Low- or No-Cost Cybersecurity Solutions for Defending the Electric Power System Against Electronic Intrusions

Allen Risley and Kevin Carson
Schweitzer Engineering Laboratories, Inc.

Revised edition released April 2006

Original edition released May 2005

LOW- OR NO-COST CYBERSECURITY SOLUTIONS FOR DEFENDING THE ELECTRIC POWER SYSTEM AGAINST ELECTRONIC INTRUSIONS

Allen Risley and Kevin Carson
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

ABSTRACT

This paper presents a factual and rational analysis of threats to the electric power infrastructure. It shows that electronic attack methods may allow an attacker to launch a coordinated attack on many targets from a safe, remote location. You can greatly reduce the chance such an attack will succeed by applying the strong access control and monitoring technologies in SEL products. The defensive techniques and strategies presented in this paper are a low-cost and effective method of protecting the electric power infrastructure from electronic attack.

INTRODUCTION

There is clearly a lot of interest in securing the electric power infrastructure. Increased awareness of the problem, and the eminent deadlines imposed by the NERC 1200 and 1300 cybersecurity standards, are causing a heightened sense of urgency throughout the industry. Utility executives and technicians alike are seeking effective mechanisms for reducing the electronic vulnerabilities in their critical communications systems. The availability of security-oriented courses and conferences has increased dramatically. Unfortunately, although many of the technical resources available to utility personnel are urging immediate increases in system security, they are failing to provide the specific techniques and methods needed. In this paper, we present concrete and actionable techniques for mitigating the most common electronic vulnerabilities in the electric power infrastructure.

You can use existing cryptographic link-security devices to lock down vulnerable communications, such as unsecured SCADA links or engineering-access links to devices with weak access-control mechanisms. In addition, you can use these devices to protect the integrity of the strong access-control mechanisms in SEL equipment. We cannot guarantee the strength of other vendors' access-control mechanisms, but SEL relays and communications processors contain very strong electronic access-control technologies for effectively securing your critical communications functions. You can reduce almost all of the electronic vulnerabilities in critical communications with low-cost or no-cost techniques and technologies.

We begin with a summary of several very effective techniques:

1. Change the passwords on IEDs and protective relays when you install them. Do not use the factory default passwords.
2. Slow password guessing by enforcing communications lockouts after failed login attempts.
3. Choose strong, hard-to-guess passwords whenever devices support them.
4. Use multi-tiered password schemes to limit control and settings privileges.
5. Consolidate electronic access using a communications processor or data concentrator.
6. Use encryption to protect the integrity of password-based authentication mechanisms.
7. Protect unsecured SCADA protocols with cryptographic link-security technologies.

8. Use cryptographic authentication to protect devices with weak electronic access controls.
9. Use firewalls and routers to enforce Ethernet network segregation.
10. Monitor all suspicious electronic activity and use real-time notification techniques.

You can take a very significant step in securing your electronic vulnerabilities by using these techniques. In the discussion that follows, we will show that SEL equipment allows you to implement these techniques to secure your critical electronic communications. SEL University also offers a cybersecurity course that includes hands-on training in applying the techniques discussed in this paper.

THREATS

Reliable electric power delivery is critical to the United States' economy. A significant (widespread and long-lasting) blackout would virtually halt factory output and productive job function within the affected area. The economic effects of such a widespread loss of productivity are hard to quantify, but the costs would add up ***very*** quickly. The East Coast Blackout of August, 2003, affected some 50 million people in eight states and one Canadian province. It took utility personnel as long as 40 hours to restore power to many parts of New York City and Toronto. The economic impact of this event has been estimated at around $10 billion (USD).

The East Coast Blackout was triggered by natural events and compounded by human error. So far, this has been the case for all major blackouts. It is, however, easy to imagine scenarios in which deliberate actions by one or more individuals could cause a significant power outage. These intentional actions could be motivated by many factors, depending on the interests of the attacker. Some potential threats include the following:

- Foreign governments
- Terrorist organizations
- Environmental activists
- Disgruntled employees or insiders
- Hackers

Certainly, individuals and organizations intent on harming the U.S. government or population are aware of this potential for serious economic impact and social disruption.

ATTACK METHODS AND GOALS

The threats to the electric power infrastructure are very real, but hard to quantify. There is a wide array of potential targets, including the electric power grid, public transportation facilities, and financial institutions. Without specific, actionable data indicating that an attack on the power system is inevitable, we cannot place a tangible quantity on the probability of a successful attack. We can all agree, however, that there are individuals or groups who want to harm the United States. A successful attack on the electric power grid would, to a large extent, accomplish this goal. These reasons alone justify the need to assess and mitigate the vulnerabilities in our electric power systems.

There are many ways that a motivated attacker could harm the electric power infrastructure. In the following discussion, we assume that the goal of the attacker is to disrupt the delivery of electric power to the largest area possible. In general, we can group a very wide range of attack methods into two categories: 1) attacks that exploit electronic communications vulnerabilities, and 2) physical attacks against critical equipment. In Figure 1 we show some potential attack scenarios that might be aimed at your system to maximize the affected area of a service outage.

For each case, we outline the relative advantages and disadvantages of electronic and physical attack methods. We present three attack scenarios:

1. **A coordinated attack on many targets at once:** Example targets include geographically separated substations, reclosers, and generation facilities.
2. **An attack on a single, high-value power transmission or generation site:** Example targets include a high-voltage transmission substation or a critical generation facility.
3. **An attack on a single target that, if compromised, would give the attacker direct network access to many other potential targets:** Example targets include a SCADA master computer with SCADA protocol connections to many sites, or a control center PC with direct engineering access connections to many sites.

