10], current industry standards for estimating cybersecurity risk are based on qualitative risk matrices. Lee et al. [12] performed an analysis of the risk of the bit-flipping attack, which might occur in LoRaWAN, a Media Access Control (MAC) protocol for Wide Area Networks, where one can change specific fields on ciphertext without decryption. Another interesting work is presented by Jacobson et al. [13] in which they dealt with risk analysis of a smart home automation system. Among all those efforts, the analysis in Cherdantseva et al. [14] is particularly interesting. The authors introduced risk assessment methods for SCADA systems related to the underlying DNPsec protocol to be used in secure communication protocols. The DNPSec is a security

 ISBN: 978-1-61208-635-4

framework of Distributed Network Protocol Version 3 (DNP3) [15][16]. DNP3 is an open and optimized protocol developed for the Supervisory Control and Data Acquisition (SCADA) Systems supporting the utilities industries.

This paper attempts to facilitate the reduction of various risks associated with some proposed smart grid security protocols. To this end, a risk assessment method to comprehensively analyze a smart meter in smart grid and countermeasures for such risks is proposed. To achieve this, a list of vulnerabilities, attacks and attackers is created. This is followed by assigning the likelihood and impact of vulnerability, attack and attacker for each combination. Finally, a risk matrix is used to evaluate risks given the likelihood and impact levels. Once all the risks have been evaluated, a necessary next step is to address all the medium and high risks. For completeness, some recommendations for managing low risks for these protocols are also stated.

The reminder of the paper is organized as follows: Section II provides an overview of a number of recently proposed smart meter security protocols together with the security tools, techniques, and methods used by them. Section III reviews the types of vulnerabilities, attackers, and attacks attracted by these vulnerabilities. Section IV describes the risk analysis of the security protocols. The countermeasures of proposed security protocol risks are considered in detail in Section V. Finally, Section VI sets the conclusion and describes future work.

II. SMART GRID PROTOCOLS OVERVIEW

Smart grids subsystems and components can be protected and their security enhanced via cryptographic software and hardware, and other security techniques. In order to prepare the grounds for the risk analysis and mitigation methodologies introduced in the next sections, the security techniques, tools, methods and approaches followed by various researchers in the field of smart grid security will be briefly introduced. These will represent the input to the qualitative analysis addressed by this paper.

Saed et al. [7] presented security protocols for smart meters in smart grid. They proposed schemes for securing the direct and indirect smart meter-to-collector communications. The schemes are based on PKI. The authors proposed two different security protocols to enhance the security of the direct communication between smart meters and collectors in a smart grid. The first proposal secured direct communication without using the certificates and relied on public key cryptology. The second proposal protected the direct communication by using certificates and also depended on PKI. On both protocols, the substation is only directly connected to the collector. They further proposed an approach for the indirect communication between smart meters and collector. In this approach, the collector (gateway) should have initially received all the public keys and identities of the smart meters (user node). On the other hand, the smart meters should have the public key of the collector using any secure process. Furthermore, the predecessor and successor nodes are identified during installation and configuration of each smart meter. These protocols are design to provide secure communications among the three entities: a server (Substation), which is a supervisory node acting as a centralized authentication center or a Certificate Authority (CA); multiple center gateways (Collectors) that provide connectivity to the user nodes (smart meters); and multiple nodes that are essentially smart meters. The purpose of those communications is to allow a node (smart meter) to provide information, such as temperature readings, and electricity consumptions, to the gateways. To facilitate secure and authenticated communication between a node and a center gateway, the server acted as a Certificate Authority to authorize nodes and gateways. These protocols are expected to run over the DNPSec.

Dong et al. [17] proposed a protection scheme for the automation of smart grid system and patch distribution from the control center to data transmission security. Some of the functions were tested on the simulation platform through intrusion detection system and by using field devices, such as smart meter. Their proposal considered the security within smart meter but not for the smart meter communication, such as smart meter to smart meter and smart meter to collector [18]. Furthermore, their proposed protection system did not use digital signature to protect against forgery.

The sparse topology information of the smart grid was utilized by Giani et al. [19] to determine the attack meter sets. However, their work lacked the discussion of the system matrix acquisition. In fact, the design of the attack vector relied heavily on precise knowledge of the system matrix. In this case, it would not be easy to obtain such confidential information for an attacker who has limited access to the smart grid. Overall, a feasible unobservable attack scheme based on the incomplete system matrix has not yet been fully investigated. The authors in their proposal weren't covering the smart meter communication attack. They only mentioned for the possible vulnerabilities related to attack meter in physical layer.

Li et al. [20] presented an efficient and robust approach to authenticate data aggregation in smart grids. Aggregation refers to the communication between the smart meters and the collector. This is achieved via deploying signature aggregations, implementing batch verification, and signature amortization schemes to reduce communication overhead and number of signing and verification operations and provide fault tolerance. The authors proposed an efficient authentication scheme for power usage data aggregation in Neighborhood Area Networks (NAN) and smart meter to collector communications. The contributions for this work were represented by deploying digital signatures so that when the collector is out of service, alternative or backup collectors can execute the authentication approach without any additional configuration or setup. Their research also

 ISBN: 978-1-61208-635-4

sought to reduce the number of signature and verification operations. However, the research is limited to authentication only. Thus, they are not securing the messages (readings) between smart meter and collector.

