A View Through the Hacker's Looking Glass

Garrett Leischner and David Whitehead
Schweitzer Engineering Laboratories, Inc.

Presented at the
42nd Annual Minnesota Power Systems Conference
Saint Paul, Minnesota
November 7–9, 2006

Previous revised edition released April 2006

Originally presented at the
8th Annual Western Power Delivery Automation Conference, April 2006

A View Through the Hacker's Looking Glass

Garrett Leischner and David Whitehead, P.E., *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Have you ever wondered what hackers are trying to do to penetrate your system, or how they may be trying to gain access to your assets? In this paper we will walk you through some possible scenarios that you may be faced with, and the security practices you can apply to help prevent them from being successful.**

I. Introduction

Years ago the main goal of hackers was to implement their belief that the purpose of the Internet was the free sharing of information, and that any person not freely sharing such information was in violation of the intended use of the Internet. They saw their role not as destructive criminals, but rather as protectors of this free access to information from which the Internet was born.

As the Internet grew, businesses, governments, and individuals started using the Internet as an essential means of communication. Company and personal information now traverses the Internet daily. As a result, unauthorized access to information has become a lucrative business. The knowledge of how to gain access to this data and the number of entities willing to pay for this access has grown and evolved. This, in turn, has created many types of hacker groups, from "computer-savvy kids misbehaving," to well-funded, well-organized hacker groups with specific targets.

The advantage always lies with the attacker. An attacker must find only one weakness to penetrate a system, but a defender must find all weaknesses and apply effective security measures. When implementing security measures, you must carefully balance security, cost, and usability as shown in Fig. 1. Favoring one of the three over the others can cause an imbalance that could leave the entire security system ineffective.

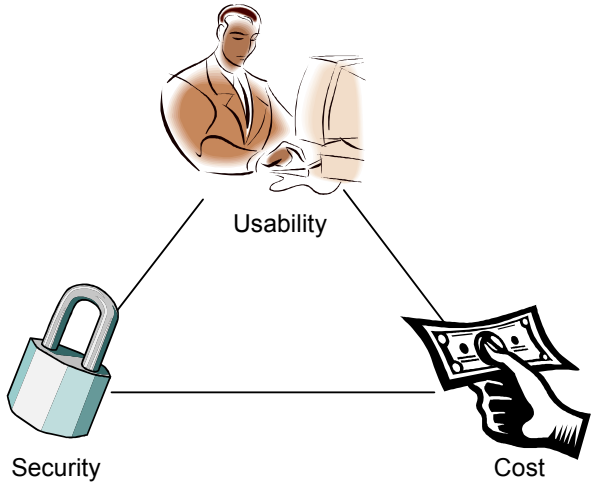

Fig. 1. Security Pyramid

In order to balance the security pyramid, you must first define what is a cyberasset and what is not. The North American Electric Reliability Council (NERC) recognized that "business and operational demands for managing and maintaining a reliable bulk electric system increasingly rely on cyberassets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data." As a result of the increased reliance on communication and/or cyber-based control systems for the reliable operation of the electric power system, these assets have become a significant target. As a result, NERC has developed Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009. The NERC CIP standards "provide a cybersecurity framework for the identification and protection of critical cyberassets to support reliable operation of the bulk electric system" [1].

Once you have identified cyberassets, you must decide how much damage would be caused to your organization if data or control of an asset was compromised, and then assign a dollar amount to the possibility.

Balance whatever security safeguards you implement with the burdens they place on the end-user. If you increase the security of a system to a point where users can no longer perform their tasks, users will either try to subvert the security or they will stop using the asset [2].

In this paper we explore a range of different scenarios, combining fictional, but very possible situations, with attack strategies and technologies already in use. We look carefully at how the attacks were constructed and implemented from the hacker's point of view, and then describe the victim's experience. We then discuss detailed protection tactics and methods that could have prevented the attacks from occurring, or from jeopardizing a company's ability to efficiently perform its day-to-day tasks.

II. Scenario #1: A Day at the Coffee Shop [3]

A. Hacker #1

As a first year computer science student with no real work experience, I paid the bills by working part-time at a coffee shop that had a wireless hotspot. One day a customer came into the shop and was having problems connecting to our network; after fixing his computer I realized that I might be able to make some extra money. I went to work setting up my laptop to emulate the hotspot logon, in an attempt to get access to customers' credit cards.

My plan was to set up a wireless access point (WAP) with a stronger signal than the coffee shop WAP, using the same Service Set Identifier (SSID). All it required was two wireless cards, some prepackaged software, and a hotspot logon created with my laptop. I set up a proxy to forward all the incom-

ing connections on one wireless card out through the other wireless card to the coffee shop's WAP. This allowed me to get credit card information and allowed the users to connect to the Internet, but not be aware of my activity. Since all user data was going through my proxy, I saved a copy of each session on my computer to analyze later.

I was amazed at how easy it turned out to be. At first I only used the credit card information for small purchases and essentials, but when more than a month passed and no one came to my door, I started purchasing bigger items.

Then I decided to really analyze the data I had saved on my computer. I spent a few hours looking for usernames and passwords that people had used, and I finally found one for a corporate web mail account. I realized this was no ordinary web mail; it was from Big Oil Industries, and they had a lot of competitors and enemies. I posted an advertisement on a trade website indicating I had some valuable and sensitive information. After about twenty responses, I realized I could make a lot of money with this information and build my reputation as a hacker.

B. Victim #1

John walked into the coffee shop and tried to connect to the wireless hotspot. He noticed that to connect he had to use a credit card or have a prepaid account. Since he had his corporate credit card with him, he went ahead and entered the card numbers to log onto the hotspot, and then checked his email without a second thought.

About a month later, someone from accounting stopped by and asked John to explain some charges, which amounted to over $12,000 dollars. They determined that the charges were not his and the company would dispute them. John wondered how someone could not only get his corporate credit card number, but also the associated expiration date and security code.