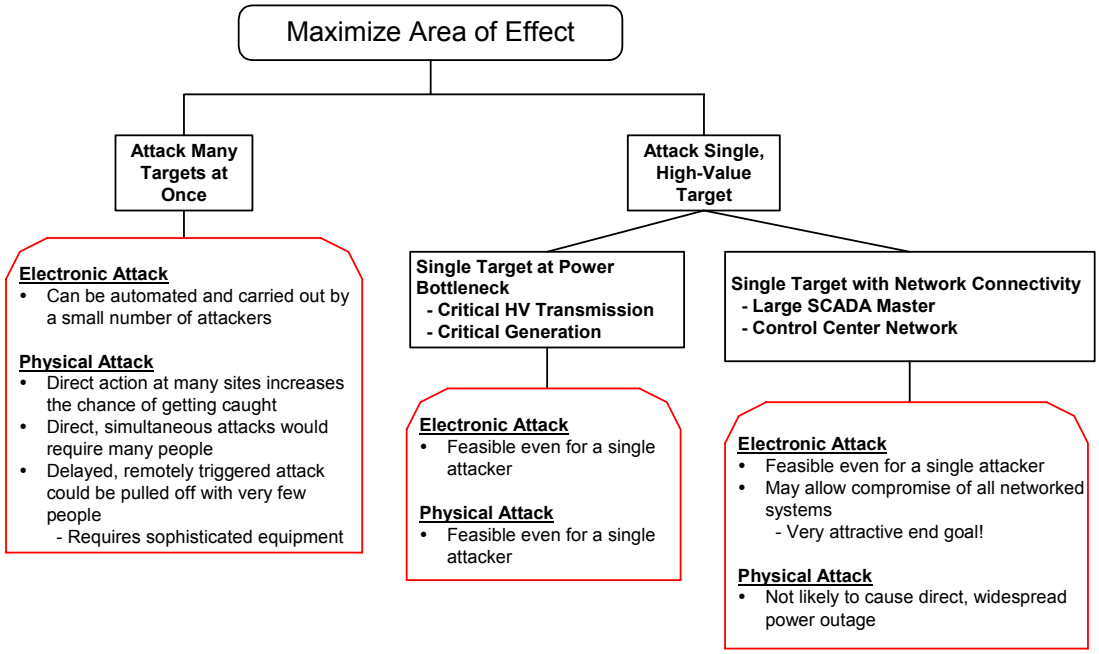

Figure 1 Possible Attack Scenarios for Maximizing the Area Affected by a Service Outage

For some of these attack scenarios, there is a distinct advantage to using an electronic, rather than a physical, attack method. For instance, a physical attack may damage or destroy a single device, but a physical attack alone cannot exploit the electronic communications connections from a control center to many remote sites. If, however, attackers can compromise a highly networked device like a SCADA master or a PC on the control center network, then they may be able to exploit electronic vulnerabilities to cause service outages in many of the remote networked devices. An example of this "force multiplication" effect is when an attacker uses a compromised SCADA master to send operation commands (i.e. open breaker) to all SCADA slave devices electronically networked to the SCADA master.

An attack against a large number of targets is another example where it may be advantageous to use electronic attack methods. In an attack against a large number of targets, it may be difficult for a group of attackers to coordinate a physical attack against many geographically separated targets. Such a method would probably require many individuals to travel to many sites to either attack the site directly or prepare a remotely triggered attack. With so many chances for error, this attack would likely have a higher chance of failure than an attack on a single site. On the other hand, if attackers can exploit electronic vulnerabilities from publicly accessible networks, they may be able to launch an automated electronic attack on several target sites from a single location.

Although physical attacks can be effective on a limited basis, scripted, automated electronic attacks have the added benefit of multiplying the force of an attack because they enable just a few individuals to simultaneously attack many geographically separated targets. Devices with a high degree of network connectivity compound this effect. They provide a very attractive target for electronic attack because an attacker can potentially exploit these network links to compromise connected devices. Any exploitable electronic vulnerabilities in your network may provide an attacker with an opportunity to launch complex, coordinated attacks on your critical systems. Furthermore, if attackers can exploit these vulnerabilities using publicly accessible networks, they may be able to anonymously launch the attack from a safe, remote location. The potential benefits of using an electronic attack scenario may make it the preferred method for an attacker. Because of these potential benefits, would-be attackers may try to use electronic vulnerabilities in your critical systems to disrupt operation of the electric power grid. Fortunately, it is not difficult to create effective barriers that reduce the chance of electronic compromise of most critical equipment.

BARRIERS TO THE SUCCESS OF COMMON ATTACKS

In Figure 1 we presented and compared some general attack scenarios. We did not, however, include the difficulty of carrying out a successful attack on a given target. In this section, we will show that we can put barriers in place that can increase the difficulty of carrying out a successful attack on a given target. In particular, we will show that it is easier to define and employ barriers to electronic attack than it is for physical or insider attack threats.