Many of the available schemes for both single-path and multipath routing are not suitable for meshed Advanced Metering Infrastructure (AMI) network [21]. Consequently, a security mechanism for multipath routing based on Elliptic Curve cryptology, digital signature, and Message Authentication Code (MAC) for such an AMI network was introduced. This approach allowed the Certificate Authority to execute a lot more work than it normally should do (issuing certificates). The extra load included controlling the nodes' creation of public and private key. In this scheme, nodes (smart meters) performed a number of computations despite their known limited computing power. This also tended to slow the system. Furthermore, having a smart meter sending its information to all the neighboring smart meters with no protection at all would introduce an immense threat. This provides a potential attacker the opportunity for attacking more than one target (smart meter) as they all have the information of the source meter. Therefore, the neighboring nodes acted as intermediate nodes, and consequently performed more calculations and broadcasting of the results. This means all other nodes (smart meters) have now the information. This implies, there are many nodes that the attacker can try and many nodes will be affected.

Yan et al. [22] introduced an interesting security protocol for AMI communications in smart grid where the smart meters are interconnected through wireless network. Their techniques indicated that the Public Key Infrastructure (PKI) is not desirable and relied on symmetric key cryptology instead. However, the number of symmetric keys used is large and possibly comparable to the number of keys should PKI have been followed. Furthermore, smart meters have limited capabilities, and therefore, verifying the MAC should have been left to the collector. The authors did not specify what would happen when the two MACs are not equal. This implies that the integrity of a meter's reading is not handled correctly.

Seo et al. [23] discussed the use of public key infrastructure (PKI) in smart grid and what security requirements need to be implemented in smart grid architecture including the smart meter to secure the smart meter communication in the AMI. The authors did not propose any security technique/protocols to secure the smart grid network but only provided a survey.

Zhao et al. [24] provided the fundamental limit of cyber-physical security in the presence of low sparsity unobservable attacks. It is shown in [25][26] that a complete system matrix can be identified using an independent component analysis method. Nevertheless, such attack schemes might not be easy to implement as all meter data are required to be known and all the meters are required to be controlled. On the other hand, several detection and defense schemes are provided based on the complete knowledge of the system matrix. The off-line method, based on the Kullback-Leibler distance, is proposed to track malicious attacks using historical data [27].

A distributed incremental data aggregation approach, in which data aggregation is performed at all smart meters involved in routing data from the smart meter to the collector unit, was introduced by Li et al. [28]. In this research, the authors presented an efficient information aggregation approach, in which an aggregation tree, constructed via breadth-first traversal of the graph and rooted at the collector unit, is deployed to cover all smart meters in the neighborhood. This protocol can let the control unit collect all smart meters' information in the area. Furthermore, to protect users' privacy, all information is encrypted by a homomorphic encryption algorithm. Since no authentication scheme is emphasized, the approach faces the potential risk that malicious smart meter can forge packets, thus causing the smart grid system to fail to detect or diagnose bogus data. Adversaries can maliciously forge their own data to manipulate the aggregation results.

TABLE I. LIST OF ACRONYMS AND SYMBOLS

Acronyms/Symbols	Meaning
A1	MITM
A2	Impersonation
A3	Single Point of Failure
A4	Key Escrow
A5	Cryptanalysis and Quantum Computer
A6	Forward Secrecy
A7	Downgrade Attack
CA	Certified Authority
DNP3	Distributed Network Protocol Ver.3
DNP3Sec	DNP3 Security
IKE	Internet Key Exchange
LoRaWAN	MAC Protocol for WAN
MAC	Media Access Control
MITM	Man-in-the-Middle
NIST	National Institute for Standard & Technology
OEM	Original Equipment Manufacture
PKI	Public-Key Infrastructure
QoS	Quality of Service
SCADA	Supervisory control and Data Acquisition
T1	Clover Outsider
T2	Knowledgeable Insider
T3	Non-Profit Organization
T4	For-Profit Organization
TLS	Transport Layer Security
V1	Lack of Authenticity
V2	Centralized Topology
V3	Weak Cryptography
V4	Misuse of Public Key Cryptography
WAN	Wide Area Network

III. TYPES OF VULNERABILITIES, ATTACKS AND ATTACKERS

In this section, the relevant building blocks of risk analysis are presented. First, the risk matrix, which determines the risk level given the likelihood and impact

levels of an attack being carried out by an attacker are introduced. Then, the different types of attackers, vulnerabilities and attacks are depicted. Some of the vulnerabilities presented here may not be applicable to these protocols but are otherwise common for other networks than smart grid. Table I presents a list of acronyms and symbols used in this paper.

A. Security Concerns

There are several security concerns for these protocols. The list below describes the completeness:

1) Loss of sensitive data: This could mean either user's personal data, or server/gateways (Substation/Collector) private data, or even statistical data that should be kept secret. Those data could be ephemeral, such as one-time session keys, or could have long term impact, such as user's credit card information or social security number.

2) Financial loss: This could indicate that the user is overcharged for services that she/he did not receive. For gateways (collectors), this could mean that the gateway did not receive the credit for the service it provided. It could also mean a malicious modification to financial data at the gateway, which incurs financial loss.

3) Denial of service (DoS): Certain attacks are able to disable partial or full part of the smart grid network, so that nodes (smart meters) do not receive services from gateways (collector). This kind of attacks may be localized, such as unauthorized access to specific smart meter at the same domain, or may also be global, such as unauthorized access to specific smart meter from different domain. Depending on the type of attack, DoS may last for a short or a long period. In addition, damage to the hardware is also a security concern here. However, this paper focuses on evaluating the secure communication protocol. Therefore, such a concern is beyond the scope of this paper.

B. Types of Vulnerabilities

Below different types of vulnerabilities are presented:

1) Lack of authenticity (V1): authenticity is missing in almost half of the protocol, namely, Section A of [7]. For the other half of the scheme, a certificate is used.

