Concerns About Intrusions Into Remotely Accessible Substation Controllers and SCADA Systems

Paul Oman and Edmund O. Schweitzer, III
Schweitzer Engineering Laboratories, Inc.

Deborah Frincke
University of Idaho

Presented at the
55th Annual Georgia Tech Protective Relaying Conference
Atlanta, Georgia
May 2–4, 2001

Previously presented at the
V Simposio Iberoamericano Sobre Proteccion de Sistemas Electricos
de Potencia, November 2000

Originally presented at the
27th Annual Western Protective Relay Conference, October 2000

CONCERNS ABOUT INTRUSIONS INTO REMOTELY ACCESSIBLE SUBSTATION CONTROLLERS AND SCADA SYSTEMS

Paul Oman and Edmund O. Schweitzer, III
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

Deborah Frincke
University of Idaho,
Moscow, ID USA

ABSTRACT

In this paper we identify threats to power substation controllers and SCADA systems, and discuss mitigating mechanisms to reduce vulnerability to malicious electronic intrusions. The U.S. National Institute of Standards and Technology lists nine threats to computer-related commerce in North America. Six of those threats are particularly pertinent to SCADA systems, and at least four are relevant to power substation controllers. Increasing reliance on automated control systems with remote access (via phone or internet) and the growing global economy have expanded the number of potential attackers with access to substation controllers and SCADA systems, and therefore magnified the risk electric utilities have from sabotage and espionage. It is estimated that industrial and foreign espionage in North America has increased over 260% in the last decade, and it has been acknowledged by the U.S. government that other countries have nationally sponsored information warfare efforts targeted against North American commerce.

The utilities industry needs to be aware of these threats to their systems and take steps to reduce risk and mitigate vulnerabilities. Protective relay developers and auxiliary service providers should use mechanisms that minimize the likelihood that persons with hostile intent can degrade or destroy commercial power systems. Product, project, and corporate-wide security policies are tools to identify vulnerabilities, assess risk, and implement mitigating mechanisms. Many of the risks involving networked controllers and SCADA systems are similar to those affecting traditional networked-based computer systems. Hence, implementations of security policies for substation controllers and SCADA systems can draw from lessons learned in commercial network and computer security. Traditional approaches for reducing vulnerability include such techniques as password protection, audit logging, multi-tiered access levels, alarm conditions, automated IED configuration and authentication, redundant controllers, time-out communication parameters, virus protection, firewalls, and intrusion detection systems. These and other mechanisms for safeguarding substation controllers and SCADA systems are discussed in this paper.

1. INTRODUCTION

Although physical destruction is still the greatest threat to the North American electric power grid, the threat of electronic computer-based intrusions and attacks is growing and needs to be addressed by the electric power industry [1, 2, 3]. In a report to the White House entitled "Electric Power Risk Assessment," the National Security Telecommunications Advisory Committee (NSTAC) found that natural disasters and physical attacks constitute the bulk of the damage to the power grid, but that the "security of electric power control networks represents a significant emerging risk to the electric power grid" [2]. Factors influencing the likelihood of physical and electronic intrusions are varied and include such diverse parameters as economic conditions, substation location, building and landscaping aesthetics, labor conflicts, uses of adjacent property, curiosity and ignorance, civil and political unrest, and the joint-use of facilities [1]. Recent literature is consistent in claiming that the threat of intrusion by electronic means is increasing due to several social, political, and technological factors:

1. The shift from proprietary mainframe-based computer control systems to distributed systems using open protocols and standards, and the expanded use of public protocols to interconnect previously isolated networks.
2. Pressures within the industry to downsize, streamline, automate, and cut costs to maintain profit margins.
3. FERC 888 and 889 requirements to provide open access to transmission system information.
4. Increased access and interconnectivity to remote sites through the use of dial-in modems and the Internet.
5. Instability in the electric power utility job market, caused by competition and deregulation.
6. Increasing incidents of international and domestic terrorism targeted against North America.
7. Increasing number of countries with government sponsored information warfare initiatives.
8. Rapid growth of a computer-literate population.
9. Widespread availability of hacker-tool libraries.

In White House communications on critical infrastructure protection [3] the above factors were identified as a potent new mix jeopardizing the electric power grid because, "while the resources needed to conduct a physical attack have not changed much recently, the resources necessary to conduct a cyber attack are now commonplace."

When viewed as a whole these factors dramatically increase the risk of computer-based intrusions into the electric power grids of all industrial nations. Further, these same factors, combined with rising overall demands and increased need for higher quality power, have created a more fragile power grid instead of the robust, survivable system that is needed to protect critical infrastructures [4, 5]. Fortunately, (and unfortunately) many of the risks involving networked IEDs, Controllers and SCADA systems are similar to those affecting traditional networked-based computer systems. In this paper we identify specific threats and discuss mitigating mechanisms to reduce vulnerability against malicious actions. We use nominal definitions and phraseology from the computer security literature with the exception that "electronic intrusion" and "electronic attack," are used instead of the more common terms "cyber intrusion" and "cyber attack." We do so to maintain consistency with the IEEE Standard governing substation security [1] that defines an *electronic intrusion* as:

> "Entry into the substation via telephone lines or other electronic-based media for the manipulation or disturbance of electronic devices. These devices include digital relays, fault recorders, equipment diagnostic packages, automation equipment, computers, PLC, and communication interfaces."

