Published in:
Critical Information Infrastructures Security
Lecture Notes in Computer Science Volume 7722, 2013, pp 264-275
http://link.springer.com/chapter/10.1007%2F978-3-642-41485-5_23

Threat modeling of AMI

Inger Anne Tøndel, Martin Gilje Jaatun, Maria Bartnes Line

SINTEF ICT, Trondheim, Norway
inger.a.tondel@sintef.no

Abstract. The introduction of an advanced metering infrastructure (AMI) into the power grid forces the power industry to address information security threats and consumer privacy more extensively than before. The industry needs practical advice on methods and tools to use in this context. Threat modeling is well-known among information security professionals as a method for investigating a system's vulnerabilities. This paper documents the threat modeling of one actual AMI configuration. The results are both a demonstration of how these techniques can be applied to AMI, and a documentation of risks associated with this specific AMI configuration.

Keywords: Smart Grid; Advanced Metering Infrastructure; Information Security; Privacy; Threat Modeling; STRIDE

1 Introduction

An Advanced Metering Infrastructure (AMI) is the most visible component of the smart grid. The new technologies in AMI and smart grid, with increased connectivity and new trust models, lead to new threats and a pressing need to deal with information security and consumer privacy [1, 2].

Information security for smart grid and AMI have been addressed by several actors. Important resources include the NISTIR 7628 report [3] that deals with security of smart grids at large and the AMI-SEC task force security profile for AMI [4]. These documents identify central components as well as security requirements. However, despite the available resources, industry is still in need of support in understanding the information security challenges they are facing. In our interactions with the Norwegian power industry, we sense a need for practical advice and easy-to-use information security methods.

Threat modeling increases awareness of threats, and is invaluable as preparation for risk assessments. In this paper, a well established threat modeling approach (Section 2) is applied to a specific type of AMI configuration (see Figure 1). The approach is lightweight and easy to apply, and results in a graphical overview of the system, threats, and the potential attacker goals. The paper i) demonstrates that general threat modeling techniques are applicable for AMI infrastructure (Sections 3-5), ii) provides an overview of threats that can be reused by industry (Sections 4-5), and iii) provides a method for working with and using threat models as input to risk assessments of AMI infrastructure (Section 6). We discuss our contribution in Section 7, and offer conlcusions in Section 8.

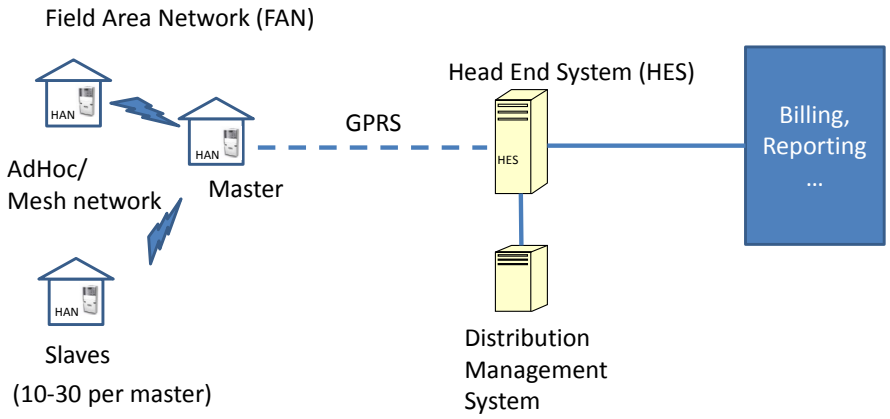

Fig. 1. An overview of the AMI system considered in this study

2 The threat modeling method

In the field of secure software engineering, threat modeling is a common activity and several techniques exist. Some are formal and require special skills, while others are more lightweight. Of the informal ones, Microsoft's technique [5] is popular and has been described as *"a practical approach, usable by non-experts"* [6]. Their technique mainly works as follows. First, the system is modeled with an emphasis on the system's entry points (using e.g. Data Flow Diagrams (DFDs)), and then the threats towards the system are identified. In order to ensure coverage, the STRIDE classification of threats (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privileges) can be used as a resource. Then threats are analysed to evaluate the system's vulnerability.

