Tools for Protecting Electric Power Systems From Electronic Intrusions

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

Presented at the
4th Annual Western Power Delivery Automation Conference
Spokane, Washington
April 2–4, 2002

TOOLS FOR PROTECTING ELECTRIC POWER SYSTEMS FROM ELECTRONIC INTRUSIONS[1]

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

ABSTRACT

The dramatic increase in the use of the Internet, also known as the World Wide Web, has opened a Pandora's box of network theft, extortion, sabotage and espionage by computer *hackers*, social and political *hacktivists*, organized crime, and foreign information warfare agents. The electric power industry faces increasing risk from computer-based electronic intrusions and attacks, similar to those plaguing the E-commerce and telecommunications industries. There is increasing risk that malicious individuals will attempt to gain remote access into the digital relays, controllers, and SCADA systems that control and protect your electric power systems. Traditional approaches for reducing vulnerability include password protection, audit logging, multitiered access levels, alarm conditions, automated IED configuration and authentication, redundant controllers, time-out communication parameters, virus protection, firewalls, and intrusion detection systems. However, in order to employ these technologies effectively it helps to understand the offensive tools being used against you. By studying both offensive and defensive hacking tools you can better structure your defensive safeguards and risk mitigation processes. This paper discusses offensive hacking techniques and corresponding defensive tools and procedures that can be used to safeguard your control and protection equipment. We describe the offensive capability of malicious individuals so that you might counteract their techniques and procedures with equally effective defensive measures. We note, however, that no system is ever 100 percent secure so continued vigilance is needed to ensure reliable operation of our electric power systems.

INTRODUCTION

Studies by the White House, FBI, IEEE, North American Electric Reliability Council, and National Security Telecommunications Advisory Committee have concluded that the North American electric power grid is vulnerable to electronic intrusions (a.k.a, cyber-attacks) that can be launched from anyplace in the world [1, 2, 3, 4]. At the heart of this vulnerability is the capability for remote access to control and protection equipment used by generation facilities and T&D utilities. Remote access to protective equipment historically has been limited to proprietary systems and dedicated network connections, but there is an increasing use of public phone services, protocols, and network facilities. Concurrent with this increased use of public connectivity is a growing, more sophisticated, worldwide population of computer users and computer hackers. These persons, regardless of location or nationality, represent an increasing threat to the safety and reliability of electric power systems, and there is a growing body of evidence suggesting that United States infrastructures have been targeted by organized information warfare groups. The North American electric power industry has been identified as one of America's "critical infrastructures." Electronic intruders randomly or maliciously

[1] Portions of this work were funded by the U.S. Department of Commerce National Institute of Standards and Technology Critical Infrastructure Protection Grant #60NANB1D0116.

operating circuit breakers, reclosers, and switchgear could have disastrous consequences on the safety and reliability of our electric power systems. While it is yet unknown if cyber-attacks have actually caused power outages, there are now several documented instances of electronic cyber-attacks on electric power generation plants and T&D utilities. Full details of the increasing risk and the spectrum of mitigating technologies are discussed in our earlier conference papers [5, 6].

Tools for attacking computer-based control equipment by phone and network connection are free and widely available over the Internet. There are literally dozens of Web sites devoted to hacking, usually providing downloadable programs or scripts to help the novice hacker get started. Similarly, there are dozens of defensive Web sites devoted to preventing or detecting hacker intrusions, many of which provide downloadable programs or scripts to identify and reduce system vulnerabilities. In this paper we identify and discuss widely available tools and procedures for attacking remotely accessible control and protection equipment, *and* present defensive tools and procedural mechanisms to mitigate risk and safeguard that equipment. Attack and defend scenarios for protective IEDs and control equipment are presented, with an emphasis on defensive postures based on a better knowledge of attack tools and techniques. We discuss hardware and software tools for improved access restriction, authentication, encryption, modem security, and network security via firewall, virtual private networks, and cryptography. Protective relay developers and electric power service providers can use these mechanisms to minimize the likelihood that hackers can intrude into protective and control equipment in order to degrade or destroy our electric power systems.

BACKGROUND DEFINITIONS

A **cyber intrusion** is a form of electronic intrusion where the attacker uses a computer to invade electronic assets to which he or she does not have authorized access. The IEEE defines **electronic intrusions** 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, PLCs, and communication interfaces. [1]

A **cyber-attack** can be an intrusion as described above, or a **denial of service attack** (DOS) where the attacker floods the victim with nuisance requests and/or messages to the extent that normal services and functions cannot be maintained. A DOS attack is also called a **flood attack**. A **distributed DOS attack** (D-DOS) is a flood attack launched simultaneously from multiple sites.

Electronic eavesdropping is a less visible form of intrusion not covered by the above definitions. Eavesdropping can be achieved in all communications media by intercepting or tapping into communication signals. Telecommunications **wiretaps** are physical junctions into metallic or optic conductors. Eavesdropping in Local Area Networks (LAN) and Wide Area Networks (WAN) is called **sniffing**. A **sniffer** is a program that accepts and opens network packets that are not addressed to your equipment. Wireless eavesdropping and sniffing can also occur on virtually all commonly used wireless networks including, radio, satellite and microwave transmissions. Eavesdropping can also be achieved by hacking into computers that control telecommunications and network switching.

A **hacker** is a person who engages in cyber-attacks and/or computerized eavesdropping.[2] A **hack** is an intrusion or sniffing event. A **hacktivist** is a hacker motivated by social or political causes, while a **script kiddie** is a novice hacker whose attack knowledge is limited to downloading and running attack scripts available on the Internet. Hackers and script kiddies attack through network and computer vulnerabilities, flood programs and scripts, or via information gleaned through eavesdropping and **social engineering** (deducing confidential information via public sources or by manipulating insiders). **Phone Phreaks** are hackers that focus on telecommunications computers; their illicit access to telecommunication controllers enable them to eavesdrop, record, and re-route communications traffic. Hackers also target Internet Service Provider (ISP) computers and routers in order to eavesdrop, record, and re-route network packets. **Spoofing** is another technique used by hackers to gain confidential information. Bogus e-mails, network packets, and Web sites can be created with **spoofed** (i.e., not genuine) sender/site addresses to fool victims into responding or entering data they would not normally divulge to unknown persons.

Insiders are people with legitimate access to the computer system or network being threatened or attacked. They can be employees, partners, customers, service personnel, etc. A **dupe** is an insider who is tricked into doing something that jeopardizes the computer system or network. Malicious activities include the spread of **viruses** (harmful programs that spread via human interactions, like e-mail), **worms** (that spread across networks autonomously), **Trojan horses** (programs implanted by intruders or insiders to allow easy unauthorized access), and **logic bombs** (destructive programs implanted by intruders or insiders and timed to go off at a later date).

REMOTE ACCESS VULNERABILITIES

Figure 1 shows a hypothetical Integration and Automation (I&A) substation configuration with a variety of local and remote electronic access points. The configuration of the system and its remote access points create vulnerabilities, indicated by lightening bolts, that can be attacked by electronic intruders. In this scenario we embedded most of the common vulnerabilities, including (clockwise from #1):

1. Modem access via telecommunications providers.
2. Public network access via the Internet.
3. Wireless network access.
4. Long-run private network lines.
5. Leased network lines (e.g., ATM or Frame-Relay connections) using telecommunications providers.

We also recognize physical access vulnerabilities, like gaining access to the inside of a substation and changing settings, but physical security parameters are more well defined and deployed in our industry. In fact, most substation IEDs, controllers, and SCADA systems have features for both local and remote access control (e.g., passwords). For that reason we begin our discussion with technologies of authentication and access control, and then analyze password attacks and defenses. Following the discussions on user authentication and passwords, we provide more in-depth analyses of the five electronic access vulnerabilities identified above.

[2] The term "hacker" is also used to describe a programmer who writes quick and dirty code.

