The Twin Towers #1, 33 Jabotinsky St.
Ramat Gan, Israel. Tel: +972-3-6134703
www.c4-security.com

The Dark Side of the Smart Grid -

Smart Meters (in)Security

Abstract

This whitepaper will first demonstrate why Smart Grid technologies pose a complex yet critical security issue for the utility adopting it.

Following the demonstration of the need to secure the Smart Grid, 9 critical attack vectors and vulnerabilities relevant to Smart Grid deployments will be presented. These scenarios are investigated for two main reasons:

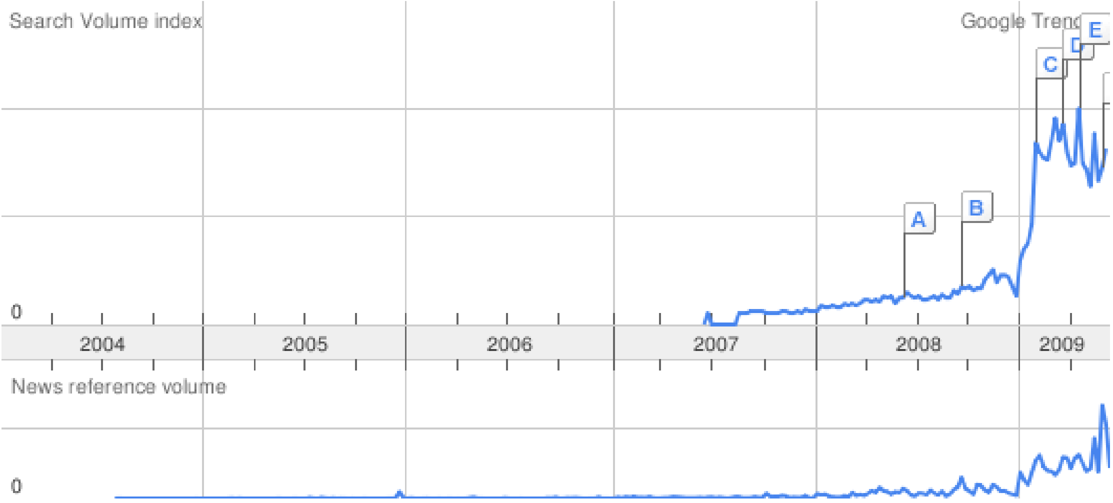
1. Raise the security awareness regarding the new threats introduced by implementing a Smart Grid

2. Encourage a discussion about potential remedies to mitigate these vulnerabilities

The information and vulnerabilities mentioned in this whitepaper are a result of security audits performed by C4 Security on 3 Smart Grid deployments – one for a water pipeline utility and two for electric grids.

Introduction

Smart Grid implementations for electric, gas and water distribution are the latest trend in the fields of green technology, demand management and network stability and advanced customer services. Even if this technology is yet to reach your home, rest assured that deploying smart meters is a frequently discussed matter in the meeting rooms of your utility companies. The growing interest in this concept can also be seen in a quantitative measurement of search volume as measured by Google, indicating an increase of over 800% from 2007 to 2009. This measurement graphically demonstrates the increase of public interest in this domain, as observed by Google's search application:



Source: Google Trends – Smart Grid search volume over time:

http://www.google.com/trends?q=smart+grid

Smart Grid Definition

The first important thing to understand about the Smart Grid is that there's no single, widely-accepted definition to what it is, as it is still largely "work in progress" and multiple parties are still trying to define and influence on its scope. The common problem of "term inflation" in engineering also appears in this field – one man's AMR is another man's AMI or Master Meter. This whitepaper intentionally makes use of a small subset of terms as otherwise it would not be readable due to the many interchangeable (and sometimes contradicting) terms.

Smart Grid allows energy and water utilities to achieve 3 main goals:

1. Increased stability of the distribution network – the ability for the grid operator to receive extremely granular measurements in real-time

2. Green operation – allow variable tariffs in accordance to time of day in order to make demand fluctuations less sharp. This goal is especially important for electric grids as it decreases the need for power plants since the maximum generation capacity is decreased

3. Efficiency – remote maintenance and operation of grid endpoints allows faster handling of customers with less technicians

The above description is a simplification of the Smart Grid concept. To learn more about what the Smart Grid is, please review the DoE site at: http://www.oe.energy.gov/1165.htm.

It should be noted that commonly the term "Smart Grid" is associated with the electric grid. However, apart from the ability of customers to sell the commodity back to the grid operator, these concepts and technologies are starting to be implemented in gas and water utilities as well. Although the infrastructure of these utilities is not considered a grid, it does share similar characteristics from an end-consumer distribution aspect. For this reason, this whitepaper does not discuss transmission-level electric Smart Grid technologies such as Phasor Measurement Units. These technologies do not directly relate to the distribution of electric power and hence security issues associated with these devices cannot be generalized to similar devices in other utilities. The term Smart Grid may also apply to even more peripheral fields such as the supporting grid operations for electric cars charging/advanced billing, and likewise this whitepaper will not cover these areas in order to keep a well-defined scope.