2) Centralized topology (V2): the protocol uses a centralized structure, where a single server (substation) is responsible for handling enrollment and certificates for all collectors and smart meters.

3) Weak cryptography (V3): A protocol may employ a weak cryptography that is vulnerable to cryptanalysis, or it may employ a strong cryptography that is secure against cryptanalysis today, but will be broken in the future. An example of the first case is SHA-1 hash function [29], and an example of the second case is RSA [30] or ECC [31] against cryptanalysis using quantum computer in the future. For the protocol to be analyzed, the underlying cryptography primitives are not specified [32]. That it deploys RSA or ECC based solutions is assumed, as well as SHA2 [33] or SHA3 [34] functions at a desired security level. This assures the protocol to be robust against today's cryptanalysis, but still render to the vulnerability of quantum cryptanalysis in future.

4) Misuse of public key cryptography (V4): the protocol uses public key cryptography to establish secure communication channels between entities. However, in modern cryptography [35], public key cryptography is usually used to establish a session key, rather than used directly for communication, in order to provide additional security features, as well as improved performances.

C. Types of Attacks

Attacks that exploit above mentioned vulnerabilities are described here:

1) Man-in-the-Middle (MITM) (A1)

MITM attacks are one of the most classical attacks in cryptography and network security. In Moore [36], the author gives a tutorial of MITM attacks. In terms of the MITM attacks against analyzed protocol, the following are observed:

a) Attacking strategy: the attacker secretly relays and possibly alters the communication between two parties, such as smart meter to collector who believe they are directly communicating with each other.

b) Assumptions: it is reasonable to assume that the attacker is able to passively eavesdrop the communication between two entities; it is however hard or infeasible for the attacker to break the authentication within real time.

c) Common vulnerability for this attack: lack of authentication methods, for examples, certificates and/or pre-shared keys.

d) Consequences: the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.

2) Impersonation (A2)

Impersonation is another classical attack in cryptography and network security [37]. The secure communication protocols with impersonation attack are analyzed as follows:

a) Attacking strategy: the attacker claims to be someone else, a legitimate user (smart meter) or a substation node.

b) Assumptions: the attacker is able to get the public keys and IDs from all entities (smart meter, collector and substation); but has no access to the secret keys.

c) Common vulnerability for this attack: lack of authentication methods, for examples, certificates and/or pre-shared key.

 ISBN: 978-1-61208-635-4

d) Consequences: the attacker convinced entities that he/she is a legitimate owner of an ID.

3) Single Point of Failure (A3)

Single point of failure attack is common in network securities [38]. The proposed protocols in [7] are analyzed with this attack due to the centralized network topology that the protocol employs:

a) Attacking strategy: the server (substation) is a single point of failure. The attacker focuses its resources to attack this single point rather than the whole smart grid system.

b) Assumptions: the attacker is able to break into the server (substation).

c) Common vulnerability for this attack: having a centralized structure

d) Consequences: Total compromising of the protocol.

4) Key Escrow (A4)

Key escrow attacks, as described in OH et al. [39], is a common attack in cryptography as observed in the following:

a) Attacking strategy: the server (substation) is responsible for authentication, so it is able to authenticate a fake user (smart meter) or revoke a legitimate user.

b) Assumptions: the server (substation) is malicious, or is compromised by the attacker

c) Common vulnerability for this attack: have a centralized structure

d) Consequences: Total control of the protocol

5) Cryptanalysis and Quantum Computing (A5)

This attack exploits the weakness in cryptography, using cryptanalytic methods, such as Shor's algorithm [32]:

a) Attacking strategy: use cryptanalytic tools (with quantum computers [20], if necessary) to break the existing cryptosystem.

b) Assumptions: the underlying cryptosystem is vulnerable to cryptanalysis and quantum computers.

c) Common vulnerability for this attack: RSA [30] and ECC [31] are both vulnerable to quantum computers.

d) Consequences: Total capturing of the protocol.

6) Forward Secrecy (A6)

Forward secrecy is a notion associated with network security and secures protocol designs [40]. The proposed protocols in [7], have the following properties:

a) Attacking strategy: once the attacker gains control of a session (through other attacks, for example, MITM), the session key is used to learn previous and future keys.

b) Assumptions: the attacker is able to learn the secret information of at least a single session.

c) Common vulnerability for this attack: a bad key update schedule; usage of statistical keys; lack of short term (one time) keys.

d) Consequences: the attacker steals secret information of entities (smart meter, collector and substation) causing all previous/future data to be at risk.

For completeness, the following attack is also presented. Currently, this is not applicable to the protocols in [7]. When these protocols will evolve in the future, and there will be more than one version available for use, this attack becomes applicable.

7) Downgrade Attack (A7)

This type of attack exploits the fact that some earlier version of the protocol uses weaker cryptography. For historical and legacy reasons, the current protocol needs to be able to communicate with those earlier versions [41].

D. Types of Attackers

It is important to model the attackers, as different attackers have different likelihood to launch attacks, and the consequences, even for a same attack, may vary for different attackers. Therefore, four types of attackers are considered in this risk analysis [42].

1) Clever Outsider (T1): Examples include a high school student, hacker, and researcher. Those types of attackers are usually limited to their knowledge of the underlying cryptography and the topology of the network. They are also likely to be constrained by the hardware they can access. For example, they are not likely to be able to launch attacks from multiple computers in parallel. In most cases, they are honest but curious. It implies that they will only exploit vulnerabilities that are exposed to them; they will not actively look for vulnerabilities. The goal of their attack is usually financial gains or publicity.