Attack trees [7] are also widely adopted in the information security community. Such trees model how attackers may go about achieving their attack goals. Experiments show that attack trees are easy to grasp [8], which makes them particularly useful for communicating threats among stakeholders. They are also to a large extent reusable [7, 9].

In this paper the threats towards AMI are addressed from two viewpoints:

- *Threat overview:* The AMI system is modeled using DFD and the interfaces are identified. For all interfaces, threats are identified using STRIDE. (Section 4)
- *Attacker strategies:* The most important assets of the system are identified in a brainstorming session [10] and by investigating the system. Then attack goals are associated with these assets, and the possible ways to achieve the goals are detailed in attack trees. (Section 5)

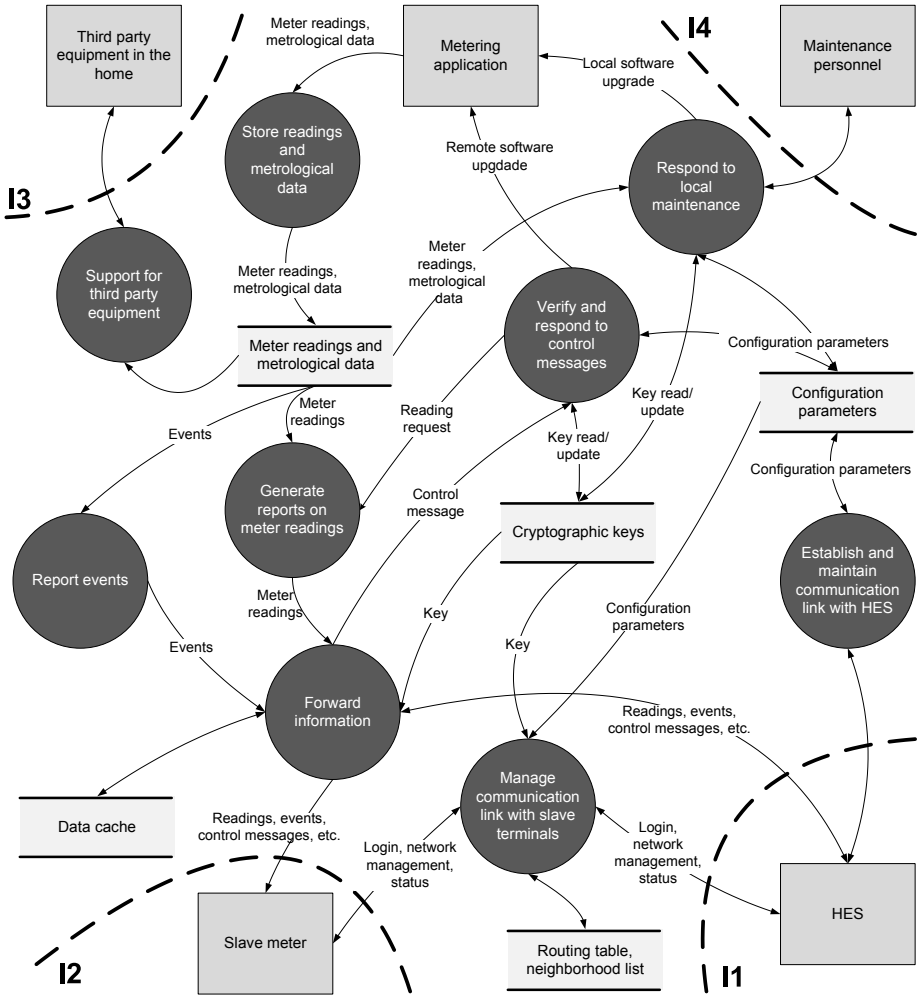

Fig. 2. A Data Flow Diagram (DFD) showing the data flow related to a master meter

3 Scope: The AMI system

As was shown in Fig. 1, we consider AMIs where meters are organised in mesh networks and communicate with the Head End System (HES) of the Distribution Service Operator (DSO) via GPRS. In each mesh network, one node (the master) is responsible for the communication channel towards the HES, and the other nodes (the slaves) communicate with HES via that node. At the DSO, the HES is connected to other systems, such as the distribution management system and systems for billing.

