SECURITY RISK ANALYSIS AND EVALUATION OF INTEGRATING CUSTOMER ENERGY MANAGEMENT SYSTEMS INTO SMART DISTRIBUTION GRIDS

Christian HÄGERLING
TU Dortmund University – Germany
christian.haegerling@tu-dortmund.de

Fabian M. KURTZ
TU Dortmund University – Germany
fabian.kurtz@tu-dortmund.de

Christian WIETFELD
TU Dortmund University – Germany
christian.wietfeld@tu-dortmund.de

Davide IACONO
Resiltech SRL – Italy
davide.iacono@resiltech.com

Alessandro DAIDONE
Resiltech SRL – Italy
alessandro.daidone@resiltech.com

Felicita Di GIANDOMENICO
CNR/ISTI – Italy
f.digiandomenico@isti.cnr.it

ABSTRACT

The subject addressed by this paper is the analysis and evaluation of different architectural concepts for securely integrating Customer Energy Management Systems into smart distribution grids. Nowadays approaches target the active integration of Distributed Energy Resources, Demand Side Management and Automated Meter Reading into the households in order to enable a manageable and controllable smart distribution grid. Therefore a comprehensive, secure and reliable communication network architecture, reaching down to the customers' premises equipment, needs to be deployed. These networks are usually located at public domains and are connected to the critical infrastructure of the Smart Grid control network. Together with this it represents potential points of failures and possible risks, including malicious attacks and system faults, for the overall system architecture. To reduce the risks associated with connecting the households to the comprehensive monitoring and control architecture, a risk analysis of the multiple communication network architectures is performed. Through this analysis the impact of different access network strategies on security can be assessed to select the most appropriate one, to ensure a reliable operation of the mission-critical Smart Grid communication network infrastructures.

INTRODUCTION

In the last years information and communication technology (ICT) infrastructures have been widely used in a variety of cyber physical systems. In particular in electrical (smart) grids, in order to remotely control and/or monitor the systems, the importance of ICT infrastructures rapidly increases. In low voltage grids the introduction of Low Voltage Grid Controllers (LVGC) enables Costumer Energy Management Systems (CEMS) at the households for an advanced energy management based on tariff information and an integration of distributed energy resources (DER) for a more balanced grid stability. A basis for this control network needs to be established by the deployment of a comprehensive Advanced Metering Infrastructure (AMI) for Automated Meter Reading (AMR) monitoring the electricity consumption of households collected by smart meters. The integration of these devices located at public domains represents potential point of failures and possible risks for malicious attacks, which are analyzed in this paper.

RELATED WORK AND METHODOLOGY

The pervasive utilization of ICT control infrastructure exposes the controlled system to security vulnerabilities. In this context, system architects need to verify system robustness against security attacks in order to make trade-off decisions. To do so, the ADVISE tool [1], which allows the evaluation of model-based quantitative security metrics, is used in the presented work. ADVISE lets the system architects model the system, in terms of system vulnerabilities and countermeasures, and its adversaries by taking into account the attackers' goals and capabilities, i.e. the probability of the adversaries being able to reach their objectives.

Smart Grids are critical infrastructures involving safety critical applications where failure or malfunction may result in: serious injury to people (possibly death); loss of, or severe damage to equipment; environmental harm.

In order to mitigate the impact of these situations, several methodologies have been developed. In industrial environments the processes aimed at mitigating harmful situations have been standardized. Safety critical systems should be compliant with international standards which state requirements about their development and subsequent operational lifecycle. The most important normative in this field is the IEC 61508 [2]. The standard defines harm as physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment. A hazard is defined as a potential source of harm. Thus, a hazardous situation is a circumstance in which a person is exposed to a hazard(s). Consequently, a hazardous event is a hazardous situation which results in harm. Risk is defined as a combination of the probability of occurrence of harm and the severity of the harm.