2) Knowledgeable Insider (T2): Examples include a disgruntled employee. Unlike outside attackers, inside attackers are much more knowledgeable of the required skills to launch attacks. They are also more capable of identifying critical point of the network in order to maximize the impact of the attack. However, inside attackers work alone, as they are not organized (c.f T3 and T4) and do not want to be identified. Therefore, just like T1 attackers, they are also likely to be constrained by the hardware they can access. In addition, it is safe to assume that they are malicious. They know about all the vulnerabilities of the protocol. The goal of their attack is usually financial gains and vengeance.

3) Non-Profit Organization (T3): Examples include research groups, and collaborators on the Internet. Those are potentially at large scale organized groups,. Therefore, these groups consist of experts in the related area. Since they are large scale organizations, they are able to launch distributed and parallel attacks. As non-profit organizations, the goal of their attack is usually research or charity oriented publicity.

4) For-Profit Organization (T4): Examples include a competitor Original Equipment Manufacturer (OEM) and a tier-1 supplier. Similar to T3 attackers, being large

organizations means they have access to all sorts of resources related to the attack, including both the required skills and knowledge, and necessary equipment's. In addition, since they are profitable organizations, it is also possible for them to hire/buy additional resources to maximize the impact of their attacks. Those attacks are usually profit-oriented.

IV. RISK ANALYSIS

In this section the risk analysis of the security protocols will be described.

A. Risk analysis metrics

In carrying out the risk analysis, it is important to de-couple the assessments of likelihood from that of impact, otherwise the same factor would be counted twice. However, doing this, in general, is rather difficult. The likelihood of an (vulnerability, attack, attacker) combination is assessed, and only look at factors like, for the level of difficulty needed by the attacker to exploit the vulnerability, and if the attacker requires some special tools/knowledge. On the other hand, when assessing the vulnerability of the combination (vulnerability, attack, attacker), it is already assumed that the exploitation of the vulnerability is possible, and then try to determine the impact in terms of loss in Quality of Service (QoS) or financial impact. The following metric are adopted in this paper:

1) Low: Assigned when compromising a small part the network, and incurring minimal or no financial loss.

2) Medium: Allocated when compromising a large part of or the whole network for a limited time, and incurring some financial loss;

3) High: Vilified when compromising a large part or the whole network for a very long time or compromise of sensitive information like private keys, credit card numbers, and incurring significant financial loss.

Table II shows the risk matrix that maps a (likelihood, impact) combination to a risk, all of them have three levels: low, medium and high. Throughout this paper, this table will be used to determine the risk level [43].

TABLE II. RISK MATRIX

Impact	**Likelihood**		
	Low	***Medium***	***High***
Low	Level=Low	Level=Low	Level=Medium
Medium	Level=Low	Level=Medium	Level=High
High	Level=Medium	Level=High	Level=High

B. Detailed risk analysis

In the following subsections, a detailed risk analysis of every possible combination of vulnerabilities, attacks and attackers is carried out. A summary of the risk analysis is presented in Table III. It is worth mentioning that there are 112 combinations (4 vulnerabilities x 7 attacks x 4 attackers). As different combinations of vulnerabilities, attacks and attackers, vulnerabilities are not independent of attacks example, the combinationV1 and A3 is not a valid one since a single point of failure attack cannot exploit the protocols lacking authenticity vulnerability. This paper will concentrate on the most common combinations.

1) (V1, A1, T1): To carry out an MITM attack, an attacker requires the knowledge of the underlying cryptography, network topology, and protocol design. A clever outsider is unlikely to possess all this knowledge. For example, if the attacker does not know the topology of the network, they cannot easily identify a gateway (collector), or the link from a smart meter to the collector. Therefore the likelihood is assigned to be low. In terms of impact, a clever outsider is unlikely to compromise more than one segment of the smart grid network at a time, which would incur minimal financial loss. Here, the impact to be also low. Hence, the risk is low.

2) (V1, A1, T2): As stated in IV-B-1, this attack requires the knowledge of the underlying cryptography, network topology, and protocol design. A knowledgeable insider is likely to possess some, if not all, of this knowledge. The likelihood is assessed to be medium. Just like IV-B-1, a knowledgeable insider is unlikely to compromise more than one segment of the smart grid network at a time, which would incur minimal financial loss. So, the impact will be stated low. Accordingly, the risk is low.

3) (V1, A1, T3): Compared to IV-B-2, a non-profit organization is also likely to possess some, if not all, knowledge of the underlying cryptography, network topology and protocol design. However, unlike IV-B-4, the motivation for such an attacker is not strong. Such an attacker is mainly interested in personal gains, such as producing research papers or personal publicity. Therefore, the likelihood is stated to be medium. In terms of impact, a non-profit organization has the capability to compromise a large part of the smart grid network at a time, which would incur a non-negligible financial loss. The impact is assessed to be also medium. Hence, the risk is medium.

4) (V1, A1, T4): A for-profit organization is likely to possess all the required knowledge for this attack. In addition, the motivation of such an attacker is quite strong. Usually, such an attacker will have financial interest and brand reputation. Therefore, the likelihood is high. Just like IV-B-3. A for-profit organization has the capability to compromise a large part of the smart grid network at a time, which would incur a non-negligible financial loss. Consequently, the impact is set to medium. Hence, the risk is high.

 ISBN: 978-1-61208-635-4

5) (V1, A2, T1): Similar to an MITM attack, an impersonation attack, require an attacker to be knowledgeable of the underlying cryptography and protocol design. A clever outsider is unlikely to possess all this knowledge. This implies the likelihood should be low. The impact of this attack is also similar to that of MITM attacks. A clever outsider is unlikely to compromise more than one segment of the smart grid network at a time. A minimal financial loss is expected. The assessment of the impact is low. Hence, the risk is low.

