CHAPTER

Threats and Impacts: Utility Companies and Beyond

3

INFORMATION IN THIS CHAPTER

- Confidentiality
- Integrity
- Availability

We discussed the threats and their impact to consumers in the last chapter, but now let us focus on those that are relevant to utility companies, businesses, and governments. Some of these threats are similar, some are unique, but attacks against utility companies, businesses, and governments will have a broader impact than attacks against consumers.

The threats are broken down into the components of the CIA triad, depicted in Figure 3.1 below: confidentiality, integrity, and availability. The impact of these threats is presented in a hypothetical scenario format. However, these threats and their impact could very easily become reality. In some cases, they already have.

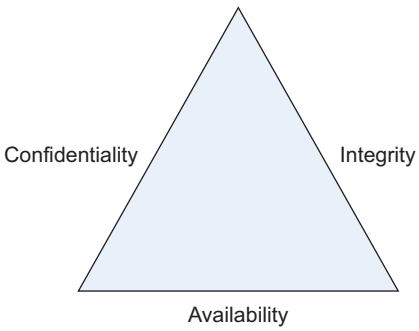

FIGURE 3.1

The CIA triad.

A Guide to Kernel Exploitation. DOI: 10.1016/B978-1-59749-570-7.00003-0

CONFIDENTIALITY

Confidentiality is attained when information is protected from unauthorized disclosure. A loss of confidentiality has the greatest effect on consumers. However, the aggregation of personal information about consumers by the utility companies makes them a significantly larger target to hackers.

Consumer Privacy

Utility companies collect and store customer information such as name, address, social security number, and consumption data; all information you and I expect to remain confidential. Breaching this confidentiality to access such information is the goal of many hackers, as highlighted in Verizon Business' 2009 Data Breach Investigations Report, "… criminals have had to overhaul their processes and differentiate their products in order to maintain profitability. In 2008, this was accomplished by targeting points of data concentration or aggregation…"[1]

However, hackers may not be the only ones who want this information. With the adoption of smart grid technologies, consumers will more frequently interact with their utility companies through Internet accessible Web applications. These applications will allow consumers to monitor and control their power consumption, and even control their smart devices. Law enforcement could utilize this information to support investigations, much like mobile phone data, such as global positioning satellite (GPS), is used today.

> **NOTE**
>
> Security and Privacy blogger Christopher Soghoian published findings on December 1, 2009 that Sprint, a United States based wireless carrier, provided law enforcement agencies customer GPS location data between 2008 and 2009. Over a 13-month span, Sprint provided customer GPS location data more than eight million times to different law enforcement agencies through a special Web portal.[2]

PII

As discussed in the previous chapter, smart grids present a host of threats to consumers. While we previously discussed targeted threats and impacts, compromising the confidentiality of consumer data housed by the utility companies presents a far greater reward than compromising the confidentiality of single consumer.

Scenario

- **Threat** – Hackers are able to compromise consumer databases operated by the HackMe utility company.
- **Attack vector** – A Structured Query Language (SQL) Injection vulnerability within the HackMe Web site utilized by consumers to manage their accounts, monitor their usage, and make payments.

- **Impact** – Hackers obtain the personally identifiable information (PII) of 500,000 HackMe customers. This information includes customer names, addresses, birth dates, social security numbers, and account numbers. For those customers who utilize automatic or online bill payment, Hackers also obtain customers' credit card numbers and bank account information. The hackers sell this information on the black market, and HackMe's customers are left to deal with repercussions. Government agencies, regulatory bodies, and customers become enraged that this information was compromised and the utility company is fined for not protecting the information properly.

NOTE

SQL Injection is an attack that consists of inserting a malicious Structured Query Language (SQL) query into data that is passed from the application client to the backend database server. Such attacks can allow an attacker to manipulate data within application databases. Often, these databases include sensitive information such as usernames, passwords, credit card information, social security numbers, and more. You can learn more about SQL Injection at www.owasp.org/index.php/SQL_Injection or Justin Clarke's *SQL Injection Attacks and Defense* (ISBN: 978-1-59749-424-3).