According to IEC 61508, in the first phases of the safety lifecycle it is envisaged to perform a hazard and risk analysis to determine:

- Hazards and hazardous events for all reasonably foreseeable circumstances including fault conditions and misuse.
- Event sequences leading to hazardous events.
- Risks associated with hazardous events.

introduced into the system. The second option shown in b) utilizes different broadband access networks for both AMR Gateway and CEMS. Through the deployment of two independent interfaces with higher data-rate the robustness

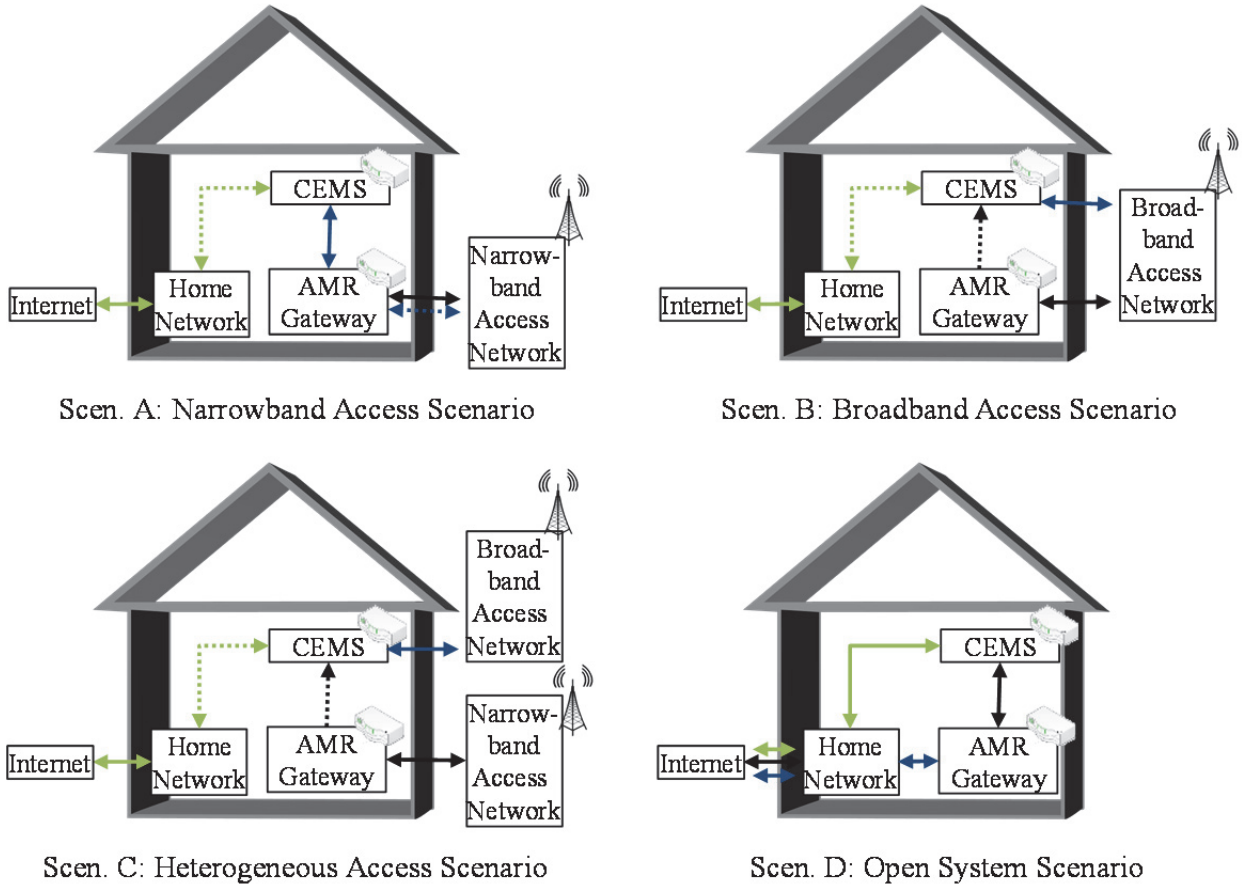

Figure 1 - ICT Architectural Options for Integrating AMR and CEMS into Smart Distribution Grids