To date there have been no documented instances of electronic intrusions or attacks causing outages or damage to the electric power grid, but there have been cases where hackers targeted electric utilities [2, 6]. The NSTAC report cites three such incidents:

1. Hackers have attacked electric utilities' business and information systems.
2. A radical environmental group was caught trying to hack into a utility's information system.
3. In Texas a disgruntled ex-employee posted a note in a hacker journal that he had sufficient information to electronically attack the power grid.

The extent of the electronic intrusion problem is as-yet unknown because few utilities are running intrusion detection systems and fewer still are reporting intrusions. A study cited in the NSTAC report found that only 25% of electric power utilities use any kind of electronic intrusion detection system and an FBI study cited in the same report found that less than 17% of 428 companies polled said they would report intrusion incidents. This lack of reporting is consistent with the banking and telecommunications industries where the majority of companies do not report intrusions for fear of negative publicity and lost consumer confidence.

These findings suggest that remotely accessible IEDs, Controllers, and SCADA systems -- and more importantly, substations controlled by those devices -- are vulnerable to electronic attacks. Physical intruders have been known to "open valves, push buttons, and operate circuit breakers, reclosers, and switches" [1], so it is assumed that electronic intruders would likely do the same. Because of the nature of the activities and systems controlled by electronic devices in the substations, misuse of those devices could have disastrous consequences that could lead to loss of life and/or property. The electric power industry needs to address and mitigate these risks.

In response to the 1997 risk assessment, White House documents called for increased awareness and R&D funding for technological solutions to the problem [2, 3]. More recently, the IEEE and the FBI moved toward meeting this challenge. The new IEEE Standard 1402-2000, *Guide for Electric Power Substation Physical and Electronic Security*, discusses mechanisms for mitigating risks, and calls for increased awareness and training in network security [1]. It concludes:

> "The introduction of computer systems with on-line access to substation information is significant in that substation relay protection, control, and data collection systems may be exposed to the same vulnerabilities as all other computer systems. As the use of computer equipment within the substation environment increases, the need for security systems to prevent electronic intrusions may become even more important."

And in another development, the FBI and the North American Electric Reliability Council (NERC) worked together to form the National Infrastructure Protection Center's (NIPC) "Electrical Power Indications and Warning System" to assist utilities with incident reporting and prosecution [7]. In his testimony to the Senate Judiciary Committee hearing on cyber-crime, Michael Vatis, NIPC Director, said his organization would be the "hub of a nationwide alert network designed to react quickly against cyber attacks targeting the computerized controls of the North American power grid."

All of the organizations studying the problem conclude that heightened awareness and increased training is needed within the industry in order to mitigate the problem before the electric power grid is jeopardized. In this paper, we respond to the call for increased awareness and training by enumerating the risks to remotely accessible IEDs, Controllers, and SCADA systems used within the electric power industry, and discussing how to mitigate those risks. The next section lists threats to the electric power industry. In Section 3 we present an example attack scenario. Section 4 demonstrates the value of strong password protection. Sections 5, 6 and 7 provide mitigation mechanisms and suggestions for safeguarding computer equipment in substations, control stations, and IT environments. And finally, conclusions calling for a proactive stance from the electric power industry are presented in Section 8.

2. THREATS TO IEDS, CONTROLLERS, SCADA SYSTEMS, AND CORPORATE NETWORKS

White House communications on critical infrastructure protection lists ten threats to utilities [3], while the NIST handbook on computer security identifies nine threats to U.S. Commerce [8], and the IEEE standard on substation protection lists nine intrusive threats [1]. Table 1 is a compendium of the types of threats identified in each document.

Table 1. Threats to Substations and Computer Networks

NIST 1994	White House 1997	IEEE 2000
Physical and Infrastructure	Natural Events and Accidents	Natural Disasters
Threats to Personal Privacy	Accidental Physical Damage	Economic Conditions
Errors and Omissions	Blunders, Errors, and Omissions	Curiosity and Ignorance
Disgruntled Employees	Insiders	Labor Conflicts
Malicious Hackers	Recreational Hackers	Civil/Political Unrest
Malicious Code	Criminal Activity	Location
Industrial Espionage	Industrial Espionage	Use of Adjacent Property
Foreign Espionage	Terrorism	Aesthetics
Fraud and Theft	National (Foreign) Intelligence	Joint-use Facilities
	Information Warfare	

While all of the threats listed in Table 1 are of concern to electric power utilities' IT environments at the enterprise level, several of these items are of specific concern to electronic attacks on IEDs, Controllers, and SCADA systems:

