BACHELORS: INFRASTRUCTURE IN NATIONAL SECURITY INTELLIGENCE

Infrastructure in National Security and Intelligence

Unit 3

Industrial Network Security: ICS & SCADA

ICS and SCADA

ICS and SCADA

Supervisory Control and Data Acquisition (SCADA) is a subset of Industrial Control Systems (ICS).

SCADA generally refers to control systems that span a large geographic area, such as a gas pipeline, power transmission system or water distribution system.

SCADA is often better known by the press, government officials and the public, but ICS is probably the technically correct term to use if you are referring to industrial automation of all types

Understanding Industrial Networks

Before attempting to secure an industrial network, it is important to understand what an industrial network really is.

An industrial network is most typically made up of several distinct areas, which are simplified here as a business network or enterprise, business operations, a supervisory network, and process and control networks SCADA, or Supervisory Control and Data Acquisition, is just one specific piece of an industrial network, separate from the control systems themselves, which should be referred to as Industrial Control Systems (ICS), Distributed Control Systems (DCS), or Process Control Systems (PCS). Each area has its own physical and logical security considerations, and each has its own policies and concerns.

Understanding Industrial Networks

Critical Infrastructure" is referring to critical network infrastructure, including any network used in the direct operation of any system upon which one of the defined "critical infrastructures" depends.

SCADA Security Defined

SCADA security is the practice of protecting supervisory control and data acquisition (SCADA) networks, a common framework of control systems used in industrial operations. These networks are responsible for providing automated control and remote human management of essential commodities and services such as water, natural gas, electricity and transportation to millions of people. They can also be used to improve the efficiencies and quality in other less essential (but some would say very important!) real-world processes such as snowmaking for ski resorts and beer brewing. SCADA is one of the most common types of industrial control systems (ICS).

These networks, just like any other network, are under threat from cyber-attacks that could bring down any part of the nation's critical infrastructure quickly and with dire consequences if the right security is not in place. Capital expenditure is another key concern; SCADA systems can cost an organization from tens of thousands to millions of dollars. For these reasons, it is essential that organizations implement robust SCADA security measures to protect their infrastructure and the millions of people that would be affected by disruption caused by an external attack or internal error.

SCADA Network Security Threats

From local companies to governments, every business or organization that works with SCADA systems is vulnerable to SCADA security threats. These threats can have wide-reaching effects on both the economy and the community. Specific threats to SCADA networks include the following:

Hackers

- Individuals or groups with malicious intent could bring a SCADA network to its knees. By gaining access to key SCADA components, hackers could unleash chaos on an organization that can range from a disruption in services to cyber warfare.

Malware

- Malware, including viruses, spyware and ransomware can pose a risk to SCADA systems. While malware may not be able to specifically target the network itself, it can still pose a threat to the key infrastructure that helps to manage the SCADA network. This includes mobile SCADA applications that are used to monitor and manage SCADA systems.

Terrorists

- Where hackers are usually motivated by sordid gain, terrorists are driven by the desire to cause as much mayhem and damage as possible.

Employees

- Insider threats can be just as damaging as external threats. From human error to a disgruntled employee or contractor, it is essential that SCADA security addresses these risks.

Critical Infrastructure Protection Defined

Critical Infrastructure Protection (CIP) is the need to protect a region's vital infrastructures such as food and agriculture or transportation. Every government in every nation has a responsibility to protect these essential critical infrastructure against natural disasters, terrorist activities and now cyber threats. From energy organizations to transportation companies, it is paramount that security in all critical infrastructure sectors is of the highest standard and that disaster preparedness, response and recovery are top priorities. Common components of critical infrastructure needing security considerations include Industrial Control Systems (ICS), Operation Technology (OT), and SCADA Systems.

The world is changing, and digital and physical systems are converging. Systems that once stood alone managing critical infrastructure operations are connecting to the internet and sharing sensitive data. This new world structure brings with it new security problems. Critical infrastructure organizations must use a robust framework that can anticipate and mitigate disaster across their entire critical infrastructure environment. Critical Infrastructure Protection (CIP) helps organizations to prepare for and respond to serious incidents involving critical infrastructure environments and to protect against an ever-growing number of threats

Critical Infrastructure Security Recommendations

Although there are many recommendations in securing critical infrastructure, the four areas identified here are the industry recommended "best practice" standards:

1. Identifying what systems need to be protected
2. Separating the systems logically into functional groups
3. Implementing a defense-in-depth strategy around each system
4. Controlling access into and between each group

Identifying what systems need to be protected

The first step in securing any system is determining what needs to be protected. Identifying the assets that need to be secured, as well as identifying their individual importance to the reliable operation of the overall process control system, is necessary for a few primary reasons: it tells us what should be monitored, and how closely; it tells us how to logically segment the network into high-level security enclaves; and it, therefore, indicates where our point security devices (such as firewalls and intrusion detection and prevention systems) should be placed.