ICT ARCHITECTURE FOR AMR AND CEMS INTEGRATION

Several ICT architectures for the integration of CEMS entities are presented in this section. Common approaches target a dedicated infrastructure for connecting the CEMS and AMR gateway devices to the monitoring and control infrastructures usually maintained by energy utilities. Aside from this strategy, shared approaches exist which rely on public networks like the customer's Internet access or public cellular networks. These architectural options are shown in Figure 1 and represent the basis for the risk analysis conducted for this paper. Sub-figure a) represents a scenario in which the AMR and CEMS use a shared narrowband access network (AN) for connecting to the overall Smart Grid infrastructure. As both devices relevant to Smart Grid functionality share one interface with comparably low data-rate, any impairment of this connection directly affects the functionality provided by both AMR and CEMS. Thus a single point of failure is against the failure of one AN increases. This further resilience increased in cases in which CEMS and AMR are connected, therefore enabling each one to use the AN of the other should its own interface fail. However such a solution is associated with high costs. Those cases which feature a narrowband connection for the AMR and a broadband AN for the CEMS are shown in the heterogeneous access scenario of C). Here the same principles as in B) apply, with some restrictions to the capabilities of the AN technology used by the AMR Gateway, which in normal operation does not impair the AMR since its comparatively low bandwidth demands are met. All the ICT options presented up to this point employ the customers' Internet connections for the home network (if present). Scenario D), the "open system scenario", possesses this Internet connection as the only AN option.

ID	Information/ Flow Name	Flow Source/ Sink	Flow Direction	Functionality	Associated Hazards	Critical.
1	Meter reading	AMR-GW	Outbound	The meter readings are provided to the aggregator and the meter management system.	Meter readings are disclosed and an attacker may retrieve behavioral information about the consumer.	High
2	Meter reading request	AMR-GW	Inbound	A request to the AMR-GW for a meter reading. The AMR-GW then sends a meter reading to the applicant.	An attacker sends a fraudulent meter reading request and the AMR-GW sends to it the meter data (e.g. masquerade or man in the middle attack).	High
3	Meter reading schedule	AMR-GW	Inbound	A request to the AMR-GW for scheduling meter readings with a specific rate or in specific time instant.	An attacker sends a fraudulent meter reading scheduling request and the AMR-GW send to it the meter data (e.g. masquerade or man in the middle attack).	Medium
4	Tariff parameters	AMR-GW	Inbound	Parameters that represent consumer account arrangements like payment mode, tariff scheme, prices are sent to the AMR-GW.	An attacker sends false tariff information to an AMR-GW which can alter the payment mode, tariff scheme and prices (e.g. masquerade or man in the middle attack).	High
5	Consumer information	AMR-GW	Inbound	Information relevant to the consumer (e.g. pricing) is sent to the AMR-GW in order to be displayed.	An attacker could send false pricing data, causing the consumer to behave disadvantageously.	Low
6	Load and Generation Management	CEMS	Inbound	Signals and metrological information are provided to the CEMS.	An attacker sends fraudulent load and generation command to the EMG (e.g. masquerade or man in the middle attack).	Medium
7	Flexibility information	CEMS	Outbound	The CEMS provides to the higher layer controller flexibility information.	An attacker sends fraudulent flexibility information to the higher layer controller. (e.g. masquerade or man in the middle attack).	High
8	Price and environ-mental information	CEMS	Inbound	Energy price and environmental aspects are sent to the CEMS in order to perform optimization consumption scheduling.	An attacker sends fraudulent price and environmental information to the CEMS. (e.g. masquerade or man in the middle attack).	High
9	Miscellaneous Flows	AMR-GW	Bi-directional	Provides gateway functionality to the AMR devices.	An attacker can apply a DoS attack which brings the AMR-GW to halt failure. Then the controller aggregator is not able to get.	Low
10	Miscellaneous Flows	CEMS	Bi-directional	Provides CEMS functionality to the household.	An attacker can apply a DoS attack which brings the CEMS to halt failure.	Low

Table 1: Information Flows and associated hazards

This imposes special requirements with regards to the quality and reliability of the Internet connection as the shared resource necessitates strict rules for Quality of Service (QoS) in order to prioritize critical Smart Grid related traffic over e.g. web-browsing. Also a single point of failure for all ICT dependent applications of the household is introduced.

RISK ANALYSIS AND EVALUATION

The risk analysis of the previously defined architectural options, which focuses only on security related threats, is presented in this section. First of all the information flows that are present in the scenario are listed in Table 1 and their criticality is evaluated in terms of three levels:

- High: the information flow contains sensitive data that needs to be authenticated and/or maintain a certain degree of confidentiality.
- Medium: the information flow contains data that can be sensitive and that may be authenticated and/or maintain a certain degree of confidentiality.
- Low: the information flow does not contain sensitive data and no security protection is needed.