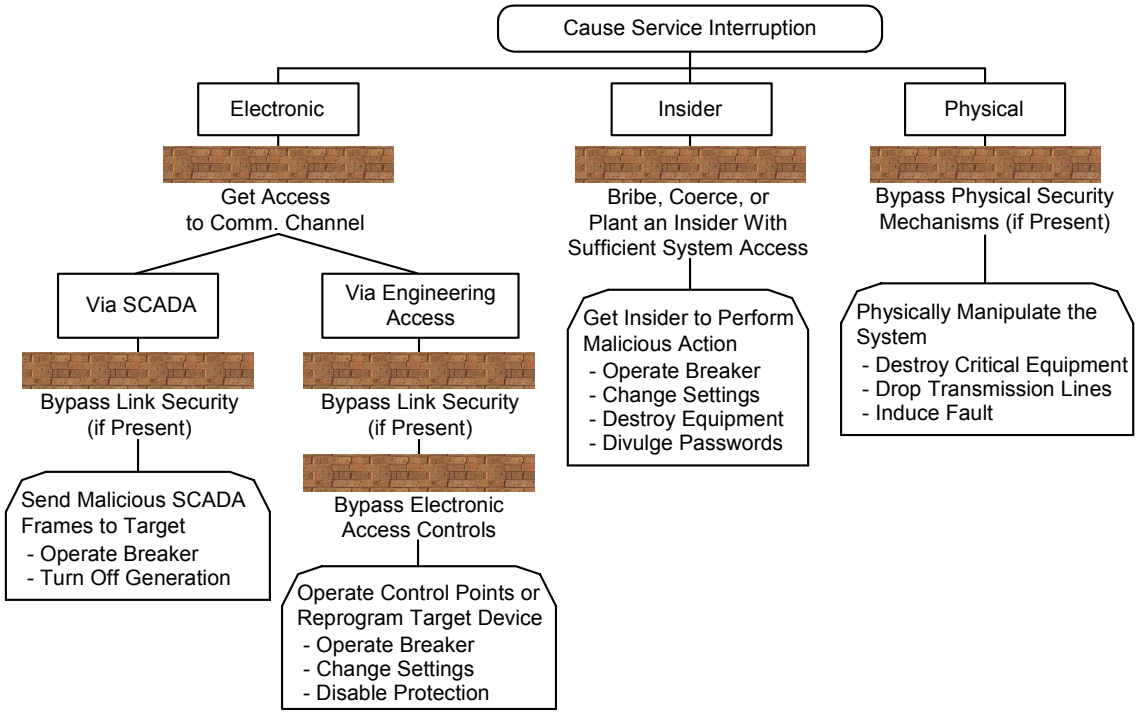

Figure 2 Attack Tree Showing Possible Attack Scenarios Against a Single Target

In Figure 2 we show four mechanisms for attacking a single target with the goal of causing a service outage. An example target could be a Remote Terminal Unit (RTU) or protective relay in a substation, a transmission line, or any other piece of equipment critical to electric power delivery.

Any of these targets can be vulnerable to physical attack. The only barriers to the success of such attacks are physical defense mechanisms. For instance, locked buildings, walls, secure fences,

guards, and intrusion monitoring equipment protect many potential targets. Generators and turbines will almost always be inside relatively secure buildings. Transformers and transmission lines, on the other hand, may be less protected or not protected at all. The massive size of the electric power infrastructure virtually ensures that some points will be vulnerable to physical attack. We can, however, reduce these risks by physically protecting our most critical, hard-to-replace equipment and having contingency plans in place to speed recovery from any significant event.

Malicious attackers are not merely outside the power system; malicious insiders also pose a potential threat. An insider can be a current or former employee, a third-party contractor, or any other individual with privileged access to your critical infrastructure or knowledge of sensitive information within that infrastructure. Insiders may be motivated by job dissatisfaction, financial gain, bribery, or blackmail. It is even possible that an attacker may plant an insider within your organization, rather than targeting legitimate employees. Barriers that you can use to reduce the threat posed by insiders include performing background checks on all new employees and strictly limiting specific knowledge and access privileges to those individuals who need them for their job function. Even with these measures in place, it is impossible to guarantee that the intentions of all possible insiders are innocent. This risk clearly increases with the size of your organization.

An attacker may use the SCADA network connections or engineering access connections to launch an electronic attack on the target device. There may also be electronic connections into your critical networks that do not fall into a strict SCADA or engineering access definition. Examples are energy management, file sharing, or real-time protection network links to a given device. Most of the points that we are about to make are general enough to apply to these connections. There are three potential barriers to the success of any electronic attack.

- **Difficulty gaining access to the communications channel**: The attacker must be in a position to read data from the communications channel and/or write data to the communications channel.
- **Difficulty bypassing link-security mechanisms**: The attacker must defeat any defensive technologies protecting access to the communications channel. Link-security technologies include encryption, authentication, and modem key-lock pairs.
- **Difficulty bypassing electronic access-control mechanisms**: The attacker must defeat any electronic access-control mechanisms on the target device itself. Common access-control mechanisms include passwords, PINs, and access lockouts.

We have made a distinction between link security and device electronic access control because many potential target devices in the electric power infrastructure do not have integrated electronic access-control mechanisms. For example, SCADA connections are automated data retrieval links that do not contain security provisions such as requirements for user-name and password entry. To secure such connections, we must place security devices, like cryptographic modules, on the link itself. In contrast, engineering access connections are often protected by electronic access-control mechanisms such as password or PIN entry requirements. For these connections, we can create very strong multilevel electronic defenses by using cryptographic link-security mechanisms to protect the integrity of the electronic access-control technologies that exist in the target device itself. We will discuss these concepts further in the sections that follow.

As shown in Figure 2, there are very often significant barriers that make a successful electronic attack difficult. However, these barriers may be ineffective or nonexistent for some of the critical electronic communications links in your system. For example, gaining access to a dialup channel is easy: anyone with a phone line and a modem can connect to your dialup modems. A critical SCADA link, on the other hand, may be implemented using a reasonably secure leased line, but may not have effective cryptographic link security to further secure the channel. It is extremely

important to identify the links with inadequate attack barriers and use effective technologies to mitigate these vulnerabilities. In the following sections, we will show you how to limit access to your communications channels, place effective cryptographic link-security technologies on a communications link, and use effective device security techniques in SEL products to reduce any electronic vulnerabilities in communications links.

LIMIT ACCESS TO COMMUNICATIONS CHANNELS

A control site (substation, generation facility, etc.) is likely to have electronic communications links for SCADA/metering, real-time protection, engineering access, file sharing, and/or Energy Management Systems (EMS). There are a variety of communications technologies for implementing these links, including point-to-point wireless links, dial-up or leased connections over the public switched telephone network (PSTN), or dedicated fiber or copper wire links.

Often, the cost of linking two physically separated devices or networks is inversely proportional to the level of security risk incurred by using a given communications technology. For example, a 28,000 bits per second (bps) connection from a given site to anywhere in the world can cost as little as $30 per month: $15 for the phone line and $15 for an account with a local Internet service provider. However, such a connection can expose this site to millions of potentially hostile Internet users whenever the connection is online.