6) (V1, A2, T2): A knowledgeable insider is likely to possess some, if not all, of required knowledge, so, the likelihood is medium. Just like IV-B-5, a knowledgeable insider is unlikely to compromise more than one segment of the smart grid network at a time, which would incur minimal financial loss, Therefore, the impact is assessed to be low. Hence, the risk is low.

7) (V1, A2, T3): A non-profit organization is likely to possess some, if not all, of the knowledge of underlying cryptography, as well as the protocol design. Nonetheless, the motivation of such an attacker is not strong, since the attacker is mainly interested in publicity gains rather than financial gains. So, the likelihood is assessed to be medium. In terms of impact, a non-profit organization has the capability to compromise a large part of the smart grid network at a time, which would incur a non-negligible financial loss.The impact is stated to be also medium. Hence, the risk is medium.

8) (V1, A2, T4): As stated in IV-B-5, this attack requires the knowledge of the underlying cryptography, protocol design. A for-profit organization possesses this knowledge. On the other hand, for the motivation, is strong for such an attacker, due to potential financial gains or brand reputation gains. Therefore, the likelihood of such an attack will be high. In the meantime, a for-profit organization has the capability to compromise a large part of the smart grid network at a time, which would incur a non-negligible financial loss. The impact is assessed to be medium. Hence, the risk is high.

9) (V1, A3, T1): This protocol has a single point of failure, a centralized server (Substation), that is responsible for authentication. An attacker can try to take it offline to cause disruption in service. Alternatively, if he/she can break the server (Substation), he/she can authorize unauthorized nodes, (smart meter, collector) or revoke authorized nodes (smart meter, collector). However, such an attack would require access to points of failure, which a clever outsider is unlikely to possess. The likelihood is assessed to be low. In terms of impact, if the attacker is able to launch this attack, then there will be significant disruption in smart grid service. However, it is unlikely that this attack alone would lead to loss of sensitive information. So the impact is assessed to be medium. Hence, the risk is low.

10) (V2, A3, T2): Unlike IV-B-9, a knowledgeable insider will likely have access to the topology of the network. This will help him/her to gain access to the server (substation), which is a single point of failure. In addition, this attack does not require a lot of internal knowledge or resources. The likelihood is assessed to be high. For the impact of the attack, there is not much difference between this attack and that of IV-B-9. Hence, the impact is assessed to be medium. Hence, the risk is high.

11) (V2, A3, T3): Just like IV-B-9, a non-profit organization is unlikely to have access to points of failure, if there are any. Such an access requires inside knowledge of the smart grid network. Therefore, the likelihood is assessed to be low. Compared to IV-B-10, it is quite interesting to notice that a more capable attacker has a lower likelihood to launch this attack. Similar to IV-B-9 and IV-B-10, a non-profit organization will be able to significantly disrupt the service of the smart grid via this attack, without causing losses of sensitive information. As a result, the impact is assessed to be medium. Hence, the risk is low.

12) (V2, A3, T4): Even though a for-profit organization may not have easy access to points of failure, such attackers usually have more resources available to them than a nonprofit organization. In addition, the motivation of a for-profit organization is stronger than all other three types of attackers. The likelihood is assessed to be medium. The impact of this attack remains medium for the same reason stated before. Hence, the risk is medium.

13) (V2, A4, T1-T4): The proposed security protocols in [7] have assumed that the server (Substation) is always trusted, so the likelihood is assessed to be not applicable (N/A). In terms of impact, if such an attack is successful then there will be a non-negligible financial loss. The impact is assessed to be medium. Still, the risk is (N/A).

14) (V3, A5, T1-T2): Modern cryptographic schemes have strong mathematical foundations and are usually designed to be secure for the foreseeable future. Cryptanalyzing these schemes is extremely difficult, if not impossible. The likelihood is assessed to be low for now. With the recent research on quantum computers, it is possible that there will be usable quantum computers in the next couple of decades [44], which would mean that most of the existing cryptographic schemes could be broken. However, such a quantum computer, if it did exist, wouldn't be easily accessible to a clever outsider or a knowledgeable insider. The likelihood is assessed to be medium for future. In terms of impact, if this attack is successful, the attacker will have access to sensitive information and there will most

likely be significant financial loss, so the impact is assessed to be high.

15) (V3, A5, T3-T4): Just like IV-B-14, cryptanalyzing schemes is extremely difficult, if not impossible, even for large organizations. The likelihood is assessed to be low for now. If and when there will be a quantum computer, a large organization would be able to get access to it. The likelihood is assessed to be high for future. Just like IV-B-14, if this attack is successful, the attacker will have access to sensitive information to the smart grid network and there will most likely be significant financial loss, so the impact is assessed to be high.

16) (V4, A6, T1): To carry out this attack, an attacker requires the knowledge of the underlying cryptography, as well as the protocol design. A clever outsider is unlikely to possess all this knowledge. In addition, this attack is meaningful only if some other attack like MITM is also successful, so the likelihood is assessed to be low. In terms of impact, a clever outsider is unlikely to compromise more than one segment of the smart grid network at a time, which would incur minimal financial loss. The impact is assessed to be also low. Hence, the risk is low.

17) (V4, A6, T2): A knowledgeable insider is likely to possess some, if not all, knowledge of the underlying cryptography and the protocol design. However, as stated in IV-B-16 this attack requires some other attack, such as the MITM to be also successful. Therefore, the likelihood is assessed to be low. In the meantime, a knowledgeable insider is unlikely to compromise more than one segment of the smart grid network at a time, which would incur minimal financial loss. The impact is assessed to be low. Hence, the risk is low.