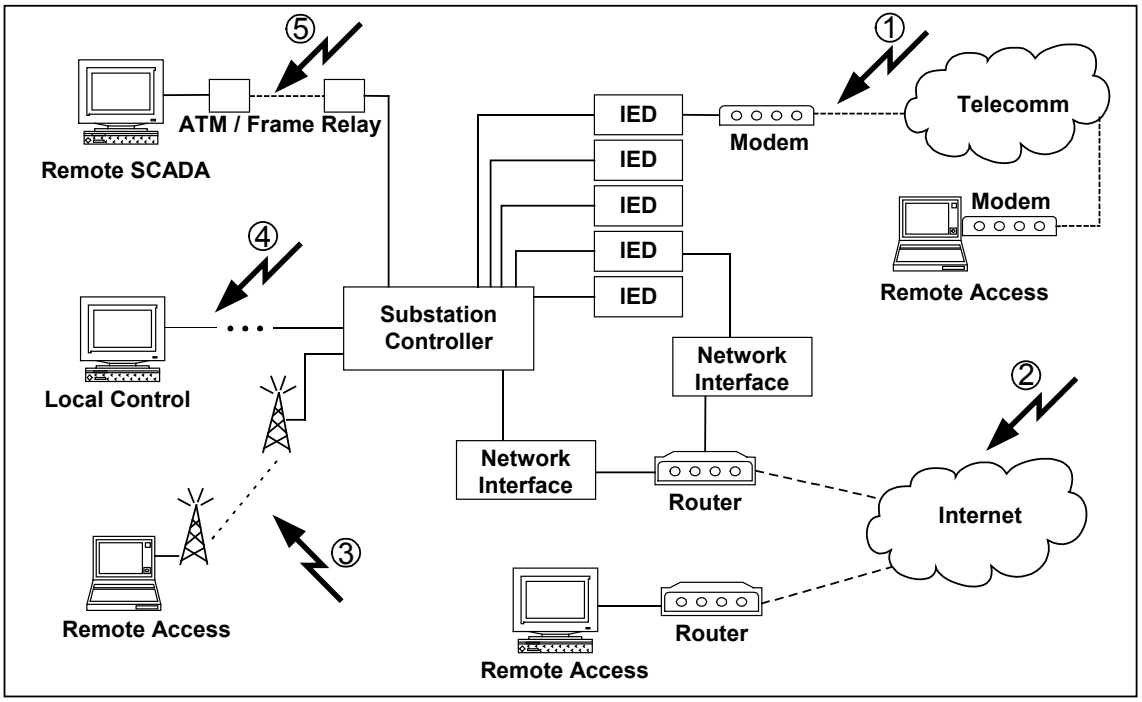


Figure 1 Electronic Access Vulnerabilities

ACCESS RESTRICTION AND USER AUTHENTICATION

Access restriction and user authentication are the cornerstones of all security. Both physical and electronic means of access restriction should be used, but physical access restriction is common in our industry so we will focus our attention on electronic access restriction. Passwords and Personal Identification Numbers (PINs) are the most common means of electronic access restriction. A PIN is just a password defined from a numeric character set; although PINs are not as strong as passwords, we collectively include PINs in all following discussions of passwords.

A password can be keyed to an entire system or individual devices, databases, and even selected data records or fields. The level or layer of security is defined by the software or firmware implementing the password control. If several users have the same password, then you have a simple access restriction technique, but you do not have user authentication or user accountability. User authentication occurs only when there is a one-to-one mapping between the user and the access key. User accountability occurs only when every access attempt is recorded. For example, assigning each person a unique password keyed to a specific system, device, database or data record allows the system to authenticate that person as a legitimate user of the secure entity. Logging that access, or attempted access, enables the system to maintain audit records establishing user accountability. The strength of your user authentication is a function of the details retained in the access logs and the number of factors used in the authentication process. Access logs (aka, audit logs) record instances of access attempts, both valid and invalid, and session information like date and time stamps (among other things) to create a record of activity documenting who did what. These logs are indispensable when diagnosing and recreating events, and for prosecuting cases of unauthorized electronic intrusion.

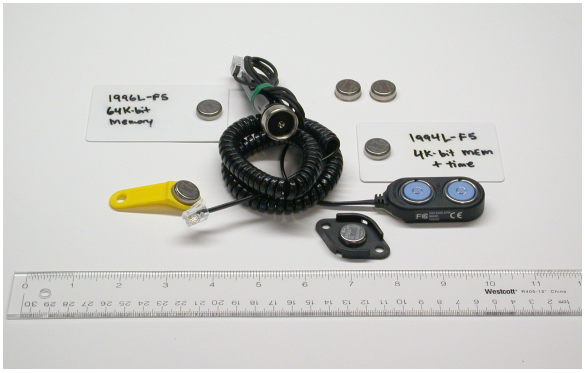
Passwords are not the only means of access restriction and user authentication, however. Electronic authentication via encryption key(s) is common for secure communications and is

discussed in later sections of this paper. Other electronic identification devices, like access badges, SmartCards, magnetic strips, barcodes and embedded chips, are all physical authentication mechanisms. Fingerprints, retinal eye patterns, voice prints, facial patterns, and other characteristics are biological authentication mechanisms. When viewed together, these different techniques form the three vectors, or factors, of authentication: (1) something you know, (2) something you have, and (3) something you are. In all cases the authenticating data is entered into or placed near a reader that checks the authenticity of the data and enables or denies access to the secured system. For remote access the local device reader sends an authentication code to the remote authentication server that, in turn, verifies the legitimacy of the access and enables or disables remote access accordingly.

For many years, single-factor authentication, usually via password or PIN, was considered adequate for computing systems. However, the increased use of computer networking, and the corresponding increase in electronic theft and espionage, has led many organizations to use two-factor and three-factor authentication. Two-factor authentication usually involves a password and an electronic ID device. Common three-factor authentication employs a password, an ID device, and a simple biometric like a fingerprint. You need to match the strength of your authentication to the criticality of the data and equipment being protected. Two-factor and even three-factor authentication may be needed in safety-critical operations. Figure 2 shows four types of authentication devices: (a) proximity badge reader, (b) random number generators, (c) programmable, wearable buttons, and (d) fingerprint scanner. Prices for physical and biometric authentication devices range from a few hundred to several thousand dollars.

(a) Proximity Reader and Badge

(b) Random Number Generators



(c) Programmable Buttons

(d) Fingerprint Scanner

Figure 2 Low Cost Authentication Devices

PASSWORD ATTACKS AND DEFENSE

Hackers have automated password attack programs and dictionaries that contain thousands of commonly used passwords, including street slang, foreign words, and entertainment names and buzzwords like C3PO, Wookie, Gandalf, and Coolio. If your password is disabled, easily guessed, or *cracked*, intruders can not only shut down your system, but they can use your system to distribute bogus data and sabotage other interconnected systems within your company and worldwide across the Internet.

There are two types of password attacks. **Password hacking** occurs when hackers launch a real-time attack against your system by stealing or guessing passwords. Passwords can be stolen by physical or electronic theft, telecommunications wiretaps and sniffs, insider observations and/or coercion, or dumpster diving. Passwords can be guessed randomly, through social engineering, from a cracker dictionary, and by generating all possible permutations of character strings from the password character set. **Password cracking** occurs when a hacker obtains encrypted passwords from telecommunications packets or operating system password files, and runs a **cracker** program to decrypt the passwords. Figure 3 shows a popular cracker program that works on both Unix and Microsoft® encrypted passwords. There are several ways hackers gain access to encrypted passwords, but that will not be discussed here. Instead, we focus on defenses against password cracking.