A pair of direct, dial-up modems over the PSTN infrastructure can implement the same level of service for the additional cost of any incurred long-distance charges. The benefit of spending the extra money is that such a connection does not expose the system to the hostile Internet environment. This solution does, however, have an intermediate level of risk because anyone with a telephone line, a modem, and some motivation to probe the system, can potentially compromise the accessible electronic equipment.

Implementing the connection with a dedicated, leased line further increases security. A would-be attacker must then compromise the phone company switching equipment or physically tap the local wire to compromise the connected equipment. However, a 28 kbps leased-line implementation will almost certainly cost more than several hundred dollars per month, with the final cost depending on the geographic distance between the connected points and other determining factors.

Finally, if your desire is to maximize electronic security at all costs, you can make the connection using a fully owned copper or fiber network. Such a network can be very expensive to build and maintain, but a wholly owned network infrastructure ensures that the link itself is unlikely to be remotely compromised by an attacker.

It is very important to choose communications technologies that limit your exposure to remote compromise. We always recommend using the strong defensive strategies discussed in the sections that follow, regardless of the communications technology that you use to implement your communications link. However, these strategies are even more important if you use publicly accessible networks (Internet, dialup, or wireless) for critical links.

DEFINE YOUR ELECTRONIC SECURITY PERIMETER

By defining security perimeters, you can identify all remote access points entering and leaving the logical boundaries containing your critical equipment. These remote access points represent potential doorways into your critical network segments and must be properly secured with adequate electronic access controls. Fortunately, it is often quite easy to identify all electronic access points into or out of a particular physical location. With these entry points identified, the task of securing each of them becomes tractable and well defined.

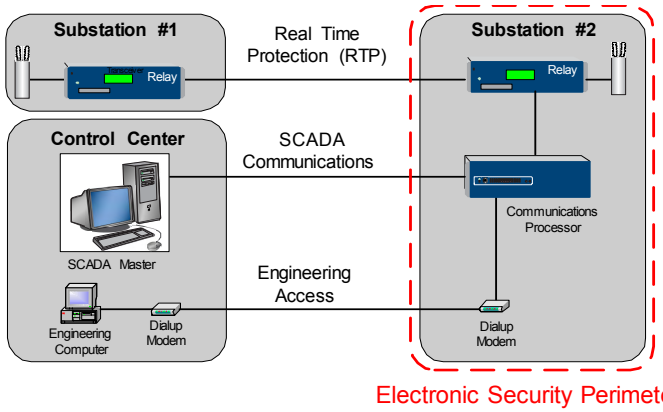

Figure 3 Diagram Showing an Example Electronic Security Perimeter Around a Substation

Identifying electronic access points includes the critical task of defining the nature and location of these access points. For the example given in Figure 3, there are only three access points entering the electronic perimeter surrounding Substation #2: the dial-up engineering access, SCADA, and the real-time protection communications links. Mitigating electronic vulnerabilities requires access controls on all remote access points into an electronic security perimeter. We will discuss the process of securing these remote access points in the sections that follow.

IMPLEMENT STRONG LINK SECURITY

Link-security technologies provide a very effective means of limiting access to the communications media itself and protecting the contents of the data that travels over the media. Inline cryptographic devices exist for serial data links, Ethernet networks, and virtually any other common communications technology. Many of these devices provide strong cryptographic security in the form of:

- **Encryption**: ensures that data cannot be read by unauthorized individuals.
- **Authentication**: ensures that data is sent by an authorized individual.

The importance of these two functions cannot be overstated. Encrypting all data transmitted on a communications link protects sensitive data like passwords, device settings, and system status information from being intercepted and read by unauthorized individuals. Authentication mechanisms prevent unauthorized individuals from sending malicious data to the devices serviced by the communications link.

It is extremely important to remember that most password authentication mechanisms transmit the password unencrypted. A strong password is extremely hard to guess with automated attack tools, but even the strongest password will fail if an attacker can intercept it and read it directly from the communications channel.

In Figure 4, we show the contents of Ethernet frames captured from the communications channel during a Telnet session with a protective relay. It is very easy to simply read the password value typed by the user. An attacker can use similar procedures to intercept and read unprotected passwords from serial communications lines. Strong link encryption prevents password interception by scrambling the data prior to transmission. The scrambling function can only be reversed by an authorized individual with knowledge of the secret encryption key. Link security, combined with strong device security, provides very effective multilevel access control for remote engineering access connections. The link encryption functionality provided by cryptographic devices protects the integrity of password-based security functions implemented in

the connected equipment. These technologies work in tandem to provide strong and effective electronic access control.