- *Blunders, Errors, and Omissions* – These include accidental setting/resetting of protective devices, and improper or negligent device or network maintenance that introduces significant security vulnerabilities.
- *Fraud and Theft, Criminal Activity* – Electronic fraud and theft are increasing nationwide, losses exceed $123 million annually.
- *Disgruntled Employees and Insiders* – Insiders can enter wrong settings, plant logic bombs, enter data incorrectly, crash systems, change or delete data, and hold data hostage.
- *Curiosity and Ignorance, Recreational and Malicious Hackers* – Although current losses due to hacker attacks are significantly smaller than losses due to insiders, the hacker problem is widespread and growing.
- *Industrial Espionage* – Stolen information includes pricing data, manufacturing processes, product development specification, basic research, strategic plans, negotiating positions, and contract data. In 1999 computer-based espionage losses exceeded $60 million [9].
- *Malicious Code* – The number of known viruses is increasing exponentially, including viruses, worms, Trojan horses, and logic bombs.
- *Foreign Espionage and Information Warfare* – Numerous countries have nationally sponsored information warfare capabilities, some of which have explicitly targeted U.S. government and commerce.

Misuse involving an IED, Controller, or SCADA product may occur in many venues: in-house, in transit, or in-situ. For example, *Errors and Omissions* would compromise in-house IT stability, *Disgruntled Employees and Insiders* could tamper with products in transit, and *Malicious Hackers* could intrude into an in-situ IED, Controller, or SCADA system. All of these threats are distinct risks to the electric power industry's reliability and integrity. Furthermore, with increased automation comes the increasing interdependence of critical infrastructures. For instance, a teenage hacker's attack on the phone system in Worcester, MA, in 1997, not only knocked out phone service to 600 homes, but effectively shut down the local airport's control tower, weather service, radio transmitters, and runway lights activated by those transmitters [10]. Hence, there is great concern as to the potential damage which could be caused by the more professional, more malicious, and better trained individuals who are known to exist.

Although misuse may certainly occur accidentally, in this paper we focus on situations involving an individual or individuals who might be motivated to "attack" or misuse a protective relay, controller, or SCADA system. The motivations of these individuals vary:

- **Hacking**: Some intruders enter systems *simply because they can*. The relatively benign "hacker" is often motivated by curiosity or the challenge of exploration, without overt malicious intent. Others are vandalous in nature, with the intent of gaining notoriety, or causing damage. Hackers of either variety can be insiders or outsiders.

- **Espionage**: The possibility of gaining industrial or political advantage is a huge incentive for information gathering through both legal and illegal means. Insiders – and outsiders who gain inside access – may be involved in illegal espionage by acquiring and distributing confidential information. But outsiders may also gain valuable information through examination of public information such as web pages, product descriptions, and promotional literature. Therefore, even when an organization is not concerned about internal espionage, it is important to take precautions regarding the kinds of information which are publicized.

- **Sabotage**: The motives for sabotage are frequently rooted in desires for personal, economic, or political gain. Depending upon the root cause and the opportunities available to the saboteur, the consequences of sabotage could be the destruction of the entire organizational structure and/or loss of market share. "Hactivism" is an emerging form of sabotage wherein hackers deface corporate IT resources (i.e., web pages) in the name of some radical cause.

- **Vandalism**: There are many possible motivations for vandalism -- the destruction of property value without personal gain -- and some of them are similar to those for other categories (particularly sabotage). However, vandalism should be treated separately from espionage and sabotage because it is typically haphazard, random, and relatively localized. That is, the long term consequences of vandalism are usually much less severe than those of espionage and sabotage. Vandalism is primarily associated with outsiders.

3. VULNERABILITIES, THREATS, ATTACKS, AND RISKS

The NSTAC risk assessment report concluded that power substations were "the most significant information security vulnerability in the power grid," mainly because the remotely accessible devices used within substations are largely unprotected against intrusion. The authors of the report also recognized that electronic attacks could result in widespread disruption of power at regional and even national levels for up to 24 hours. The weak link permitting such disastrous

results is the publicly accessible communications lines between substations, control centers, and corporate computer networks. And it's not just the Controllers and SCADA systems that are at risk – all electronic devices used to monitor and control power systems are susceptible to electronic intrusions, including IEDs, PLCs, and RTUs. The NSTAC report states:

> "Both the RTUs and the new automated devices {IEDs} are susceptible to electronic attack. By dialing into a port on a digital breaker, a utility engineer can reset the device or select any of six levels of protection. An electronic intruder …could dial into an unprotected port and reset the breaker to a higher level of tolerance than the device being protected can withstand. By doing this, it would be possible to physically destroy a given piece of equipment within a substation. The intruder could also set the device to be more sensitive than conditions for normal operations and cause the system to shut down for self-protection."

For illustrative purposes we now take a brief look at an example substation with remote access via dial-in modem or LAN/WAN connection over public communications lines. Figure 1 shows electronic access points (vulnerabilities) in a hypothetical substation configuration.