Fig. 2 gives an overview of the main data flow related to a master meter. Slave meters would have similar data flows, except from the communication link

Table 1. Interfaces

ID	*Where*	*Communication*
I1	Meter - HES	Establishment and maintenance of communication link; Readings and events; Control messages (including software updates, configuration changes, meter reading requests and updated keys); Login management; Status
I2	Meter - Meter	Network management; Readings and events; Control messages; Login management; Status
I3	Meter - Third Party Equipment	Meter readings; Reading requests
I4	Meter - Local Maintenance	Requests; Credentials; Configuration data; Stored meter data and logs; Test results

with the HES. In the DFD, interactors are represented as rectangles, processes are represented as circles, data stores are represented as horizontal lines and data flows are represented as arrows. The model shows four main interfaces: An interface with the HES (I1), an interface with other meters (slaves) (I2), an interface towards third party equipment such as displays (I3) and an interface towards maintenance personnel with physical access to the meter (I4). The meter itself can be considered to consist of two parts: A metering application that measures power consumption as well as metrological data, and a terminal responsible for all communication. The terminal's main tasks include reporting of meter values, generation of events, and responding to control messages and local maintenance. Master terminals are also responsible for establishing and maintaining communication with the HES and with slave terminals in its mesh network. All terminals are expected to forward messages from/towards slave nodes. A description of the main communication on the interfaces is given in Table 1.

4 Threat overview

In this section we go through the STRIDE threat effect classification for each interface of a master terminal. The identified threats are listed in Table 2.

4.1 Spoofing

Spoofing is defined by Swiderski and Snyder [5] as something that *"[a]llows an adversary to pose as another user, component, or other system that has an identity in the system being modeled."* On I1 and I2, spoofing of meter identities and HES identities are potential threats (T1-T3 in Table 2). With HES spoofing, attackers will get access to messages and will be able to send fake commands to the system. Meter spoofing can result in increased access to information (e.g. in the case of master spoofing) and false meter reports. On I3, spoofing is not considered relevant as communication is not dependent on any identities. On I4, spoofing of meter identity is not an issue as the physical location of the meter,

Table 2. Threats

ID	*Name*	*Interface*
Spoofing		
T1	Fake HES	I1
T2	Fake meter ID	I1, I2
T3	Fake master meter	I2
T4	Attacker is authenticated as maintenance personnel	I4
Tampering		
T5	Tamper with communication between HES and master meter	I1
T6	Tamper with communication in mesh network	I2
T7	Tampering before forwarding message	I1, I2
T8	Local maintenance alters meter data or software	I4
T9	Meter reports wrong data to local maintenance	I4
Repudiation		
T10	Meter denies having received a message	I1, I2
T11	Meter denies sending of message	I1, I2
T12	Maintenance dispute	I4
Information disclosure		
T13	Eavesdrop on communication between master and HES	I1
T14	Meter leaks configuration information	I1, I2
T15	Eavesdrop communication in the mesh network	I2
T16	Leaking of forwarded messages	I2
T17	Meter leaks information about third party equipment	I3
Denial of service		
T18	Denial of service attack on HES	I1
T19	Meter errors/attacks make meter unable to communicate with HES	I1
T20	Communication failure on the link between HES and master meter	I1
T21	Meter refuses to communicate with HES	I1
T22	Denial of service attack on meter	I2
T23	Disrupt communication in mesh network	I2
T24	Node lockout	I2
T25	Meter unavailability caused by third party equipment	I3
T26	Meter unavailability due to local maintenance	I4
T27	Physical disabling of meter communication	I4
Elevation of privileges		
T28	Remote access to HES	I1
T29	Remote access to meter	I1, I2, I3
T30	Local meter compromise	I3, I4

and thus the real identity, is known by the maintenance personnel. The ability to spoof as maintenance personnel (T4) should however be considered.

A system's vulnerability towards these threats depends on the authentication mechanisms in place as well as procedures for contact establishment and the presence of spoofing detection mechanisms.

