THE EFFECT OF MESSAGING SECURITY ON THE DEMAND RESPONSE PROGRAMS

Elif Ustundag Soykan[1], Mustafa Bagriyanik[2]
[1]TUBITAK BILGEM
[2]İstanbul Technical University, Department of Electrical Engineering
Corresponding author: Elif Üstündağ Soykan, e-mail: elif.ustundag@gmail.com

REFERENCE NO

MANG-02

Keywords:
Smart Grid, Demand Response, Security, Notification Messaging

ABSTRACT

As the smart grid is an inevitably developing area, security and privacy of the smart grid have been the subject of various studies, projects and standardization efforts. However there is lack of attention to the security and privacy of the demand response especially on the communication channels with the customer that may adapt different IT technologies. In this study, we focused on DR programs' notification message security with a risk assessment approach that uses the SGIS toolbox to identify threats, conducting impact analysis and estimating likelihood of the attacks for various attacker types and motivations.

1. INTRODUCTION

Demand Side Management (DSM) is a mechanism that comprises the planned and implemented methodologies in order to balance demand with supply by guiding consumers to alter their consumption with demand response (DR) methodologies. The U.S. Department of Energy defines the DR as: "Changes in electricity usage by end-use consumers from their normal consumption pattern in response to changes in the price of electricity over time, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardized.", [9].

As it can be seen in the Fig. 1, DR methods fall into two categories, price-based and incentive-based namely. Price based methods comprises real time pricing, time of use and critical peak pricing programs and aims to balance the consumption of the peak periods by adopting hourly basis prices to reflect real-time cost to the consumers. Incentive based programs direct consumers to reduce their consumption by offering special rewards to manage excessive demand.

While DR programs are very effective tool to save the peak demand (up to %20 according to "US Federal Energy Regulatory Commission's report"), consumer involvement is key to success of any DR program as well as the other planning and execution parameters.

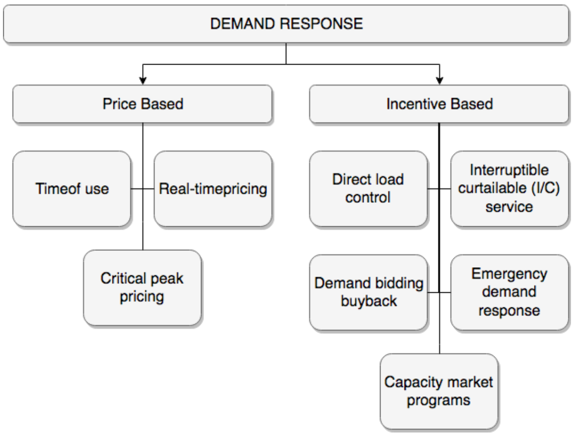


Fig. 1. DR programs

One way to increase consumer interest to the DR programs is using notification messages via some end point communication methods. There are different types of DR notification messages. Some of them aim just to give information about their usage via Energy Orbs. (a light to visualize electricity consumption) or via commercial products like Energy Detective [11] while some messages aims to direct users to change their usage for energy saving by giving them monetary incentives which can be Short Messaging Service (SMS) [24] based notifications or tablet based wall displays that are installed resident house. In this study we focused on SMS based messages since the most effective notifications are monetary based messages as experienced in [10]. Additionally, it requires no additional cost for users since an additional commercial product is not needed, and mobile phones penetration is high.

DR programs are not only important for customers but also for the stability of the smart grid since they leverage the reliability of the grid by balancing the load. A vital part of ensuring reliability is securing the grid from cyber-physical attacks. In order to protect the grid, the first step is to understand how an attack would affect the grid asset, what the probability of a specific threat scenario to happen is, and how to react if that attack occurs. This leads us to risk management practices.