Consumption Data

We previously covered, in the "Illegal Activity" section of the previous chapter, how law enforcement agencies may utilize consumption information to determine if utility companies' customers are producing illegal substances. However, alternate uses by law enforcement include using similar information to determine the location of suspects during crimes.

Scenario

- **Threat** – Consumers become disenfranchised with smart grid technologies after the repeated use of consumption information in the prosecution of criminals.
- **Attack vector** – Law enforcement reviews suspects' historical consumption information to determine the likelihood that they were located at their residence during the time of crime.
- **Impact** – Customer backlash at the alleged misuse of consumption information forces utility companies to modify their smart grid deployments. These modifications pose a significant financial burden to the utility companies, and the public backlash slows the adoption of smart grid technologies.

Proprietary Information

Utility companies possess valuable information beyond that of their customers' PII. Proprietary information, such as trade secrets, will be targeted by hackers who

believe they can sell the information to competing organizations, governments, or terrorist groups.

Scenario

- **Threat** – A foreign government, frustrated by the sanctions imposed by the United Nations, utilizes its own hackers to compromise an American utility company and obtain trade secrets. These trade secrets will allow the foreign government to significantly increase its power-generating capabilities despite the imposed sanctions.
- **Attack vector** – An exploit is placed on the utility companies' Web site that leverages vulnerability in an unpatched version of a popular Web browser. When a utility company employee visits the Web site, the vulnerability is exploited, and malware is installed on their system. This malware allows the foreign government's hackers to gain access to the utility company's internal network and ultimately steal trade secrets on power generation.
- **Impact** – The foreign government is able to increase power generation despite the United Nations imposed sanctions. The utility company losses their competitive advantage as the trade secrets are eventually made public on the Internet. The utility company sees its profits drop significantly as their competitors reduce the gap that was once created by the trade secrets.

INTEGRITY

Integrity is attained when information is protected from unauthorized modification. A loss of integrity has the greatest effect on the utility companies, which is manifested in fraud and service theft.

Service Fraud

Regardless of the deployment architecture chosen by a particular utility company, their customers will have access to the smart meters deployed in their homes and businesses. While tamper-resistant mechanisms should be employed, countermeasures will undoubtedly be published on the Internet.

Once information on how to hack smart meters makes its way onto the Internet, the masses, ranging from hackers to curious consumers, will possess the knowledge on how to defraud their utility company. Some will steal services, while others will be as bold as to collect money from the utility companies by fooling the system to believe that the dwelling generated electricity for the grid instead of consuming it.

Service Theft

The most predictable threat to the utility companies as a result of smart meter tampering is service theft through under-reporting. Given the current state of the

economy, significantly lower utility bills may sound too attractive to resist to the average consumer.

Scenario

- **Threat** – Consumers hack their smart meters to modify the usage information being sent to the utility company.
- **Attack vector** – A vulnerable network device driver within the customers' smart meter allows remote code execution when properly exploited. Customers download and install custom software off of the Internet that exploits the vulnerability and loads custom firmware onto the smart meter.
- **Impact** – Customer is able to under-report their usage to the utility company. Thus, the customer obtains a lower bill while the utility company unknowingly subsidizes their customer.

Net Metering

The most profitable threat for consumers as a result of smart meter tampering is manipulation of net metering data. Net metering allows consumers to provide the utility companies with power generated by the consumers utilizing technologies, including wind and solar. In turn, the utility companies either provide the consumer with an account credit, or issue a check for the amount of energy provided by the consumer to the utility company.

Scenario

- **Threat** – Consumers hack their smart meters to modify the power generation information being sent to the utility company.
- **Attack vector** – An easily guessed password on an administrative interface (Secure Shell [SSH]) of the customer's smart meter allows complete access to the device, including the net metering data. The customer modifies the data using a tool they downloaded from the Internet.
- **Impact** – Customer is able to over-report the amount of power being provided to the utility company. Thus, the customer obtains a larger credit or even a check from the utility company, while they unknowingly are paying their customer for nothing.