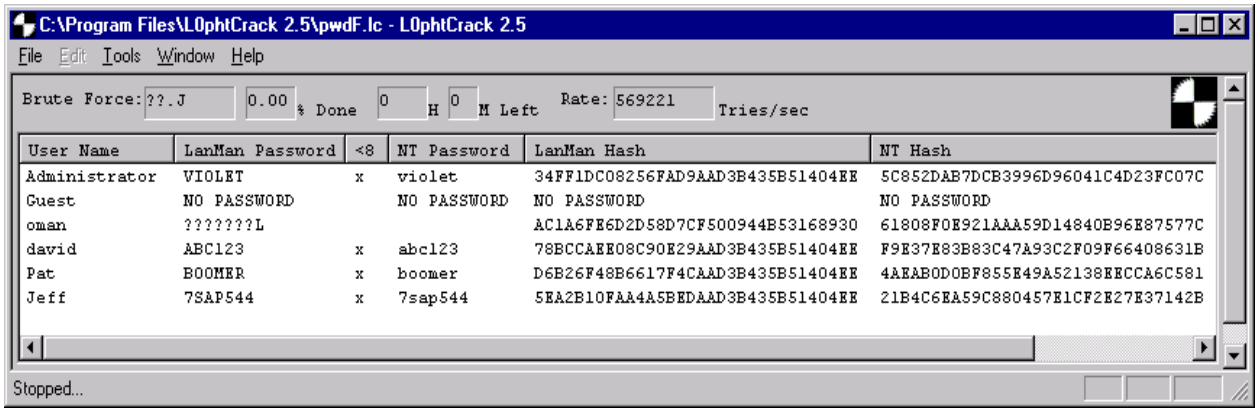


Figure 3 Password Cracker

All security experts agree that strong password selection is still your best defense against electronic intrusion and other forms of unauthorized access (e.g., physical front-panel access). Regardless of what other security mechanisms you use, a good password not only protects your equipment against unauthorized settings, but also safeguards the integrated system and helps ensure the reliable operation of a substation or SCADA system. A well formed, strong password is virtually impossible to guess and may take thousands of hours to crack, whereas an ill-chosen password may be guessed or cracked in just a few minutes. It is extremely important to maintain the security of your system by using strong passwords in protective relays, controllers, and remote access points to your SCADA systems.

You need to choose passwords that are not based on existing words or popular culture. Strong passwords consist of six or more characters, with at least one special character or digit and mixed-case sensitivity, but do not form a name, date, acronym, or word. Examples of valid, distinct strong passwords include:

P3a5t7 A24.68 Ih2dcs 4u-Iwg Ic-4.7

Passwords formed in this manner are less susceptible to password guessing and automated attacks. Password generation programs are available as operating system features and via the Internet, but there is an easy way to create strong passwords without resorting to password generators. Simply take the first letter of each word in a memorable phrase and insert a non-alphabetic character somewhere in the resulting character string. For example, the phrase "I love to ride my horse, Blue" can be used to form and remember the password **Il2rmhB**, which is difficult to crack because it cannot be pronounced and it is not meaningful. Similarly, the phrase "The Palouse has four beautiful seasons" can be used to create the password **tPh4bs**, which is simple and easy to remember because of the sentence from which it is formed.

Unfortunately, having a strong password is not sufficient to thwart determined hackers with high-speed connectivity and lots of time (e.g., days or weeks) to run a brute-force attack on your password. But it is easy to frustrate them so they give up and turn toward easier targets. By implementing communication channel time-outs, and bad-password delays and disconnects, you can slow their attack down to a point that they could not crack your password in 100 years of continuous trial and error guessing. Three bad passwords in a row should trigger a 30 second or 1 minute channel time-out where all communication is discarded; even better protection would be issuing a channel disconnect after the third invalid password. Another safeguard would be communication disconnects after periods of channel inactivity, say 5 or 10 minutes. Figure 4 shows examples of IED and communication processor channel time-outs and disconnects. Other password cracking defenses are procedural. Here is a list of recommended practices to maintain strong password defenses:

- Strong passwords consist of six or more characters with mixed case and special characters. Do not use common words, acronyms, or personal information like birthdays and names.
- Run a cracker program on your own system password files to see how easily they can be cracked.
- Change passwords periodically (e.g., quarterly). Change passwords immediately after instances of contractor installation and maintenance, after suspected intrusions, and when personnel turnover or strife increases insider risk.
- Teach password security and monitor compliance. If passwords must be recorded store them in secure, non-obvious locations.
- Limit the number of failed attempts to enter a password; disconnect and time-out the communications line after a set limit.
- Terminate remote communication sessions after periods of inactivity and ensure that all communication ports are properly closed so the next user does not inherit unauthorized access privileges.
- Keep communication system details and network access information private. Remove welcoming "banner" screens and replace them with "no trespassing" warning signs.
- Log all access attempts and analyze that data for abnormal activity (e.g., repetitive attempts during off-hours and from unusual locations).

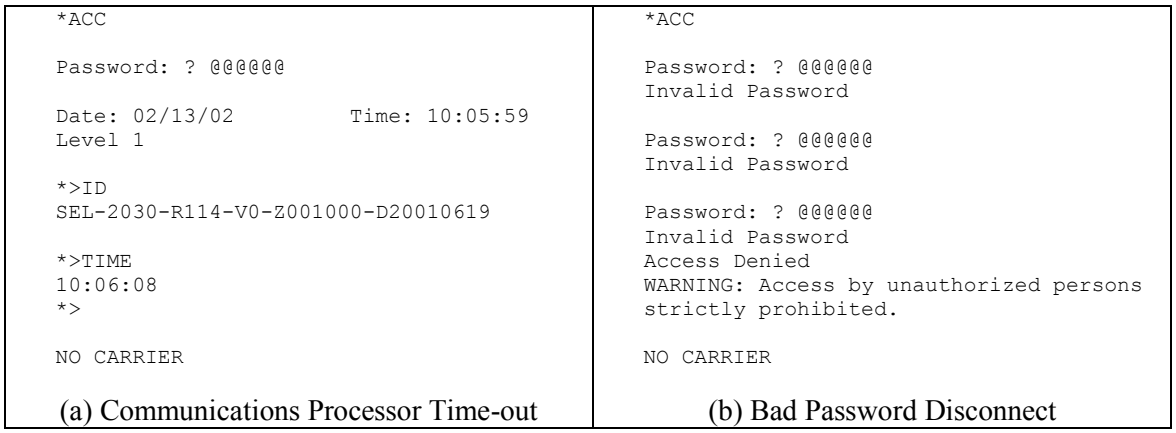


Figure 4 Communications Processor Time-Outs and Disconnects

MODEM ATTACKS AND DEFENSES

Hackers use computer programs called **war dialers** to automatically dial hundreds or thousands of phone numbers looking for answering modems. When an answer is detected, the war dialer will either notify the hacker or simply log the phone number into a list of possible targets for later attacks. Hackers will run these programs overnight, or for days at a time, gathering lists of phone numbers that are potentially exploitable. When the hacker tries to connect to the modem, you must have your security measures in place. Modem security ranges from literally nothing to very strong authentication and encryption. On a scale from worst to best, you have:

1. No security – answer all direct connections.
2. Dial-back security – recognize incoming calls, hang up, and originate a call to a predefined phone number.
3. Password controlled access – answer incoming calls but force the caller to enter a predefined password prior to any other data interchange.
4. Password controlled dial-back security – requires a valid password prior to hanging up and dialing a predefined phone number.
5. Modem key-lock pairs – the originating and receiving modems authenticate every connection with predefined tones, passwords, or PINs.
6. Encrypting modems pairs – the originating and receiving modems authenticate every connection with predefined cryptographic techniques, and all data interchange is also encrypted using a predefined or negotiated cipher.

Figure 5 contains pictures of three types of modem security: (1) an inexpensive modem key/lock pair costing about $150 per pair, (2) a pair of crypto-modems costing roughly $1200 per pair, and (3) a stand-alone password-controlled dial-back modem costing less than $350.

Dial-back security was once common in the electric power industry, but is no longer adequate because of **dial-back spoofing**. Hackers have learned to fake the hang-up tone and remain on the line while the called modem attempts to dial its predefined dial-back number. Hackers just ignore the incoming dial tones and issue an answer tone that reestablishes connection to the dial-back modem. Thus, the dial-back has been spoofed or fooled into an unauthorized connection.

(a) Modem Key/Lock Pair

(b) Matched Crypto-Modems

(c) Programmable Password-Controlled Modem

Figure 5 Low-Cost Secure Modem Devices

Regardless of how the hacker gains a viable connection to the modem, once access is granted, he or she will begin probing the equipment that is connected to the modem. Hence, it is prudent to implement a second tier of access control by password or PIN on the equipment itself. Further, communication time-outs and disconnects on that equipment, and on the modem itself, will provide added security. Figure 6 shows a password-controlled dial-back modem at work. The left side of the figure shows a valid connection, while the right side shows a bad-password time-out and disconnect. Following is a list of recommended practices when implementing modem security:

- Direct connect and unsecured dial-back modems are no longer adequate without some form of authentication and access control implemented within the remote equipment itself.
- Use strong passwords and maintain good password practices, as described earlier.
- Use communication time-outs and bad-password disconnects, as described earlier.
- Use authenticating modem key/lock devices, password-secured dial-back modems, or encrypting modems for public phone system access to critical equipment. Match the strength of your authentication to the importance of the equipment control.
- Use war dialers within your own phone number domain to locate unauthorized or forgotten modems.