There are a lot of risk management methodologies based on the ISO27005 framework; examples are HMG IA [2], ISO/IEC 31000 [16], NIST 800-30 [17] frameworks that can be used for organizational information security risk assessment. Although they are not specified for smart grid use cases, may support as guidance. The Smart Grid Information Security (SGIS) toolbox [8] was issued by the standardisation bodies CEN, CENELEC and ETSI to address cyber security and risk assessment in smart grids in regards to the M/490 Smart Grid Mandate by the European Commission. The toolbox is adopted by several EU funded projects, such as SPARK [4], SOES [18], for smart grid use cases. Although there are some deficiencies of the SGIS toolbox (see Annex C of [4]), it is still the most appropriate methodology for smart grid risk assessments as it is tailored for the domain. Hence, in this study we have embraced this methodology for the demand response use case.

To determine the risk level for an information asset, the SGIS methodology foresees six steps; we have neglected the third step, identification of supporting components step, as it adds extra complexity to the use case. So we have five steps to conduct the risk assessment of the use case that is shown in the Fig. 2. We discuss each step of the toolbox in section 3 in more detail.

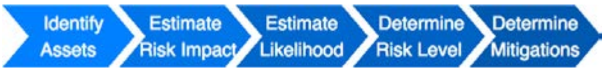


Fig. 2. SGIS Risk Assessment Steps

The paper continues as follows; the demand response use case using SMS notification messages is given in section 2 together with a system model, actors and network interfaces. Security risk assessment based on SGIS toolbox is given in section 3 including impact, likelihood analysis and security mitigations. The paper concluded in section 4.

2. DEMAND RESPONSE USE CASE

The use case aims to balance the load by sending a DR notification message via SMS to the consumer. The SMS message can be a simple one, like; “Reduce your consumption during 7-9 am tomorrow”, or it can be more specific, like, “Reduce your consumption to 5 kWh during 7-9 am tomorrow by switching off TV and avoid using your air-conditioner.”

In the next section we give the use case actors and interfaces between these actors. The communication interfaces of the use case are given in Fig. 3.

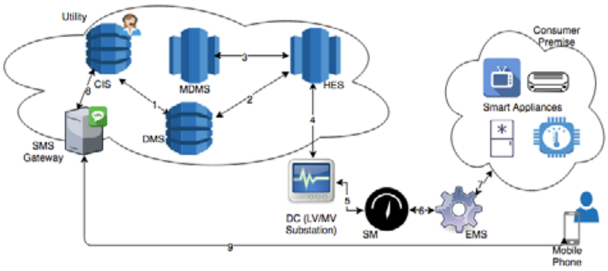


Fig. 3. Communication model of use case

2.1 Use Case Actors and Interfaces

Customer Information System (CIS): Utility’s back-end system or application that stores long term information for energy customers such as contacts, meter ID, bills, etc. It interacts with distribution management system and SMS Gateway via web services.

Data Concentrator (DC): A device working as an intermediary gateway between Smart Meters (SM) and the central Head End System

(HES) in order to communicate with SM and collect meter data. They are located at Distribution LV/MV Substations. It interfaces with SM over PLC (IEC 61334) [19] or DLMS/COSEM (IEC 62056) [20] and HES over IEC 62056 or IEEE 1377 [21]

Distribution Management System (DMS): A system that provides services to monitor and control a distribution grid from a centralized centre. Distribution automation is a function of DMS that provides real time management of failures, load and voltage change without operator involvement. DMS communicates with HES and CIS over web services.

Energy Management System (EMS): It aims at the optimization of the energy consumption based on commands received from the DMS (through HES, DC and SM), customer's parameters, and performance of device constraints. It then sends the commands to smart appliances through PLC or Zigbee (IEEE 802.15) [22].

Head End System (HES): Utility's central data system collecting consumption data from smart meters in its service area. In our use case we assume that it is owned by the Utility. It communicates with DMS, meter data management system (MDSM) over web services and DC over EN 62056 or IEEE 1377 interfaces.

Meter Data Management System (MDMS): Utility's system for managing the metering data, coming from the HES, which is a unidirectional communication over IEC 61968 [23].