NOTE

Within Section 1251 of the Energy Policy Act of 2005, the U.S. Congress mandated that all public electric utilities must make net metering available to their customers.[3]

Sensor Data Manipulation

Smart meters will include sensors that will allow the utility companies to perform myriad tasks ranging from post mortem forensic analysis to power system

restoration, to distribution network monitoring, restoration, and self healing. However, if the integrity of the sensor data is compromised, the result will be disastrous.

Scenario

- **Threat** – Brett, a self-taught hacker, is curious about how the "whole smart grid thing works." Being in high school, Brett lives with his parents, whose house was recently fitted with a smart meter. Brett spends hours upon hours playing with the smart meter and eventually is able to create a program that would send false sensor data for his entire neighborhood.
- **Attack vector** – The sensor data is sent from the smart meters to the utility company in an unencrypted format. Brett uses this insecure configuration to capture, manipulate, and successfully transmit false sensor data to the utility company. He is also able to capture network traffic for his neighbor's smart meters and obtains their Internet Protocol (IP) addresses. Using his custom written program, Brett sends false sensor information to the utility company, indicating that Brett's entire neighborhood is without power.
- **Impact** – The utility company, unsure of how a single neighborhood can lose power, sends a crew out to investigate. Upon arrival at the neighborhood in question, the crew reports that there is no outage. The utility company underestimates the criticality of the issue and simply chalks its up to a system malfunction. Brett, amused by the situation, performs similar attacks over the next two years, ultimately costing the utility company thousands of dollars in wasted man hours.

AVAILABILITY

Availability is attained when the service provided by the utility companies is protected from unauthorized interruption. A loss of availability has a significant impact on utility companies and those that rely on their services. This includes consumers, organizations, businesses, and governments.

Consumer Targets

Consumers will be the targets of attacks on the availability of the power to their houses. These attacks will most likely come from script kiddies or people the victims know. Despite the relatively innocuous intent of the attackers, the impact of their exploits will wreak havoc on their victims.

> **NOTE**
>
> Script kiddies is a term for hackers who rely on the tools of others to attack computers and network devices. It is a derogatory term that generally suggests unskilled adolescent attackers whose motivation is notoriety.

Scenario

- **Threat** – Carla's ex-boyfriend, Andy, wants revenge for Carla breaking up with him. Andy is able to attack Carla's smart meter to create a blackout localized to Carla's townhouse.
- **Attack vector** – Carla's default wireless router configuration allows Andy to easily access her wireless network and connect to the Web front end of her smart meter. Once access to the smart meter was obtained, Andy changed its default password, and shutdown power to Carla's townhouse.
- **Impact** – Carla is left without power and is unable to connect to her smart meter to re-enable power as her wireless network is down and she no longer knows the password to the unit.

TIP

Ever wondered what the default password was for a device you own? Or a device someone else owns? Phenoelit-US.org maintains a comprehensive and up-to-date list of default vendor passwords at www.phenoelit-us.org/dpl/dpl.html.

Organizational Targets

Much like consumers, organizations will be the targets of attacks on the availability of the power to their locations. These attacks will come from script kiddies, professional hackers, or people the organizations know. However, unlike the attacks on consumers, the intent of the attackers will most certainly be malicious and may result in extortion.

Utility Companies

The most obvious organization targeted by those attacking the new smart grid is the utility companies. The utility companies will represent the "holy grail" of targets to attackers. Script kiddies will try and compromise the utility companies for notoriety, while professional hackers may be sponsored and have more malicious drivers. We will cover these drivers shortly.

Scenario

- **Threat** – A historical script kiddie, Mike, wants the credibility and notoriety he thinks he deserves. He contacts one of the largest hacking crews and asks how he can join. They respond by saying that he must hack one of the country's largest utility companies and cause a power outage that makes the evening news.
- **Attack vector** – Mike, yearning for membership in the exclusive hacking crew, studies the smart grid infrastructure and targets his local utility company. Exploiting the weak physical security of his utility company's local management station, Mike is able to plug directly into the management station and gain access to an internal utility company network. From here, Mike

performs a denial-of-service (DoS) attack against all of the management stations on the local subnet.

