An Exercise in Trust: Examining the Future of Cryptographic Technology in Electrical Control Systems

Colin Gray
Schweitzer Engineering Laboratories, Inc.

Presented at the
South East Asia Protection, Automation and Control Conference
Melbourne, Australia
March 14–15, 2017

An Exercise in Trust: Examining the Future of Cryptographic Technology in Electrical Control Systems

Name	Company Name	Email Address
Colin Gray	Schweitzer Engineering Laboratories, Inc.	colin_gray@selinc.com

Keywords: Cybersecurity, Cryptography, SCADA, ICS

Contents

1 Abstract

Ethernet networks are increasingly used to transfer protection, high-speed automation, SCADA, engineering access, and metering messages as part of the trend to combine all substation communications onto a single shared network. With the compounding complexities of modern communications methodologies, cybersecurity is now beginning to reach the forefront of electrical system design and implementation efforts. Infrastructure owners are looking to enhance digital defences to address growing concerns about the possibility of state- and national-level attacks against electrical infrastructure. Many industrial control system (ICS) technologists now consider cryptography to be the most readily available means to create defensible—and trustworthy—critical networks.

This paper presents actionable information regarding the critical requirements of a fully trusted ICS network. It examines the strengths and weaknesses of existing solutions for implementing trust management, including current IEC and NERC CIP standards and IEC and IEEE secure protocols. A survey of existing cyberattack mitigation methods is also examined, including the use of wrapper protocols such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec).

Finally, this paper proposes an architecture for a trust management solution based on concepts found in the Initiative for Open Authentication (OATH).

2 Introduction

Cybersecurity has been an aspect of IT enterprise domains for years, and with the introduction of substation LANs with potential access to the outside world, securing our systems has become a vital part of smart network design.

2.1 What Is Cybersecurity?

"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."[1]

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."[1]

Cybersecurity is the measures put in place to prevent cyber intrusions.

2.2 Why Do We Need to Consider Cybersecurity?

Infrastructure owners are looking to enhance digital defences to address growing concerns about the possibility of attacks against electrical infrastructure. These cyberattacks can be instigated from anywhere in the world and seek to find and exploit vulnerabilities in software, protocols, system designs, and defensive measures. "At the heart of this vulnerability is the capability for remote access to control and protection equipment used by generation facilities and Transmission and Distribution (T&D) utilities."[1]

2.3 Are Cyberattacks Likely to Happen?

The December 2015 cyberattack on the Ukraine power grid was the first time attackers were able to successfully infiltrate an electrical network and cause a power outage.[3] More than 50 substations were affected, 100 MW of load was shed, and 225,000 customers were without power for up to six hours.

The following coordinated attacks took place:

- Spear-fishing emails targeting individuals with files that appeared to be from the Ukrainian Energy Ministry.
- Installation of the BlackEnergy malware package on compromised computers.
- Compromise of the Microsoft Active Directory® domain controllers to harvest user credentials.
- Pivoting to the control system from compromised IT systems.
- Gaining access to control system HMIs.
- Attack on the uninterruptible power supply (UPS) remote management interfaces to shut down server UPSs.
- Execution of KillDisk malware to render computer systems inoperable.
- Launch of a telephony denial of service (TDoS) attack to hinder restoration efforts.

This is the first instance of a malware tool being used to bridge the gap between enterprise and ICS networks.

2.4 What Can We Do?

ICSs (which include SCADA, distributed control systems [DCSs], energy management systems [EMSs], and building management systems [BMSs]) have different requirements and operate under different parameters than enterprise networks. Table 1 shows the differences between the two disciplines. Enterprise networks have clearly established security procedures, tools, and applications. ICS devices are not typically tested with antivirus solutions because of the need for constant updates to their virus databases.

Security logging, incident response plans, and forensic analysis for ICSs are rare. Typically, once ICS computers are installed and brought online, very few updates or changes occur on those systems.

Enterprise computers are replaced every two to three years, while an ICS computer can be in operation for ten to twenty years. Any new vulnerabilities will most likely remain unpatched until the control system is replaced.

Blacklisting and whitelisting are techniques used to identify and either restrict or allow communications or other actions on the network. A whitelist lists all of the allowable actions; a blacklist lists those that are denied. Blacklisting is commonly used in enterprise networks to block access to known "bad" elements such as known infected websites or compromised IP addresses.