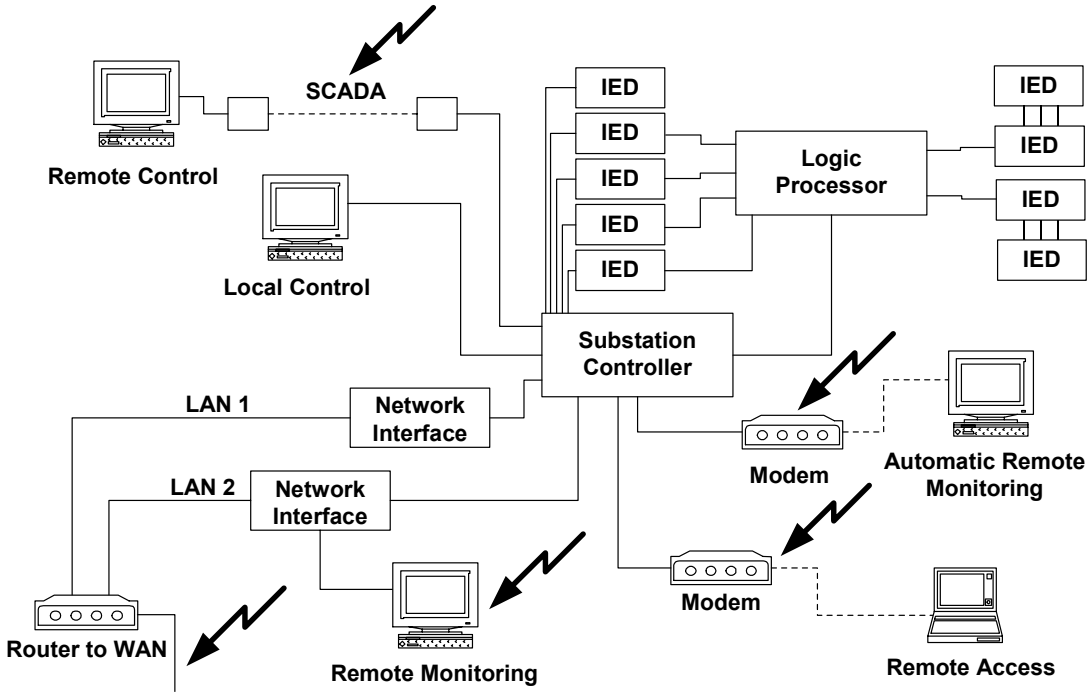

Figure 1. Electronic Intrusion Vulnerability Points

The *vulnerability* in this scenario is the public access to the communication lines to/from the substation. The *threat* is malicious intrusion and/or espionage. The *attack* unfolds something like this:

1. Using a war-dialer, the potential intruder scans hundreds of phone numbers above and below the utility's publicly available phone numbers, looking for answering modems.

2. Alternatively, the intruder could use a ping-sweep program to scan several thousands of IP addresses above and below the utility's publicly available IP address.

3. When a probable connection is found, multiple returns, question marks, "HELP" and "HELLO" are entered to probe the connection and look for clues as to the kind of connection.

4. Once a login dialog has been acquired the intruder uses *social engineering* to determine login information, or launches a *dictionary-based* or *brute-force* password attack.

5. When the connection has been completed and the intruder is "inside" the IED, Controller, or SCADA system, any of the following activities could ensue:

    a. Shut down the substation, or any portion of the subsystem controlled by compromised device, either immediately or in a delayed manner.

    b. Change settings to inhibit or degrade the functionality of any portion of the subsystem controlled by the device in such a way as to jeopardize the reliability of the substation.

    c. Gather data that could later be used to launch subsequent attacks with the intent of performing the shut-down or degradation mentioned above.

    d. Change (perturb or pollute) the data in such a manner as to trigger an inappropriate action by the device.

    e. Plant instructions (malicious code) that could later be used in a delayed, coordinated attack.

In this manner electronic intruders can gain access, alter setting to cause degradation or damage, and be gone – all while maintaining a high degree of anonymity and leaving virtually no physical evidence as to the nature and extent of the attack.

4. THE IMPORTANCE OF "HARD" PASSWORDS

It is well known that password protection is flawed and susceptible to automated attacks, but securing devices via "hard" passwords is still effective because it serves to slow down the attacker, thereby increasing the probability that the attack will be detected and/or the attacker will abandon the attack and turn to easier targets. This is especially true when password protection is just one component of an integrated system of protection including authentication, access restriction, intrusion detection, etc. Specific techniques for securing computer systems will be discussed in the next section; here we demonstrate the value of implementing "hard" passwords.

We define a hard password as containing six or more characters, with at least one special character or digit and mixed case sensitivity, and not forming a name, date, acronym, or pronounceable word. Passwords formed in this manner are less susceptible to dictionary attacks, wherein a common list of words, acronyms, and names is used in an automated attack against the access control. The tools used to run these attacks are readily available on the Internet and are quite easy to use. It is not uncommon for password crackers to run tests offline using full dictionaries in several different languages – so the use of a foreign word is not adequate protection. Password "guessing" performed in this way typically begins by checking all words, then by adding leading or trailing digits to words, then by combining short words. Hard, or "hardened" passwords, are still susceptible to brute-force password cracking and decryption techniques, but those processes take more time and effort than dictionary attacks, thus decreasing the probability of a successful attack.