III. Scenario #1 Protection Strategies

The attack scenario described above is preventable through the use of several existing technologies and precautions. These include:

- Using only trusted wireless networks.
- Only divulging sensitive information on Secure Socket Layer (SSL)/Transport Layer Security (TLS) secured websites.
- Using a secured VPN when accessing the corporate network.

A. Use Only Trusted Wireless Networks

Each wireless network is identified by a unique SSID. Wireless networks consist of two types: access points or ad-hoc networks. Access points generally allow your computer to join a connection point to a corporate LAN or the Internet. Ad-hoc networks are generally computer-to-computer networks. Common sense dictates using only networks that you know are legitimate. It is crucial that you understand, especially when dealing with wireless technologies, that any data you send over a nonencrypted medium can be read through interception.

You should always apply built-in security features to help minimize data compromise when using wireless networks. All IEEE 802.11a, b, and g wireless devices support Wired Equivalent Privacy (WEP) encryption. Although WEP contains flaws and exploits to hack WEP are well documented, you should always enable WEP if no other security mechanism is available. New versions of 802.11 fix the WEP security flaws. Specifically, 802.11i (commonly known as WPA2) provides a robust set of security improvements that fix all of WEP's known security problems [4].

If you do not have 802.11 wireless protection features available (e.g., using a hotel or coffee shop's WAP), then other programs can supplement WEP by first encrypting and authenticating data before it is sent over the wireless network. One strengthening method is to implement a Virtual Private Network (VPN) to create a secure and encrypted tunnel between your computer and a trusted computer you wish to communicate with (e.g., a corporate email server). These will not only encrypt the data being sent over a wireless connection, but will also authenticate the connection by means of its key or certificate.

B. Use Only SSL-Secured Websites

SSL, and the more recent TLS, provide authentication, confidentiality, and integrity using cryptography to provide data security. Because data are often sent over media that is not secured itself, implementing SSL/TLS over such media provides proven cryptographic security to protect it. An advantage of SSL and TLS is that they both function between your application (e.g., Internet Explorer) and your network connection (e.g., IEEE 802.11). This provides information security that does not rely on WEP. Fig. 2 shows how SSL/TLS relates to your web browser application (HTTP) and the Ethernet protocol (TCP/IP). SSL/TLS provides application security that is independent of the Ethernet connection.

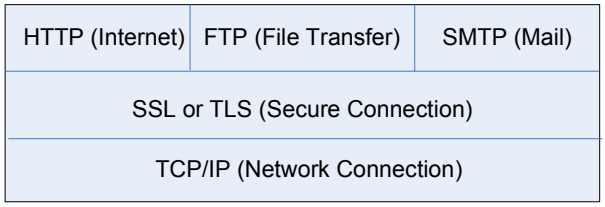

Fig. 2. SSL/TLS Application to Ethernet Relationship

SSL has become the de facto standard for transactions when entering sensitive information on the web; an SSL transaction is noted by the presence of a closed lock or unbroken key at the bottom of your browser window (see Fig. 3). If you see a broken key or open lock, then SSL is not protecting the transaction.

Fig. 3. Secure Transaction Lock Icon

Even when a closed lock is present, you still need to verify that the certificate represents the actual server you were planning on connecting to. Without this check, you may be con-

necting to an intermediary Man-in-the-Middle (MITM). A MITM could create a secure connection between a target and itself, and then again between itself and the desired site (see Fig. 4). This is exactly what Hacker #1 did. When the data goes through MITM, it is no longer encrypted by the desired end-destination SSL computer, and is easily accessible by the MITM.

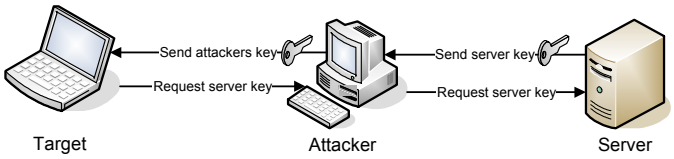

Fig. 4. MITM Connection Process

The best way to avoid this form of attack is to check the certificate to verify that it is valid and that it is indeed the system you actually intended to connect to. In either Firefox or Internet Explorer, you can do this by double-clicking on the lock in the bottom right corner of the web browser. This will inform you to whom the certificate was issued, as well as the signing authority, which is useful in determining whether the site you are currently using is the site you expected to be using.

Although attacks on SSL may still seem to require specialized knowledge, the creation of software attack toolsets such as dsniff could enable most computer-savvy individuals to figure out how to plan and execute a MITM attack [5].

This is why it is important to verify that the connection you are making has a valid certificate and to identify such attacks before sensitive information is compromised.

C. Use a Secured VPN When Accessing a Corporate WAN

VPNs create secured communications links between geographically distant locations. There are two types of VPNs: trusted and secured. A trusted VPN allows computers across geographic boundaries to have the same type of security as though they were in the same building, but does not ensure privacy. A secured VPN uses cryptographic tunneling protocols to attain privacy. Within a secured VPN, confidentiality, sender authentication, and message integrity ensure privacy. Table I shows the elements necessary for achieving privacy.

TABLE I
SECURITY TYPES FOR ACHIEVING PRIVACY

Confidentiality	Sender Authentication	Message Integrity
Prevention of Snooping	Prevention of Identity Spoofing	Prevention of Message Alteration

Examples of cryptographic protocols used in a secured VPN include the following:

- IP Security (IPSec)
- SSL tunneling
- Point-to-Point Tunneling Protocol (PPTP)

IPSec is an OSI Layer-3 protocol for securing Internet Protocol (IP) communications by encrypting and/or authenticating IP packets. The data are secured for communication with either Encapsulating Security Payload (ESP) or Authentication Header (AH). ESP provides each type of security needed for privacy (as shown in Table I); AH provides only authentication and message integrity, but does not encrypt the data contained within the packet.