18) (V4, A6,T3): A non-profit organization is likely to be knowledgeable about cryptography and network design. However, the likelihood is assessed to be low for two reasons. First, as stated earlier, this attack is dependent on other attacks. Secondly, the motivation of such an attacker is not strong, since such an attacker is mainly interested in research publications or personal publicity. In terms of impact, a non-profit organization has the capability to compromise a large part of the smart grid network at a time, which would incur a non-negligible financial loss. The impact is assessed to be also medium. Hence, the risk is low.

19) (V4, A6, T4): The likelihood for a for-profit organization to launch this attack is medium. Such an attacker maintains the required knowledge. It is also motivated since a successful attack will lead to financial gains. However, this attack depends on other attacks which reduce the likelihood of this attack. Just like IV-B-18, a for-profit organization has the capability to compromise a large part of the smart grid network at a time, which would incur a non-negligible financial loss. The impact is assessed to be medium. Hence, the risk is medium.

TABLE III. RISK ANALYSIS SUMMERY

Attack	Risk Analysis		
	Likelihood	***Impact***	***Risk***
(V1,A1,T1)	Low	Low	Low
(V1,A1,T2)	Medium	Low	Low
(V1,A1,T3)	Medium	Medium	Medium
(V1,A1,T4)	High	Medium	High
(V1,A2,T1)	Low	Low	Low
(V1,A2,T2)	Medium	Low	Low
(V1,A2,T3)	Medium	Medium	Medium
(V1,A2,T4)	High	Medium	High
(V2,A3,T1)	Low	Medium	Low
(V2,A3,T2)	High	Medium	High
(V2,A3,T3)	Low	Medium	Low
(V2,A3,T4)	Medium	Medium	Medium
(V2,A4,T1-T4)	N/A	Medium	N/A
(V3,A5,T1-T2)	Low	High	Medium
(V3,A5,T3-T4)	Low	High	Medium
(V4,A6,T1)	Low	Low	Low
(V4,A6,T2)	Low	Low	Low
(V4,A6,T3)	Low	Medium	Low
(V4,A6,T4)	Medium	Medium	Medium

V. RISK MITIGATIONS

The countermeasures of proposed security protocol risks are considered in detail in this section.

A. *Mitigations of Medium and High Risks*

1) (V1, A1, T3-T4), (V1, A2, T3-T4): A straightforward way to mitigate MITM and impersonation attacks is to use digital certificates, such as Public-Key Infrastructure (PKI) and secure the channel using protocols like Transport Layer Security (TLS) [5]. With authentications, when a sender sends packages to a receiver, the receiver will check the authenticator associated with the sender and the package. This can be done via a digital signature for the sender's identical, signed by a Certificate Authority, and a MAC that binds the identity, the signature and the package. In this case, if one wishes to launch a MITM attack or an impersonate attack, he or she will have to break the underlying cryptography, which is prohibited by the given vulnerability, attack and attacker combinations.

2) (V2, A3, T2), (V2, A3, T4): Forthright way to mitigate vulnerabilities like the single point of failure is to decentralize the server by replication of resources and sharing the cryptographic key materials. This effectively stops attacks on single point of failures as even if one server is compromised, there are still adequate number of servers remains to provide required functionalities.

3) (V3, A5, T1-T4): To mitigate the medium current risk and possibly high risk in future, the use of cryptographic schemes that have at least 128-bit security is recommended (see, for example, NSA's suite B Cryptography Standards [45]). Standardized 128-bit secure cryptography is believed

 ISBN: 978-1-61208-635-4

to be robust against any existing cryptanalysis. The number of operations to break the cryptography is over 2128 bit operations, which is beyond the capability of classical computers. A even better solution, nonetheless, is to use cryptographic schemes that are believed to be quantum-safe, such as New Hope Key exchange algorithms [46], NTRU cryptosystems [47], in a hybrid mode [48]. The hybrid mode means one uses a quantum-safe scheme, for example, NTRU, in parallel with a classical scheme, such as Diffie-Hellman key exchanges. With a right configuration, the system will be as strong as the stronger scheme of the two. This provides sufficient security against classical attackers today, as well as potential quantum attackers in future.

4) (V4, A6, T4): To mitigate the risk of forward secrecy attacks, the use of ephemeral keys instead of static keys are recommended. Connections via ephemeral keys are sort of a de facto method to design secure communication protocols, such as TLS [5] and IKE [49]. In those protocols, the session key that was used for communications are derived from a long time authenticated key and an ephemeral key generated at run time. Therefore, for each session, the key is different and independent from all previous ones. As a result, a leakage of either a session key or the long time authenticated key will only have localized effect. The attacker will learn information about the particular session only, not the entire sessions that the user has participated.

B. Mitigation of Low Risks

In principle, there isn't really any need to address the low risks in the system right away, but it is important to keep an eye on them, as those risks may become medium or high in future depending on several parameters like scientific, technological, and algorithmic developments. An example is that of cryptanalysis attacks using quantum computers, whose likelihood is rated as low at the moment because quantum computers don't exist, but there is a non-negligible chance that quantum computers will become viable in the next decade or so, and therefore, the likelihood is rated as medium for future. The mitigations of low risks are given for the sake of completeness. It is worth noting that their mitigations are usually very similar to the medium/high risks in the same attack/vulnerability category. In a bit more details, (V1, A1, T1), (V1, A1, T2), (V1, A2, T1), and (V1, A2, T2) can be mitigated using techniques similar to Section IV-A-1. Those attacks rely on the lack of authenticity. As discussed earlier, with authenticators, one can effectively check the integrity and the authenticity of the packages it receives, and therefore, defeats those attacks. (V2, A3, T1) and (V2, A3, T3) can be mitigated using techniques similar to Section IV-A-2. They rely on single point of failure. So using a decentralized topology safely is assumed these attacks will fail. Similarly, using ephemeral keys will effectively stop attacks in (V4, A6, T1-T3) as shown in Section IV-A-4. With ephemeral keys, the leakage of a single key does no longer imply the leakage of all keys as suggested in.