- **Impact** – All of the management stations in Mike's town are impacted by his DoS attack. As Mike properly planned his attack, the units were down during the period in which the utility company polls for usage data. Subsequently, the utility company's billing process is delayed and an announcement is made through local media outlets informing customers of the delay. No mention of the attack is made; however, Mike demonstrates the attack for the hacking crew and is offered membership.

Other Organizations

Much like consumers, organizations, other than the utility companies, will be the target of availability attacks. Attackers will most likely be script kiddies or people the organizations have a relationship with, such as a former employee or a customer. The motivation behind such attacks will most likely be revenge or extortion.

Scenario

- **Threat** – Victor, a former employee of the local gas station, wants revenge for his recent firing. Victor, who is computer savvy and was formerly responsible for paying the gas station's bills, is able to cut off the power to his former employer.
- **Attack vector** – The gas station utilized the local utility company's online account management Web application to pay its bills. This Web application also allows users to close their accounts without any additional verification. Victor simply logs on to the Web application from his home, using the same login and password that he used while he was an employee of the gas station, and requests the account to be closed.
- **Impact** – The gas station's account is closed within a week. As a result, the power to the local gas station is shutoff on a holiday weekend. The gas station is forced to operate on its backup system, but quickly drains the system as a result of the high demand for gas. The utility company cannot send anyone out until the following Tuesday, as a result of the holiday weekend. The local gas company is forced to shutdown midday on Sunday, losing sales on one of its busiest days of the year. Additionally, the utility company will lose revenue from not supplying the gas station and will need to spend time remediating the situation.

Vertical Targets

In the previous section, we walked through scenarios that attacked specific organizations. These attacks were the result of disgruntled employees or ambitious script kiddies seeking revenge or notoriety. However, a different class of attackers, with different motivation will target specific industries in order to achieve their objectives. The impact of these attacks will be significantly greater than those targeting specific organizations.

Activists

Many organizations are in business despite the best efforts of activists. A typical example of this is fur coat manufacturers. Animal rights organizations have historically done everything in their power to prevent these manufacturers from operating their business. The adoption of smart grid technologies presents an additional avenue for these activists to attack the manufacturers.

Scenario

- **Threat** – Lisa, an animal lover her whole life, is also a computer science major. During an animal rights protest on her university's campus, she is recruited by activists to attack the manufacturing operations of three of the most prolific fur coat brands during the period leading up to the holiday shopping season.
- **Attack vector** – Using a targeted phishing e-mail, Lisa is able to install malware on the computers of each of the targeted manufacturers. This malware captures logins and passwords to all sites that are used by the accounting department and sends them to Lisa. Once Lisa obtains the logins and passwords to the utility company's Web applications used by the manufacturers, she simply requests an account suspension for each manufacturer during the period of peak manufacturing. Lisa also changes the account information and secret questions to prevent the manufacturers from easily reactivating their accounts.
- **Impact** – The manufacturers experience power outages during their peak manufacturing periods. They contact the utility companies to inquire about the outage and learn of the suspension. Despite their documented information, they cannot successfully authenticate themselves with the utility companies and are forced to provide supplemental information in order to reactivate service. Once service is finally restored, the manufacturers have lost a total of three days of production, which significantly impacts their ability to meet order requests.

Market Manipulation

Financial gain continues to be the single greatest driver behind computer attacks. With the adoption of smart grid technologies, attackers will exploit weaknesses for financial gain. Extortion is the easiest example of how attackers can obtain financial gain: by withholding organizations power service until a ransom is paid. However, more sophisticated, and potentially more lucrative, attacks are possible.

Financial

Sophisticated movie plots depict hackers as financially motivated individuals who bring specialized skills to a team that includes nontechnical members. Unfortunately, these plots will not remain bound to the silver screen for much longer. Hackers, teaming with those who understand financial markets, can easily exploit the adoption of smart grid technologies to gain significant amounts of money in a short period of time.

