tim yardley

SCADA: issu vulnerabil future dire

Tim Yardley is a Technical Program Manager in the Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign. His focus is on research and development in the cybersecurity and control systems space. He with open source initiati technologies from kernel development to user-interface design. Prior to jo industry, focusing on trusted operating systems, hardened network appliances, and management and control platforms.

yardley@iti.uiuc.edu

ple explos; nuclear rea tor shut down; sewage spi streets; trains derailed. drastic events? They are, events reported in the me when control systems eith compromised. How could th easy is it? In this artic control systems protectin structure, the risks they being done to protect the

Background

A Supervisory Control And Data Acquisition (SCADA) system is most simply described as a system that is monitoring and controlling a process or set of processes. Some examples of processes that might be controlled by SCADA systems are the opening and closing of water valves, control of power relays, and switching of train tracks. It comprises four basic components: a human interface, administration systems (systems that handle data acquisition and control commands on the control LAN), sensors, and a communication network. These SCADA systems are what were responsible for controlling the above-mentioned facilities, and in each case these were either compromised or failed.

In the past, a lot of these control systems operated in isolated environments with proprietary technologies. Consequently, they faced little to no cybersecurity risk from external attackers. But today, modernization and the adoption of available commercial technologies have resulted in these systems becoming increasingly connected and interdependent. In fact, almost every major operating system is being used across the range of vendor products. Typically, products with operating systems such as Windows XP and Linux in this space are installed on rugged machines that can handle industrial conditions and utilize redundancy in the design of the hardware.

A reference implementation of a traditional architecture might look like Figure 1.

Let's go into a little detail about the subsystems in Figure 1. The Human Machine Interface (HMI) systems provide information to the operators as to the state of the control system and its sensors (typically, housed at the field locations) and also provide a means to take action on that data via the administration systems (connected to the con-

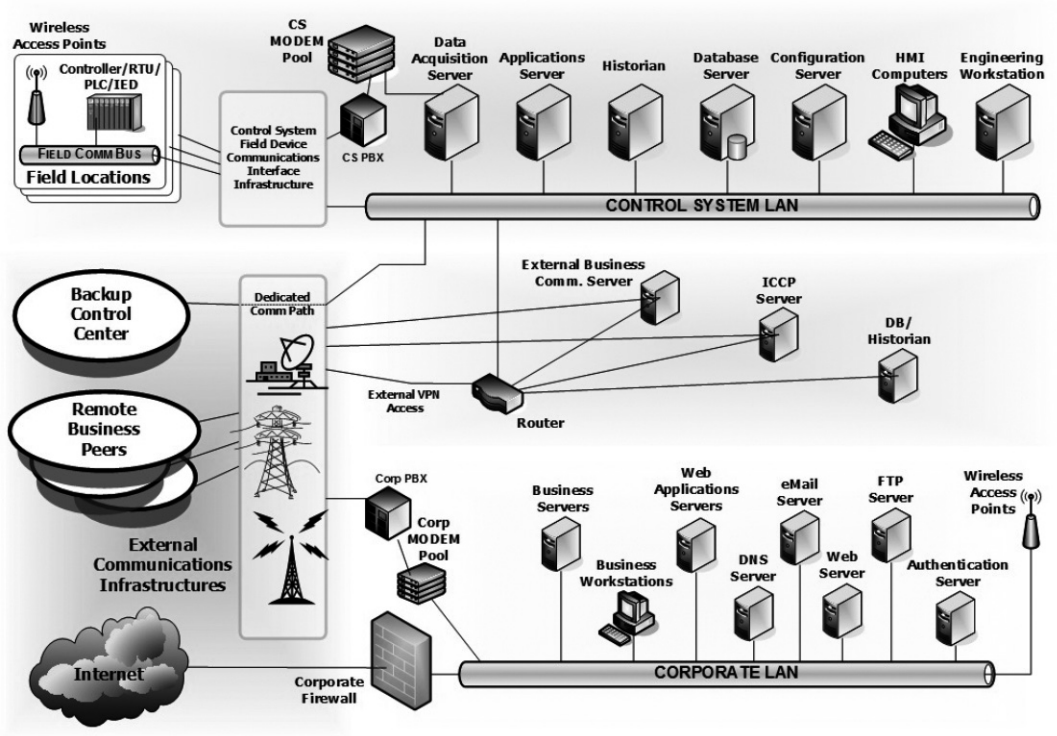

Figure 1: Representation of a typical SCADA architecture (Courtesy of the "Control System Cyber Security: Defense in Depth Strategies" document)