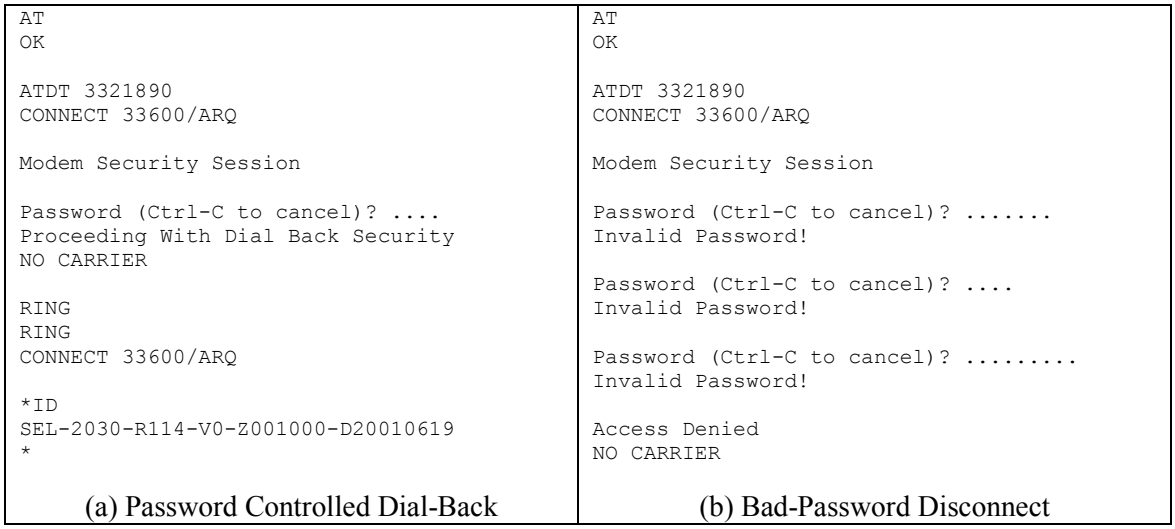


Figure 6 Example Secure Modem Connections and Disconnections

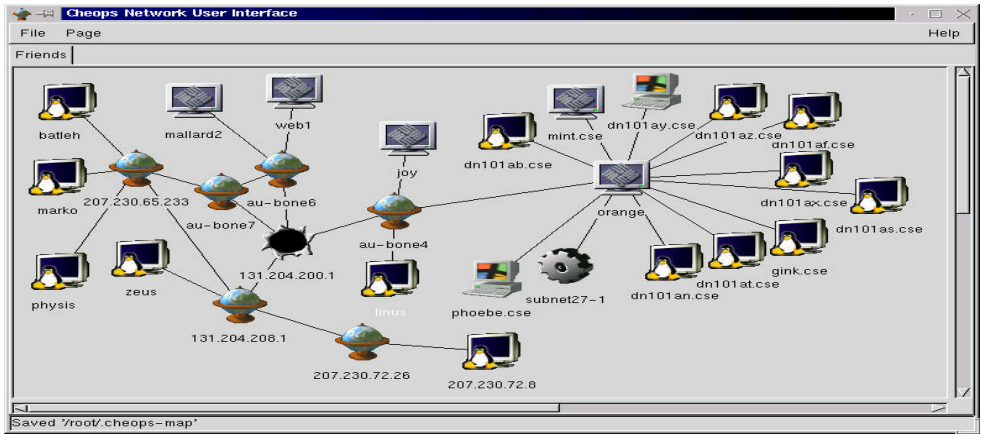
PUBLIC NETWORK ATTACKS AND DEFENSES

The most important thing to remember when attaching equipment to the Internet is that you are literally giving access to everyone in the world unless you deliberately restrict that access by implementing security controls. The Internet does not have any built-in security features and, unfortunately, it is awash in offensive tools to bypass your add-on controls. Fortunately there are several tools and techniques that can be borrowed from the computer-networking world and used to safeguard your electric power system controls and protection. Still, we emphasize that the battle between Internet offense and defense is a race where the defense typically lags behind the offense.

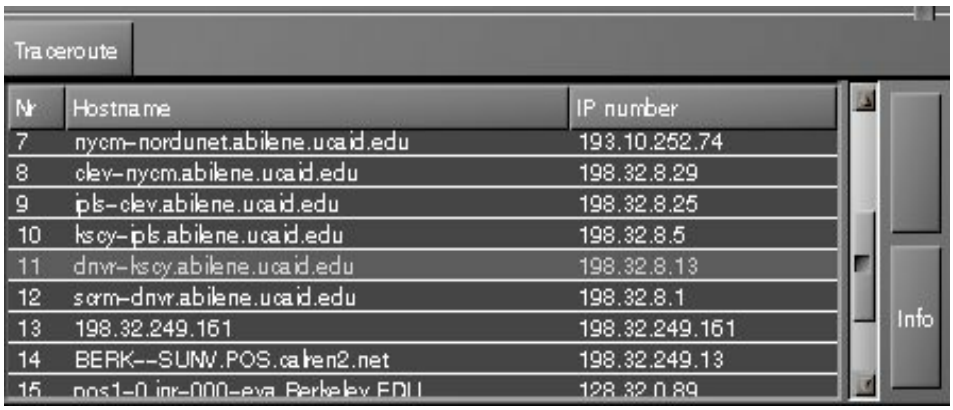
Hackers have a plethora of offensive Internet-based attack tools. On one hand you have script kiddies downloading attack scripts to launch against unpopular corporate computers and nuisance hackers flooding servers and defacing Web pages just "for fun." On the other hand, you have career criminals and organized crime penetrating corporate databases to steal credit and identity information, foreign information warfare agents deliberately stealing corporate and national secrets, and terrorists looking for ways to use your own assets against you. The one thing they all have in common is the high-speed anonymous access provided by the Internet. Experienced hackers rarely attack directly from their own computers. **Anonymizers** are e-mail servers and Web sites that obscure e-mail and network addresses so the recipient of the attack cannot directly identify the attacker. Hackers will obscure their paths through several layers of hacked computer systems and anonymizers, so their back-trail gets lost in layer upon layer of bogus accounts. Once hackers obfuscate their identity, they usually start their attack with a **ping sweep**, **trace router**, and/or a **port scan**. A ping sweeper will actively ping (i.e., send a "please acknowledge" message) to a wide range of Internet addresses (e.g., thousands) looking for active addresses. Once an active address is found, a route tracing tool will show the hacker where that equipment is relative to his or her location. Figure 7 demonstrates the functionality and sophistication prevalent in trace route tools available free on the Internet. Figure 7(a) shows an example graphical trace route output, while Figure 7(b) shows text output from a trace route tool. Similar tools, like Traceroute and Ping, are standard features on most Unix systems and can be used both offensively and defensively. For example, Ping is useful to determine if your equipment is

responding properly, but it also has an option that will flood a target Internet address with nuisance packets as fast as it can.

Once a probable target is located, a port scan will determine what kind of communication ports are available, and how vulnerable those ports are to attack. Some port scans actually rate the attack success probability on a scale from "trivial" to "extremely difficult – don't even bother." Figure 8 shows the results of a commonly used port scan freely available on the Internet. After the hacker determines the route to the target, the target's operating system, and the list of attackable ports, he or she only needs to decide how best to attack. Scripts, programs, and procedures for attacking all commonly used computer operating systems, network servers, and Web servers are freely available on the Internet. Attack scripts and programs exploit known vulnerabilities that are defects or design flaws in the system or server. Other attacks focus on manufacturer default settings and passwords that are often not changed during installation. Still others exploit encryption weaknesses in security features like access lists and password files. Recent intrusion incidents point to a disturbing trend in hacking vendor-supplied network routers and switches. Hackers are obtaining and studying vendor documentation in order to discover default settings, passwords, access control lists, and maintenance backdoors.