Smart Appliances (SAs): It is a controllable smart device (dishwasher, ventilation, refrigerator etc.) that has the optimization capability in accordance with a signal from the grid. The signal can be information like the cost of energy or a Demand Respond signal (delay load signal or other related information). They communicate with EMS via PLC or Zigbee interfaces.

Smart Meter (SM): Utility's metering end device at customer's premises that has bidirectional communication functionality. It communicates with EMS and DC over PLC or DLMS/COSEM (IEC 62056).

Short Messaging Service (SMS) Gateway: It is a gateway that provides SMS application interface to the utility's corporate server and communicates with GSM network in order to deliver the message to the recipient customer.

2.2 Use Case Information Flow

The use case is triggered when the DMS detects the need for lower power consumption in a certain area. It then asks for information from the CIS regarding which customers have enrolled to the DR program, resulting with a reply from CIS with a list of customers. DMS checks customer's consumption from HES, selects customers and then informs CIS which customers will be receiving SMS messages together with the content of the message.

CIS prepares the SMS message content and identifies the customers phone numbers. Then, SMS gateway delivers the message to the customer thorough the GSM infrastructure. When the customer receives the message, he/she decides whether to accept the power saving offer, and then replies to the message. If CIS receives an approval response from customer, DMS is informed so that it can send load reduction request to the HES (including the parameters power to be saved, begin time, end time and other parameters required by the communication). HES then delivers the request to the SM via DC and the request is finally sent to the EMS. After evaluating the message and status of the SAs, EMS sends positive or negative acknowledgement (ACK/NACK) to the DMS (through SM-DC-HES) regarding the result.

We assume that the customer is a registered user of the utility and has already enrolled to the utility's DR program. It is also assumed that CIS possesses required customer data.

3. RISK ASSESSMENT OF THE USE CASE

We have performed risk assessment on the DR use case for each information asset identified. The following subsections explain the detail of each risk assessment step.

3.1 Identifying Assets

As a first step of the risk assessment approach, here we identify the assets of the use case.

In order to simplify the analysis, we group them according to the network area they belong. We assume attackers might target the following components of the DR Messaging Use Case:

- Utility Corporate Network (CIS-MDMS)
- Utility Operational Network (DMS-HES)
- DC
- Customer Network (SM-EMS-SAs)
- SMS Network (SMS Gateway-GSM Infrastructure-Mobile Phone)

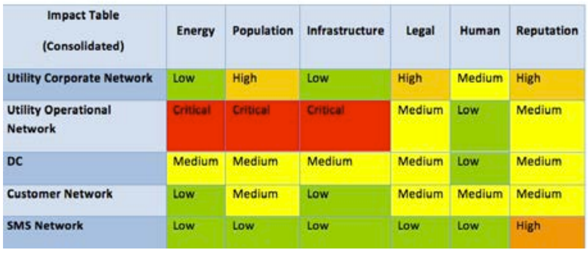
3.2 Impact Analysis

Risk impact is derived from different measurement categories and stated in five Risk Impact Levels. SGIS Impact Analysis methodology identifies five different categories: Operational (Energy, Population Infrastructure), Legal, Human, Reputational and Financial. So, each category is measured for their impact levels according to Confidentiality, Integrity, and Availability requirements. At the end of this process, three different risk impact levels are determined by grouping the results of each type of scenario (availability, integrity and confidentiality) for the analysed asset; and then the highest level is considered.

We first start with identifying possible threats to the system depicted in the use case. We have benefited from NESCOR study [13] that provides DR threat scenarios and adapted them to our use case. The possible threats identified are as follows;