trol-system LAN). The sensors gather data from the field, which is then transmitted to the administration systems via the communication networks. Sensors can be analog or digital, and communication networks can be anything from serial lines and radio links to Ethernet LAN/WAN networks. Typically, there is also a corporate LAN that connects the rest of the company's systems and another segment that is dedicated to backup and providing external access to query statistics for interoperation.

It's a fairly straightforward setup if you look at it from a traditional IT perspective, but keep in mind that control systems can often have hundreds of thousands of points they are monitoring; as a result, the whole system gets complicated quickly. Some of the complexity is found in multiple sensors, varied communication networks, and geographic distribution of these devices.

Common Issues and Vulnerabilities

These control systems and protocols were often designed decades ago, when security was of little concern because of the closed nature of the communications networks and the general model of trusting the data on them. As these systems have been modernized, they have become interconnected and have started running more modern services such as Web interfaces and interactive consoles (telnet/ssh) and have implemented remote configuration protocols. Sadly, security has been lagging during the increased modernization of these systems.

For example, there is very little implementation of standard security mechanisms such as encryption and authentication. In these systems, encryption is sometimes hard for the legacy systems to support owing to lack of processing power, slow links (with 300 baud not being uncommon), and the legacy protocols themselves. The primary issue with the slow links is the byte-time latency (time to transmit 1 byte) incurred from buffering the data for encryption. Although adding encryption to these systems is generally trivial, maintaining the other properties such as timing and data integrity with the encryption in place is not as trivial. Authentication is equally troublesome. Vendors discourage the use of authentication by not supporting

it at all, supporting only weak authentication, or suggesting that all devices share the same authentication credential (password).

In the case of authentication, it is fairly common for devices in the control space to use default passwords for access and control. Most of these default passwords are very easy to find when using search engines. This is a similar issue to network monitoring agents such as SNMP that often come configured by default with known public and private access phrases.

The problem is further complicated by the move toward commercial, off-the-shelf (COTS) appliances and systems being integrated with the networks or part of the control systems themselves. While cutting costs and eliminating some of the proprietary nature of control systems, these appliances and systems bring with them the well-known passwords and vulnerabilities that each product may be subject to. Often these COTS systems may end up providing a point of entry for an attacker into the critical control network.

As seen by the events highlighted, there are some severe consequences of failure in these control systems. This makes these systems prime targets for attack. Thus, interest in this space has also increased the knowledge of the protocols used and the weaknesses present in those protocols. Vendors designed the SCADA protocols to make it easy to debug systems, and these very features also facilitate data interception and manipulation, modification of logs, and denial of service. The lack of support for encryption, signatures, and authentication just makes these attacks easier to accomplish.

There are many protocols involved in this space, and therefore there is a lot of potential for action against the protocols themselves. Mark Grimes pointed out many protocol vulnerabilities in his "SCADA Exposed" [2] presentation. Briefly, some of those protocol issues are:

- Modbus+ protocol
  - Report Slave ID—information disclosure
  - Force Single and Multiple Coils—actuator manipulation
  - Preset Single and Multiple Registers—information forging
  - Diagnostic functions for restarting communications and forcing listen-only mode
  - Get and Clear stats
- DNP3 protocol
  - Cold restart
  - Configuration rewrites via Save Configuration
  - File manipulation via open, close, and delete file
  - Denial of Service attacks via NEED_TIME bit
- GOOSE protocol
  - Name discovery
  - Retraining to modify name allocations
  - Interception and data modification
  - Denial-of-service attacks

As you can see from this list, there are quite a number of known issues, even at this point, in the protocols. Furthermore, most of the devices these protocols are running on are subject to standard attack vectors such as ARP spoofing and packet flooding. In additon, the networks associated with these devices are rarely hardened, making attacks like this even more feasible.