Table 2 shows the differences between the expected completion times of dictionary attacks and brute-force attacks on passwords of 4, 6, and 8 characters in length. Data for the dictionary attack is based on the 25,143 word Unix spell-check dictionary containing words, numbers, acronyms, and common names. Unique passwords of lengths up to 4, 6, and 8 characters were generated from the dictionary and launched in an automated script against a typical substation Controller. The time to complete the attack is shown for each of five connection speeds, ranging from the commonly used substation dial-in speed of 2400 bps up to the nominal Internet access speed of 10 Mbs. At 9600 bps the 20,721 word attack can be launched and completed in 3.5 hours – far too short a time to deter an electronic intruder. Even at 2400 bps the dictionary attack against an eight character password is only 5.3 hours, which is still not a serious obstacle for a determined hacker.

Table 2. Time Differences in Dictionary vs. Brute-Force Password Attacks

Attack	# Words	2400 bps	9600 bps	19200 bps	38400 bps	10 Mbs
Dictionary						
4 char.	11,022	2.4 hours	1.9 hours	1.4 hours	1.3 hours	0.9 hours
6 char.	20,721	4.6 hours	3.5 hours	2.7 hours	2.5 hours	1.7 hours
8 char.	23,955	5.3 hours	4.0 hours	3.1 hours	2.9 hours	2.0 hours
Brute-force						
4 char.	66,347,190	14,707 hours	11,168 hours	8,625 hours	7,961 hours	5,528 hours
6 char.	$5.3741 \cdot 10^{11}$	13,598 years	10,326 years	7,975 years	7,361 years	5,112 years
8 char.	$4.3530 \cdot 10^{15}$	110,150,114 yrs	83,647,831 yrs	64,599,315 yrs	59,630,136 yrs	41,409,817 yrs

Note: Attack speeds are not linearly proportional to communication speeds due to wait states in the authentication process.

Data for the brute-force attack is based on the U.S. Department of Defense (DOD) calculations for password vulnerabilities [11]. Although dated, the principles embodied in the DOD password management guidelines are easily updated to today's communication speeds. The number of possible passwords of length n characters is a permutation of the C characters in the total character set taken n at a time with repetition allowed (e.g., "aaaa"):

$$P(C,n) = C^n$$

For example, some protective relays and controllers use six character passwords constructed from the typical keyboard character set. This set consists of 52 upper and lower-case characters, plus 10 digits and 28 special characters. Thus, `C = 90` and `n = 6`; so for passwords of strictly six characters, there are

$$P(90,6) = 90^6 = 531{,}440{,}000{,}000$$

possible password permutations. However, even stronger password protection can be achieved by allowing *up to six* characters, giving additional permutations of the password set, specifically

$$(C,1)+P(C,2)+P(C,3)+P(C,4)+P(C,5)+P(C,6)$$

$$= C^1+C^2+C^3+C^4+C^5+C^6$$

$$= \sum_{i=1,6} C^i = 537{,}410{,}000{,}000$$

Hence, there are over 537 billion possible passwords when allowing a length of from one to six characters in a 90 character set. Using DOD calculations for the expected time to "crack" a hard password of lengths four, six, and eight characters in a 90 character set yields the times shown in Table 2. The data clearly shows that even a four character "hard" password is significantly stronger than an eight character common name, word, date, or acronym.

5. SUBSTATION VULNERABILITY MATRIX

We have established that the protective equipment and controllers within substations, the SCADA systems connecting substations to control stations, and the utility's information processing networks are at risk to electronic intrusions. The vulnerability, and hence the risk, increases with connectivity. Thus, devices connected to public communications networks are the most accessible to the largest group of people, and therefore are the most "at risk." For example, the use of an Ethernet LAN/WAN has inherent, traditional vulnerabilities for unauthorized access and use (as compared to leased line, dial-up, and wireless connections), but there are also known technological mitigations to these same problems. Table 3 shows a listing of the vulnerabilities, risks, and mitigation strategies for devices ranging from protective relays up to computer networks.

Table 3. Substation and Computer Network Vulnerability Matrix

Device	Vulnerability	Risk	Mitigation Mechanisms
Relays, IEDs, PLCs	• Physical access by authorized or unauthorized personnel	• Protective equipment accidentally set/reset • Protective equipment deliberately set/reset by unauthorized persons	• Implement access control via password or PIN IDs • Instruct engineers on the importance of password/ PIN management • Advocate the use of "hard" passwords in documentation and training materials • Implement two tiered "show" vs. "set" access control • Obfuscate the password length[1]
Controllers not connected to networks	• Physical access by authorized or unauthorized personnel • Subsequent access to attached protective equipment	• Controller accidentally or deliberately set/reset • Protective equipment accidentally or deliberately set/reset	*The above Basic mitigations apply.*
Controllers, RTUs, PCs, and SCADA systems *connected to private lines*	• Physical and electronic access by authorized or unauthorized personnel • Subsequent access to attached protective equipment	• Control devices accidentally or deliberately set/reset • Protective equipment accidentally or deliberately set/reset	*Basic mitigations apply, plus:* • Issue access warning statements[2] • Implement automated reporting features to detect when lines are disrupted

[1] Password masking characters should exceed the maximum length of passwords so potential intruders cannot limit their password cracking efforts to a known password length.