(a) Graphical Trace Routing



(b) IP List Trace Routing

Figure 7 Example Trace Route Tools

Your defenses against Internet-based attacks are many, but two strategies stand out as most effective. First, maintain strong password practices, up-to-date security patches, and always change default vendor password settings. Second, employ experienced network administrators and charge them with regular scrutiny of access logs and system events. Diligent monitoring of system logs is absolutely crucial. Experienced network administrators can detect and shut off intrusions as they unfold. Although an automated Intrusion Detection System (IDS) can identify and (sometimes) prevent common intrusions, nothing matches the flexibility and adaptability of a human expert. IDSs, virus scanners, Firewalls, and Virtual Private Networks complement, but do not replace, experienced network administrators.

An automated IDS is used to determine if insiders or external users are misusing the system. There are two types of IDS: signature detection systems and anomaly detection systems. Signature detection systems match known, observable intrusion characteristics against a database of intrusion profiles and determine if a match is likely. Anomaly detection compares ongoing system behavior against a profile of normal system behavior and warns when anomalous behavior is occurring. When an intrusion profile is matched or abnormal activity is detected, the IDS will attempt to shut down the intrusion and inform the system operator. Both types of IDS have the same common problem: too sensitive a setting generates false positive warnings, or false alarms when there is no intrusion, and too insensitive a setting generates false negatives, or misdiagnosed

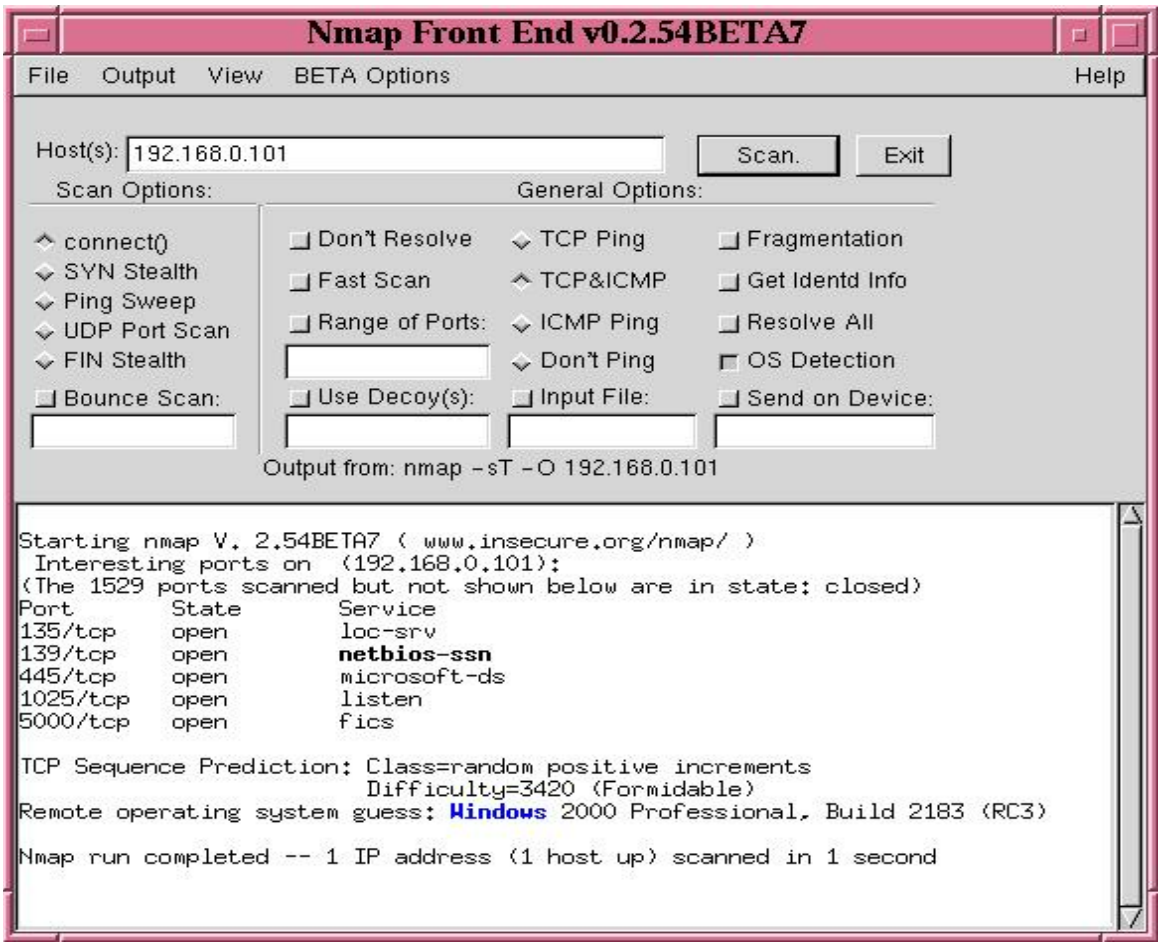


Figure 8 Port Scanning Tool

actual intrusions that go unnoticed. IDSs can be implemented in computer operating systems and/or firewalls and routers. Software versions range in cost from free via the Internet to several thousand dollars commercially; hardware versions typically cost several thousand dollars.

Virus scanners are programs that scan incoming files (usually e-mail messages, but other datastreams as well) to see if those files contain characteristics of known computer viruses. They look for embedded or attached executable programs, macros, and scripts. Good scanners have an up-to-date database of virus profiles. When a target profile is identified, the virus is either removed or the recipient is warned that the file may contain a virus. Any computer receiving files via e-mail, Ftp, Java or Javascript, Active-X, or Web-based cgi program is susceptible to virus infection. Free virus scanners can be obtained through the Internet, but commercial versions only cost a few hundred dollars and the timely vendor upgrades and virus alerts are invaluable when trying to ward off the latest plague of contaminated e-mails flooding your mail servers.

A Firewall is a protected gateway, usually a network router or proxy server, that stands between the outside accessible network and the resources requiring protection. The Firewall looks at incoming data packets and filters out undesirable requests and activity. In essence, Firewalls create segmented networks with restricted access into and between the segments. While most industrial Firewalls are programmable network routers, many combinations of hardware and software filters can be used to protect your substation equipment. Software Firewalls are available free via the Internet or at costs ranging from a few hundred to a few thousand dollars commercially. Hardware Firewalls start at a few thousand dollars and go up from there.

Virtual Private Networking (VPN) is an implementation of network packet encryption working in conjunction with Firewalls to form point-to-point secure messaging over public networks like the Internet. By encrypting and encapsulating the low-level data within other protocols and data packets capable of Firewall-to-Firewall addressing, you can send a secure message that can only be opened by the receiving VPN device. This is often called *tunneling* because the secure message is, in effect, tunneled through a public network. VPNs always work in pairs with both the sender and receiver encrypting and deciphering the data packets being transmitted between the two devices. VPNs can be implemented as software running on servers, but more commonly they are integrated within a hardware Firewall router. Software VPNs can be obtained freely through the Internet, or commercially for up to a few thousand dollars. Hardware VPNs start at around $500 and go up to over $25,000 for combined router/firewall/VPN capabilities.

Figure 9 shows how cryptographic devices like secure modems and VPNs can be used to safeguard your substation communications, while Figure 10 shows how VPNs and Firewalls can safeguard your enterprise-level IT systems.

Here are some recommended practices for safeguarding systems attached to the Internet:

- Use strong passwords and maintain good password practices, as described earlier.
- Use communication time-outs and bad-password disconnects, as described earlier.
- Change all vendor-supplied passwords and access control lists.
- Use a port scan tool to identify your own active, unguarded ports.
- Use a ping sweeper to find unauthorized or forgotten IP addresses within your own domain.