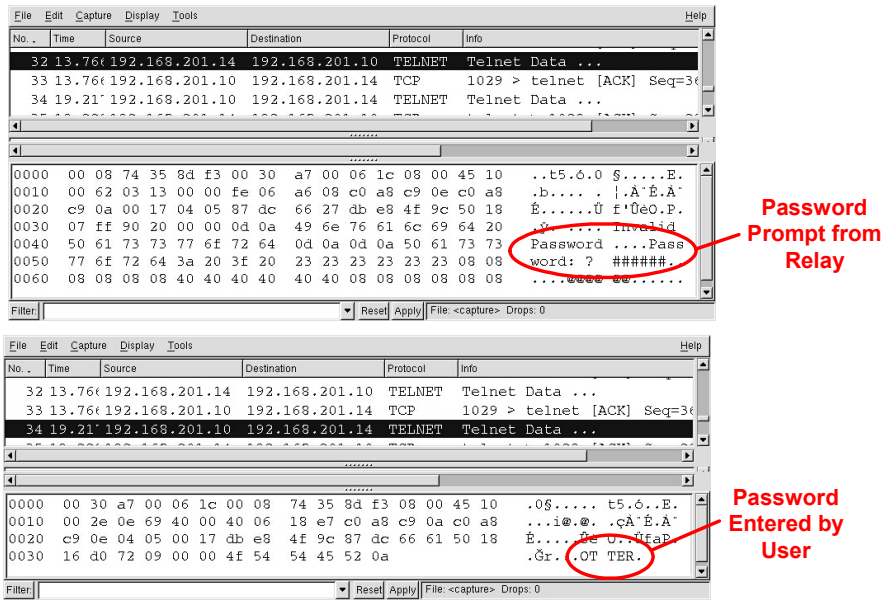

Figure 4 Figure Showing Electronic Capture of Unencrypted Passwords

Cryptographic authentication mechanisms are also extremely important because they provide a method for verifying that the data was sent by an authorized individual. Link-authentication mechanisms are independent of any electronic access controls (passwords, etc.) in the protected devices themselves. Because of this, they provide a means of locking out unauthorized access to otherwise unprotected communications access points such as SCADA protocol ports. It is important to note that the SCADA protocols in use in the electric power industry do not provide an additional layer of device security. This situation places additional importance on the link-authentication functions provided by cryptographic devices.

Examples of effective cryptographic devices include the SEL–3021 Serial Encrypting Transceiver for serial data links and Virtual Private Network (VPN) devices for Ethernet data links. VPN devices have been used to protect Ethernet network connections for years. The IPSec security protocol used in these devices has proven effective at securing connections to hostile public networks like the Internet. The technology is very mature; there is a wide range of inexpensive products that you can use to secure your critical Ethernet network links.

The SEL–3021 is a FIPS 140-2, Security Level 2-compliant bump-in-the-wire encryption device that provides very strong cryptographic link security for serial data communications.[1] A bump-in-the-wire encryptor is one that can be placed in an existing serial communications network without altering the configuration of the other devices on the network. The SEL-3021 was designed to be compatible with all of the network architectures common in the electric power industry. In particular, you can use the SEL–3021 in the following network topologies:

- **Point-to-Point architectures:** common to a single SCADA network leg or a dialup engineering access connection.
- **Point-to-Multipoint architectures:** common to multidrop SCADA networks.

[1] FIPS Security Level 2 is a standard developed by the National Institute of Standards and Technology (NIST) to define and verify the security requirements for a cryptographic module. Because the SEL-3021 meets these stringent requirements, the end user is assured that SEL has implemented the best practices in the design, testing, and manufacturing of the SEL–3021.

Figure 5 SEL-3021 Serial Encrypting Transceiver

The SEL–3021 was designed to provide a strong cryptographic security solution that you can install in existing, active SCADA networks while minimizing the performance impacts both during and after installation. It was designed with functionality that allows you to install the devices on the SCADA master and all remote SCADA devices without bringing the network down, except while physically connecting and powering up each device. Once installed, all SEL-3021 devices on the network can be commanded to perform a coordinated transition from pass-through to secure mode. Once operating, the SEL–3021 will encrypt and protect data without introducing significant amounts of data latency that can lower the polling rate of the SCADA system, and without adding intercharacter delays that can prevent the protected device from properly discerning SCADA protocol frame boundaries in the decrypted data stream.

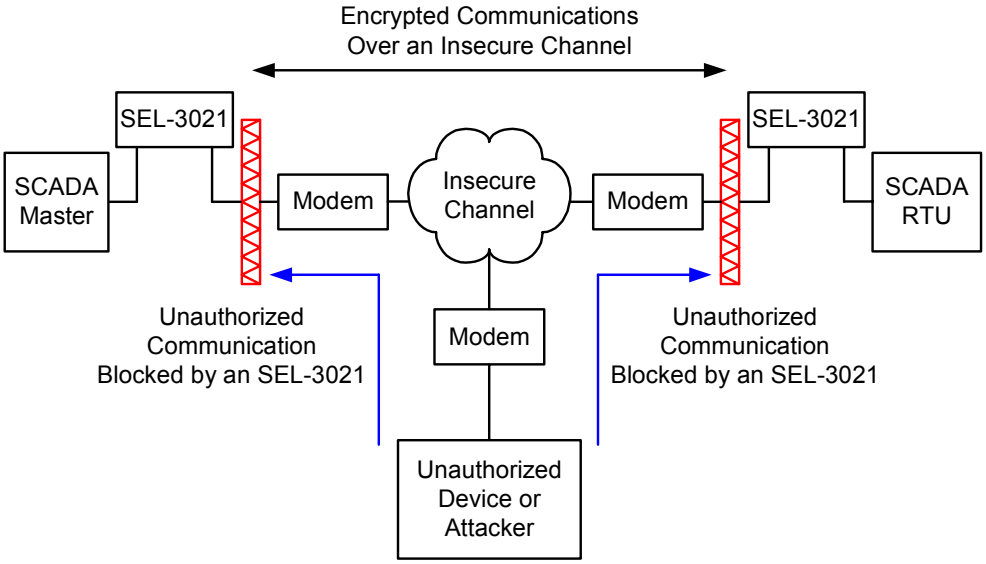

Figure 6 Diagram Showing a Serial Communications Link Secured by the SEL-3021

As shown in Figure 6, the SEL–3021 encrypts all data transmitted over the insecure communications channel and blocks all unauthorized, potentially hostile electronic traffic. It is effective for protecting password-based device authentication schemes and for locking down access to SCADA functions.

In addition to using the cryptographic link-security technologies just mentioned, you can add further security by using the SEL-2032 communications processor to manage the availability of your electronic access points. The SEL-2032 contains programmable output contacts that you can use to disable a modem or other channel access device when it is not needed.

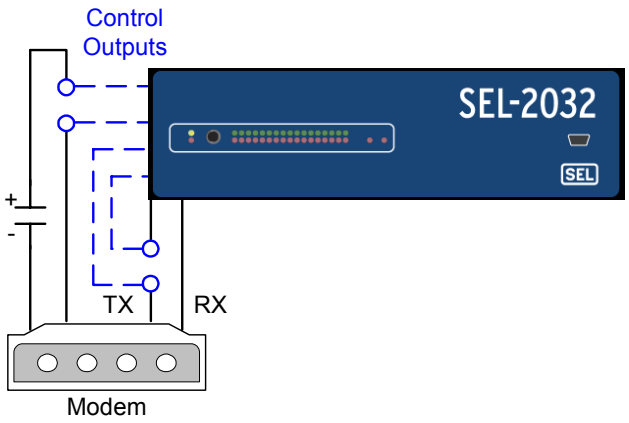

Figure 7 Use the SEL-2032 to Control the Availability of Channel Access Devices.