[2] Access warning statements should be issued at every access attempt, e.g., "Warning: Unauthorized use of this device is prohibited by law."

Table 3. Substation and Computer Network Vulnerability Matrix – continued

Device	Vulnerability	Risk	Mitigation Mechanisms
IEDs, PLCs, RTUs, Controllers, and SCADA systems *connected to modems*	• Dial-in number accessible via social engineering or war-dialer • Access control circumvented by password attack • Electronic access by authorized or unauthorized personnel • Subsequent access to attached protective equipment	• Control devices accidentally or deliberately set/reset by intruder • Protective equipment accidentally or deliberately set/reset by intruder • Unauthorized access to Controllers and SCADA	*Basic mitigations apply, plus:* • Issue access warning statements[2] • Issue disconnects after three bad password attempts[3] • Use dial-back modems[4] • Use encrypting modems[5] • Use authentication cards with modems[6] • Create a multitiered (multi-sign-on) access hierarchy[7]
IEDs, PLCs, RTUs, Controllers, and SCADA systems *connected to public networks*	• Network address accessible via social engineering or automated scan (e.g. ping-scan) • Access control circumvented by password attack • Electronic access by authorized or unauthorized personnel • Subsequent access to attached protective equipment • Data packets not secure • Address vulnerable to Denial of Service (DOS) attacks	• Control devices accidentally or deliberately set/reset by intruder • Protective equipment accidentally or deliberately set/reset by intruder • Unauthorized access to Controllers and SCADA • Data packets visible via network sniffer • Loss of functionality caused by service request overload (DOS attack)	*Basic mitigations apply, plus:* • Issue an access warning statement[2] • Issue a disconnect after three bad password attempts[3] • Implement application level device authentication[6] • Create a multitiered (multi-sign-on) password hierarchy[7] • Implement packet level data encryption[8] • Implement COTS IPSec[9] • Implement PKI Certificates[10] *No mitigation for DOS attacks.*

[3] Connections should be terminated upon three successive failed attempts at access.

[4] Dial-back modems are not secure, but they are more secure than single-answer modems.

[5] It is, as yet, unknown if encrypting modems are secure from dial-back spoofing.

[6] Hardware authentication devices are strong dial-in security where IPSec or PKI is not practical.

[7] Implement different passwords on each level of the device hierarchy.

[8] Implement software or firmware data encryption between the network sending and receiving devices.

[9] Implement Commercial Off The Shelf (COTS) software/hardware security at each end of the public line (e.g. SSL, VPN).

[10] Properly implemented, Public Key Infrastructure (PKI) certificates enable authentication, encryption, and non-repudiation of data transmissions.

Table 3. Substation and Computer Network Vulnerability Matrix – continued

Device	Vulnerability	Risk	Mitigation Mechanisms
Enterprise-level networks connected to *public networks*	• All traditional computer system vulnerabilities apply	*All of the above risks apply, plus:* • Theft of proprietary data and information • Theft of personal information and identify • Theft of credit card numbers and back account information • Theft of strategic planning and product development specifications	*Basic mitigations apply, plus mitigations for public network connections (directly above), plus:* • Use preset expired passwords on new installations[11] • Change passwords 3–4 times per year[12] • Use active password checkers to identify and eliminate week passwords[13] • Implement virus scanners and update them regularly • Implement Firewalls and Intrusion Detection Systems • Review access logs and other security-relevant files regularly • Have a defined Enterprise-level computer network security policy

[11] "Pre-expire" passwords to force the customer to set their own passwords, thereby giving them the responsibility (and liability) for password management.

[12] The U.S. National Security Agency recommends changing passwords monthly or quarterly.

[13] Programs that scan system-level password files looking for weak (i.e., "crackable") passwords are readily available over the Internet.

6. NETWORK SECURITY, FIREWALLS, AND INTRUSION DETECTION SYSTEMS

Modern configurations of substation controllers and SCADA systems are essentially systems of distributed intelligent devices that resemble traditional networked computing systems. Because of the increased interconnectivity of substations and SCADA systems, and the increased risk of unwanted external access, it is important to address all the traditional network threats associated with remote communications. Typical ways to manage such threats involve authentication of communicating partners, increasing the security of the connection between sites, protection of the virtual periphery of a site, and identification of attacks if they should pass the periphery and enter the network.