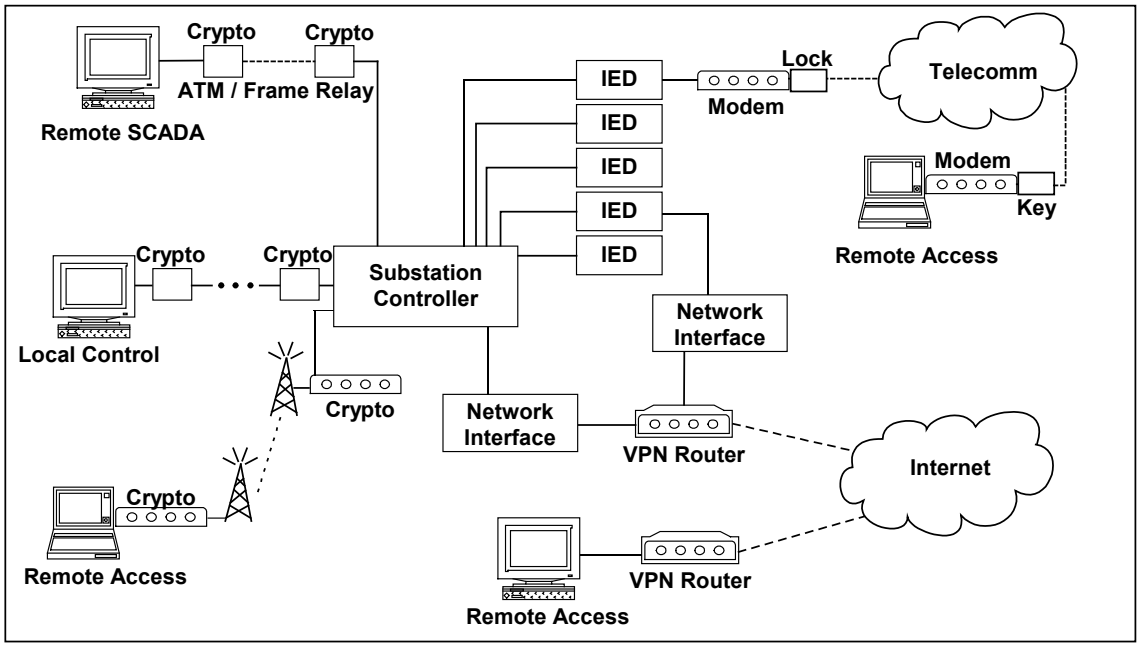


Figure 9 Securing Substation Communications

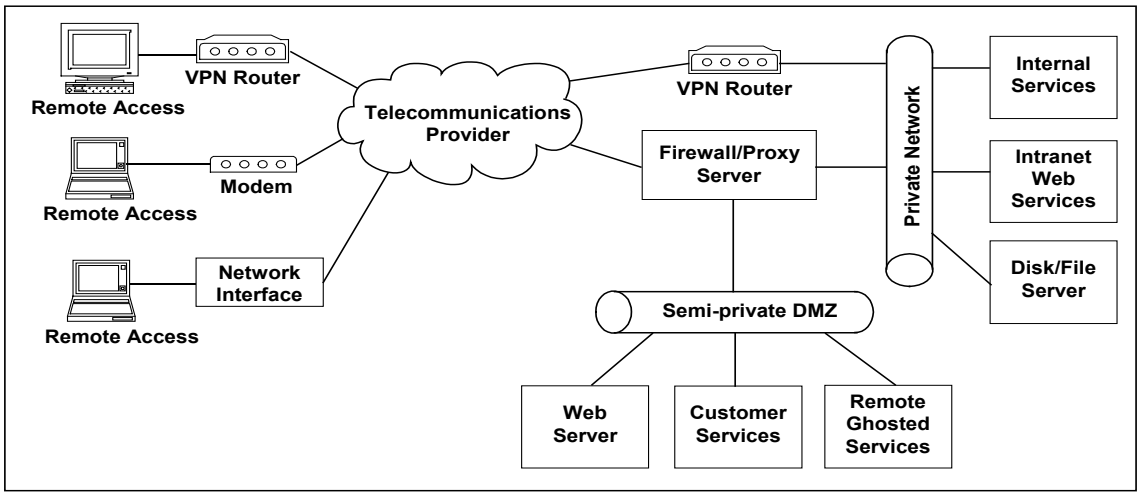


Figure 10 Securing Enterprise IT Systems

- Use a network sniffer and/or a trace route tool to verify that your network configuration is what it is supposed to be.
- Use network switches, not hubs, to isolate subnets and eliminate multipoint broadcasts.
- Eliminate unused and unnecessary ports, user accounts, and operating system services (e.g., rwho, rlogin, anonymous logins and anonymous ftp).
- Enable Web-browser security options and site restrictions; Disable Active-X controls, anonymous logins, Java and JavaScript.
- Regularly apply vendor patches and upgrades to ward off automated attack scripts and maintain state-of-the-practice security.

- Use VPNs to encrypt communications to and from critical control equipment and enterprise-level IT systems.
- Use IDSs, virus scanners, and Firewalls, as appropriate for the systems you are trying to protect.
- Separate enterprise-level IT systems from SCADA systems using Firewall/routers; better yet, segregate them completely.
- Have systems personnel view system logs and access lists daily.

WIRELESS NETWORK ATTACKS AND DEFENSES

Wireless networks are only slightly different from public networks in that wireless communication vendors typically incorporate security features in their products to ward off simple eavesdropping. You need to remember, however, that even directional line-of-sight signals can be intercepted and decoded. Bluetooth and 802.11 are the emerging favorites in radio-based wireless networking. They both have spread-spectrum frequency hopping capabilities, but that does not stop hackers from eavesdropping on your communications with inexpensive wireless sniffers called **war drivers** [7, 8]. Satellite and microwave transmissions are typically more secure than radio networks, but they both have reliability concerns that may preclude their use for some critical high-speed control situations [9]. Further, most organizations deploying radio-based wireless networks are using that capability for ease-of-access into enterprise-level LANs and WANs. Thus, a hacker penetrating the wireless network not only sees network traffic containing internal user accounts and passwords, but has a trusted backdoor into the enterprise computer network!

Fortunately, several vendors are now selling wireless routers and modems with built-in Firewall and VPN capabilities. Spread spectrum hoppers and Wireless Application Protocol (WAP) transceivers with built-in security functions are available for just a few hundred dollars. Integration and application engineers need to be careful however, because most of the wireless products are shipped with security options turned off, and several of them have known, posted vulnerabilities that are already being exploited by hackers. Here are some recommended practices for safeguarding wireless network systems:

- Assume your wireless network is a public network; follow all recommended practices for public networks, as described earlier.
- Turn on all vendor-supplied security features; change all vendor-supplied passwords and access lists.
- Use a wireless sniffer to verify that your broadcasts are encrypted properly and that account and password information has been completely obscured.
- Use wireless Firewalls and VPNs whenever they are available in your communications media. Do not use wireless communications for critical control systems without secure VPN tunneling.

PRIVATE NETWORK ATTACKS AND DEFENSES

Private networks of dedicated metallic or fiberoptic conductors are your most secure networking solution, but even then you are not 100 percent secure because of the threat from insiders and wiretapping. Studies show that insider abuse constitutes the majority of losses and damage to U.S. business, and the most recent CSI/FBI survey on computer crime shows that wiretapping and other forms of electronic eavesdropping is a multimillion dollar problem in the U.S. [10]. Fortunately, there are many network crypto-devices that you can use to safeguard your long-run communications. Off-the-shelf products (like VPNs) are available for as little as $500; custom solutions can be designed around high-speed crypto-chips enabling secure serial or network communications with little loss of throughput.[3] Encryption is discussed further in the next section. Here are some recommended practices for safeguarding your private network systems:

- Assume you will eventually have an insider problem; implement access controls and audit logs to ensure accountability across employees.
- Do not assume that your long-run lines will not be tapped for industrial espionage.
- Have systems personnel regularly view access logs.
- Implement alarm conditions for abnormal use (e.g., off-hours, extremely long connections).
- Star topologies (i.e., long-run lines) are more "survivable" than ring or bus topologies. Ring and bus topologies suffer from one-down-all-down failures.
- Use encrypted communications for critical applications when there is a likelihood of insider abuse and/or wiretapping or sniffing.