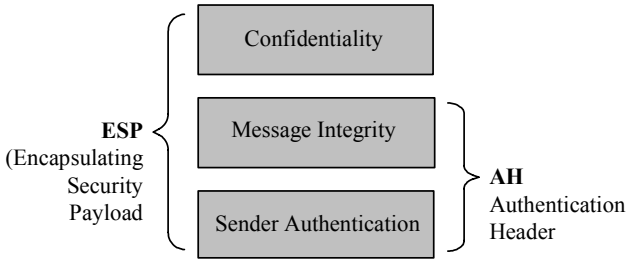

Fig. 5. IPSec Encryption and Authentication Methods

The key difference between IPSec and SSL is that IPSec communications are secured to each computer, SSL/TLS communications are secured to each application session.

As SCADA protocols advance, traditional Information Technology (IT) security practices will be incorporated. As an example, IEC Technical Council (TC) 57, Working Group (WG) 15 is developing IEC 62351, which is a set of specifications for data and communication security that incorporates TLS to secure applications like IEC 60870, IEC 61850, and DNP3 over IP.

Protected Extensible Authentication Protocol (PEAP) and Tunneled Transport Layer Security (TTLS), which are based on TLS, are two commonly used methods for implementing VPN technology over a Wireless Local Area Network (WLAN). The structures of TTLS and PEAP are quite similar: both are two-stage protocols that establish security in stage one, and then authenticate in stage two. Stage one in both protocols establishes a TLS tunnel and authenticates the client to an authentication server with a certificate.

TTLS and PEAP use certificates to authenticate the wireless network to the user, but only a few certificates are required; therefore, these protocols are very manageable.

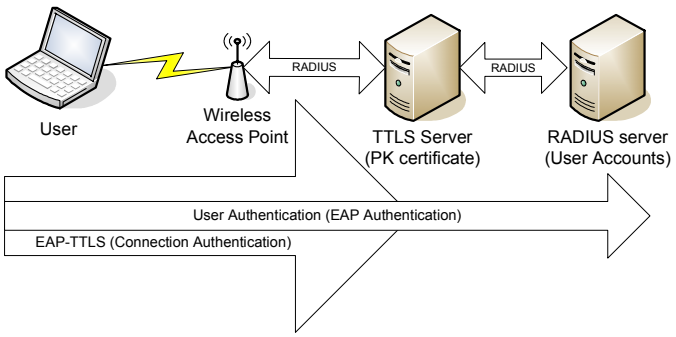

Fig. 6. TTLS Authentication Process

Once a secure channel has been established, client authentication credentials are exchanged in stage two [6].

Fortunately, VPN technology is now readily available in popular computer operating systems, including Microsoft® Windows, Linux, and Apple OS X. VPN technology is increasingly being used in embedded and industrial Ethernet-based equipment designed to interface directly with the Internet.

IV. Scenario #2: The Disgruntled Employee

A. Hacker #2

After the company moved its servers to an offsite location to outsource their support, I was fired. I had worked hard at the utility, done what was asked of me, put in overtime—nobody fires me and gets away unscathed.

The utility's biggest mistake was that they did not lock out my accounts. Even if they had, it really did not matter because there was still the shared administrative account that everyone had the password for.

It was a simple matter for me to take over their website, their face to the outside world. It did not require any special computer knowledge because there were so many free guides on the Internet. All I had to do was a little copy-and-paste job, with a few modifications. Online hackers were really helpful, sharing all the information I needed to accomplish my goal.

First, while I was logged into the company system, I copied a list of all the user names on the network. Next, I downloaded a brute force password-cracking program, not to actually crack the password, but as a tool to lock everyone out of their accounts. I then went in and deleted or modified project files, knowing this would probably set most of their projects back a month, as they tried to rebuild them from back-up tapes.

I had conceived the password-lockout idea when I accidentally locked myself out by mistyping my password three times and saw that it locked my account for fifteen minutes. I loaded the password cracker onto one of the machines and set it up to do an online attack against the user list. It ran dictionary attacks against each user's password, and after three attempts it locked out the account. Fifteen minutes later the program again attempted three passwords in rapid succession, and it locked them out again, over and over. All they would see was "Your account has been locked out, please contact your system administrator."

B. Victim #2

On Superbowl Sunday Kent received an emergency call from the office, "The network servers are down, the web servers are rerouting people to illicit sites, and the mail server is attaching a picture of a red stapler to all outbound email." Kent asked why they had not shut down the servers and was told, "we cannot log into any of the systems; we are locked out!"

Kent booted his laptop and tried to log onto the corporate network over the VPN, and got the same message: "Your account has been locked out, please contact your system administrator." Recently, as a cost-saving operation, Kent had moved all the servers to an offsite location. Someone would have to drive out to the remote site and try to login at the console or at least unplug the machines.

On the long drive out to the server site, he began to connect the dots. It was his security policies that had worked against the network and allowed this Denial of Service (DoS) attack to occur. The DoS attack, so called because it prevents the intended and appropriate use of resources by legitimate users, was turning every computer on the network into an expensive paperweight.

V. Scenario #2 Protection Strategies:

The case described above could have been prevented through the use of the following policies, technologies, and precautions:

- Use different passwords/passphrases for each system.
- Use two-part user authentication.
- Promptly change passwords and/or remove accounts after an employee separates from the company.
- Create unique user accounts for individuals.
- Identify critical assets and examine effectiveness of security polices used to protect them.

A. Use Different Passwords and Passphrases for Each System

Kent should have required each user to have different passwords for each server and should not have had a default administrator password at all. If you use one password for different systems, and that password gets compromised, all your systems are compromised. Users should have a different password for each system in order to increase the overall security of networks. However, this presents an accessibility problem—how can a user remember all the required passwords?