VI. CONCLUSION

Security protocols for the smart grid are designed and implemented to protect the communications between various components within the grid. If these protocols reveal weaknesses, devastating consequences could take place. Therefore, these protocols should be fully analyzed and studied to ensure they provide robust security. In an attempt to participate in the effort of ensuring strong security implementation, this paper provides a framework for analyzing qualitative risk in smart grid security protocols. Risk factors are extracted together with their related issues. This analysis concluded nine low risks, six medium risks, and three high risks in these protocols. Countermeasures are proposed, and appropriate mitigation techniques for the identified risks are suggested.

REFERENCES

[1] S. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status," Renewable and sustainable energy reviews, vol. 15, no. 6, pp. 2736–2742, 2011.

[2] S. Finster and I. Baumgart, "Privacy-Aware Smart Metering: A Survey," IEEE Communications Surveys & Tutorials, pp. 1088–1101, 2014.

[3] K. Herter, P. McAuliffec, and A. Rosenfeld, "An exploratory analysis of california residential customer response to critical peak pricing of electricity, " Energy, pp. 25–34, 2007.

[4] Future-Proofing Smart Grid Infrastructure Meter Designs. [Online].Available: https://www.microsemi.com/applications/industrial-m2m-wireless/smart-metering, [retrieved: March 2018].

[5] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol," Version 1.2. Internet Engineering Task Force, 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246, [retrieved: March 2018].

[6] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," Internet Engineering Task Force, 1998. [Online]. Available: https://tools.ietf.org/html/rfc2406, [retrieved: March 2018].

[7] M. Saed, K. Daimi, and N. Al-Holou, "Approaches for Securing Smart Meters in Smart Grid Networks," International Journal on Advances in Systems and Measurements, vol. 10 no. 3&4, pp. 265-274, Dec. 2017.

[8] W. Stallings, "Network Security Essentials - Applications and Standards," (4. ed., internat. ed.). Pearson Education, 2010.

[9] NIST, "Guide for Conducting Risk Assessments," National Institute of Standards and Technology, 2012. [Online]. Available: http: //doi.org/10.6028/NIST.SP.800-30r1, [retrieved: March 2018].

[10] L. Allodi, W. Shim, and F. Massacci, "Quantitative Assessment of Risk Reduction with Cybercrime Black Market Monitoring," In 2013 IEEE Symposium on Security and Privacy Workshops, pp. 165–172, May 2013, CA, USA.

[11] L. Allodi and F. Massacci, "Security events and vulnerability data for cybersecurity risk estimation," International Journal on Risk Analysis, vol. 37, no. 8, pp. 1606–1627, Aug. 2017.

[12] J. Lee, D. Hwang, J. Park, and K.-H. Kim, "Risk Analysis and Countermeasure for Bit-Flipping Attack in LORAWAN," in 2017 International Conference on Information Networking (ICOIN), Jan 2017, pp. 549–551.

[13] A. Jacobsson, M. Boldt, and B. Carlsson, "A Risk Analysis of a Smart Home Automation System," Future Generation Computer

Systems, vol. 56, no. Supplement C, pp. 719–733, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X15002812, [retrieved: March 2018].

[14] Y. Cherdantseva et al. “A Review of Cyber Security Risk Assessment Methods for SCADA Systems,” Computers and Security, vol. 56, no. Supplement C, pp.1–27, 2016.

[15] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, “DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework,” Dordrecht: Springer Netherlands, 2006, pp. 227–234.

[16] TriangleMicroWorks, “Modbus and DNP3 Communication Protocols ,”2017. [Online]. Available: http://trianglemicroworks.com/docs/default-source/referenced-documents/Modbus_and_DNP_Comparison.pdf, [retrieved: March 2018].

[17] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, “An Integrated Security System of Protecting Smart Grid Against Cyber -Attacks,” Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 19-21 January 2010.

[18] M. A. Rahman, and H. Mohsenian-Rad, “"False Data Injection Attacks with Incomplete Information Against Smart Power Grids," In Proc. IEEE Conf. Global Commun. (GlobeCom), Dec. 2012, pp. 3153-3158.

[19] A. Giani, et al. “Smart Grid Data Integrity Attacks," IEEE Trans. Smart Grid, vol. 4, no. 3, pp. 1244-1253, Sep. 2013.

[20] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, “Efficient Authentication Scheme for Data Aggregation in Smart Grid with Fault Tolerance and Fault Diagnosis,” Innovative Smart Grid Technologies (ISGT), IEEE PES, pp. 1-8, 2012.

[21] B. Vaidya, D. Makrakis, and H. Mouftah, “Secure Multipath Routing for AMI Network in Smart Grid,” In Proc. IEEE 31st International Conference on Performance Computing and Communications (IPCCC), Austin, TX, pp. 408-415, 2012.

[22] Y. Yan, Y. Qian, and H. Sharif, “A Secure and Reliable In-network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid,” In Proc. IEEE Wireless Communications and Networking Conference (WCNC), Cancun, Quintana Roo, pp. 909-914, 2012.