Authentication of communicating partners for distributed systems is still primarily password based, sometimes augmented by use of smart cards (one time password generators) or Public Key Infrastructure (PKI) technologies. Smart cards can be used either to directly supply authentication information or as a means to augment authentication information typed in by a user (e.g., random keys or magnetic "swipes"). One major advantage of using smart card technology to augment user passwords is that the automated authentication is only valid for a short period of time before a new key is generated. Normally passwords are transmitted directly across a network and can be captured by hardware or software that is "listening in" on the line, then reused at a later time. Authentication keys generated by smart cards are not valid for very long past the original transmission, which makes subsequent reuse by an attacker improbable.

A lengthy discussion of PKI public key encryption is beyond the scope of this paper, but there are many excellent papers and books describing the subject [12]. Through appropriate use of cryptography and cryptographic algorithms, it is possible to achieve private communications with improved assurance of communicating partner identity. Designers of integrated substation solutions and SCADA systems may find that public key technologies are useful in adding an additional layer of network security to their systems.

Firewalls are often used to defend a site against external threats, and a properly managed Intrusion Detection System (IDS) can be a useful way to identify both internal misuse and external attackers who succeed in gaining internal access. A firewall is a protected gateway that stands between the resources requiring protection and the "outside." A firewall can be implemented via a router that filters out undesired traffic, or through more complicated combinations of hardware and software solutions. To be effective, a firewall must guard *all* access to the internal network, including modem connections as well as remote network access. Internet Protocol Security (IPSec) and Virtual Private Networks (VPNs) are closely allied technologies that provide the means to protect communications between physically distant sites. IPSec uses encryption to safeguard data and embed authentication information in TCP/IP packets. VPNs combine IPSec technology and firewalls to form a point-to-point secure connection over public networks, so that from a privacy standpoint it appears to be a single internal network.

An IDS is a good companion defense to a firewall system that focuses on the internal side of the firewall (although some do examine incoming network traffic). The intent is to determine if insiders or external users are misusing the system. Intrusions often have attack signatures (similar to virus signatures) that are patterns associated with misuse of the system. Recognizing the attack signature as it unfolds and shutting off the attack or notifying the system administrator that an attack is occurring is the mission of the IDS. Another common implementation involves profiling, where an IDS has an internal model of what is nominal (versus abnormal) activity. For example, an IDS might look for activity during an abnormal time of day, or for extended access and high usage from overseas external users.

7. RECOMMENDATIONS

Recommendations for "hardening" substation devices, SCADA systems, and utility computer networks against electronic intrusions are many and varied. Each organization involved in electric power production and distribution needs to conduct their own risk assessment. While there is no sense of a national crisis or immediate threat, the White House report did express a certain degree of urgency in the following statement (emphasis added):

> "We suggest consideration of these immediate actions prior to the completion of a formal risk assessment:
>
> 1. Isolate critical control systems from insecure networks by disconnection or adequate firewalls.
> 2. Adopt best practices for password control and protection, or install modern authentication mechanisms.
> 3. Provide for individual accountability through protected action logs or the equivalent."

Following is a compendium of Do's and Don'ts from [1, 2, 3, 8, 11] and our own experiences securing computer network systems. We have organized these recommendations by usage category so relationships are more apparent.

Password Management:

- Use "hard" passwords of six or more characters with mixed case and special characters
- Don't use common words, acronyms, or personal information like birthdays, names, etc.
- Memorize passwords, don't write them down
- Change passwords periodically (the U.S. National Security Agency recommends monthly or quarterly)
- Change passwords immediately after instances of contractor installation and maintenance, suspected intrusions, and when personnel turnover or strife increases insider risk
- Use different passwords in differing locales, equipment and systems; don't be tempted by single sign-on ease of use
- Ensure that passwords are issued and controlled locally (and not widely distributed)
- Teach password security and monitor compliance – force periodic password change, use password checkers to identify and eliminate weak passwords
- Avoid using devices with inadequate password protection (e.g., numeric-only passwords of less than eight digits)

Alarm Events:

- Issue alarm contacts for access, password, and settings events
- Monitor alarm contacts and events diligently – not only for intrusion detection, but to verify device functionality
- Log alarm events and suspicious activity (e.g., failed password attempts) in non-volatile memory
- Scan access logs and audit files regularly
- Automate the response to alarm conditions with preprogrammed disconnects, auto-dial warnings, and increasing audio and visual alarms

Network Connections:

- Use private communication lines when possible to limit public eavesdropping and potential intrusions
- Implement access hierarchies with different levels of permission for viewing and setting devices
- Use point-to-point star topologies (i.e., "home-run lines") from IEDs to controller to increase survivability and avoid "one down, all down" vulnerabilities
- Use passwords, access restrictions, and user authentication to guard against unauthorized access
- Secure SCADA and IT systems with virus scanners, firewalls, and intrusion detection systems
- Limit access to communication systems design and network access information

Connectivity:

- Use "warning banners" to discourage electronic intrusions and enable electronic monitoring and trespass prosecution
- Use secure dial-back, encrypting, or authenticating modems and network devices
- Terminate interactive sessions after long periods of inactivity – ensure that the open port is properly closed so the next user does not inherit unauthorized access privileges
- Limit the number of failed attempts to enter a password – disconnect and time-out the communication line after a set limit

8. CONCLUSIONS

It is clear that the risk of an electronic intrusion into an IED, Controller, or SCADA system is possible, which calls for the need to adapt stronger security measures. The final determination regarding how much effort should be expended towards adapting stronger procedures – and the associated business changes – should be determined by a formal risk assessment conducted by the company or utility.