- Publicly disclosing the private information on the communication channel by eavesdropping on the network. This threat can be classified under the “Confidentiality” category and violates privacy of the customer and utility. It may cause legal effects for the utility.
- Modifying or spoofing messages (e.g. smart meter last gasp message) on the communication link. This threat can be classified under the “Integrity" category and violates the reliability of the grid (triggering an inappropriate DR event). It may cause power loss and financial effects for both customer and the utility.
- Preventing legitimate DR messages from being retrieved and transmitted by tampering with the communication or flooding channel by other messages. This threat can be classified under the “Availability" category and violates both the reliability of the grid and the cost.
- Compromising one or more DR system devices causing inappropriate DR messages at undesired times to be sent to unintended devices/customer. This threat can violate confidentiality, integrity and availability of the grid depending on the compromised device and the motivation of the attack.
- A malware injection to the one or more DR system device causing malicious use of system resources (slowing down the system, sending unwanted DR messages etc.), and unauthorized access to customer data. This threat can violate the confidentiality, integrity and availability of the grid depending on the compromised device and the motivation of the attack.

In order to estimate the impacts on the assets, the SGIS tool describes seven categories that must be evaluated during this process for identifying the risk impact produced by security incidents, namely energy, population, infrastructure, legal, human, reputation and financial. We have neglected financial category due to evaluation complexity. On the other hand we foresee that financial impact is not higher than its counterparts. We evaluate the impact on the energy category based on the size and type of grid affected by the threats we have defined. In the population category, we determined the level based on the size of population affected in the target area of DR program. Infrastructure category impact level depends on how many critical, essential or complimentary infrastructures could be affected by the threats. In the Legal category the SGIS tool focuses on Data Protection law hence the impact level is measured in accordance to the former version of GDPR [25]. Although we think that this should be updated, we keep levels as they are, as we do not have legal expertise on this subject matter. Finally, while the human category measures how threats directly or indirectly impact people's health, the reputation category measures how they damage an organization's reputation.



Impact Table (Consolidated)	Energy	Population	Infrastructure	Legal	Human	Reputation
Utility Corporate Network	Low	High	Low	High	Medium	High
Utility Operational Network	Critical	Critical	Critical	Medium	Low	Medium
DC	Medium	Medium	Medium	Medium	Low	Medium
Customer Network	Low	Medium	Low	Medium	Medium	Medium
SMS Network	Low	Low	Low	Low	Low	High

Fig. 4. Consolidated Impact Table for Confidentiality-Integrity-Availability

3.3 Likelihood Analysis

The SGIS methodology does not offer its own likelihood analysis method rather it refers to the HM/IS1 standard's [2] method. It gives suggestions on the threat factors in [3] without considering vulnerability factors (leaving them for the next update of the document). In this study we combine both the SGIS methodology and OWASP [15] methodology that considers the likelihood analysis in a broader sense. In order to combine the two methodologies, we adopt OWASP's ratings into a five-scale approach.

Here, we give brief information about what the threat factors we considered mean. Threat capability criteria and threat interest factors are excerpted from SGIS methodology while threat opportunity, ease of discovery and ease of exploit factors come from OWASP methodology.

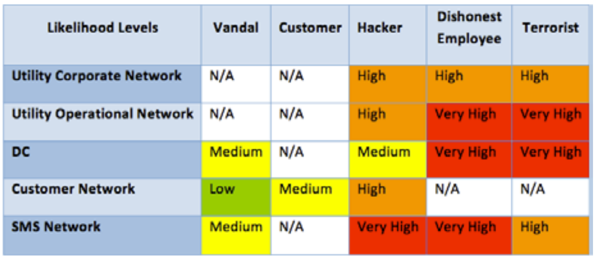
- Threat capabilities criteria shows how technically skilled the group of threat agents are.
- Threat interest shows how motivated this group of threat agents is to find and exploit the vulnerability.
- Threat opportunity means what resources and opportunities are required to find and exploit the vulnerability.
- Ease of discovery is a vulnerability factor used to estimate how easy for the attacker is to discover the vulnerability
- Ease of exploit is a vulnerability factor used to estimate how easy for the attacker to actually exploit the vulnerability.

In order to estimate the likelihood level, we first identify the attacker types. Then for each type and asset we determine the scale for all threat factors (1 to 5) that we described above. Finally we calculate the summation and normalize it according to the equation (1). The result will be our final level for that asset.