Asset management is important in securing any infrastructure. This process will help to separate devices into two categories:

Critical Assets
Noncritical Assets

Network Segmentation/Isolation of Systems

The separation of assets into functional groups allows specific services to be tightly locked down and controlled, and is one of the easiest methods of reducing the attack surface that is exposed to attackers. Simply by disallowing all unnecessary ports and services, we also eliminate all of the vulnerabilities—known or unknown—that could potentially allow an attacker to exploit those services.

Don't forget to control communications in both directions through a firewall. Not all threats originate from outside. Open, outbound traffic policies can facilitate an insider attack, enable the internal spread of malware, enable outbound command and control capabilities, or allow for data leakage or information theft.

Defense in Depth

Defense in depth (also known as deep or elastic defense) is a military strategy; it seeks to delay rather than prevent the advance of an attacker, buying time and causing additional casualties by yielding space. Rather than defeating an attacker with a single, strong defensive line, defense in depth relies on the tendency of an attack to lose momentum over a period of time or as it covers a larger area.

Defense in Depth

Application:

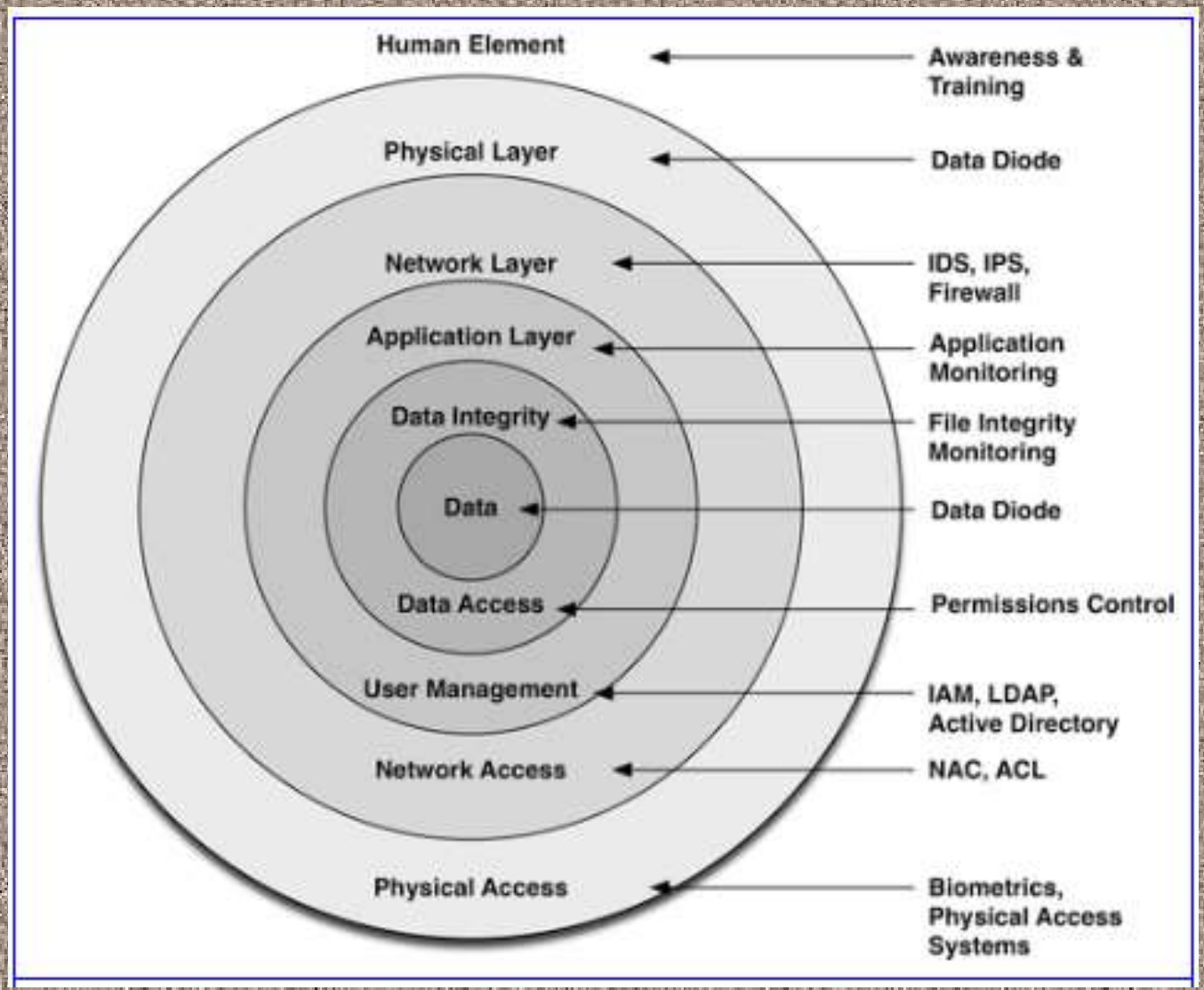
Multiple layers of defense. Do not rely completely on a single point of security, no matter how good it is. Differentiated layers of defense. Make sure that each of the security layers is slightly different. This ensures that just because an attacker finds a way past the first layer, they don't have the magic key for getting past all the subsequent defenses. Context and threat-specific layers of defense. Each of the defenses should be designed to be context- and threat- specific