Table 1 Enterprise vs. ICS Security Procedures

Topic	Enterprise	ICS
Antivirus	Very common; easily deployed and updated; blacklisting used	Restrictions on new systems; can be difficult to deploy on legacy systems; whitelisting used
Patch management	Easily defined; enterprise-wide remote and automated	Typically requires vendor validation and owner/operator testing
People	Office environment	Operations environment
Incident response and forensics	Well-defined, understood, and deployed; extensive forensics possible	Uncommon beyond system resumption activities; no forensics beyond event recreation
Asset management	Performed periodically	Infrequent
Cybersecurity testing and audit (methods)	Can use widely available tools and methods	Widely available tools and methods are often inappropriate for ICS
Technology lifecycle	Two to three years	Ten to twenty years
Software changes	Frequent	Rare

A blacklist allows anything not specifically denied. A whitelist blocks anything except what has been approved. Whitelisting is becoming more common in ICS networks.

ICSs have a much smaller set of possible communications or actions than enterprise systems, a set that is unlikely to change. It is possible to create a list of exactly what should be communicating or acting and deny everything else in an ICS; this would be nearly impossible in an enterprise network.

3 The CIA Triangle

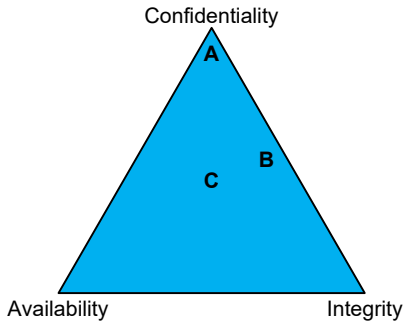

Figure 1 The CIA Triangle

The CIA Triangle shown in Figure 1 is a security model that shows the three key goals of cybersecurity. CIA stands for confidentiality, integrity, and availability.

- Confidentiality is the ability to hide information from unauthorized access.
- Integrity is the ability to maintain data accurately and unchanged.
- Availability is the need to ensure that important information is readily available at all times.

This triangle illustrates the challenges involved in trying to provide confidentiality, integrity, and availability. All three of these goals have their own demands on the system. Often those demands are counterproductive to the other goals. For example, the most confidential computer in the world is one that is coated in concrete and sunk to the bottom of the Mariana Trench. It is completely confidential; no unauthorized user can improperly access the data on that computer. However, we have completely lost the availability of the computer. No authorized user can access the data, either.

To design a system with the focus solely on confidentiality (Label A) is to lack any availability or integrity. A balancing act (Label C) often results in mediocre results for all three goals, but it is a hard one to reach. It is also possible to create decent results for two of the three (Label B) goals, which results in no results for the third goal.

These trade-offs have to be dealt with and decided by an individual with an appropriate understanding of the system. For example, in financial systems, confidentiality is typically the most important of these concepts. Banks want to keep accounts, passwords, balances, and so on secret to prevent malicious actors from gaining access to their systems and stealing money.

In ICS networks, confidentiality is not the most important. In the energy sector, availability is usually considered to be the most important of the three. In other systems (for example, the manufacturing sector), data integrity could be the most important.

4 NERC CIP

In 1998, Presidential Directive PDD63 set up a program for critical infrastructure protection (CIP). The North American Electric Reliability Corporation (NERC) was founded from the North American Electric Reliability Council, which was formed in 1968 to ensure the reliability of the North American bulk power supply. NERC has been tasked with implementing CIP measures in the power infrastructure sector.

NERC CIP Version 5 revised standards CIP-002 and CIP-009 and added CIP-010 and CIP-11.

The following list provides the core goals of cybersecurity:

- Know the system (CIP-002)
- Use baseline-approved systems (CIP-010)
- Practice need-to-know (CIP-004)
- Train staff (CIP-004)
- Establish defence-in-depth (CIP-005 and CIP-007)
- Protect the data (CIP-011)
- Log and monitor the system (CIP-Throughout)
- Have redundant communications paths
- Maintain peak performance of the system (CIP-Throughout)
- Establish access controls (CIP-005)
- Plan and practice for incidents and responses (CIP-008 and CIP-009)
- Practice physical security (CIP-006 and CIP-014)

We should know and understand what we are trying to achieve in any cybersecurity effort. The bottom line is, we want to preserve the integrity of the system we are protecting so that it can operate in a safe, reliable, and economical manner. To do this requires facing some tough challenges.