Considering the attacker capabilities and their motivations to perform an attack, we identified the five attacker types, which are Vandal, Customer, Hacker, Dishonest Employee and Terrorist actors. They differ in motivation (money, grudge, political aspects etc.), tools they used, capabilities and access privileges to asset. We assume that Customer type is more focused on home area network (HAN) level assets and can not access Utility site. Hence likelihood level is only applicable for HAN level. Contrary to this, Terrorist and Dishonest Employee types are barely interested in HAN level, rather they aim to attack Utility's site. For Hacker type we should consider that it could have penetrate in each level. Vandal type don't have high privileged so damaging easily accessible networks are more attractive for them.

$$Likelihood\ Level = (Rating\ (Threat\ Capability + Threat\ Interest + Opportunity + Ease\ of\ Discovery + Ease\ of\ Exploit))/5 \quad (1)$$

The likelihood levels computed according to (1) are shown below:



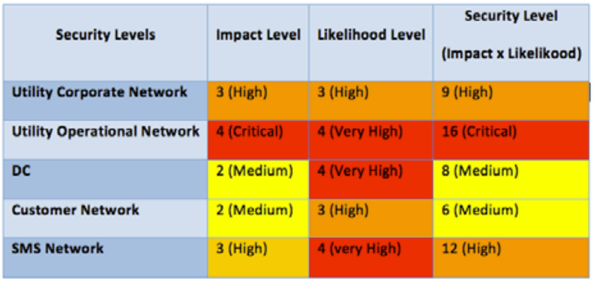
Likelihood Levels	Vandal	Customer	Hacker	Dishonest Employee	Terrorist
Utility Corporate Network	N/A	N/A	High	High	High
Utility Operational Network	N/A	N/A	High	Very High	Very High
DC	Medium	N/A	Medium	Very High	Very High
Customer Network	Low	Medium	High	N/A	N/A
SMS Network	Medium	N/A	Very High	Very High	High

Fig. 5. Likelihood Levels

As it can be observed from the Fig. 5 each asset has more than one likelihood level. As the SGIS approach suggests, in order to estimate the security level we take the highest likelihood level for each asset as the final level.

3.4 Security Level

The next step is to combine the Impact and Likelihood Tables in order to find out “Security Levels” table that represents the risk levels. We adopted the “third approach” suggested by SGIS methodology, as we think that it is more appropriate to the context. The approach estimates the security level by multiplying impact and likelihood ratings then the result is mapped to the appropriate level as given in Fig. 6



Security Levels	Impact Level	Likelihood Level	Security Level (Impact x Likelikood)
Utility Corporate Network	3 (High)	3 (High)	9 (High)
Utility Operational Network	4 (Critical)	4 (Very High)	16 (Critical)
DC	2 (Medium)	4 (Very High)	8 (Medium)
Customer Network	2 (Medium)	3 (High)	6 (Medium)
SMS Network	3 (High)	4 (very High)	12 (High)

Fig. 6. Final security levels for each information assest

3.5 Security Discussions and Mitigations

In practical use, SMS messages are not encrypted by default during transmission. Even tough there are certain security measures in the technical specifications for SMS in ETSI TS 03.48, they are not mandatory requirements. Confidentiality and integrity protection is not available for SMS messages. There are a lot of well-known threats regarding SMS usage and implementation like message disclosure, spamming and SMS phishing. From the privacy point of view, the message disclosure threat must be a concern, as it reveals energy consumption data like peak hours, SAs being used, consumer behaviour etc. However SMS threats have more devastating effects on the grid reliability as it allows attackers to change the SMS content leading to wrong decisions made by the customer, e.g. customer receives an altered message that encourages to increase consumption even if the actual load is high.

Cybersecurity attacks create implications about trust and confidence with the customers that may affect consumer’s penetration to the DR programs, as they allow the utility to access the consumer’s home and turn on/off components to achieve more reliable grid. Hence utilities must address trust issues in their risk management plans in order to implement the program successfully.