Defensively Challenged

The networks are not only subject to attack and relatively unsecured, but these systems are also growing in size and increasing in complexity. Control networks are real-time oriented and even slight timing issues can cause huge failures. Architecturally, this provides its own challenges and complexities, but it also exposes the systems to more potential constraint attacks based on the timeline properties associated with many of the control systems. Furthermore, the fact that these control systems often control critical infrastructure (such as the North American power grid) presents a particularly enticing target to hackers or other malicious users, especially when there is a monetary or political agenda behind the attack.

Owing to system complexity, there exists a likelihood of an unintentional lack of separation between standard corporate networks and the critical control networks. A seemingly common culprit in that arena is that of a lab within the corporation that needs access to both networks for research or development purposes. Muddling the waters even more is IT/Vendor support for these devices. Often this requires full remote access to the control network. If this access is misused, it represents another attack vector. These remote access points of entry may be Internet connections or simply dial-up modems. Either way, they are not tremendously difficult to gain access to.

Control systems are often controlling critical processes and therefore cannot be subject to failures or brought down for maintenance easily. They typically have a very long lifespan in the field and are not updated regularly. This can be due to lack of availability or access or to financial constraints or simply the capabilities of the hardware itself. These systems are tightly coupled as well, so any patching or updates would have to be thoroughly tested before being deployed. One way this is done is with a research lab that runs a shadow system that receives and processes the data but takes no control actions. Another way is to use backup systems and roll over. Both of these methods are potentially dangerous and can require months of planning and testing to implement.

Lastly, just like any other application out there, these control systems are partially software. As such, they are subject to the same sort of attacks as any other software. Some common attack vectors are data injection, buffer overflows, and format string issues.

In the power industry, there continues to be a push toward a smarter power grid. As a result, the technological issues faced in this space increase. A smart grid is best described as an augmentation to the current power grid with more modern computing equipment. This modern equipment is designed to provide facilities such as real-time pricing, adaptive load shedding, and bidirectional communications down to the meter. The more modern these systems are, the more critical securing them becomes.

Exploitattstaærkd Vectors

Drilling down through the layers, we can expose a number of locations that offer potential exploits and attack vectors for adversaries in the control system space. With the HMI systems being involved in critical decision-making, there are a number of problems that could be caused by adversaries. Malicious data could be injected into the system in order to cause misinformation, or data could simply be withheld to cause denial of service. As a result, the operator could get confused about what the readings are and therefore fail to take action in time or take the incorrect one. As you can see, the operators play a very key role in the system. Do keep in mind that some systems are designed to operate at least in part with automated responses. In such cases, these automated responses can be fooled into taking the wrong actions, just as human operators can, and can potentially lead to cascading failure.

Attacks focusing on inserting faulty data can originate at the sensors on the communication networks that carry the data. Sensors that provide information about the control systems are subject to data falsification. As you can imagine, if the system cannot get reliable data from the sensors, then the actions taken on that data cannot be trusted. Further, the communication network could potentially be compromised as well, and therefore it would be subject to blocking or modification of information transiting that network. This could be anything from a serial pass-thru interception to a promiscuous Ethernet device or a radio link interception or interference.

The largest issues related to attacks in modern systems probably lie in the administration systems, as they are the core of the control system and provide a fairly centralized point of control and data aggregation. These systems are subject to directed exploits in the control system software, exploits against the operating system, trojans, malware, spyware, and pretty much any attack other computers are subject to. These administration systems are becoming increasingly connected and in some installations may be accessible from the Internet either via busi-

ness networks or through misconfigurations. Obviously, the more accessible the systems are, the more prone they are to attack.

It is also not uncommon for a control system to be taken down by a standard PC infection from the corporate network or from unauthorized browsing from the control network. These types of incidents have become more visible; as a result, policy and standards have addressed this concern. Compliance is obviously still up to the location, but fines are a good motivator.

Steps Toward Solutions

Awareness of these problems has greatly increased and our nation has progressed from warnings to a roadmap on how to secure the space. In the energy sector, articles such as "Critical Foundations: Protecting America's Infrastructures" (1997) [3], "Making the Nation Safer" (2002) [4], and "Roadmap to Secure Control Systems in the Energy Sector" (2006) [5] have begun to pave the way to a more secure national infrastructure. The roadmap was an industry-driven synthesis of public and private sector input that set forth milestones to address the energy sector's most current critical control system challenges and research needs.