TELECOMMUNICATION NETWORK ATTACKS AND DEFENSES

Unencrypted data communications over phone or network lines are susceptible to eavesdropping via insiders, phone taps, Phone Phreaks, and network sniffers. Electronic intrusions against telephone switching centers can be traced back over 30 years and are as common today as hacker attacks against corporate IT systems. In a similar manner, a successful cyber-attack on a long distance leased-line provider, or an Internet Service Provider (ISP), gives the intruder access to all the data packets flowing into and out of that provider's equipment. Figure 11 shows that when communicating via leased or public telecommunications lines from any office to a substation (or vice versa), the communications path goes through the telecommunication service provider's computer-controlled switching network. If someone hacks into that network-switching computer it is relatively easy to listen to, or reroute, the data traffic on the telecommunications lines. It does not matter whether the provider is a local telephone company, a long-distance carrier, or an ISP – if their switching computer is remotely accessible, then it is vulnerable to cyber-attack. And even if it is not remotely accessible, the provider's equipment is still vulnerable to insider attack and eavesdropping.

[3] Intel claims 113 Mbps throughput running 168 bit Triple-DES encryption.

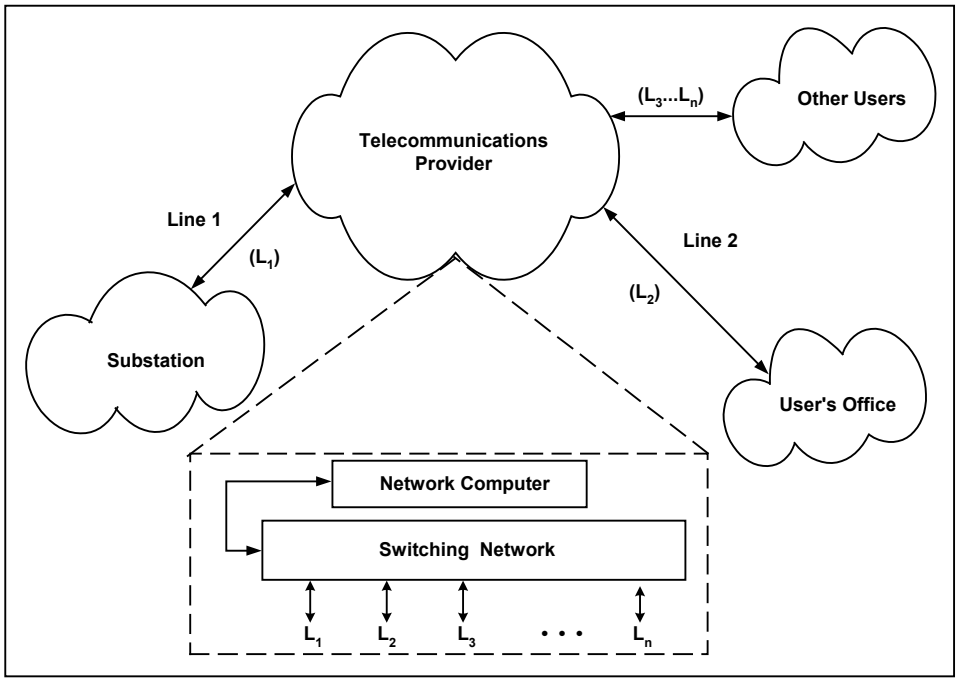


Figure 11 Hacking Telecommunication Provider's Switchgear

The PhoneMasters hacker gang compromised computer-controlled telephone switching in virtually every major telephone provider across the U.S., to the extent that they could listen, record, or reroute public telephone calls at will. Similarly, by hacking into an ISP and dropping a sniffer, network hackers can intercept and view TCP/IP, UDP, or UCA packets transmitted across a network and record all packets going to/from a specified target. The hackers then come back at a later time, retrieve their sniffed packets and start looking for valuable information like passwords, credit cards, account and identity information. Figure 12 shows the output from a network sniffer available free over the Internet. The bottom portion of the sniffer display shows the actual text or control information contained in the packet selected in the top portion of the display.

Leased telecommunications facilities are somewhat more secure than public telecommunications lines, but they are not without vulnerabilities. Asynchronous Transfer Mode (ATM) networks and Frame-Relay Permanent Virtual Circuits (PVCs) are the most popular mode for leased line network communications. The ATM and PVC solutions have reliability and quality of service suitable for critical applications and are probably the most reliable communications pathways outside of wholly owned dedicated lines. It should be noted, however, that all leased lines are vulnerable to unauthorized electronic intrusions. Longstaff, et al. [11] take a very pessimistic view of our connections via unguarded communications channels:

> …the ever-increasing use of SCADA systems to remotely operate our critical infrastructures through the telecommunications network has rendered our information systems more vulnerable to intrusions and the transmission of malicious misinformation and signals… International boundaries have been eliminated …{such that} universal access to computers has enabled hackers and would-be terrorists to attack information systems and critical infrastructures worldwide.

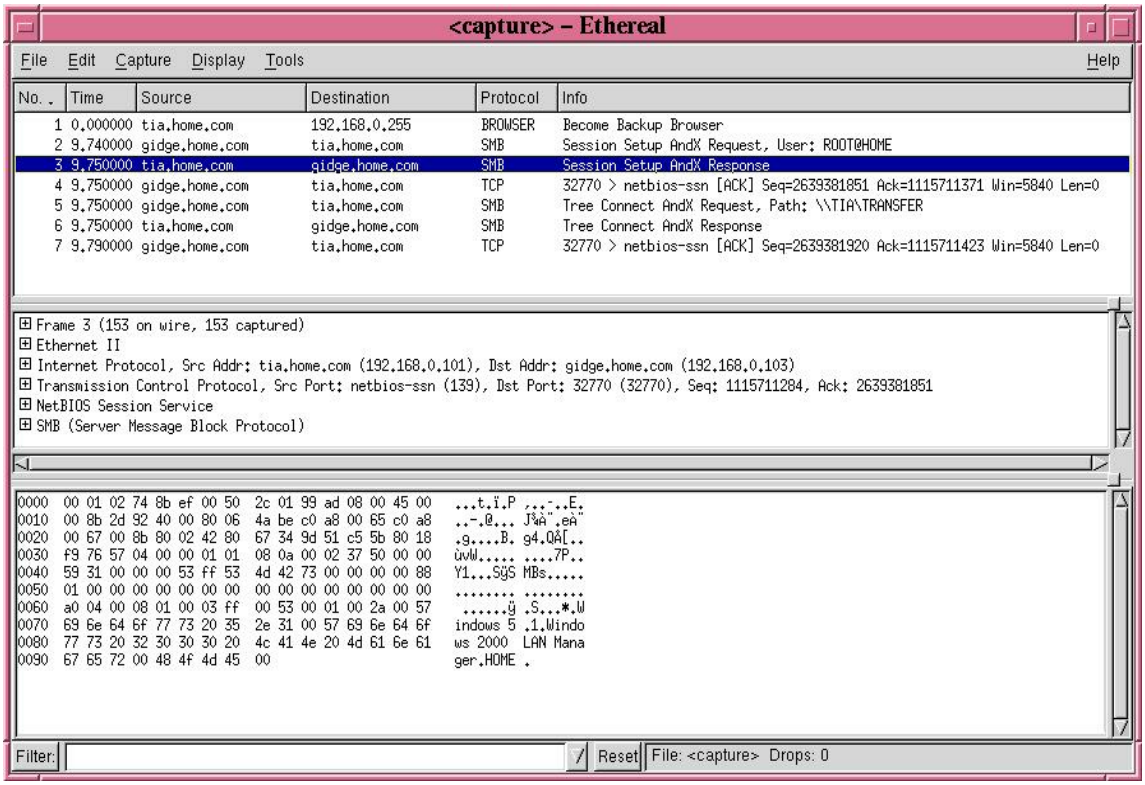


Figure 12 Network Sniffer Display

Defense against all forms of telecommunication attack is strong authentication and message encryption. Data encryption safeguards the contents of transmitted data packets while in transit from source to destination. Fortunately, all telephone and network data packets can be encrypted so the data contents are unreadable. Advanced levels of encryption can also obscure the final source and destination addresses so that network traffic analysis (used in industrial espionage) is difficult. Methods of data encryption are beyond the scope of this paper, but Figures 9 and 10 show how cryptographic devices can be used on all communications media. The cost of these devices ranges from a few hundred dollars per pair to several thousand dollars per device.