The first thing we must do is get to know the system we are tasked with protecting. Second, we should practice need-to-know and only share information about the security systems with those people whose jobs require that knowledge. The principle of least privileges allows authorized people to gain just enough access to the system to accomplish their jobs.

Cybersecurity success hinges on the people who work at the organization performing their jobs in a secure way, and the only way they will know how to do this is to train them.

Next we need to engineer a defence-in-depth architecture, i.e., have multiple layers of complementary defensive technology blocking or slowing down attackers until an operator is alerted to the attack and can respond.

Protecting data requires knowing when data are in transport and at rest. This usually involves cryptographic solutions, including encryption, digital signatures, and authentication, which are discussed later in this paper. Another solution to data protection is offline storage with removed and powered-down memory.

We need to continually monitor what's happening on the system so that we can respond as quickly as possible. Redundant communications paths are key. When one path is under attack or rendered unavailable, the other path allows the logs and alerts to get out and an incident response team to get in.

Maintenance of the devices and technology that make up the system includes hardware tests, software patch management, and configuration validations.

We must limit logical access to only those people who are authorized to gain access, and we need to make sure that we have proven that they are who they say they are before granting them access. This is authentication.

Incidents will happen and we need to plan for them.

5 Substation Security Model

Creating a secure substation model is the most effective way to protect critical infrastructure. We can segregate our substation into tiers, as shown in Figure 2.

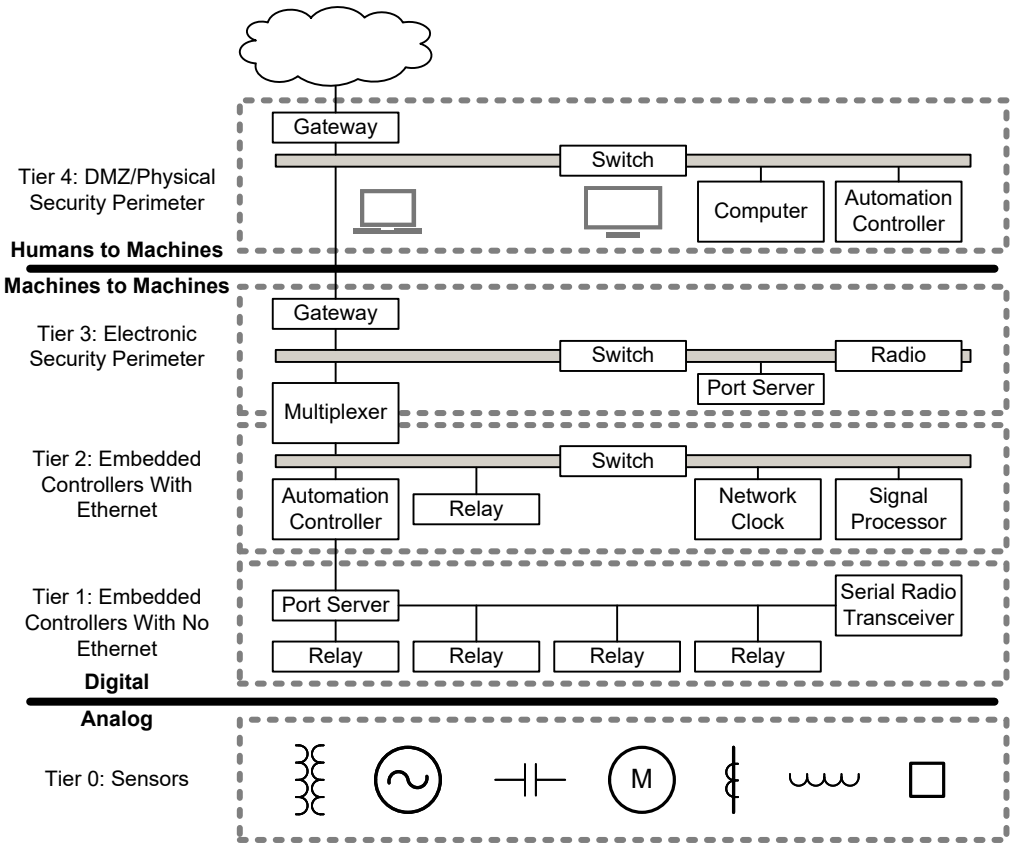

Figure 2 Substation Security Model

Tier 0 is our IED or process. It includes the devices we rely on to protect our networks, and doing so should be their primary goal. We do not want to burden these devices with security processing overhead.