A number of standards have been created to help with securing these systems through compliance. Some of the standards involved are North American Electric Reliability Corporation (NERC) CIPs, ISA SP99, National Institute of Standards and Technology (NIST) SP800-53, NIST SP800-82, NIST Process Control Security Requirements Forum (PCSRF) protection profiles, ODVA CIP, and American Gas Association (AGA) 12. Each of these standards serves a different purpose, but they combine to provide a more encompassing guideline to help secure these control systems. Some of these standards have recently been ratified and are now being enforced. Being out of compliance with some of the NERC CIPs standards can result in large daily fines. This is serious business.

With support from the U.S. Department of Energy, an industry-led initiative called the North American SynchroPhaser Initiative (NASPI) [6] is investigating placing higher-grade measurement devices called Phasor Measurement Units (PMUs) into the current power infrastructure. On the surface this may seem like a simple swap-out, but it is much more complicated than that, as these new devices have requirements far beyond what most of the current infrastructure can support. These requirements include the need for high-speed networks, device management, and advanced security.

An independent, nonprofit organization, the Electric Power Research Institute (EPRI) [7], has recently focused on promoting smart grid technology and working toward providing security on that architecture. This works hand-in-hand with other industry efforts in the Advanced Metering Infrastructure (AMI) space. As the demands of consumers increase and the visibility required for programs such as real-time pricing becomes more expansive, the power grid must become even more advanced. These Smart Grid initiatives will again pose security challenges, both new and old. As such, task forces such as AMI-SEC [8] have been formed to help guide these, as well.

National laboratories are also focusing on testing and research in the SCADA space. Some of these centers include the Idaho National Laboratory (INL) [9], the Pacific Northwest National Laboratory (PNL) [10], and Sandia's Center for SCADA Security [11]. More recently, INL and Sandia have combined their efforts to form the National SCADA testbed. These centers have done security assessments of SCADA equipment and facilities based on standardized recommendations and their own research and have been instrumental in helping to secure our current national infrastructure.

To further these efforts, academic research centers are focusing on forward-looking security solutions for these control networks. Some of these include the Trustworthy Cyber Infrastructure for Power Grid (TCIP) [12] center led by Illinois and supported by the National Science Foundation (NSF), Department of Energy, and Department of Homeland Security; the TRUST Science and Technology Center [13] led by Berkeley and supported by NSF; and Europe's CRUTIAL program [14]. The research done by these institutes looks more toward providing long-term solutions and applying both industry and academic work to the problem. As such, these institutes remain very

connected and interact regularly with industry to make sure the research is gauged to provide a positive impact on the national infrastructure.

There have been other tools to address the security of SCADA systems, including commercial tools such as Achilles (from Wurldtech) [15] and Tofino (from Byres Security) [16]. Several open source projects have been created for various efforts in the SCADA space as well, including items ranging from snort signatures to protocol-specific firewalls and encryption overlays. Some work has been released in the attack vector space as well, such as SCADA protocol scanners and information-gathering tools.

To help advance the collective knowledge and tools developed by industry, government, and academia, several open forums have been set up. These forums provide opportunities to learn about and discuss important problems for securing control systems via workshops, meetings, and published articles. The Process Control Systems Forum (PCSF) [17] focuses on accelerating the design, development, and deployment of more secure control and legacy systems. The NIST Process Control Security Requirements Forum (PCSRF) [18] focuses on supporting the development and dissemination of standards for process control and SCADA security. The interactive DOE roadmap focuses on the goals and priorities for improving the security of control systems in the electric, oil, and natural gas sectors over the next decade. The DHS National Cyber Security Division's Control System Security Program (CSSP) focuses on reducing control system risks within and across all critical infrastructure sectors by coordinating efforts among federal, state, local, and tribal governments, as well as control systems owners, operators, and vendors.

What might an implementation look like after developed and standardized security tools are applied? Figure 2 is the same reference implementation for us with everything applied from the "Control Systems Cyber Security: Defense in Depth Strategies."