Scenario

- **Threat** – Dan, a longtime ethical hacker at a financial institution, is let go because of corporate downsizing. He is approached by fellow coworkers in the commodities division about an opportunity to make a lot of fast money. Without any promising job prospects, Dan agrees to help his former coworker in exchange for a significant cut of the take.
- **Attack vector** – Using a combination of his technical knowledge and the market knowledge provided by his former colleagues, Dan performs a DoS attack against several of the country's largest utility companies during the peak of winter. Dan utilized a remote file-inclusion vulnerability in a common software package deployed as part of the utility companies' Web applications. This vulnerability allowed Dan to discontinue all power-generating activities at the utility companies for several hours.
- **Impact** – Dan's former coworkers strategically purchased a significant amount of heating oil before Dan's attack on the utility companies. In the panic that ensued within the commodities market as a result of the DoS attack, the price of heating oil skyrocketed, increasing by 25 percent. Dan's coworkers promptly sold their holdings at the peak of the panic, and made enough money to retire comfortably.

National Security Target

With the announcement in October of 2009 that the United States issued 100 grants, totaling $3.4 billion for smart grid technologies, it is clear that President Obama sees smart grid technology as a priority.[4] As a presidential priority, smart grid technologies will undoubtedly make their way into America's next generation electric infrastructure. Additionally, the high priority given to smart grid technologies will also increase the scrutiny of its security, by friends and enemies alike.

Domestic

Domestic terrorism is a reality that Americans have learned to live with ever since they watched the horror of the attacks on the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, on April 19, 1995. The adoption of smart grid technologies will provide domestic terrorists with a readily available target.

Scenario

- **Threat** – Kyle, a former private in the armed forces, has become disgruntled with his country's alleged occupation of a foreign country. During his tenure in the armed forces, Kyle learned how to attack enemy infrastructure, including those that support utility companies.
- **Attack vector** – Leveraging an outdated version of a Web server running an Internet facing government Web site, Kyle is able to ultimately gain access to a sensitive network that controls regional power distribution for the east coast of the United States. Kyle obtains this access by exploiting the outdated Web

server and weak configurations within the numerous subnets located between the sensitive network and the Internet facing the Web server.

- **Impact** – Kyle is able to shut down power generation to the Northeastern states of the United States. Panic ensues as federal, state, and local authorities scramble to identify the cause of the blackout. Riots and looting occur, as the blackout extends into the evening. All told, the Northeast is without power for hours, and damages as a result of rioting and looting total into the billions.

WARNING

Before you assess a company or government's security posture, make sure you are familiar with all applicable laws. Laws and their subsequent punishments vary by locality. You can read more about individual state's laws at www.ncsl.org/default.aspx?tabid=13494. Similarly, you can review federal laws at http://definitions.uslegal.com/c/computer-hacking/.

International

As much as the images of the Oklahoma City Bombing of 1995, as shown in Figure 3.2, resonate in the minds of Americans, the world has never been the same since the attacks of September 11, 2001. Terrorists targeted the world's financial center and successfully destroyed the Twin Towers in New York City. The adoption of smart grid technologies will create a similar center for the United States' power distribution. This center will become a target of significance to international terrorist groups like Al-Qaeda.

Scenario

- **Threat** – Thierry, a professional hacker for hire, has been approached by Al-Qaeda to attack the United States' power grid. As a professional hacker, Thierry is financially motivated, and despite his reservations of dealing with a terrorist organization like Al-Qaeda, he simply cannot resist the money offered.
- **Attack vector** – Utilizing social engineering attacks that leverage malicious e-mail attachments, Thierry is able to create a worm that infects a majority of the United States' major utility companies. Thierry's worm has command and control capability, which allows him to gain further access into each organization's internal infrastructure. By the time Thierry executes his attack, he has administrative access to 75 percent of the largest utility companies' distribution networks.
- **Impact** – Thierry is ultimately able to shut down power generation at 75 percent of America's utility companies simultaneously. Much like the attack previously conducted by Kyle, the domestic terrorist, panic ensues as federal, state, and local authorities scramble to identify the cause of the blackout. However, this time the scope is nationwide. The blackout encompasses 90 percent of the United States and lasts for three days until the worm can be eradicated. The damage, both financially and psychologically, is devastating to the United States and its final toll is incalculable.