EXPERIMENT SETUP

The scenarios shown in Figure 1 are used as reference architecture in the analysis. Two likely attacker goals are identified for this study from the hazards listed in Table 1. Goal 1 refers to the aim of the adversary to obtain metering data from AMR gateways. Goal 2 refers to the aim to compromise the interaction between the CEMS and LVGC and thus either sending false flexibility data to the LVGC or corrupting set points sent to the CEMS. In this case the manipulation of data stored in the CEMS is also considered. The same adversary profile was used for all scenarios. In ADVISE we characterized the adversary by three weights corresponding to reducing attack costs w_c, maximizing attack payoff w_p (i.e. reaching the goal) and avoiding detection w_d. ADVISE uses a dimensionless unit of time, as it provides a means for comparing different strategies without the ability to specify concrete timescales to carry out the simulated attacks. It is thus a measure of effort put into the attack. In our study we assumed that basic attack steps, like gaining access to the Internet or making an attempt to login to either CEMS or AMR, requires one unit of time. More complicated attack steps, like forging the CEMS protocol or disclosing AMR data requires exponential execution time with respect to the basic one.
This study is based on the following assumptions:

[A.1] The adversary has no direct access to the CEMS and AMR gateway devices (i.e. the adversary is external to the customer's premises).
[A.2] In scenario B and C, where CEMS and AMR are directly connected, reaching Goal 2 (i.e. CEMS intrusion) includes reaching Goal 1, since the AMR metering information is also available through the CEMS through a unidirectional link from AMR to CEMS.
[A.3] The command/control interface of AMR gateway and CEMS is telnet/web-based.
[A.4] No intrusion detection system is deployed.
[A.5] Forging the protocol between LVGC and CEMS has the same difficulty for both directions.
[A.6] In scenario A, the AMR only forwards messages to the CEMS and has no access to the CEMS data.
[A.7] Gaining access to a narrowband AN has the same difficulty as to a broadband AN.
[A.8] Gaining access to either the narrowband or broadband AN is fifty times more difficult compared to accessing the Internet, with the probability of connecting to the Internet equal to 1.
[A.9] CEMS and AMR have an equal difficulty to log into, which is ten times more difficult than accessing the customer's Internet modem.
[A.10] The adversary does not care about detection and is more attracted by the potential payoff than the attack step cost ($w_c = 0.2$, $w_p = 0.8$, $w_d = 0$).

As for the attack path, in order to reach Goal 1 (i.e. disclosure of metering data), the adversary has two options: (i) access the AMR gateway and get the metering data or (ii) sniff AMR messaging. In order to do that, the adversary has to access dedicated access networks in scenarios A, B and C, and the Internet in scenario D (see Figure 1). In scenario D, the adversary, in order to get access to the AMR gateway, firstly needs access to the household network. In a similar way, in order to reach Goal 2, the adversary has two options: (i) forging the CEMS-LVGC communication protocol, in order to either send fake flexibility data to the LVGC or to fake set points to the CEMS; or (ii) accessing the CEMS and alter the received set points. It is worth noting that scenarios A and B are equivalent from the point of view of the adversary for Goal 1, due to assumption [A.7]. Moreover, scenarios B and C are equivalent for Goal 2, given assumptions [A.2] and [A.7]. The result graphs of the next section clearly show these equivalences.

ANALYSIS RESULTS AND DISCUSSION

Figure 2 and Figure 3 show the results of the simulation carried out through ADVISE. In particular, the figures show the probability that the adversary reaches its goal (i.e. the probability of successfully attacking the system P_{as}) over the