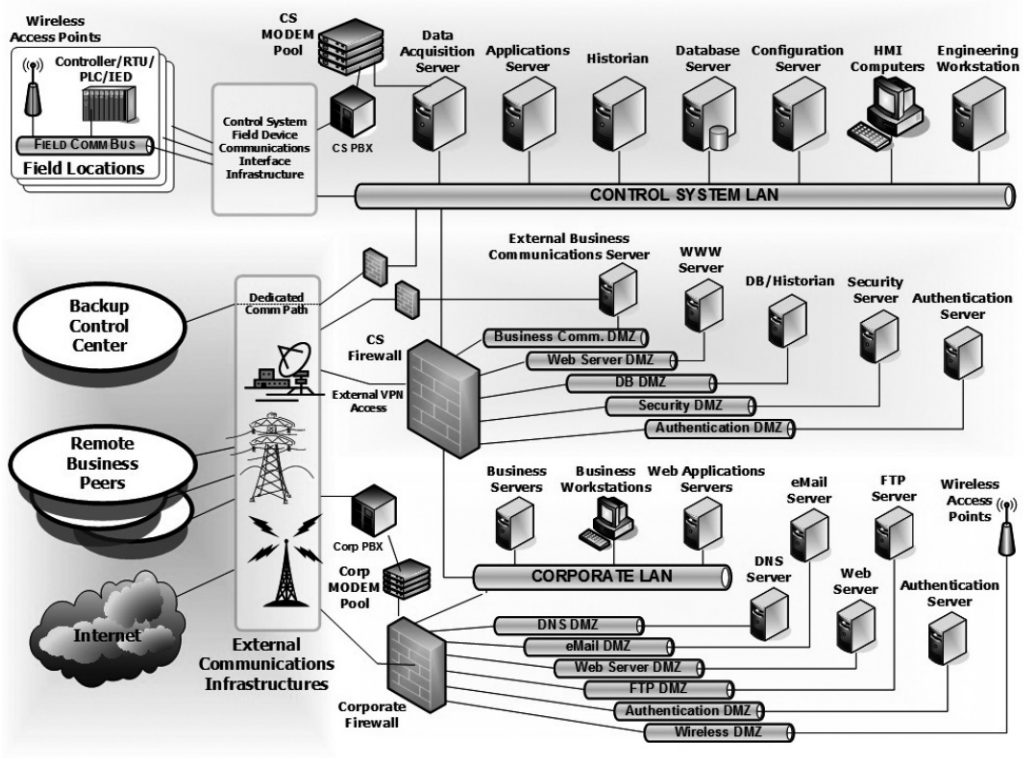

Figure 2: Reference Implementation Diagram Showing the Suggested Control System Cyber Security: Defense in Depth Strategies

Conclusion

Figure 2 makes the situation look a lot better! Should you be scared? Well, probably a bit scared, at least. But the situation is getting better every day as more organizations move toward implementing designs similar to this reference implementation shown in Figure 2. The research, standards, panels, and tools that have been developed or are being developed are making great strides in providing a more secure infrastructure and control. A lot of work remains to be done, however, and many areas have yet to be fully explored.

Join in the efforts: your help is needed. After all, it is pretty cool to say you're working to help save the world (or at least the infrastructure that powers it), isn't it?

References

[1] "Control Systems Cyber Security: Defense in Depth Strategies," May 2006, INL/EXT-06-11478.

[2] M. Grimes, "SCADA Exposed," *ToorCon 7*, 2005.

[3] http://www.ihs.gov/misc/links_gateway/download.cfm?doc_id=327&app_dir_id=4&doc_file=PCCIP_Report.pdf.

[4] http://www.nap.edu/catalog.php?record_id=10415.

[5] http://energetics.com/csroadmap.

[6] http://www.naspi.org/.

[7] http://intelligrid.epri.com/.

[8] http://osgug.ucaiug.org/utilisec/amisec/.

[9] http://www.inl.gov/scada/.

[10] http://www.pnl.gov/.

[11] http://www.sandia.gov/scada/.

[12] http://tcip.iti.uiuc.edu/.

[13] http://www.truststc.org/.

[14] http://crutial.cesiricerca.it/.

[15] http://www.wurldtech.com/healthcheck/.

[16] http://www.byressecurity.com/pages/products/tofino/.

[17] https://www.pcsforum.org/.

[18] http://www.isd.mel.nist.gov/projects/processcontrol/.