SCADA Security Background

In order to fully understand the damage potential and probability, a brief recap of Control/SCADA security is needed. Control systems were initially built from relatively simple electric and mechanical devices. A typical control room would have hundreds of buttons, dials, levers and gauges in every form, shape and color. The control system as a whole was dedicated solely for the control purposes and therefore was stand-alone in nature. In the past 20 years three changes impacted the security of control systems, technological and business-induced:

1. As the computing power and "off the shelf" capabilities of general purpose PCs and servers increased dramatically over the years, standard computers and commercial operating systems gradually replaced their electrical and mechanical predecessors.

2. Another technological shift that soon followed was a change from proprietary, serial communications to IP based networking. It is nowadays rare to find a control center that is not using IP as its primary communication protocol, and recently more and more field devices have a standard Ethernet/IP port alongside or instead of the more traditional RS232 port.

3. The corporate environment is constantly getting more competitive, and business executives became more computer-literate. These two factors lead for a demand by the corporate executives to obtain real-time data from the control network in order to improve their business performance. This need led to interconnection between the control and corporate networks.

The abovementioned changes caused general-purpose IT frameworks and connectivity to "infiltrate" to the control systems zone, which traditionally was not designed with data security in mind. The overall effect is that systems that were previously considered as an unknown "black box" isolated from the outside world, are now accessible and relying on technologies that every computer programmer or administrator is familiar with.

For more information regarding SCADA security vulnerabilities found by C4, go to: http://www.c4-security.com/index-5.html

Smart Grid = Micro SCADA?

Smart Grid at the distribution level allows two main functions:

1. The control center can read meters data
2. The control center can control meters by sending connect/disconnect commands that shut off or connect the water or power supply to the consumer

These services combined can be viewed as a "micro-SCADA" system – command and control over the process control network from a centralized control center. In the case of the Smart Grid, the smart meters are either controlled from the actual SCADA control center of the distribution company (water or electric), or by a dedicated Smart Grid NOC.

The command and control nature of the Smart Grid data network poses a difficult challenge from a security perspective. No longer are the nodes of the control network located in secured server rooms or located inside a fenced cabinet with an alarm and/or video surveillance system. The nodes, or meters in this case, are located in the homes and businesses away from the public eye and with almost no possibility for the utility to restrict access and detect tampering events. In other words – the end points of this micro-level command and control network are a sitting duck. The utility must assume that these devices will be investigated, audited and tampered with. Imagine what an interesting case study such a meter poses to any engineering student or aspiring computer hacker who wants to pave his way to fame at the expense of the utility.

The ease and discreteness of access to the Smart Grid nodes, along with the traditional lack of security state of affairs common in control/SCADA systems field protocols is a dangerous mix. Two of the SCADA attack vectors, Field to Field and Field to Control Center, become easily exploitable – all one has to do to attack is become a customer of the utility. Gaining access to a control network has never been easier. In a sense, this new deployment puts utilities in a similar security stance as the Cable/Satellite set-top box industry, where the end devices are considered to be at a high risk of tampering and therefore the potential damage (mainly financial loss in the latter case) must be contained even under these circumstances. This is not an easy task, and took most manufacturers over a decade to come to an industry-wide solution that managed to meet the challenge.

Smart Grid Vulnerabilities

The Smart Grid vulnerabilities are all deductions from the Field to Field and Field to Control Center attack vectors. Some are general SCADA security vulnerabilities, while others are Smart Grid specific. The listed vulnerabilities are not necessarily ordered according to severity, which is affected by the particular utility type, infrastructure, potential attacker profile and many other factors that need to be determined in the general risk assessment process.

1.1 Use of Public Telecom Infrastructure

Deployment of millions of meters in households makes the use of public telecom infrastructure a very appealing alternative to private telecom solutions. However, relying on an external party for such a critical element of the system raises some security concerns:

1. Which of the employees at the telecom company can access the equipment? What are their credentials and security clearances?
2. Is the telecom company conducting audits to secure this part of the network?
3. Is the networking equipment accessible from the internet or to companies other than the telecom company via extranets?
4. Does the telecom company have a DRP (disaster recovery plan) procedure that includes the network that is assigned for the utility's use?

The answers to these questions should be backed up by printouts and procedure documents to satisfy the utility that security precautions are being taken and that they meet the overall security requirements of the Smart Grid.

Failure to provide a positive answer to any of these questions exposes the network to unnecessary risk. For example, if a router has a public IP address although it's only used for the Smart Grid communication, a DDoS (distributed denial of service) attack can disrupt all communication via that router, resulting in loss of communication between the utility and the meters. This attack can be launched from anywhere around the world.

1.2 Network Management from Remote Nodes

Each meter is a node in the Smart Grid network. Although the processes being executed on the network require only data to be read and commands to be sent to the meter, the management applications and services remain exposed and available for all the nodes.