4.2 Tampering

Tampering refers to *"[t]he modification of data within the system to achieve a malicious goal"* [5]. Tampering attacks the data integrity, a quality that is essential for AMI, e.g. for the purpose of billing [3].

In this study we only consider the security of the meter node and its communication link towards the HES and other meters. Tampering that occurs at, e.g., the HES is out of scope. For interface I1 and I2 we are thus left with threats related to tampering on the GPRS link, the RF/mesh network and at the intermediate nodes on route to HES (T5 - T7 in Table 2). Such tampering may lead to errors in meter reading reports, wrong configuration settings, unauthorized changes of software, or erroneous or missing alarms. It can also open up for attacks on the HES or on the meter nodes (exploits). Tampering of data from third party equipment (I3) is not considered a threat, as no such data is stored in the meter. On interface I4, tampering can happen at both sides, either by local maintenance personnel altering meter data or software[1], or by meters that report wrong data to local maintenance (T8 - T9 in Table 2).

A system's vulnerability towards threats T5 - T7 depends on the security of the communication infrastructure and protocols, and the strength of any integrity protection. For threat T8, the vulnerability towards threat T4 (Attacker is authenticated as maintenance personnel) and also the ability to detect unauthorised changes are essential. Threat T9, and also T7, depend on the extent to which meters can be compromised (see Subsection 4.6 on elevation of privileges).

4.3 Repudiation

Repudiation threats allow adversaries *"to deny performing some malicious activity because the system does not have sufficient evidence to prove otherwise"* [5]. Cleveland [1] points at accountability or non-repudiation as critical for AMI and its financial transaction, metrology information and responses to control commands. On I1 and I2, meters may deny the reception of messages or the sending of messages (T10 and T11 in Table 2). On I3, it is possible to imagine scenarios where an erroneous message from a meter causes harm to third party equipment, and that the meter denies sending the message. This threat is however considered out of scope. On I4, there is the threat that maintenance is denied, either from the meter side or the maintenance personnel side (T12). This may reduce the abilities to identify the source of problems with meters.

A system's vulnerability towards threats T10 and T11 depends on the ability to prove the origin of messages, as well as on the integrity protection of messages and the extent to which responses are required. For threat T12 it is relevant to consider any logging functionality in the meter or in the maintenance equipment, and the protection of the audit logs.

[1] Note that in this study we do not consider physical tampering of meters in order to change the way power consumption is measured.

4.4 Information disclosure

Information disclosure results in *"[t]he exposure of protected data to a user that is not otherwise allowed access to that data"* [5]. As shown in Fig. 2, data stored and communicated in an AMI includes private consumption data, encryption keys, alarms, control messages and software upgrades. Information disclosure can happen at the meter; by meters leaking configuration settings, keys or software received from HES (T14), by meters leaking messages that are forwarded through the meter (T16), or by meters leaking information about the third party equipment connected to the meter (T17). Information disclosure can also happen at the communication links (T13 and T15).

A system's vulnerability towards these threats depends on similar factors as those of tampering. One should consider the security of the communication infrastructure and protocols, the strength of the encryption and how easy meters can be compromised.

4.5 Denial of service

A *Denial of service* (DoS) attack *"[o]ccurs when an adversary can prevent legitimate users from using the normal functionality of the system"* [5]. NISTIR 7628 states that *"[a]vailability of meter data is not critical, since alternate means for retrieving metering data can still be used."* AMIs, however, process a variety of data, and the dependence on e.g. timely alarms and control messages should be assessed. Below we mainly consider the unavailability of individual components. When assessing consequences, the effects of having several components unavailable simultaneously in critical situations need to be taken into account [1].

On I1, attackers could reduce availability of the HES[2], the meter or the GPRS link (T18 - T21 in Table 2). On I2, DoS attacks may affect meters or the mesth network (T22 - T24). In general, DoS attacks may be of two types: i) A distributed denial of service (DDoS) attack where a large number of requests from a multitude of sources render a node unavailable for legitimate requests, and ii) malware or specifically crafted messages that exploit vulnerabilities in such a way that the node is made unavailable. DoS may also be caused by errors, e.g. in software or configurations (T19). Attacks may affect a large number of nodes (e.g. by jamming the mesh network (T23)) or individual nodes (e.g. by refusing to forward messages to/from a given node in the mesh network (T24)). In addition to the above, the sending of a fake circuit break command could be considered a special case of DoS (denial of power), but this is covered by other threats[3].