In the United States, encryption standards are established via Federal Information Processing Standards Publication 140-1, *Security Requirements for Cryptographic Modules*. FIPS 140-1 defines four levels of cryptographic security ranging from Level 1, basic security via integrated circuitry, through Level 4, the highest level of secure communications and processes. Most encrypting modems operate at Level 2 or Level 3, the difference being that Level 3 requires users to identify themselves by entering a password or PIN. Hence, Level 3 encrypting modems are, by definition, two-factor authentication devices. Similarly, most encrypting network communications cards or boxes operate at Levels 3 and 4, so they are also multifactor authentication devices.

Here are some recommended practices for safeguarding your communications that flow through telecommunication providers:

- Be aware that employees of the telecommunication provider are insiders with access to your data; assume that all your data is visible unless you encrypt it.

- Use encrypting modems, wireless transceivers, and VPN devices whenever sending and receiving critical information across leased or public telecommunication lines. Turn on all security options. (Many devices are shipped with security features turned off.)
- Change the default vendor encryption settings so hackers cannot break your encryption just by reading the vendor documentation.
- Implement alarm conditions for abnormal use (e.g., off-hours, extremely long connections).

SUMMARY AND CONCLUSION

Modern configurations of electric power control systems and protection devices are essentially systems of distributed intelligent devices resembling networked computing systems. As we move to increased integration and automation in our power stations, the temptation of easy remote access brings both opportunities and challenges. You need to recognize remote access vulnerabilities and apply mitigating technologies to remove or reduce those risks. We have discussed a variety of tools and techniques you can use to safeguard against electronic intrusions into computer-based networks controlling electric power generation, transmission, and distribution. Figure 13 shows an example vulnerability assessment tool that can be used to identify and mitigate your own network vulnerabilities.

Cyber-attacks are now commonplace in the computer and telecommunications industries, and the attacks are increasing in frequency and magnitude, so the probability of a serious electronic intrusion into an electric power station IED, substation controller, or SCADA system is growing. Recommendations for hardening substation devices, SCADA systems, and utility computer networks are many and varied. Each organization involved in electric power production and distribution needs to conduct its own risk assessment and decide where to focus its efforts. Fortunately, there are many tools and techniques, with a wide range of pricing and complexity, that can help you safeguard your IEDs, substations, and SCADA systems.

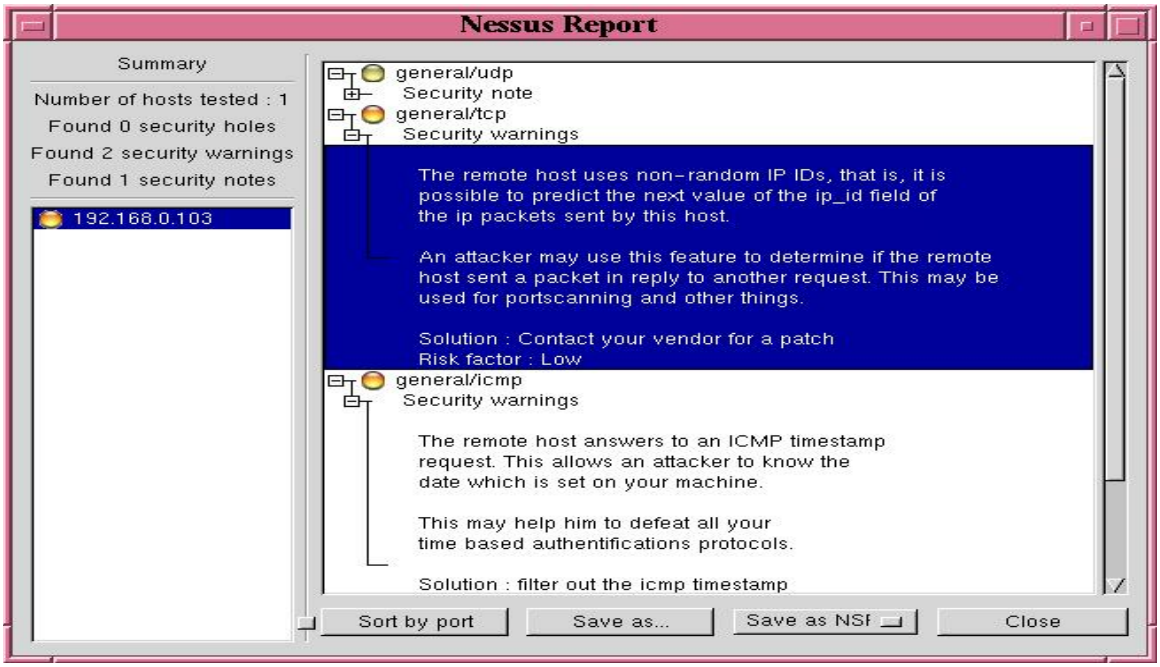


Figure 13 Example Network Vulnerability Analysis Tool

REFERENCES

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

[2] National Security Telecommunications Advisory Committee Information Assurance Task Force, *Electric Power Risk Assessment*, March 1997. (see 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*, October 22, 1997. (see http://www.julieryan.com/Infrastructure/IPdoc.html)

[4] U.S. Federal Bureau of Investigation, National Infrastructure Protection Center, 2000. (see http://www.nipc.gov)

[5] P. Oman, E. Schweitzer, and D. Frincke, "Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems," *27th Annual Western Protective Relay Conference*, Paper #4, (October 23–26, Spokane, WA), 2000. (see http://www.selinc.com)

[6] P. Oman, E. Schweitzer, and J. Roberts, "Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions," *Proceedings of the 2001 Western Power Delivery Automation Conference*, Paper No. 1, (April 9–12, Spokane, WA), 2001. (see http://www.selinc.com)

[7] S. Harris, "Evaluating Wireless Technologies for Distribution Automation," *Utility Automation*, Vol. 6(6), Sept./Oct., 2001, pp. 25–28.

[8] I. Armstrong, "What's Happening with WAP?," *SC Magazine*, Feb. 2001, pp. 32–34.

[9] P. Oman and J. Roberts, "Barriers to a Wide-Area Trusted Network Early Warning System For Electric Power Disturbances," Paper #CSSAR, *Hawaii International Conference on System Sciences*, (Jan. 7–10, Kona, Hawaii), 2002.

[10] Computer Security Institute, "CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends*, Vol. 6(1), Spring 2000.

[11] T. Longstaff, C. Chittister, R. Pethia, and Y. Haimes, "Are We Forgetting the Risks of Information Technology?," *IEEE Computer*, Vol. 33(12), December 2000, pp. 43–51.

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 computer security and 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; he is a Senior Member in the IEEE and is active in the IEEE Computer Society and the ACM.

Dr. Edmund O. Schweitzer, III is recognized as a pioneer in digital protection, and holds the grade of Fellow of the IEEE, a title bestowed on less than one percent of IEEE members. He has written dozens of technical papers in the areas of digital relay design and reliability and holds more than 20 patents pertaining to electric power system protection, metering, monitoring, and control. Dr. Schweitzer received his Bachelor's degree and his Master's in electrical engineering from Purdue University, and his Ph.D. degree from Washington State University. He served on the electrical engineering faculties of Ohio University and Washington State University, and in

1982 he founded Schweitzer Engineering Laboratories to develop and manufacture digital protective relays and related products and services.

Jeff Roberts is a Research Fellow at Schweitzer Engineering Laboratories in Pullman, WA. Prior to joining SEL he worked for Pacific Gas and Electric as a Relay Protection Engineer. He received his BSEE from Washington State University in 1985. Mr. Roberts holds 19 patents and has several other patent applications pending; he has written many papers in the areas of distance element design, sensitivity of distance and directional elements, directional element design, and analysis of event report data. He has delivered papers at the Western Protective Relay Conference, Texas A&M University, Georgia Tech, Monterrey Symposium on Electric Systems Protection, and the South African Conference on Power System Protection. He is a Senior Member of the IEEE.