One option is to write down the different passwords, whether with a pen and paper or in a password storage program. In practice, writing down a password should be avoided; however, even if you wrote down your passwords and properly secured them in a physical location, the physical premises would have to be compromised before all your systems were compromised. Also, you are more likely to use stronger passwords, and to use different passwords for separate systems, if you are not required to memorize them all.

1) Passphrases

Simple passwords like names, months, etc. are susceptible to automated attacks. Oman, Schweitzer, and Frincke discussed in a paper delivered at the 2000 Western Protective Relay Conference how simple passwords can be easily determined [7]. For example, a simple, six-character password on a 9600 bps link could be determined in 3.5 hours (this assumes a 25,000-word dictionary; 50 percent likelihood of success; and an average guess/attack rate of one per second, based on typical SCADA IED serial interfaces) and that same password on a 10 Mbps link could be determined in 1.7 hours (this assumes a 25,000-word dictionary; 50 percent likelihood of success; and an average guess/attack rate of two per second, based on typical SCADA IED slow Ethernet interface). Difficult passwords (a combination of lowercase and uppercase letters, numbers, and characters) force attackers to use exhaustive search methods. If the difficult password is six characters or more in length, then a brute-force attack becomes unrealistic, taking 8,425 years on a 9600 bps link and 4,213 years on a 10 Mbps link.

A passphrase can simplify password memorization. A passphrase is simply a sentence or string of words used to represent a password, such as the following:

- My access to Dilbert's mad engineers laboratory.
- Mickey Mouse and I use 3 Accounting Systems.
- Goofy Drooled on the Substation!

These passphrases contain all the necessary complexity requirements, and are easy to remember, so it is more likely that they would be used to secure separate systems.

There are some situations where the maximum password length limitations of a system would keep you from using a passphrase. Trying to remember a long pseudo-random alphanumeric password for each system is more difficult. For example, a user could choose a random password such as **dfn^3PrN!**.

While this password is considered very strong, the user may find it difficult to remember and so may want to use the same password throughout multiple systems. Using the same password across different systems could cause system-wide security compromise. In these cases, implement a mnemonic, a variation of a passphrase. With a mnemonic, instead of using the exact passphrase, you can create a slight variation. This technique achieves the complexity of a password while retaining the simplicity of a passphrase. The following are examples of mnemonics for the previous passphrases [8]:

- **Ma2Dmel** (My access to Dilbert's mad engineers laboratory)
- **MmaIu3AS.** (Mickey Mouse and I use 3 Accounting Systems.)
- **GDotS!** (Goofy Drooled on the Substation!)

2) Word Changing

Word changing can also be an alternative for creating easy to remember passwords. You can do this by taking an easy to remember word and replacing individual letters with a numeral or symbol, such as in the following examples:

- Electr 1c!
- K3ystrok3 10ggr

You must take care not to select easy to identify word-changing words. Many dictionary attack programs account for simple word derivatives.

3) Super Passwords

In normal situations, complex passwords such as passphrases are sufficient for securing your data. However, in some situations you may want to implement a password that is more resistant to brute-force cracking. To do this, use characters outside of the standard ASCII text range, such as characters contained in the Unicode set or extended characters.

Within some special applications such as system services or Daemons, it may be advantageous to use a Unicode character-based password. This is because in these instances the password does not need to be entered often, and the difficulty of entering it is sufficiently offset by the inherent brute-force resistance.

Extended characters, such as the nonbreaking space {ALT + 0160}, are also more hacker-resistant. These characters appear as a space, and only after looking at the actual ASCII code could someone notice that it was different.

There are some significant downsides to using super passwords. You need to enter an Alt + {number}, which can be tricky and may take less time to break through by brute force means than if you had just added those extra characters to your password.

"For example, a five-character password made up of high-ASCII characters will require 25 keystrokes to complete. With 255 possible codes for each character and five characters, the total possible combinations are 255^5 (or 1,078,203,909,375). However, a 25-character password made up of only lower-case letters has 26^25 (or 236,773,830,007,968,000,000,000,000,000,000,000) possible combinations." Clearly, this demonstrates that only in special cases would it beneficial to use such characters [9].

B. Use Two-Part Authentication

Two-part authentication is another alternative for strengthening the authentication of your system. Authentication occurs in these systems by means of what users have (i.e., physical token), or what users are (i.e., biometrics), and what users know (i.e., password). The major advantage of a two-part authentication is that users (or hackers) must have two separate means of authentication to validate themselves on the network. If hackers steal the token, they do not have the associated password, so they cannot be authenticated. If an employee is terminated, the token is returned to the company, so even though the employee may have memorized the password, it is not enough to gain access to the network. Fig. 7 shows a variety of typical physical tokens.

(a) Token (b) USB eToken (c) Smart/RFID Card (d) Biometric Reader

Fig. 7. Two-Part Authentication Devices

Thus, successful attackers need to gain access to both the authentication token and the password in order to breach a system. Another benefit of two-part authentication devices is that they have a low impact on users' day-to-day tasks, so they are widely accepted and used.

C. Promptly Change Passwords After Employee Separation

Another important part of any security policy should be password expiration. It is generally a good security practice to change passwords frequently. This is because the more times you use a password, the higher the likelihood that someone else could have obtained it. Your policy should recommend, as a basic security practice, expiration of passwords after a reasonable amount of time. That way if a password is cracked or compromised, the time frame of its effectiveness will be limited. Changing passwords frequently is especially important when multiple users are required to use the same account. The U.S. National Security Agency recommends changing passwords monthly or quarterly [10].

D. Create Unique User Accounts for Individuals

Each user that needs access to a specific system should have an independent account on the system. This allows implementation of restrictions and limitations, such as how and when individual users are able to access the system.