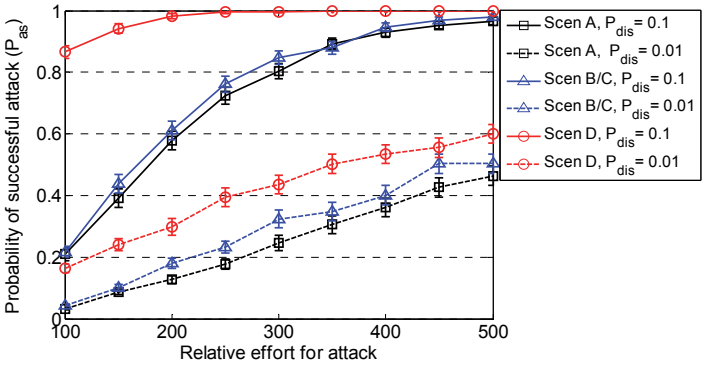

Figure 2: Success probability P_{as} for attack Goal 1

relative effort required for performing the attack. The results are obtained for two different values (0.1 and 0.01) of the probability of successfully disclosing the AMR communication protocol (P_{dis}) and successfully forging the CEMS communication protocol (P_f).

As described in the previous section, scenarios B and C are equivalent with respect to Goal 1, given assumption [A.7]. Indeed in both scenarios, once the adversary gains access to the dedicated access network, it can try to log into the AMR. In these scenarios the adversary can obtain the metering data also from the CEMS, given assumption [A.2]. Figure 2 shows that scenario D has the highest probability to be successfully attacked. This is reasonable, since the adversary has a higher probability to gain access to the household network through pervasive Internet connections like the customer's DSL. Scenarios A, B and C perform similarly for Goal 1, with B and C being slightly less robust than scenario A. This is due to the fact that the adversary can obtain metering data not only through logging into an AMR gateway, but also by logging into the CEMS which has access to the AMR's metering data.
As for Goal 2, the adversary can either log into CEMS from AN or from AMR gateway in scenarios B and C, because of assumption [A.2]. From Figure 3 we can observe that scenario D has the lowest robustness against the adversary attack, since the adversary has a higher probability to get

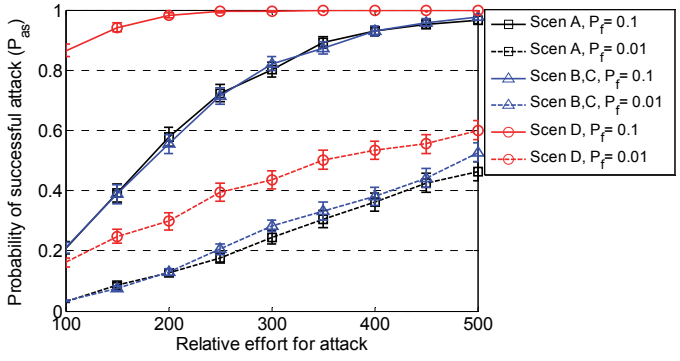

Figure 3: Success probability P_{as} for attack Goal 2

access to the LAN through Internet with respect to a dedicated network. Scenarios B and C perform slightly different with respect to scenario A, because an attacker can log into the CEMS also through the AMR gateway. Since it can be reasonably assumed that an adversary's choice to perform an attack through the AMR gateway is less probable than a direct attack from the AN, these scenarios do not show very significant differences.

CONCLUSION

The presented results show the impact of integrating additional CEMS and AMR devices into low voltage grid control networks through a risk analysis which considers different architectural options for integrating these devices. The probability of a successful attack has been evaluated as a function of the relative efforts for attackers to compromise these systems. The results show the relative robustness of the considered architectures as a support to the design of highly secured and reliable infrastructures down to these ICT devices in the households.

ACKNOWLEDGEMENT

This work has been supported by the European FP7 Project *SmartC2Net* under grant agreement no. 318023). Further information is available at www.smartc2net.eu [4].

REFERENCES

[1] Elizabeth LeMay, Michael D. Ford, Ken Keefe, William H. Sanders, Carol Muehrcke "Model-based security metrics using adversary view security evaluation (advise)." Eighth International Conference on Quantitative Evaluation of Systems (QEST), IEEE, Aachen, Germany, 2011.

[2] IEC 61508-1:2010, "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements," Technical Report, 2010

[3] C. Hägerling et al., "SmartC2Net Communication Architecture and Interfaces", Technical Report, EU FP7 Project SmartC2Net, Sep. 2013.

[4] European Commission - FP7. (2012, December) SmartC2Net – SMART Control of energy distribution grids over heterogeneous Communication NETworks. [Online]. Available: http://www.smartc2net.eu