As shown in Figure 7, you can use the programmable output contacts in the SEL-2032 to disable power to the modem or to sever the electrical connection between the transmit pin on the modem and the receive pin on the communications processor. Both techniques will completely eliminate communications access from the outside whenever the contact output is open. The contact output will close or open, thus allowing or disallowing communications access, according to the state of an internal logic bit that you can control in many ways. With this approach you can allow access to the channel based on time of day (i.e. during business hours only), via a SCADA command, or via a set of user-defined logic expressions.

IMPLEMENT STRONG ELECTRONIC ACCESS CONTROLS

SEL relays and communications processors contain very strong electronic access-control technologies. These technologies are included with every SEL device that you purchase and do not cost anything to enable.

Strong Password Support in SEL Relays and Communications Processors

Strong password protection is an extremely effective defense against electronic intrusion and other forms of unauthorized access. If your password is disabled or easily guessed, intruders may gain unauthorized access to your critical equipment and successfully execute the electronic attacks presented in Figure 2. A well-formed, strong password is virtually impossible to guess, whereas an ill-chosen password may be guessed in just a few seconds.

Hackers have access to automated password attack programs that apply password guesses extracted from a huge list of compiled passwords. These password attack dictionaries can be downloaded from the Internet and contain thousands of commonly used passwords, including street slang, common spouse and pet names, and foreign words. As a result, passwords that are not based on existing words are immensely strengthened. Strong passwords consist of at least six 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 distinct, strong passwords include:

Ot35f7~~ A24.68!s #Ih2dcs4 @4u-Iw2g

All SEL protective relays and communications processors support strong passwords [2]. SEL products allow the user to program passwords made up of any of 90 characters (uppercase letters, lowercase letters, numbers and non-alphanumeric characters). In addition, all SEL devices support a password length of at least six characters. Newer SEL devices and communications processors support password lengths of up to 12 characters. Table 1 shows a comparison of the password strengths supported by power protection devices made by different vendors.

Table 1 Password Strength Comparison in Protective Relays from Different Vendors

	SEL	Vendor 1	Vendor 2	Vendor 3	Vendor 4	Vendor 5
(#Char, Length)	(90, 6)	(10, 10)	(10, 6)	(26, 4)	(14, 4)	(2, 3)
Combinations	537 B	11 B	1 M	475 K	41 K	14
Password Defaults	OTTER TAIL	Null	000000	AAAA	0000	-+-
Time Required to Brute-Force[2]	18 Years	201 Days	17 Minutes	5 Minutes	27 Seconds	4 Millisecond

SEL relays and communications processors have the strongest password protection in the business. A six-character password space on an SEL product can provide over 537 billion unique password values. If an attacker were to send every possible six-character password to an SEL relay in a continuous stream using a fast 57,600 bps serial line, it would take almost 18 years to transmit all of the passwords! In reality, it would take a ***lot*** more time than 18 years to attempt to log into an SEL relay using all possible passwords in turn. This is because the relay must transmit the password prompt and other feedback strings between password attempts, and it takes time to process each password attempt. If you choose a strong password value and protect it with link encryption, you can make it virtually impossible for an attacker to compromise the password-based authentication mechanisms in an SEL device.

Multilevel Password Support in SEL Relays and Communications Processors

The SEL–2032 communications processor and all SEL protective relays support multilevel password-authentication schemes.

Table 2 Summary of Multilevel Password-Authentication Mechanism in SEL Devices

Access Level	User Privileges	Authentication Requirements
0	View Device Identification Strings	N/A
1	View Settings	Level 1 Password
2	View and Change Settings	Level 1 and Level 2 Passwords
BREAKER (Protective Relays Only)	Operate Breakers	Level 1 and Breaker Level Password

This multilevel password authentication scheme provides a much stronger access-control mechanism than single-level password authentication for the following reasons:

- An attacker must compromise two independent passwords to reach Level 2 or BREAKER level access on an SEL device.
- The system administrator can grant limited, read-only access to an SEL device to a group of users without giving them the ability to change critical device settings or operate control points.

The multilevel password scheme makes it much more difficult for an attacker to gain an access level with a high enough privilege to cause significant system damage. If we assume that the goal of a malicious cyberattack is to change device settings or to operate critical control points, then

[2] This is the amount of time required to transmit all possible, maximum-length passwords in a continuous stream over a 57,600 baud serial line (assuming a 10-bit serial format).

the multilevel password scheme doubles the difficulty of carrying out a successful attack using password-guessing techniques, such as a dictionary or brute force attack. This is because an attacker has to successfully guess the Level 1 password before beginning an attack on the Level 2 password.

The SEL multilevel password mechanism also provides a system administrator with more control over the privileges granted to a given user. It is important to limit the dissemination of critical passwords as much as possible. The multilevel password authentication scheme outlined above allows you to grant a group of users the ability to view device settings and status, download event reports, or check metering data without simultaneously granting them the ability to perform potentially damaging actions.

Time-Outs and Channel Disconnects Slow Password-Guessing Attacks

The SEL–2032 and many newer SEL protective relays are designed to temporarily lock out the communications port in the event of three failed password-entry attempts. The lockout period of one minute on the SEL-2032 effectively limits the rate of a password-guessing attack to less than three password attempts per minute. This functionality increases the effective strength of the password-based authentication scheme on the SEL–2032 communications processor and all SEL relays with this feature. In addition, whenever the SEL–2032 locks out the remote communications port, it will also disconnect the current engineering access session by forcing the modem to hang up or by terminating the Telnet connection. This action further reduces the effectiveness of a password-guessing attack by forcing the attacker to redial the local modem or reestablish the Telnet connection every three failed password attempts.

