

Securing Power Monitoring and Control Systems

by Chad Lloyd and Mathew Losey

Executive summary

Hacking critical control systems for power networks is increasingly making headlines as exemplified by power grid threats in the Ukraine and Israel in late 2015 / early 2016. By applying best practices to power monitoring and control systems, security vulnerabilities can be reduced. This paper introduces the potential risks posed by hacking, identifies common system vulnerabilities, and provides strategies to mitigate against hacking. It does not, however, guarantee that it will prevent all future hacking.

Introduction

Recent cyber security attacks in the Ukraine and Israel targeted the computer networks used to control the power grid. In some cases, these attacks shut down portions of the grid during bitterly cold winter conditions. The attack on the Ukraine's power grid exploited security vulnerabilities allowing the attacker remote control right in front of the operator¹. The attacker entered the operator's compromised password and opened multiple circuit breakers taking entire substations offline in an instant.

As attackers are targeting power infrastructure at an alarming rate, the need to be proactive about cyber intrusions for critical systems is increasing. Unfortunately, many power systems computers employ simple antivirus solutions that protect against known vulnerabilities, not against the 0-day attacks that are becoming more prevalent. A 0-day attack, defined as an attack that is recently discovered and not known to the widespread security community, requires more defenses such as network and application based allowlisting, firewalls and user access management and training. Intrusion detection systems can assist in mitigation by providing real-time monitoring of the communications network.

Planning and implementing cyber security management to a power Supervisory Control and Data Acquisition (SCADA) system can significantly reduce the probability of vulnerabilities in the system. Training users to be aware of social engineering attacks is paramount to securing a system. Many attackers gain initial access to target systems by performing simple social engineering attacks against unsuspecting victims.

¹ <http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

Techniques used by hackers

Attacks against critical systems generally originate from educated and well-organized hacking groups (including those politically motivated, corporate espionage or even foreign and domestic terrorism). These groups employ experts in the technical trade and are well versed in social cues. These attacks often begin with large-scale reconnaissance and research and may take many weeks, months, or even years to plan. Most attacks include a form of social engineering to gain initial access (either local or remote) and then attempt to break down barriers using known vulnerabilities or 0-day custom-crafted attacks.

We generalize these tactics into three groups: People, Operations, and Technology.



Figure 1

Attack tactics can be grouped by: people, operations, and technology.

When an attack enters the execution phase, the attacker must gain access to a system. The attacker may use social engineering techniques (people) or technology-related techniques (traditional hacking). The earlier planning phase determines if a local or remote connection is possible. Attackers attempting remote connections will use tools widely available for this purpose. These tools exploit known vulnerabilities for popular web servers, ftp servers and similar entry points. The tools will also look for misconfigured network devices (such as firewalls or switches). Remote access may also be gained by using common social engineering techniques against authorized users of the system. Examples include email phishing attacks (to gain passwords), malicious email attachments, or web links to viruses that provide backdoors into target systems.

If a system does not have an Internet connection, it is necessary for the attacker to gain local access. In many cases, this is physically plugging into the onsite infrastructure by employing social engineering techniques. This may include visiting the site for a meeting and plugging into the Ethernet port in a conference or waiting room. There may be an Ethernet port available on external equipment (in a generator control panel, for instance). With a hardhat and a clipboard in hand, the attacker may not look out of the ordinary when connecting a PC to an external control panel.

Critical systems are increasingly incorporating WIFI into the infrastructure creating a new attack surface. When properly secured, WIFI is reasonably secure; however, the misconfiguration of WIFI continues to be prevalent due to technical limitations of client devices (not supporting advanced encryption standards) or the simple process of managing access to the WIFI network. In some cases, system integrators or vendors are targets as they have likely connected to the WIFI of target customers. As the vendor's computer will store WIFI connection details, using one of the access techniques above will likely yield the credentials needed to make the connection to the true target system.

A less invasive technique is to load a USB key with a virus containing a malicious payload. By simply dropping the USB key in the parking lot of the target, an untrained user will likely discover the USB key and plug it into their internal computer out of curiosity. The USB key will then deliver the payload to the intended victim (silently and undetected by the user). This may also be used with remote access attacks (the payload of the virus installs a backdoor to provide remote access). This technique is the "USB Key Drop" and is a very popular and successful penetration method.

Once an attacker has gained access, the next step in the attack is generally to make sure that they *retain* access. This generally involves setting up new accounts with administrative permissions. This may also involve opening up additional ports on the servers and installing tools called "rootkits" that provide a means of connection in case the initial access method becomes unresponsive. When installing a rootkit, it is also common practice to either disable antivirus software or add exclusion rules (so that the rootkit is undetected by the antivirus solution).