On I3, third party equipment can pose a threat to the availability of the meter (T25), though the likelihood of this is low due to the limited communication on

[2] As the security of the HES is out of scope, we only consider threats to the availability of the HES that originate from the meter side

[3] On I1, this threat is covered by threats T1, T5 and T28. On I2 this threat is covered by threats T6 and T7.

this interface. On I4, there is the risk that local maintenance causes unavailability of the meter (T26). It should also be noted that attackers with physical access to the meter may disable communication (T27).

For some of the DoS threats, the vulnerability of the system is related to the capacity of the communication lines used and the capacity of the nodes. Software quality is also essential, and the ability to withstand intrusion attacks (see Subsection 4.6 on elevation of privileges, below).

4.6 Elevation of privileges

Elevation of privileges occurs *"when an adversary uses illegitimate means to assume a trust level with different privileges than he currently has"* [5]. On I1, there are two systems that could be compromised, the HES and the meter (T28 and T29 in Table 2). Meters can also be attacked remotely via I2 or I3[4]. Local attacks are also possible, where attackers with physical access to the meter physically compromise the meter (T30).

For remote access threats the vulnerability of a system depends on the software quality and the general protection of the system, including the patching regime, the presence of malware protection and detection software and the security mechanisms controlling remote software updates. For local meter compromise it is important to consider the presence of any physical anti-tampering mechanism and also the abilities to detect unauthorised changes.

5 Attacker strategies

An asset is anything of value "that needs protection" [10]; assets can comprise information, processes, physical devices, and even intangible concepts such as reputation.

The main assets of the AMI system were identified in a brainstorming session [10] involving stakeholders from industry, as well as information security experts. All participants were to write down potential assets on Post-it® notes, and the resulting assets and the potential threats towards these assets were discussed in the group. After the brainstorming session, the security experts were responsible for documenting the assets and evaluating the set of assets for completeness. The resulting asset groups are listed in Table 3, together with their associated attack goals.

Attack trees have been created for all the (important) attack goals, but due to space limitation, we here only provide a partial tree for the attack goals associated with asset A7 - the meter. As the attack tree in Fig. 3 illustrates, remote access can be achieved through installing a rogue SW upgrade (containing a back door), misusing the remote control mechanism (if it exists), or employing some sort of meter-specific exploit. A rogue SW upgrade can be installed either

[4] Third party equipment is online and is compromised remotely. Attacker then attacks the meter via the third party equipment

Table 3. Assets and associated attack goals

ID	*Asset*	*Attack goal*
A1	The configuration/topology of the power grid	- Get knowledge of the topology of the power grid in order to perform physical or online attacks
A2	The identities of meters (including the ability to authenticate meters)	- Manipulate energy bills by reporting consumption as another meter - Insert a rogue meter as part of an attack
A3	Control messages, including messages such as alarms, configuration and software updates and status messages	- Injection of false control messages, in order to manipulate meters (configuration settings, software, keys) - Have meters turn off power
A4	Meter values that can reveal consumption patterns	- Get access to consumption data in order to use this for marketing, or for criminal activities, or other unintended uses - Modify consumption data in order to manipulate bills
A5	The HES	- Break into HES, and the systems beyond HES
A6	The tariffs in meters	- Cause instability of the power grid
A7	The actual meter	- Manipulation of power measurements (stored, reported) in order to reduce bill - Use meter to attack other meters or the HES - Limit the availability to access/control meters