The SEL–2032 and all newer SEL protective relays also have a port setting (‘TIMEOUT’) that you can use to force the communications port back to level 0 access after detecting a programmable amount of port inactivity. If set to a nonzero value, this feature will force all stale authenticated login sessions to be automatically terminated by the IED. This action prevents an attacker from inheriting the login privileges of a previous user.

MONITOR THE SECURITY STATUS OF ELECTRONIC ACCESS POINTS

It is extremely important to detect potential electronic attacks and react to them as quickly as possible. Strong electronic access controls can make it exceedingly difficult for an attacker to compromise your electronic devices, but they do not make it impossible. If you give attackers unlimited time to probe your critical systems for vulnerabilities, then they may eventually succeed in exploiting a weak point in your defenses. The only way to combat this is to put technologies in place that allow you to monitor your electronic connections for suspicious activity and receive timely notification of a possible attack. SEL products contain very effective electronic monitoring and alarming technologies that will allow you to detect and react to electronic attacks. We will outline these technologies in the discussion that follows.

Security Status Visibility in SEL Equipment

SEL relays and communications processors have a dedicated alarm contact that will pulse in response to the following events:

- Whenever there are three failed login attempts in a short time period.
- Whenever a user attains the Level 2, settings change, access.
- Whenever a user saves a new settings configuration to the device.

You can route the current status of the alarm bit through SCADA to detect potential password guessing attacks, or to detect unauthorized access or settings changes in the device.

In addition, you can program SEL devices to automatically send a time-stamped Sequence of Events (SOE) record in response to a change in status. You can also use SOEs to monitor changes in the internal logic bits in the device, including the alarm bit, the digital inputs, and the results of user-programmed logic equations. The event-reporting mechanism in SEL devices is extremely flexible. You can use logic equations to generate an SOE report for huge variety of conditions. Figure 8 shows a collection of SOE records collected from SEL devices in an example substation.

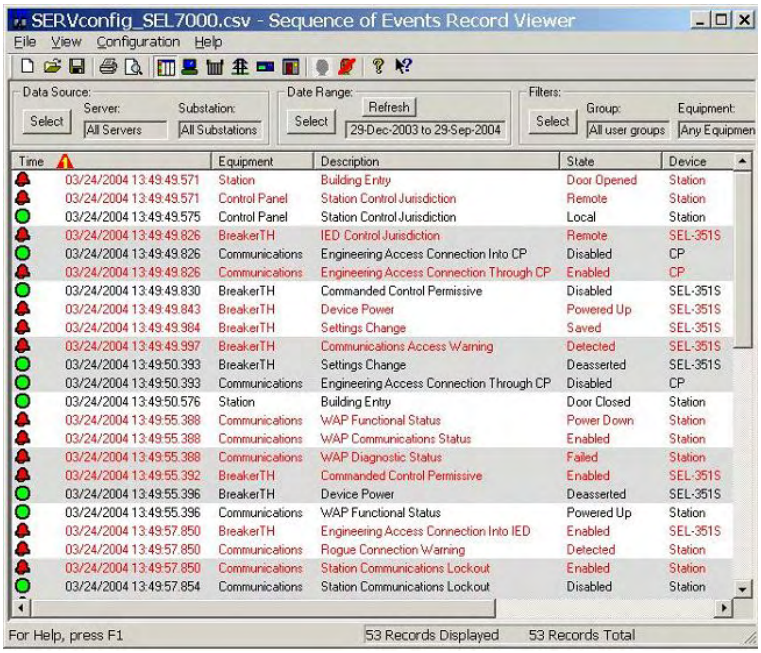

Figure 8 Sequence of Events Records Collected from SEL Devices

In this example, we are generating and collecting event records that indicate user access, physical perimeter breaches, enabling and disabling of remote breaker control, and many more valuable status indicators. The SOE mechanism, coupled with the robust logic programming capabilities in SEL devices, gives you the ability to monitor almost any event of interest. You can then consolidate and monitor these event notifications from a central location, and react to them as necessary.

Use the SEL-2032 to Consolidate and Monitor Electronic Access

The SEL–2032 communications processor can monitor and manage the connections made to every one of its 16 communications ports. The SEL–2032 contains status bits that you can monitor through the SCADA communications link to identify when transparent communications sessions are active on any one of its serial communications ports. In addition, the SEL–2032 contains control points to enable or disable the transparent communications access to any of its attached serial ports. As the communications processor receives remote commands to grant permission, it changes the connection status of the port so that remote administrators see the change in permission and the status of connection activity. Figure 9 shows a Human-Machine Interface (HMI) screen displaying the current status of all communications links controlled and monitored by the SEL-2032.