"Man-in-the-middle attacks are increasingly popular as aging infrastructure with insecure protocols are targeted."

In some cases, the attacker will seemingly pause, confident now that they can return with additional payloads in the future (using the now multiple means of access they have granted themselves). The attack may not continue for days, weeks or longer.

At this point, the attacker can access the target system at will. This may include opening and closing circuit breakers, changing the configuration (including the ladder logic) of devices and software.

Depending on the amount of logging and auditing performed on the target systems, the attacker may go as far as to modify the log entries to mask malicious actions. In other cases, the attacker may simply access and modify the logs to represent chaos, simply to bring doubt to the auditing and logging system entirely.

In some attacks, it is unnecessary to gain control of the server to perform the intended attack. For instance, if an attacker is aware of the logic performed in the SCADA system, they can emulate the input values to instruct the SCADA system to react with false information. In a power system, a load-shedding algorithm could be triggered by feeding the SCADA false values using a simple man-in-the-middle attack. In this attack, the attackers represent themselves to the SCADA as a power meter (using an industry-standard protocol such as Modbus) and provide false readings. The SCADA will be unaware that the power meter is an imposter (as the real power meter is replaced by the attackers). Man-in-the-middle attacks are increasingly popular as aging infrastructure with insecure protocols are targeted.

Mitigation strategies

Protecting against these complex attacks requires attention to detail at every level of the organization. The following mitigation strategies will help protect critical infrastructure.

Social engineering: hacking humans

The most vulnerable asset in an organization is the human being. Social engineering is the easiest method to gain access to an organization and it is the most prevalent. Unfortunately, social engineering attacks are also some of the hardest to prevent. At the very least, all individuals should be trained to spot social engineering cues, such as phishing attempts or attempts to access protected areas using pretexting.

Phishing attempts involve sending legitimate-looking email directing you to a legitimate-looking (albeit fake) website that solicits credentials. Banking sites are commonly used for this attack. Spotting phishing attempts (sometimes by the bad sentence structure, wrong URLs or blatant misspellings) should become natural to members of the organization. Be aware that phishing attempts are becoming more sophisticated (with very genuine-looking email) and you may need to look closely to identify one.

Pretexting is the act of pretending, such as a person entering the facility claiming to be a vendor visiting to service a piece of equipment. A diligent gatekeeper should verify they are expected and validate their identification, regardless of the story claimed by the individual. Additionally, if the person is expected, are they bringing in any equipment? Do they have a laptop computer or a USB key? Keep in mind that trusted individuals should also follow policy. For instance, if the vendor's computer is compromised, the infection could be transferred to the organization (which could be the attacker's plan as shown above). If the vendor must use a computer on the premises (or mobile device), you can provide a computer or ask them to verify that their equipment meets your security guidelines (antivirus, group policies).

Operations management: passwords and policies

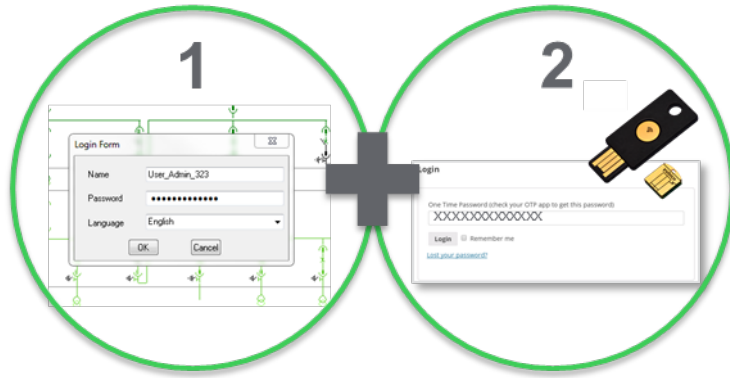
Closely related to social engineering and the human factor is operations management. This group involves setting policies to help mitigate attack vectors in the organization. Password complexity rules fall into this category. At a minimum, the SANS institute recommends a password of at least 12 alphanumeric characters (with both upper and lower case characters, at least one digit and at least one special character)². While it may seem obvious on first glance, it is imperative that all default passwords are changed on all hardware and software systems. This includes all components of the network infrastructure, such as firewalls, managed network switches, power meters and server systems.

For enhanced security, use two-factor (or multi-factor) authentication on the SCADA system. In this scenario, the user must enter valid credentials and possess a second form of identification. For internet-connected systems, this may include a text message or email with a unique number. For non-connected systems or for heightened security on connected systems, an onsite two-factor mechanism is used.