The practical implications of this scenario is that without explicit constraints, an attacker who uses the communication module of the smart meter can cause network-wide changes, ranging from disrupting the communication flow to rerouting all the traffic to his node for later manipulation.

1.3 Lack of Authentication

C4 Security has encountered numerous meters that didn't have any authentication or encryption support. This design flaw makes it possible for an attacker to impersonate the control center and send unauthorized commands to meters or read metering data. The consequence of a successful attack on meters with disconnection capabilities is particularly destructive.

It should be noted that although some of the metering protocols support encryption, which can be viewed as a network access password, most of the deployments we've encountered so far did not enable these features. Since every metering standard includes support for "no encryption" or "no authentication", it usually poses too great a temptation for the integration teams which prefer to choose these settings in order to avoid additional deployment problems.

1.4 Authentication Bypass

Several metering protocols (DLMS, IEC 60870-5-102) implementation have functions to read metering data which do not require a password, and configuration/disconnect functions that require the operator password. Two meters that we audited retrieved the password for the restricted functions using the unprotected read function. This implementation makes the authentication/password protection completely useless.

1.5 Slave Meter Data Tampering

The protocol used for communication between the master (smart) meter and the slave meter is usually considered of lesser importance as its impact is restricted to the single customer household. Although this is generally correct, from a risk management point of view it is important to identify and address a situation where a cheap "man in the middle" device is inserted between the master and slave meters which lowers the usage reading by a constant division. This manipulation is both very hard for the utility to identify and can happen in a large scale if a criminal party decides to mass produce and market these devices – much like pirate cable set-top boxes / satellite decoders.

1.6 Slave Meter Unauthorized Disconnection

Some slave meters support disconnection of the customer upon receiving a request from the master meter. Normally the associated risk is minimal as if an attacker was to disconnect the slave meter, as these meters are commonly connected by wire to the master meter the physical presence is required and therefore disconnection could be achieved by bringing a hammer. This assumption causes to set low security settings to this communication channel, as it is perceived as non-critical. Unfortunately, some of the metering protocols used between meters are wireless (e.g. WMBUS, Z-Wave) making it possible for an attacker with a potent transmitter to send a disconnect signal to multiple customers, especially in crowded urban areas. The attacker will not need receive the data back from the meters to issue this command.

1.7 Insecure Protocol Implementation

Meters from a variety of vendors that were audited by C4 Security were found to improperly handle malformed requests. When a meter firmware makes certain assumptions regarding the data it receives, and in particular the maximum size of each message type, it may be vulnerable to a very well known attack condition named Buffer Overrun/Overflow Vulnerability. This vulnerability may allow the attacker to cause system instability or freeze, change values of parameters which are saved in the memory stack or even execute arbitrary code. In most of the meters and RTUs that were audited by our "red team", such a condition was identified and exploited.

1.8 Firmware Upgrade Vulnerabilities

Firmware upgrades are a double edged sword. The existence of the capability to remotely upgrade the meter firmware is of crucial importance – as security experts like to repeat a well known, and true, mantra that "what is considered secure today may be proven otherwise tomorrow". There's no assurance that a new unforeseen attack will successfully compromise a meter model and so in order to be able to respond the operator must have the ability to securely update the meter firmware to upgrade as many meters as it can before they are compromised.

The other side of firmware upgrades is that they serve as a powerful tool for attackers, if they can be abused. For example, an attacker who can push his own firmware to other meters can execute a disconnect action and then make the meter completely unresponsive till it is returned to the manufacturer, thus making it impossible for the network operator to reverse his actions.

To conclude, it is crucial to have a remote firmware upgrade capability, but one that was designed with security in mind and audited thoroughly by experts.

1.9 Input Validation

The all-too-familiar security problem of input validation, which is unfortunately quite common in control systems, was found to exist in Smart Grid meters and servers as well. Should an attacker be able to broadcast malformed messages to a node on the Smart Grid (which we elaborated on why that can normally easily be done) it will have a relatively high success probability to cause the node to fail. The failure is a result of assuming that the data received is in the expected message format, whereas when a malformed packet is parsed it causes an exception that may even lead to arbitrary code execution.

About C4 Security

C4 specializes in attacking and protecting critical command and control systems. The company's unique knowledge and tools in analyzing protocols and reverse engineering applications ensure that all possible vulnerabilities are discovered and dealt with. These capabilities are also leveraged to development of tailored security products upon customers' request.

C4 consists of leading experts in the field of penetration testing and application security who have acquired an in-depth understanding of attackers' methodologies and unique knowledge and tools in analyzing protocols and reverse engineering during multiple years of attacking a wide range of systems and software.

The main environments in which C4 concentrates include: SCADA systems and national utilities command and control systems, military C4I systems, trading and banking applications.
C4 has multiple clients around the world including utilities, governments, banks, private companies and more.