One possible method for establishing unique user accounts is to manage all the associated settings through a network domain. System administrators can create access groups and grant permissions on an as-needed basis across all systems that are part of the domain (see Fig. 8). Within a domain, use groups and organizational units to create logical collections of people and assets, such as computers and servers. If a user changes jobs within a company (for example, moves from a position as a Relay Technician to the Communications Department), a system administrator could move the employee's user account from the Relay Technician Group to the Communications Department Group. The system administrator would make the change in one place and then replicate it throughout the organization, allowing for quick and accurate manipulation of access rights throughout the entire company.

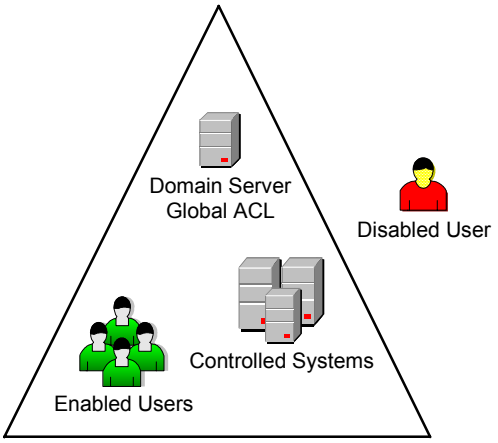

Fig. 8. Domain-Controlled Environment

Another example, explained in detail later, is to separate critical systems that have design constraints on unique users or lack the ability to join a domain. It may be possible to separate these systems onto an isolated LAN or VLAN, where access to this segment is controlled through a VPN. Each user is required to possess an individual account on the VPN, using it as a point for controlling access.

E. Determine Assets and Examine Effectiveness of Protection Policies

When implementing a security policy, you must first identify which items are assets. For example, while a password itself is not an asset, the information that the password is protecting is an asset. Once assets are identified, it is much easier to look at security policies and analyze how effectively they protect each asset.

In the disgruntled employee scenario just described, security was severely compromised by high accessibility. It was then compromised further by the application of a password lockout policy in an inappropriate manner. You should evaluate each security policy by its ability to meet a desired end result, including under abnormal or adverse applications. One end result of this scenario should be to increase the difficulty of gaining access to data assets. The National Institute of Standards and Technology (NIST), Computer Security Division, is charged by the Federal Information Security Management Act (FISMA) to design and assist with security policies for U.S. companies. This resource can assist you in implementing security policies [11, 12, 13, 14].

VI. Scenario #3: Sophisticated Cell Attack [15]

A. Hacker #3

I was hired as an accounts receivable processor for a Large Electric Power (LEP) utility, but I was really employed by a hostile foreign government to procure access to LEP's power grid controls. I did not work alone; I was part of a cell designed for the exact purpose of extracting information and finding access points. We were not just recreational hackers; we were well trained and funded. Most system administrators never saw us coming or leaving. After I settled into my new position I connected a cell-phone modem device to my computer so that a back door could be established. From this access point, holes in the firewall were made so that if by any chance someone did learn of our existence, we would appear as hackers that came from the Internet.

It was amazing how many companies had no internal security; once you were inside the security perimeter, it was easy to traverse the corporate network and even get to the SCADA network. Like many utilities, LEP thought they had separated their SCADA infrastructure from their corporate LAN. Keeping the two networks separate was a wise network architecture, but I knew that, as in so many networks I had penetrated before, the engineers would want access to both the substation and the corporate resources at the same time. This bridge would be our access point. What the well-intentioned engineers did not consider was that the corporate network is connected to the Internet, and if they can get to the corporate network from the SCADA network, we can then get to the SCADA network from the Internet. So I painstakingly scanned the network, slowly mapping the various paths from the corporate LAN all the way to the Intelligent Electronic Devices (IEDs) in the substation. All this time, other members of the cell also gathered information about the corporate and SCADA network structure.

During our network reconnaissance process, we used many different resources to determine different vectors of penetration, but that was not our only source of information. It never ceases to amaze me how much you can learn from being a customer on the other end of a phone line, or by just reading a manual. Three out of four times, if an IED shipped with a default password, it was still in use and was always documented in the manual. Alternatively, you could gather more information about a product through social engineering or calling a helpful customer service representative. Within two months we had fully reverse-engineered LEP's SCADA network, documented the SCADA protocols and passwords, and become proficient in their power systems operation, monitoring, and control systems.

With a full understanding of the corporate and SCADA LANs and substation configuration, all we needed was a high-speed access point to the Internet. A change to a router here, a jump off a computer there, and we were in business—the two worlds became one. Two months later LEP experienced the largest power outage in its history, every key substation in

LEPs network opened its breakers within five minutes of each other. The power outage cost millions of dollars in lost productivity.

B. Victim #3

John was the head of protection and got the first call asking why all of LEP's circuit breakers had opened up. He reviewed the Sequence-of-Event (SER) reports and saw that each one had received an open breaker command via the SCADA system. John called the operations control center and asked the supervisor why they had sent open commands to all breakers. The operations supervisor said they had not issued any open commands. John told the operations supervisor that all relays had received a SCADA open command, and asked the supervisor to check the operations logs. The logs did not show any circuit breaker commands, so John began analyzing how open commands could have been sent to all relays if the operations personnel did not send them. After a week of reviewing SCADA logs, John could only conclude that somehow a remote open command was sent from somewhere other than the operations center. Another week later, John and the IT department were able to find the bridge between the SCADA LAN, the corporate network, and ultimately the Internet. John finally realized that as much as he hoped to isolate the relays from outside networks, they were, and would continue to be, connected to the corporate LAN, even if through a firewall. John knew that he would have to increase his network security posture, work with the corporate IT security personnel, and implement a network-monitoring feature.

VII. Scenario #3 Protection Strategies

The situation above can be prevented through the use of several existing technologies, including:

- Implementing a cyberasset security policy.
- Monitoring system assets.
- Auditing device logs.
- Partitioning critical infrastructure.

A. Implementing a Cyberasset Security Policy

Strong security policies define how systems are to be interconnected, who has access to networks, and which rights each user has.