Tiers 1–3, the data aggregation zone, contain the network, SCADA collection and computing, and HMI equipment. In this region, all normal operational activity is machine-to-machine.

Tier 3 is the electronic security perimeter. This boundary between the human-to-machine and machine-to-machine regions needs to have cryptographic terminations and firewall controls in place. The cryptographic tools are at this level because they need to be implemented where humans regularly interact with the system through general purpose computers and where there are poor physical security perimeters. If we burden Tier 1 and 2 devices with cryptographic technology, we run the risk of decreasing availability for our real-time operations and communications network.

Tier 4 is the access zone. Here we guard the network with firewalls, access control lists, and intrusion prevention systems. This is where humans work (demilitarized zone [DMZ] and SCADA), and this is where we implement security controls, such as IPsec virtual private LANs. We can employ Secure Socket Layer (SSL) or TLS at this tier, which use symmetric key algorithms to maintain data confidentiality and integrity.

However, this is more commonly used for things like connections between a web browser and a server, Voice over Internet Protocol (VoIP), and email.

Within the IPsec protocol suite, we can use Internet Key Exchange (IKEv2) to set up an encrypted security association using X.509 certificates.

6 Establish Defence in Depth (CIP-005 and CIP-007)

Once incoming and outgoing traffic are encrypted and secure, we have to ensure that any users needing to gain access to the site have the required credentials. The CIP-007-5 System Security Management standard provides guidelines on how to achieve this.

An AAA proxy service can be used to allow user connections from the outside world as follows:

1. Authentication – verify the identity of the user using local or centralized user-based accounts.
2. Authorisation – determine what the requesting user is allowed access to.
3. Accountability – collect and log all user actions during their session.

Centralised user account servers are accessible via Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS) to manage user credentials.

Automate these processes as much as possible. Change all default passwords, change device passwords regularly, and manage these device passwords so that users only need to know their own credentials to gain access and do not have to know device passwords.

These are actionable tasks and technologies we can and should be implementing into our network infrastructures today. But what is the future direction of all of this?

7 Open Authentication (OATH)

A collaborative group called the Initiative for Open Authentication, or OATH, “offers a vision and a straight-forward roadmap for propagating strong authentication across all users, all devices, all applications, and all networks.”[4] This need for strong digital identities comes from three network trends: identity theft, the rise of federated identity networks, and the proliferation of IP devices.

According to a 2002 report by the FTC, identity theft in the United States is the biggest reason people contact consumer protection services.[4]

Enterprises now must provide access to data for customers, business partners, and employees across more and more enterprise networks. Managing the interaction between these external networks requires identification, credentials, and information to be shared, giving rise to the term federated identity networks.

The ability to distinguish the difference between trusted and rogue devices is critical.

Strong digital authentication principles are great concepts for gaining remote access control or dialling into the network from home if the system is private and not connected to the Internet.

8 Conclusion

Securing our critical infrastructure is paramount. Understanding our networks and identifying and mitigating weaknesses are activities that should not be dismissed.

Cybersecurity and the application of cryptographic technologies to enforce it is an evolving process. There is no better time to consider this than now.

References

1. P. W. Oman, A. D. Risley, J. Roberts, and E. O. Schweitzer, III, “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 2002.
2. IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security.
3. D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies,” proceedings of the 43rd Annual Western Protective Relay Conference, Spokane, WA, October 2016.
4. Initiative for Open Authentication, “An Industry Roadmap for Open Strong Authentication,” September 2015. Available: https://openauthentication.org.

List of Figures

List of Tables

Biography: Colin Gray

Colin Gray is an integration and automation support engineer at Schweitzer Engineering Laboratories, Inc. (SEL) in the Asia Pacific region. Prior to joining SEL, he was a remote analyst with Transpower New Zealand providing technical and analytical support for SCADA and substation infrastructure.

Colin has been involved in the electrical industry for the past 34 years, starting as a trainee high-voltage technician, then migrating to communications and SCADA. In the late 1990s he was part of the DNP3 User Group Technical Committee for the Australia region. He was an engineering manager with Data Engineering Ltd. for four years, providing customer support to GE Harris customers throughout Australasia before forming his own company, Netlink Systems, in 2002.