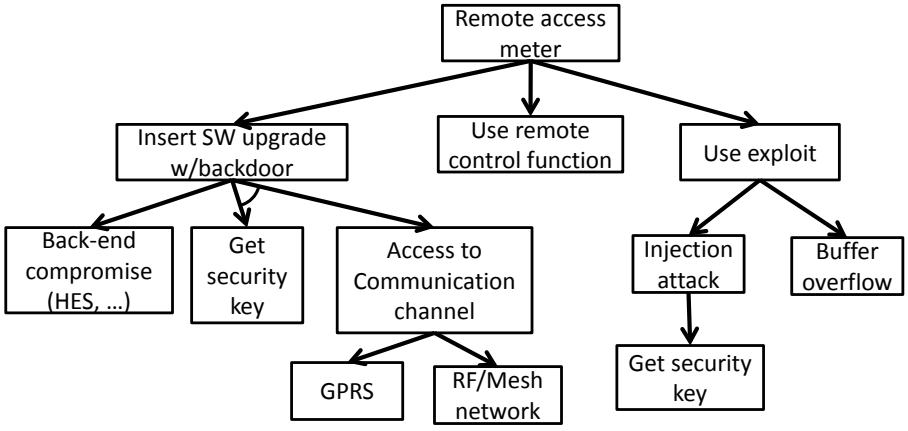

Fig. 3. An example attack tree for "remote access to meter" attack

through compromising the back-end system[5], or through the regular communication channel of the meter; in the latter case the attacker also needs to get access to the encryption key used to encrypt data sent to the meter.

[5] The back-end system could for instance be compromised by malware introduced through USB memory sticks, as in the case of Stuxnet.

When modeling the attack trees, the DFDs and the threats identified have been used as inspiration. As an example, the top node of the attack tree included in this paper is the threat T29, and the node "Communication channel" and its child nodes "GPRS" and "RF/Mesh network' correspond to threats T5-T7.

6 Method for risk assessment based on the threat models

The threat modeling activities described in this paper help identify and understand the relevant threats and attack goals. However, in order to choose how to deal with the threats identified, it is essential to evaluate the consequences of the attacks, as well as their likelihood of success. Such an evaluation is not presented in this paper, as it is highly dependent on the individual systems. Still, we sketch how the threat models can be used as valuable input to a risk assessment process below.

This paper has provided a DFD of one type of AMI configuration and identified several threats that should be considered. For systems that are similar to that described in the DFD, all threats listed in Table 2 should be evaluated to assess the degree to which the system is vulnerable to these threats. The assessment should be documented. If the system is different from the one described in the DFD, it should be assessed whether these differences change the relevance of the threats, and whether new threats should be considered. This can be done by using the STRIDE approach on the functionality that is different.

The list of assets provided in this paper can be used as input to an asset identification process for other systems. The asset identification method [10] used in this paper also recommends assigning values to the assets in order to be able to prioritise which assets are the most important. A coarse scale is sufficient (e.g. high, medium, low). If appropriate, one can also consider the value of the asset for different stakeholders (e.g. for the DSO, the energy customer or the attacker) and also which aspect of the asset is the most important (i.e. confidentiality, integrity, or availability). The value assignment is important in order to prioritise the potential countermeasures later on.

For the prioritised assets, it should be determined how attackers may go about attacking the asset. This is modeled in attack trees. When an attack tree has been created, it should be determined for each attack path whether this path is sufficiently difficult to follow for an attacker, or if additional measures are needed. In this process the assessment of the system's vulnerability towards the threats already identified (see Table 2) is essential input. These measures should then be prioritised based on the importance of the asset(s) at stake. Note that the DREAD (Damage, Reliability, Exploitability, Affected users, Discoverability) approach can be seen as a refinement when evaluating each identified threat [5].

If the system changes, the changes should be reflected in the DFD, and STRIDE should be used to assess whether the changes affect some of the already identified threats or result in new ones. Any change in threats may also affect the attack trees, thus the attack trees should be revisited with the modified threats in mind, and the necessary updates should be made. The same way, it should be

considered whether the changes add or remove assets to the system. Any change in assets may result in the need to add, delete or modify attack trees.

7 Discussion

The method we have described in this paper is easy to learn and easy to use, and has been well received in the industry. The graphical representation is an advantage in itself, resulting in models that are easy to understand both by security professionals and other stakeholders, and works particularly well for communication of security issues with the latter.

The method can assist the stakeholders in assessing how the threats change as a function of system changes that occur after the initial assessment has been carried out. Performing a STRIDE process from scratch requires not insignificant effort, but once the foundation is laid, it requires relatively little effort to update when minor system changes occur. The result is a living security model that can conveniently be kept up to date.