A security policy states, in writing, how a company plans to protect their physical and information technology assets. A security policy is often considered to be a "living document," meaning that the document is never finished, but is continuously updated as technology and employee requirements change.

An access control list (ACL) is a table that defines which access rights each user has to a particular object or device. Each object or device has a security attribute that identifies its access control list. The list has an entry for each user with his or her access privileges. Privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file or program).

B. Monitoring/Auditing System Assets

A big problem for Victim #3 was the lack of network monitoring. A real world analogy would be a bank vault. Even though it is extremely thick and physically secure, a bank vault is still monitored, because it is always possible to penetrate a defense, no matter how difficult. Monitoring alerts bank or other personnel if someone is trying, or succeeding, at entering the vault.

Intrusion detection systems (IDS) and log monitoring could have detected the attackers' actions before the final attack occurred. Proper log monitoring and analysis could have provided clues to possible network reconnaissance or login attempts, before the system itself was breached. Further, an IDS tuned to detect abnormal SCADA network activity may have detected the event that caused all the circuit breakers to open at nearly the same time.

Collecting data and system logs is the first step in detecting attacks or anomalous situations before they have a chance to cause damage; however, this information provides no value unless you use it. Remember that log management and auditing is an important part of securing your systems. Logs contain valuable information about what has been transpiring on your system, and will give you warnings when your system is experiencing benign faults or malicious attacks.

There are many different types of network monitoring, from log management and auditing of device status to implementing IDS/IPS for detecting anomalous activity on the network. With the addition of Ethernet connectivity to substations growing, so does the importance of monitoring these networks. Because of this growing SCADA security demand, there are now IDS rules for monitoring SCADA protocols, such as Modbus TCP and DNP3. These rules can be great resources for automating the monitoring of a SCADA network. While the rules are a good starting point for monitoring, you can augment them still further by setting up your own rules, such as a rule to have the IDS monitor for successful as well as invalid telnet login banners and login attempts. You can also have the IDS monitor for anomalous situations.

C. Network Partitioning

Ideally networks would be separate. However, when it is not possible to physically place critical systems on separate networks, consider creating a Virtual LAN (VLAN), which separates devices on a routing level (see Fig. 9).

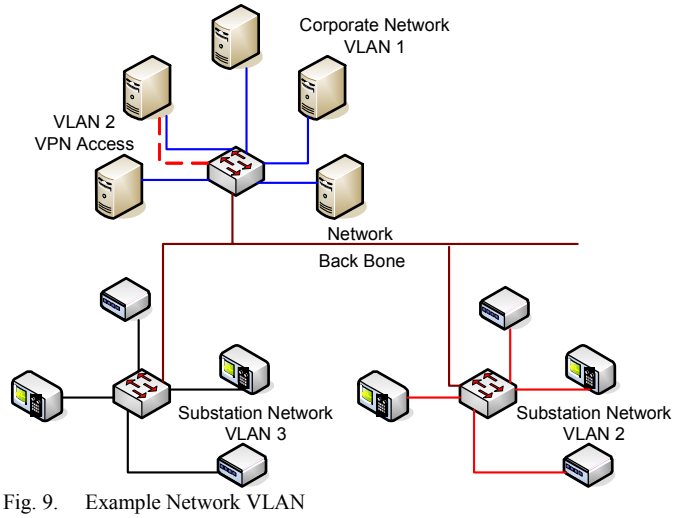

Fig. 9. Example Network VLAN

While not practical in every situation, moving critical devices onto a separate VLAN has the advantage of eliminating visible contact with the corporate network. This is similar to a physical separation, but instead of running on a separate infrastructure, the networks are separated at the routers. Access to this separated network could then be restricted through a second stage VPN, limiting access even further. While this may not eliminate your risk as much as a dedicated system, it will minimize the visibility of these assets, while also minimizing usability inconvenience.

VIII. Further Cybersecurity strategies

There are other strategies that can further secure your cyberassets and protect your valuable systems. These include:

- Evaluating and reviewing security policies
- Being aware of social engineering vulnerabilities
- Training system users

A. Policies

"Security is about risk management; it is about understanding the risks and concrete threats to your environment and mitigating those. If the mitigation steps involve taking a security guide and applying it, so be it, but you do not know that until you analyze the threats and risks."[16]

If you consider using a new security policy from an outside source, remember that it may not be the best set of solutions for your situation. Most IT security concepts are applicable to SCADA networks; however, the actual implementations may be very different. Make sure you implement a policy that fits your particular needs.

All security policies for your systems should be reviewed with at least a similar frequency as your policies for physical security, if not more often. Cyberassets do not require the attacker to be physically present for the assault; rather attackers can be miles away. Therefore, frequently reviewing policies to assess vulnerabilities from fast-changing internal and external cyber environments is critical.

B. Social Engineering

"Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people." [17]

It is human nature to want to help coworkers and customers; however, be sure you do not divulge seemingly benign but sensitive information unintentionally. Most of the methodologies for gathering such information are used because of the legitimate likelihood of these events occurring, such as:

- A new employee requesting help from the IT department for access to a database.
- A system administrator requesting a user's password to correct a problem with the user's system.
- A coworker or person cloaked in an air of authority asking for information on a project.

Social engineering is a tactic that often starts with obtaining small and what would normally seem like insignificant pieces of information, to use in conjunction with other pieces of information for the end result of penetrating a company's security [17]. As such, it is important to always be vigilant about the use and possible uses of the information you give out. Because all the technology in the world cannot foil a person being deceived through a psychological attack, the only protection is training and security policies and procedures to help guide people into identifying and responding correctly to such situations.

C. Training System Users

To reduce the exposure of systems, make sure that system users know what is expected of them and what their responsibilities are. Training in computer policies and how to handle suspicious activity should be mandatory for all new users. Periodic retraining and testing is also a good idea.