FIGURE 3.2

Oklahoma City bombing of 1995.

Source: DefenseImagery.mil[5]

Precursor to War

The threats described in the previous sections of this chapter have demonstrated the potential impact attacks can have on an organization, an industry, and nation. The impact of these attacks is primarily financial and psychological. These tolls, while not inconsequential to the longevity of a nation, are minimal in comparison to the effect similar attacks could have on a nation as a precursor to a military attack.

Scenario

- **Threat** – Country X, tired of the sanction placed on it by the United Nations, has decided to declare war on the United States. Although Country X does not possess the technology or arsenal to directly attack the United States, they have planted sleeper cells within the United States that will carry out suicide attacks when given the signal. In order to maximize the impact, Country X has targeted the smart grid technologies deployed by the United States in order to create confusion and prevent communications with their citizens, first responders, and government agencies.
- **Attack vector** – Leveraging previously unreported vulnerabilities in the operating systems and network services utilized by the United States' smart grid infrastructure, Country X is able to shut down all of America's power distribution networks simultaneously. The attacks are easily performed because of the prevalence of vulnerable systems and devices. Little to nothing was previously known about the exploited vulnerabilities.
- **Impact** – With the nationwide blackout affecting almost all Americans, mass chaos ensues. Shortly after the blackout, Country X's sleeper cells execute their suicide attacks amplifying the chaos and sinking the American people into a depression. Countless Americans lose their lives as a result of the attacks, and many more are lost as a result of the chaos that was amplified by the blackout. Much like the previously mentioned terrorist attack, the damage is devastating to the United States, and its final toll is incalculable.

SUMMARY

The benefits of smart grid technologies to the utility companies are significant. However, the risks associated with these technologies, both to the utility companies themselves, and to those that rely on them, are equally significant. Traditional threats such as service theft and fraud are likely to become the mainstream. Worse, such attacks are likely to be quickly documented and disseminated on nefarious Web sites, thereby allowing others to launch similar attacks in other areas.

Other threats, such as availability attacks, will have an increased impact as distribution networks become increasingly interconnected. The utility companies will be looked upon as the first level of defense against these threats. However,

in order to defend such attacks, a coordinated effort between governments, industries, and consumers must work effectively and efficiently. Otherwise, a "fire sale," as depicted in the movie *Live Free or Die Hard*, could become a reality.

NOTE

A "fire sale" is a term that refers to the complete compromise of a country's infrastructure, including power distribution. The compromise is obtained primarily through the use of computer hacking.

Endnotes

1. Verizon Business. 2009 Data breach investigations report [document on the Internet]. www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf; 2009 [accessed 8.1.2010].
2. Soghoian C. 8 Million Reasons for Real Surveillance Oversight [document on the Internet]. http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html; 2009 [accessed 12.12.2009].
3. United States Congress. Energy policy act of 2005. [document on the Internet]. www.epa.gov/oust/fedlaws/publ_109-058.pdf; 2005 [accessed 25.11.2009].
4. Carey J. Obama's smart-grid game plan [document on the Internet]. Business Week; www.businessweek.com/technology/content/oct2009/tc20091027_594339.htm; 2009 [accessed 26.11.2009].
5. Chasteen, Staff Sgt. Preston. F-3203-SPT-95-000022-XX-0198 [image on the Internet]. DefenseImagery.mil; www.defenseimagery.mil/imagery.html#a=search&s=april%2019%201995&n=90&guid=0f7e0c201d7cae42d9ebfbfefc5d1984645d12d7; 1995 [accessed 8.1.2010].