We have documented the increasing threat of electronic attack against substation devices, SCADA systems and utility computer networks, and we have enumerated and discussed mitigating actions to reduce risk of intrusions. The literature is consistent in the call for increased awareness and training on all aspects of computer and network security, so we repeat that call here. The electric utility industry needs to rise to the challenge of safeguarding its business in a world of interconnected computers, each of which increases the threat of electronic attack. By establishing mechanisms for the prevention, detection, response, and restoration of secure computing systems we can provide for the continued reliability of the electric power infrastructure.

REFERENCES

[1] IEEE Power Engineering Society, *IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE, New York, NY, Apr. 4, 2000.

[2] National Security Telecommunications Advisory Committee Information Assurance Task Force, *Electric Power Risk Assessment*, March, 1997: http://www.ncs.gov/n5_hp/Reports/EPRA/electric.html

[3] The White House Office of the Press Secretary, *White House Communications on Critical Infrastructure Protection*, Oct. 22, 1997: http://www.pub.whitehouse.gov/urires/I2R?urn:pdi://oma.eop.gov.us/1997/11/17/3.text.1

[4] M. Amin, "Toward Self-Healing Infrastructure Systems," IEEE Computer, *IEEE Computer*, Vol 33(8), Aug. 2000, pp. 44-53.

[5] A. Jones, "The Challenge of Building Survivable Information Intensive Systems," *IEEE Computer*, Vol 33(8), Aug. 2000, pp. 39-43.

[6] K. Poulsen, "Lights Out: NIPC Unveils Plan to Monitor Cyber Attacks on the Power Grid," an *InfoSec News* article ported to *Security Focus* web page, May 25, 2000: http://www.securityfocus.com/news/41

[7] U.S. Federal Bureau of Investigation, National Infrastructure Protection Center web page, 2000: http://www.nipc.gov

[8] U.S. National Institute of Standards and Technology, *Introduction to Computer Security: The NIST Handbook*, NIST, Dept. of Commerce, July 20, 1994.

[9] B. Sullivan, "NetEspionage Costs Firms Millions," MSNBC, Sept 12, 2000: http://www.zdnet.com/zdnn/stories/news/0,4586,2626931,00.html

[10] CNN, "Teen Hacker Faces Federal Charges," Mar. 19, 1998: http://www.compugraf.com.br/hackers.html

[11] 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.

[12] W. Stallings, *Cryptography and Network Security*, Prentice Hall, New York, NY, 1999.

BIOGRAPHIES

Dr. Paul W. Oman is a Senior Research Engineer at Schweitzer Engineering Laboratories in Pullman, WA. Prior to joining SEL he was Professor and Chair of Computer Science at the University of Idaho and was awarded the distinction of *Hewlett-Packard Engineering Chair* during his last seven years there. Dr. Oman has published over 100 papers and technical reports on software engineering topics. He is a past editor of *IEEE Computer* and *IEEE Software* journals. He has a Ph.D. in Computer Science from Oregon State University and is an active member of the IEEE, IEEE Computer Society, and the ACM.

Dr. Edmund O. Schweitzer, III received his Bachelor's degree and his Master's in electrical engineering from Purdue University, and received his Ph.D. degree from Washington State University, with a dissertation on digital protective relaying. Dr. Schweitzer continued his research in digital protective relaying while serving on the electrical engineering faculties of Ohio University and Washington State University. In 1982, Dr. Schweitzer founded Schweitzer Engineering Laboratories, in Pullman, Washington, to develop and manufacture digital protective relays and related products and services. Dr. Schweitzer is recognized as a pioneer in digital protection, and holds the grade of Fellow of the Institute of Electrical and Electronic Engineers (IEEE), a title bestowed on less than one percent of IEEE members. He has written dozens of technical papers in the areas of distance relay design, filtering for protective relays, protective relay reliability and testing, fault locating on overhead lines, induction motor protection, directional element design, dynamics of overcurrent elements, and the sensitivity of protective relays. Dr. Schweitzer holds more than twenty patents pertaining to electric power system protection, metering, monitoring, and control.

Dr. Deborah Frincke completed her Ph.D. in Computer Science at the University of California, Davis, USA, in 1992. She is currently employed at the University of Idaho, where she is an active member (co-director and co-founder) of the Center for Secure and Dependable Software (CSDS). Dr. Frincke's primary research interests involve intrusion detection systems, particularly aspects of collaboration between remote sites and investigatory techniques. Dr. Frincke has been actively involved in promoting both research and education in the security arena. She has served on program and technical committees for a variety of international and national security conferences and has given invited talks for groups ranging from the FBI to the Inland Northwest Technology Alliance.

20001004 • TP6111-01