Informing and testing users in real-life examples of how these attacks arise and allowing users to experience these attacks in controlled situations can reduce a company's exposure even further. Real-life examples allow users to gain first-hand knowledge of an attack, without putting company assets at risk.

IX. Conclusion

"Security guides provide a great starting point, but to really improve your security you need to do a lot more. Generally, you would need to resort to complex measures to stop complex attacks, and complex measures do not package well in the form of a security template." [16]

Since covering a computer in epoxy is not a practical security solution, what are your options? Working with your IT department is the first step. Most, if not all, IT-based security practices and procedures can be directly applied to SCADA systems [7].

The security methods described in this paper can be applied to corporate and SCADA networks:

- Develop well-crafted security policies. If necessary, seek professionals to develop them.
- Use a secured VPN when accessing corporate WAN.
- Secure sensitive data using SSL, TLS, or other similar methods.
- Use different strong passwords/passphrases for each system.
- For stronger authentication, use two-part user authentication.
- Promptly change passwords and/or remove accounts after an employee separates from the company.
- Where applicable, create unique user accounts for individuals.
- Identify critical assets and examine effectiveness of security polices used to protect them.
- Implement a cyberasset security policy.
- Monitor and audit system assets.
- Partition and protect networks.

X. Appendix

To emphasize some important points that make life harder for hackers, we include these ten easy steps for not protecting your network.

Ten Easy Steps to Getting Hacked [16]:

1. Do not patch anything.
2. Use poorly written applications.
3. Use the highest possible privilege.
4. Open unnecessary holes in firewalls.
5. Allow unrestricted internal traffic.
6. Allow unrestricted outbound traffic.
7. Do not harden servers.
8. Use bad passwords, in multiple places.
9. Use shared service accounts.
10. Assume everything is OK.

You can check the following Internet and print sources for examples and additional information pertaining to Scenarios #1, #2, and #3.

Scenario #1

- Detailed information on how a SSL "Man in the Middle" attack can occur. http://www.cs.umu.se/education/examina/Rapporter/MattiasEriksson.pdf
- Configuring your Wireless access point for secure use. http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx

Scenario #2

- SANS guide to security policies. http://www.sans.org/resources/policies/
- Detailed information on super passwords and common myths with passwords. http://www.securityfocus.com/infocus/1554
- CERT Security Practices. http://www.cert.org/nav/index_green.html

Scenario #3

- Understanding the Social Engineering threat. Kevin D. Mitnick, *The Art of Deception*, [17].
- IDS Snort Rules for SCADA Protocols by Digital bond. http://www.digitalbond.com/support-center/
- Top tools for network security. http://www.insecure.org/tools.html
- Common methodology for IDS Evasion. http://www.insecure.org/stf/secnet_ids/secnet_ids.html
- J. M. Johansson, S. Riley, *Protect Your Windows Network: From Perimeter to Data* [16].

XI. Glossary

802.11i—802.11i increases the security of a wireless connection by implementing encryption key protocols including the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES).

Biometrics—Is a subset of technology that relies on physical or behavioral characteristics for the purpose of authentication.

Complex Password—A complex password will normally have to meet at least three of the following requirements:

- An uppercase character (A-Z)
- A lowercase character (a-z)
- A special character ($, @ , # , !)
- A numeric value (0-9)

Dsniff—http://www.monkey.org/~dugsong/dsniff/ is a tool set designed to perform network auditing. These tools can spoof Layer 2 packet switching, allowing for MITM SSH/SSL Attacks.

Hash—A password hash is the resulting value achieved by running a plaintext password through a cryptographic function.

Keylogger—A keylogger is a program or device that records keystrokes, and can be configured to record only after specific keywords are displayed, such as password or credit card.

Mnemonic—A process or technique to remember a construct of data, such as Roy G. Biv for color spectrums.

Network Domain—A network domain defines an area of control in which the subsequent computers are managed at a central location.

OSI—The Open System Interconnection (OSI) model defines a networking framework for implementing protocols in seven layers (see Fig. 10): (http://www.webopedia.com/quick_ref/OSI_Layers.asp)

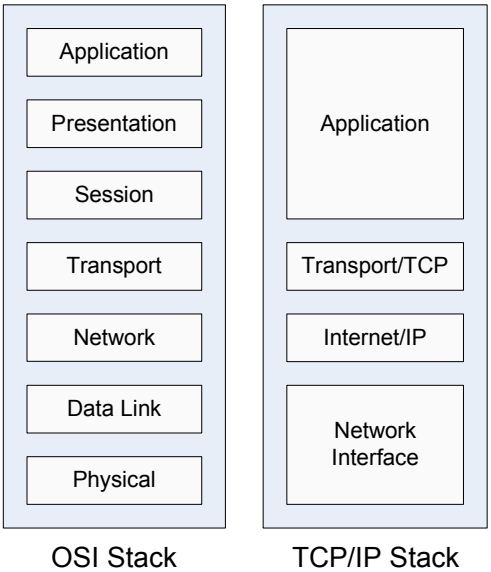

Fig. 10. Comparative Graphic of OSI vs. Hybrid TCP/IP Model

Layer 1 – Physical Layer
Transmits bits over physical medium – copper, fiber, radio link, or any other medium

Layer 2 – Data Link Layer
Moves data across one hop of the network

Layer 3 – Network Layer
Responsible for moving data from one system through routers to a destination system

Layer 4 – Transport Layer
Reliable communication stream between two systems
Layer 5 – Session Layer
Coordinates sessions between machines – helping to initiate and manage them
Layer 6 – Presentation Layer
How data elements are represented for transmission – order of bits and bytes in numbers – floating point rep.
Layer 7 – Application Layer
Actual applications that use the communication channel

Proxy—A proxy is a service that allows computers to indirectly connect to a network.

SSID—The SSID is used to uniquely identify a group of wireless devices. As such it differentiates one WLAN from another.