The brainstorming process when identifying assets and threats may be seen as possible weak spot, where the results may depend heavily upon the personal characteristics of the participating stakeholders. However, much of the uncertainty can be compensated by having security professionals participate in the process, e.g. by getting the discussion back on track in cases where it veers off course. Use of the STRIDE method also helps ensure broad coverage of security issues, even if it does not directly help with prioritizing threats.

It has been claimed that the strict real-time requirements in the smart grid represent a limitation on the kind of security solutions that are applicable [11], but our experience in the smart metering segment is that the same security considerations and solutions as for generic computer networking apply. Admittedly, the performance aspect is not given foremost attention in the threat modeling process, but any implemented controls and countermeasures clearly have to take performance into account. Even though customer privacy has not been a main focus for our efforts, we argue that there should be no inherent barrier to using STRIDE to model privacy threats, under the "information disclosure" heading.

Even a lightweight threat modeling approach requires a minimum of security expertise to ensure proper maintenance, but our experience shows that if the foundational security modeling work has been performed with the support of security experts, a domain professional with a basic working knowledge of security concepts can adequately handle the maintenance phase and smaller updates.

8 Conclusion

AMI has received a lot of attention from European data protection authorities and consumer groups, and a credible process for ensuring security and privacy is vital for an AMI deployment process to succeed. Since the DSOs are responsible for the deployment, it falls to them to ensure that suppliers of meters and

infrastructure satisfy privacy regulations of the relevant jurisdictions. Furthermore, the DSOs must satisfy the requirements from the end-users' perspective as well, and they can not expect the end-users to specify these requirements themselves. Thorough analyses of relevant threats, attackers, vulnerabilities and risks need to be performed, and in this respect the industry needs guidance regarding methods and tools.

This paper has described a threat modeling method that is simple enough to be used by all stakeholders with minimal support from security experts. We have applied this method to a specific type of AMI configuration, and our high-level results, such as threat overview and examples of attack trees and Data Flow Diagrams, can be reused by the industry.

Acknowledgments

The research reported in this paper has been supported by the Telenor-SINTEF research agreement, Smart Grid initiative. The authors thank the participating vendors and DSOs for their cooperation.

References

1. Cleveland, F.M.: Cyber security issues for Advanced Metering Infrastructure (AMI). In: 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century. 1–5
2. Maria Bartnes Line and Inger Anne Tøndel and Martin Gilje Jaatun: Cyber security challenges in Smart Grids. In: 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe). 1–8
3. The Smart Grid Interoperability Panel - Cyber Security Working Group: NISTIR 7628: Guidelines for smart grid cyber security (2010)
4. The Advanced Security Acceleration Project (ASAP-SG): Security Profile for Advanced Metering Infrastructure (2010)
5. Frank Swiderski and Window Snyder: Threat Modeling. Microsoft Press (2004)
6. Adam Shostack: Experiences threat modeling at microsoft. Modeling Security Workshop (2008) http://www.comp.lancs.ac.uk/modsec/program.php.
7. Bruce Schneier: Attack Trees – Modeling security threats. Dr. Dobb's Journal (2001)
8. Andreas L. Opdahl and Guttorm Sindre: Experimental comparison of attack trees and misuse cases for security threat identification. Information and Software Technology **51** 916 – 932
9. Per Håkon Meland and Inger Anne Tøndel and Jostein Jensen: Idea: Reusability of threat models - two approaches with an experimental evaluation. In: Engineering Secure Software and Systems, Lecture Notes in Computer Science. 114 –122
10. Martin Gilje Jaatun and Inger Anne Tøndel: Covering your assets in software engineering. In: The Third International Conference on Availability, Reliability and Security (ARES 2008), Barcelona, Spain 1172–1179
11. Hairong Qi and Xiaorui Wang and Leon M. Tolbert and Fangzing Li and Fang Q. Peng and Peng Ning and Massoud Amin: A Resilient Real-Time System Design for a Secure and Reconfigurable Power Grid. IEEE Transactions on Smart Grid **2** (2011)