Looking at the estimated Security Levels of the use case suitable mitigations should be selected. Annex B of [3] refers NISTIR 7628 for the control list. Each security measure in the NISTIR list is mapped with the SGIS security level that can be used as guidance. However these controls do not fulfil our use case regarding SMS network information asset therefore countermeasures should be extended in order to ensure that all assets are covered.

We highly recommend that all of the security measures in NISTIR 7628 should be implemented for the utility corporate network; utility operational network and SMS network as the security level of these assets are either high or critical.

4. CONCLUSIONS

In this study we demonstrated real time pricing DR use case with SMS integration for notification messages. We defined the use case and its communication infrastructure. Based on the use case, assets were derived and risk assessment was applied on these assets. The risk assessment approach followed in this study is built on two approaches: SGIS and OWASP methodologies are combined in order to close the deficit of SGIS methodology. The approach, the analysis result and mitigations are given in related sections.

The risk assessment outcomes show that the most important asset is the utility operational network due to the impact of an attack and its likelihood. The other crucial assets to be worried about are corporate network and SMS communication channel.

In order to have a more accurate assessment this study could be extended so that DR use case is realized with a simulation using benchmark suits.

References

[1] ISO/IEC 27005:2011 Information technology, Security techniques, Information security risk management (second edition), http://www.27000.org/iso-27005.htm

[2] HMG IA Standard No. 1 Technical Risk Assessment Issue 3.51, October 2009.

[3] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Information Security, Nov 2012.

[4] SPARKS project, https://project-sparks.eu/ last access on 30.10.2017

[5] CEN-CENELEC-ETSI Smart Grid Coordination Group, SG-CG/M490/H_ Smart Grid Information Security Report, December 2014.

[6] Jain et.al (2015) 'Methodologies for Effective Demand Response Messaging', IEEE Confrence on SmarGridComm, Access No 15870511

[7] Federal Energy Regulatory Commission, "A National Assessment of Demand Response Potential," 2009.

[8] http://www.theenergydetective.com Last access 31.10.2017.

[9] Office of Electricity Delivery and Energy Reliability, Benefits of Demand Response in Electricity Markets and Recommendations for Achieving them. Washington, DC: U.S Department of Energy, 2006.

[10] Jain et. Al. Methodologies for Effective Demand Response Messaging, IEEE International Conference on Smart Grid Communications, 2015

[11] www.theenergydetective.com, Last access 05.01.2018

[12] Langer et. al., Smart Grid Cybersecurity Risk Assessment Experiences with the SGIS Toolbox, 2015, SPARK Project outcome

[13] NESCOR. (2015). Electric Sector Failure Scenarios and Impact Analyses – Version 3.0, (December). Retrieved from http://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf

[14] NISTIR 7628 Retrieved from https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

[15] OWASP Risk Rating Methodology https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology last accessed on 29.01.2018

[16] ISO/IEC, "ISO 31000:2009, Risk management – Principles and guidelines," 2009, Available online at: http://www.iso.org/iso/home/standards/iso31000.htm

[17] NIST SP 800-30 Guide for Conducting Risk Assessments, 2012

[18] SOES project, http://www.soes-project.eu Last accessed by 29.01.2018

[19] IEC 61334, International Electrotechnical Commission Standard, Distribution automation using distribution line carrier systems

[20] IEC 62056, International Electrotechnical Commission Standard, Data exchange for meter reading, tariff and load control

[21] IEEE 1377, IEEE Standard for Utility Industry Metering Communication Protocol Application Layer

[22] IEEE 802.15, IEEE Standard for Information technology, Local and metropolitan area networks

[23] IEC 61968, International Electrotechnical Commission Standard, Common Information Model (CIM) / Distribution Management

[24] GSM Technical Specification 3.40 Retrieved from http://www.etsi.org/deliver/etsi_gts/03/0340/05.03.00_60/gsmts_0340v050300p.pdf , 1996

[25] EU Data Protection Directive, Directive 95/46/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en, 1995 Last accessed 29.01.2018