Unicode—Unicode is a character-encoding schema; its goal is to provide a unique number for every known character, by means of encoding underlying graphemes instead of the glyph itself.

WAN—A wide area network is a computer network that covers a large geographical area. A set of LANs connected together would constitute a WAN.

WEP—Wired equivalent privacy is a 802.11 encryption standard. Because of cryptographic problems with its implementation of static, short initialization vectors (IV) and keys, WEP has been found to be crackable.

WPA2—Please see 802.11i; WPA2 is the common name as defined by the Wi-Fi Alliance.

XII. References:

[1] North American Electric Reliability Council (NERC), CIP Standard, ftp://www.nerc.com/pub/sys/all_updl/standards/sar/CIP-002-009-1_30-day_Pre-ballot_Comment.pdf

[2] L. Cranor, S. Garfinkel, *Security and Usability: Designing Secure Systems That People Can Use*, O'Reilly Media, Inc., 2005

[3] N. Wyler, Ed., *Aggressive Network Self-Defense*, Rockland: Syngress Publishing, Inc., 2005, Chapter 2.

[4] A. Risley, J. Roberts, "Electronic Security Risks Associated With Use of Wireless, Point-to-Point Communications in the Electric Power Industry," presented at DistribuTECH Automation and Technology Conference for Utilities, Las Vegas, NV, 2003. [Online]. Available: http://selinc.com/techpprs/6144.pdf

[5] J. Viega, P. Chandra, M. Messier, *Network Security with OpenSSL*, O'Reilly Media, Inc. 2002.

[6] M. Gast. (2002, Oct. 17). "A Technical Comparison of TTLS and PEAP." (Also author of *802.11 Wireless Networks: The Definitive Guide*, 2nd ed. O'Reilly Media, Inc. 2005.) [Online]. Available: http://www.oreillynet.com/pub/a/wireless/2002/10/17/peap.html

[7] P. Oman, E. Schweitzer, D. Frincke, "Concerns About Intrusions Into Remotely Accessible Substation Controllers and SCADA Systems", presented at WPRC, Spokane, WA, 2000 and GATech, Atlanta, GA, 2001. [Online]. Available: http://www.selinc.com/techpprs/6111.pdf

[8] P. Oman, A. Risley, J. Roberts, E. Schweitzer, "Attack and Defend Tools for Remotely Accessible Control And Protection Equipment in Electric Power Systems," presented at 55th Annual Conference for Protective Relay Engineers, College Station, TX, 2002. [Online]. Available: http://www.selinc.com/techpprs/6132.pdf

[9] M. Burnett. (2002, Mar. 7). "Ten Windows Password Myths." [Online]. Available: http://www.securityfocus.com/infocus/1554

[10] U.S. Department of Defense, *Department of Defense Password Management Guideline, CSC-STD-002-85*, DOD Computer Security Center, Fort Meade, MD 20755, Apr. 12, 1985. [Online]. Available: http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.txt

[11] M. Souppaya, K. Kent, P. Johnson, "Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist," version R1.2.0. Special Publication 800-68. (2005 Nov.) [Online]. Available: http://csrc.nist.gov/itsec/download_WinXP.html

[12] Computer Security Division: Computer Security Resource Center (CSRC). [Online]. Available: http://www.csrc.nist.gov/mission.html

[13] Federal Information Security Management Act (FISMA) Implementation Project. [Online]. Available: http://csrc.nist.gov/sec-cert/

[14] Computer Security Division: NIST special publications. [Online]. Available: http://www.csrc.nist.gov/publications/nistpubs/index.html

[15] F. Cohen, "Managing Network Security: Anatomy of a Successful Sophisticated Attack," *Network Security*, vol. 1999, no. 1, Jan. 1999, pp. 16–19(4).

[16] J. M. Johansson, S. Riley, *Protect Your Windows Network: From Perimeter to Data (Microsoft Technology)*, Addison-Wesley Professional, 2005.

[17] K. D. Mitnick, *The Art of Deception: Controlling the Human Element of Security*, Wiley, John & Sons, Inc. 2003.

[18] SANS Institute. (2005, Sept.). "Mistakes People Make that Lead to Security Breaches." http://www.sans.org/resources/mistakes.php

[19] A. Paller, "What Works in Stopping Spear Phishing," *SANS Institute* https://www.sans.org/webcasts/show.php?webcastid=90643

[20] J. Leyden, "First Trojan using Sony DRM spotted," *The Register*, http://www.theregister.co.uk/2005/11/10/sony_drm_trojan/

[21] P. Roberts, "RSA: Microsoft on 'rootkits': Be afraid, be very afraid," ComputerWorld, IDG News Service, Feb. 2005. http://www.computerworld.com/securitytopics/security/story/0,10801,99843,00.html

XIII. Biographies

Garrett Leischner is an Associate Software Engineer with Schweitzer Engineering Laboratories Automation Integration and Engineering Division, where he specializes in the Rugged Computing Platform. Prior to joining SEL he worked for Cray, Inc. Garrett is currently pursuing his MSEE from the University of Idaho. He is a member of the Association for Computing Machinery and the Software Engineering Institute, and has several patents pending. During his time at SEL, he has co-authored several application guides and instruction manuals.

David Whitehead, P.E. is the Chief Engineer and Assistant Director of Schweitzer Engineering Laboratories Government Services Division. Prior to joining SEL he worked for General Dynamics, Electric Boat Division, as a Combat Systems Engineer. He received his BSEE from Washington State University in 1989, his MSEE from Rensselaer Polytechnic Institute in 1994, and is pursuing his PhD at the University of Idaho. He is a registered Professional Engineer in Washington State and Senior Member of the IEEE. Mr. Whitehead holds six patents with several others pending. For the past 11 years at SEL he has been responsible for the design of advanced hardware, embedded firmware, and PC software.