² <https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines>

Figure 2

Two-factor (or multi-factor) authentication on the SCADA system



This technique involves a USB-style device that is inserted and activated during login. This also provides enhanced security for remote connections as the unique key generated by the USB device is used one time before expiring (preventing against replay attacks). Ensure your SCADA system offers two-factor authentication.

Misconfiguration of network devices accounts for a substantial portion of attacks. This may include incorrectly configured firewall rules. Firewalls are complex devices and must be configured only by trained individuals. Never attempt to “figure out” how to configure a firewall as this will likely lead to unintended access. This applies to vendors as well; allow a vendor access to network infrastructure that they are familiar with and have received the proper certifications or training.

Policies around WIFI access should include a guest network that remains isolated from the Industrial Control System (ICS) network. This isolated network will protect the ICS network (which will likely have unsecured protocol traffic) from possible remote infections facilitated by vendor machines. Revoke WIFI credentials provided to vendors after use.

“Policies around WIFI access should include a guest network that remains isolated from the Industrial Control System (ICS) network.”

Audit user accounts and permissions on a routine basis. This may be in the form of a report that lists each user account and the role of the account (administrator, operator). Immediately investigate any unrecognizable users or changes in roles or permissions. Investigate logs of hardware and software systems to identify any unrecognizable actions or traffic. Unrecognizable items in the logs may indicate a breach (logs are usually cryptic in nature and will require a trained eye with intimate knowledge of the system(s) to detect abnormalities).

Always apply “least privilege” when assigning account roles and permissions. Do not provide roles or permissions for convenience. Consider if the user truly needs a role or permission before granting.

Ideally, all computers on the network are part of a domain (such as Microsoft’s Active Directory) and adhere to group policies. This will allow much easier administration of the systems as well as assist in user and permission auditing. Group policies should be carefully applied giving each user only the amount of access required to successfully do their job. Remember that security overrides convenience. For instance, users should not be able to download executable files on their computers. In the event that they have a legitimate need, they should approach a member of the security team to do this for them. Group policies can also be used to apply password complexity and change management. Ensure your SCADA system is compatible with password management via domain services such as Microsoft’s Active Directory.

Antivirus software and other security products such as Intrusion Detection Systems and Allowlisting Applications should require a password to change the configuration or to disable the product. Unlike consumer-grade antivirus products, commercial antivirus and security products provide this ability (as well as the ability to set grouping policies and remote administration). Never use consumer-grade security software or devices on a critical network.

Software and hardware should be routinely updated to include any security updates as provided by the vendor(s). Security updates may be available in the form of service packs or upgrades to the product. If in doubt, contact the vendor to ensure that your systems have the latest version of the software with all security related patches.

Technology: architecting for security

A properly secured SCADA system employs a defense in depth strategy. This means that multiple barriers confront an attacker at various physical levels of the network. Looking from the left to right in the image below (for Internet-connected systems), an edge router (R1) should be followed by a firewall (F1). Beyond this firewall you have what is known as the DMZ. It is in this area where you will typically find publically-available web servers and other servers. You will not find control system servers in this area. Beyond this area you will find another firewall (F2) that connects to the corporate network. This area will include display clients, corporate workstations and ancillary devices such as printers. A third firewall (F3) then connects to the ICS network (where you find the SCADA servers and sensor/devices).

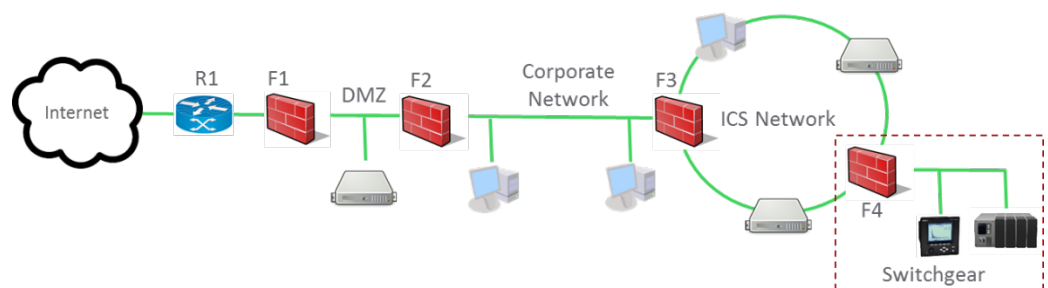


Figure 3

Example of the 'defense in depth' strategy.