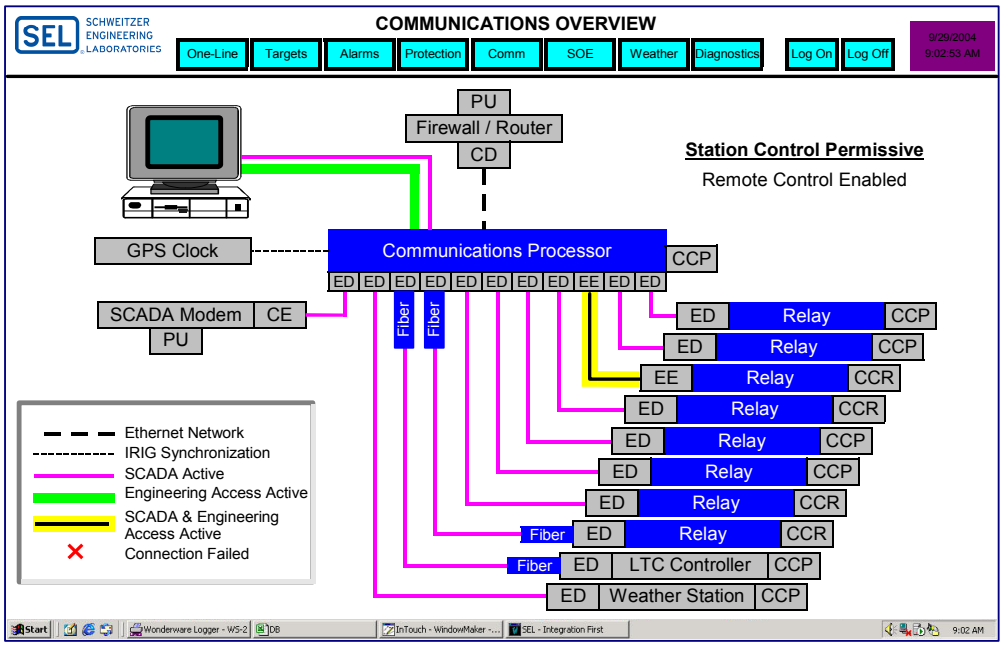

Figure 9 HMI Screen Showing Status of Substations Communications and Control Status

Controlling and monitoring the communications status points via the remote SCADA link allows you to control and monitor engineering access permissions from a central control center. An HMI Communications Overview screen such as the screen pictured in Figure 9 gives remote administrators the ability to grant engineering access to each serial or Ethernet connection independently for security and safety. This prevents unauthorized connections but also prevents unintended operation by validating that the user is connected to the appropriate IED. You can use the same procedure to manage and monitor remote breaker control in all relays connected to the communications processor.

Decrease Alarm Response Time With the SEL-3010 and SEL-2522

The SEL-3010 Event Messenger provides another means of delivering real-time alarm and event notification to the personnel who can quickly react to the situation. You can program the communications processor to generate an ASCII text message in response to a change of state of any status point. The SEL–3010 will receive these text messages and automatically dial a preconfigured telephone number to notify the recipient of the event. The SEL–3010 will turn the contents of the text into a computer-generated voice message that will inform the recipient of the nature of the detected event. You can also display alarms in control centers using the SEL–2522 Alarm Panel. Status changes cause an alarm horn and external light to alert operators to events and alarms when they occur. These devices can greatly improve operator response time, helping to ensure a timely reaction to any potential problem.

CONCLUSIONS

Reliable operation of the electric power system is critical to the U.S. economy. We can be sure that individuals and organizations intent on harming the U.S. government or population are aware of this vulnerability. As shown in this paper, electronic attack methods provide distinct advantages over physical attack methods for many potential attack scenarios. We have described techniques and methodologies that you can apply to your critical IEDs and remote communications links to mitigate the risks of electronic intrusion and malicious data injection. Many of these practices make use of very effective access-control and monitoring features in SEL

products. All of the techniques and technologies presented in this paper are free or low-cost solutions that you can implement in your systems with minimal effort. Although you can never completely remove the possibility of remote electronic attack, you can greatly reduce the probability of success and the severity of resulting effects by applying the suggestions outlined in this paper. These steps will greatly improve the overall security of your critical communications.

REFERENCES

[1] P. Oman, A. Risley, J. Roberts, and E. Schweitzer, "Attack and Defend Tools for Remotely Accessible Control and Protection Equipment in Electric Power Systems," Proceedings of the 55th Annual Conference for Protective Relay Engineers, College Station, TX, April 8–11, 2002. (see http://www.selinc.com/techpprs.htm for any of the following technical papers.)

[2] P. Oman, E. Schweitzer, and D. Frincke, "Concerns About Intrusions Into Remotely Accessible Substation Controllers and SCADA Systems," Proceedings of the 27th Annual Western Protective Relay Conference, Spokane, WA, October 24–26, 2000.

[3] P. Oman, E. Schweitzer, and J. Roberts, "Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions," and "Tools for Protecting Electric Power Systems from Electronic Intrusions," Proceedings of the 3rd and 4th Annual Western Power Delivery Automation Conferences, Spokane, WA, April 2001, 2002.

[4] J. Roberts, A. Risley, and P. LaDow, "Electronic Security of Real-Time Protection and SCADA Communications", Proceedings of the 5th Annual Western Power Delivery Automation Conference, Spokane, WA, April 1–3, 2003.

[5] A. Risley and J. Roberts, "Electronic Security Risks Associated With Use of Wireless, Point-To-Point Communications in the Electric Power Industry," Proceedings of the DistribuTECH Conference and Exhibition, Las Vegas, NV, February 4–6, 2003.

BIOGRAPHIES

Allen D. Risley is a Senior Research Engineer at Schweitzer Engineering Laboratories in Pullman, WA. Prior to joining SEL, he worked at Advanced Hardware Architectures as a Senior Research Engineer specializing in information theory and forward error correction. He received his Master of Science degree in Electrical Engineering from Washington State University in 1998. He has presented papers at the 1998 Conference on Information Sciences and Systems, the 2001 ISCTA conference, as well as many electric power industry conferences. His work has been published in the *Proceedings of the International Symposium on Information Theory* and the *IEEE Transactions on Communications*.

Kevin Carson studied graphic design and graduated with a BFA in 1981 from Washington State University. Working in the early years of CAD and computer graphics systems, he developed an interest in computer systems and networks and sought additional knowledge and training. During this time he worked on software development projects that included work for IBM, Lotus Development, and Microsoft. He also managed a technical support department, became an IT Department Director and built large-scale networks. In 1997, he received a Masters of Public Administration from the University of Idaho and joined SEL from the public sector in 1999. After 18 years of experience in the field, he is a Cisco Certified Network Associate (CCNA) and a Microsoft Certified Professional (MCP). Kevin worked as a Network Engineer until 2001. He is currently the Data and IS Security Manager for SEL.

Copyright © SEL 2005, 2006
(All rights reserved)

20060412
TP6206-01