[23] J. Seo and C. Lee, “The Green Defenders,” IEEE Power and Energy Magazine, VOL.9, NO.1, pp. 82-90, January/February 2011.

[24] Y. Zhao, A. Goldsmith, and H. V. Poor, “Fundamental limits of Cyber Physical Security in Smart Power Grids," In Proc. 52nd IEEE Conf. Decision Control, Florence, Italy, pp. 200-205, Dec. 2013.

[25] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, “Bad Data Injection in Smart Grid: Attack and Defense Mechanisms," IEEE Commun. Mag., vol. 51, no. 1, pp. 27-33, Jan. 2013.

[26] M. Esmalifalak, et al. “A Stealthy Attack Against Electricity Market Using Independent Component Analysis," IEEE Syst. J., to be published.

[27] G. Chaojun, P. Jirutitijaroen, and M. Motani, “Detecting False Data Injection Attacks in Ac State Estimation," IEEE Trans. Smart Grid, vol. 6, no. 5, pp. 2476-2483, Sep. 2015.

[28] F. Li, B. Luo, and P. Liu, “Secure Information Aggregation for Smart Grids Using Homomorphic Encryption,” In Proc. 2010 IEEE Conf. Smart Grid Communication, pp. 327-332.

[29] X. Wang, Y. L. Yin, and H. Yu, “Finding Collisions in the Full Sha-1,” In Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, Proceedings, 2005, pp. 17–36, Aug. 2005.

[30] R. L. Rivest, A. Shamir, and L. M. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

[31] N. Koblitz, “Elliptic Curve Cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987.

[32] P. W. Shor, “Algorithms For Quantum Computation: Discrete Logarithms and Factoring,” In FOCS, 1994, pp. 124–134.

[33] NIST, “FIPS180-4:Secure Hash Standard,” [Online]. Available: https://csrc.nist.gov/csrc/media/publications/fips/180/4/final/documents/fips180-4-draft-aug2014.pdf, [retrieved: March 2018].

[34] M. J. Dworkin, “SHA-3 Standard: Permutation- Based Hash and Extendable-Output Functions,” 2015. [Online]. Available: https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions?pub id=919061, [retrieved: March 2018].

[35] W. Mao, “Modern Cryptography: Theory and Practice,” Ser. Hewlett-Packard Professional Books, Prentice Hall PTR, 2003. [Online]. Available: https://books.google.com/books?id=OOUnYAAACAAJ, [retrieved: March 2018].

[36] S. Moore, “Meet-in-the-Middle Attacks,” 2010. [Online]. Available: http://stephanemoore.com/pdf/meetinthemiddle.pdf, [retrieved: March 2018].

[37] C. Adams, “Impersonation Attack. Boston, MA,” Springer US, 2011, pp. 596–596. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5 80, [retrieved: March 2018].

[38] K. Dooley, “Designing large-scale LANs,” Ser. O’Reilly Series. O’Reilly,2002.[Online].Available: https://books.google.com/books?id=xwBTAAAAMAAJ, [retrieved: March 2018].

[39] J. Oh, K. Lee, and S. Moon, “How to Solve Key Escrow and Identity Revocation in Identity-Based Encryption Schemes,” Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 290–303. [Online]. Available: https://doi.org/10.1007/11593980 22, [retrieved: March 2018].

[40] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, “Handbook of Applied Cryptography,” CRC Press, 1996.

[41] Praetorian, “Man-in-the-Middle TlS Protocol Downgrade Attack,”

[42] “Linux Security Threats: The 7 Classes of Attackers,” 2017. [Online]. Available: https://www.linux.com/news/chapter/Linux-security/linux-security-threats-7-classes-attackers, [retrieved: March 2018].

[43] V. Dumbrav, “Using Probability Impact Matrix in Analysis and Risk AssessmentProjects,”2013.[Online].Available: http://www.scientificpapers.org/wp-content/files/07_Dumbrava_Iacob-USING_PROBABILITY__IMPACT_MATRIX_IN__ANALYSIS_AND_RISK_ASSESSMENT_PROJECTS.pdf, [retrieved: March 2018].

[44] M. R. Bauer, “Quantum Computing is Going Commercial with the Potential to Disrupt Everything,” 2017. [Online]. Available: http://www. newsweek.com/2017/04/21/quantum-computing-ibm-580751.html, [retrieved: March 2018].

[45] “NSA Suite B Cryptography - NSA/CSS.” [Online]. Available: https://www.nsa.gov/ia/programs/suiteb cryptography/, [retrieved: March 2018].

[46] E. Alkim, L. Ducas, T. P¨oppelmann, and P. Schwabe, “Post-Quantum Key Exchange - a New Hope,” In 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016, pp.327–343. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim, [retrieved: March 2018].

[47] J. Hoffstein, J. Pipher, and J. H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” In Algorithmic Number Theory, Third International Symposium, ANTS-IV, Portland, Oregon, USA, June 21-25, 1998, Proceedings, 1998, pp. 267–288. [Online]. Available: http://dx.doi.org/10.1007/BFb0054868, [retrieved: March 2018].

[48] J. M. Schanck, W. Whyte, and Z. Zhang, “Circuit-Extension Handshakes for Tor Achieving Forward Secrecy in a Quantum World,” PoPETs, vol. 2016, no. 4, pp. 219–236, 2016. [Online]. Available: https://doi.org/10.1515/popets-2016-0037, [retrieved: March 2018].

[49] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” Internet Engineering Task Force, 1998. [Online]. Available: https: //tools.ietf.org/html/rfc2409, [retrieved: March 2018].