Note that in critical facilities it is most common to have an “air-gapped” ICS network, meaning there is no connection to the corporate network or DMZ. Further, some ICS networks have firewalls (F4) at each piece of switchgear in the electrical system, providing further defense in depth. In some cases, these previously air-gapped systems are connected to other networks by unidirectional gateways (commonly called “data diodes”). These devices provide a hardware one-way communication path from the ICS network to outside networks. This is useful for situations where control is critical, but energy usage reporting is desired. (Unidirectional gateways guarantee one-way traffic by using a single optical path as opposed to a bidirectional link as achieved by standard fiber optic cable.)

Firewall selection is critical when designing for security. A firewall must understand the protocols that are expected to pass to fully protect the network. For instance, a standard commercial-grade firewall is used on the edge while an industrial-grade firewall (that has knowledge of industrial protocols such as Modbus) should be used on the ICS network. Industrial firewalls have knowledge of industrial protocols such as Modbus and can perform Deep Packet Inspection (DPI) of data to further secure the network. To perform DPI, the firewall disassembles and parses each packet to determine if the data is legitimate for the protocol and if it makes sense within the session. Keep in mind that firewalls are not equal and the quality of DPI protection will vary greatly between models or manufacturer.

Proper security design also includes the physical security of the network. Are all access points to the system within a secure area? Are any external devices (such as generators, external switchgear or air handlers) providing unintentional and unprotected access to the network? These devices should be physically secured and alarmed to insure the network is not accessed. Network closets and server enclosures should always remain locked and processes should ensure that only authorized persons have access.

Network security should be complemented by an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS). This system monitors network traffic in a passive mode and issues an alarm if it detects unrecognized clients or abnormal traffic.

Servers should be carefully configured to limit remote access. All unused ports should be closed. It should be well understood why any port is open on a server. For instance, web traffic is generally on port 80. If a server has port 80 open and there are no web clients expected or being used in the solution, port 80 should be closed. To reiterate, you should only open a port if the functionality is required, not if it is merely present.

All computers on the ICS network (including servers) should include application allowlisting to reduce the possibility of attack by infection. An application allowlisting component requires all active processes and accessed files to be present in the "allowlist". Any unknown process or file is prevented from execution or access. This is critical for protecting against 0-day attacks or custom methods (as antivirus alone is not capable of stopping these advanced attacks). Ensure your SCADA system is compatible with application allowlisting.

The ICS network should also be secured against USB attacks. Due to the prevalence of air-gapped ICS networks, USB attacks are popular against these critical facilities. In addition to social engineer awareness training, additional steps can be taken to prevent against these attacks. Group policies can be set to prevent USB devices from automatically loading on computers. Unused USB ports can be disabled in the BIOS of some computers (or unplugged from the motherboards from others). In extreme circumstances, filling a USB port with adhesive will render it permanently useless. Keep in mind that USB devices may not be a storage device. Some new hacking tools are available that emulate a keyboard (to avoid the group policies blocking storage devices). The point here is that group policies are not sufficient alone.

Conclusion

Securing critical power monitoring and control systems start with training your users to spot social engineering attempts and prevent malicious access. Complement this by enforcing well-defined security policies as described and remain diligent with audits and system monitoring and updates. Finally, deploy a security-driven architecture as shown to minimize vulnerabilities to the critical systems.





Further information on defense in depth and general security practices can be found at the SANS Institute Reading Room at <https://www.sans.org/reading-room>.

About the authors

Chad Lloyd is a Certified Ethical Hacker and a Senior Edison Fellow (Level 2) with Schneider Electric. Chad obtained his M.S. in Computer Science and his M.S. in Computer Engineering from Middle Tennessee State University and has been with Schneider Electric since 2007 where he is involved in software development and is currently the Architect for PowerSCADA Expert. He is a member of the Schneider Cyber Security Team and has also received BlackHat Black-Ops certification from the SensePost Company. Chad was also an adjunct professor at Middle Tennessee State University, teaching Local Area Networks with an emphasis on network security. He holds numerous patents related to Schneider Electric Hardware and Software.

Mathew Losey is the Offer Creation Manager for Power Software and Systems at Schneider Electric. He holds a B.F.A in French Literature and International Studies as well as an MBA in Marketing and Sustainability from the University of Kansas. He also holds a Master in Management, International Business from the Clermont Graduate School of Business in Clermont-Ferrand, France. He has been with Schneider Electric since 2012. Mathew has diverse and internationally focused experience working in France, Canada and the United States in strategic and offer marketing, sustainability, and energy and power management.



-  [A Framework for Developing and Evaluating Utility Substation Cyber Security](#)
White Paper
-  [5 Best Practices to Improve Building Management Systems Cyber Security](#)
White Paper
-  [How Test Labs Reduce Cyber Security Threats to Industrial Control Systems](#)
White Paper
-  [Browse all white papers](#)