Defense in Depth

Although the definitions of "defense in depth" vary somewhat, the philosophy of a layered or tiered defensive strategy is considered a best practice. The following diagram and tables illustrate a common defense-in-depth model, mapping logical defensive levels to common security tools and techniques. You can choose either method that leads to a defense-in-depth path.

Defense in Depth

DIAGRAM



Defense in Depth

T

	Defense in Depth	Corresponding Protective Measure			Defense in Depth	Corresponding Protective Measure
1	Data	Data Diode		1	Data	Data Diode
2	Data Access	Permission Control		2	Data Ingrity	File Integrity Monitoring
3	User Management	IAM, LDAP, Active Directory		3	Application Layer	Application Monitoring
4	Network Access	NAC, ACL		4	Network Layer	IDS, IPS, Firewall
5	Physical Access	Biometrics, Physical Access systems		5	Physical Layer	Data Diode
6	Human Element	Awareness training		6	Human Element	Awareness Training

Access Control

Access control is one of the most difficult yet important aspects of cyber security. By locking down services to specific users or groups of users, it becomes more difficult for an attacker to identify and exploit systems. The further we can lock down access, the more difficult an attack becomes. Although many proven technologies exist to enforce access control—from network access control (NAC), authentication services, and others—the successful implementation of access control is difficult because of the complexity of managing users and their roles and mapping that to the specific devices and services that relate specifically to an employee's operational responsibilities.

Challenges in Defending Critical Infrastructure

Protection of critical infrastructure against cyber-terrorism, faces complex challenges among international states and organizations:

- 1. **International fragmentation:** differences in approach to cybersecurity, data jurisdiction and legal enforcement (as well as culture, language and politics) across jurisdictional and territorial boundaries can make it difficult to effectively prevent, investigate and prosecute attacks committed through the Internet;
- 2. **International norm-setting:** international political differences and country-specific agendas can make it difficult to develop consensus norms regarding cybersecurity;
- 3. **Roles with respect to the private sector:** the varying and sometimes confrontational roles that the public sector must play can create tensions and trust deficits with the private sector

Challenges in Defending Critical Infrastructure

- 4. **Misalignment of incentives for cybersecurity best practices:** Companies often fail to take basic steps to protect their systems and their users because they are placed in the difficult position of balancing the market pressures of rapid innovation against sustained investments in cybersecurity, which may raise costs or delay delivery of products to market
- 5. **Ecosystem complexities:** Today's software and hardware environments are increasingly complex ecosystems populated by a network of interacting devices, networks, people and organizations. This means that cybersecurity solutions often require the voluntary engagement, cooperation and investment of many independent entities, even though the incentives and mechanisms for taking such actions are distributed inconsistently across the ecosystem

SCADA & security of critical infrastructures

Industrial control systems (ICS) and Supervisory Control And Data Acquisition (SCADA) systems are critical components for the operation of industrial facilities and critical infrastructure. Successful cyberattacks could paralyze internal processes, cause financial losses and potentially lead to the loss of human lives.

Many organizations in critical infrastructure have deployed SCADA/ICS to automate the control of processes and data collection. These systems have become high-value targets for attackers looking to disrupt business operations

SCADA & security of critical infrastructures

Unfortunately, many ICS are not designed to be resilient to cyberattacks and threat actors are targeting these systems with more intensity.

Most of the attacks against the industrial networks are not complex. Threat actors could use different attack vectors by taking advantage of existing configuration flaws in the industrial devices and network segmentation, as well as OS vulnerabilities.

The majority of security experts involved in the testing of corporate information systems revealed that they have insufficient perimeter protection against external attacks and industrial networks are not properly isolated from corporate systems.

The Stuxnet Attack Legacy

Since the Stuxnet attack, many other incidents involved ICS/SCADA systems and security experts discovered several threats specifically designed to compromise these families of devices, including Duqu/Flame/Gauss (2011), Shamoon (2012), Havex (2013), Dragonfly (2014), Black Energy (2015) and Triton (2017).

The above threats targeted systems used in nuclear plants, electric grids, dams, gas pipelines, water facilities and industrial environments. These events confirm that ICS/SCADA components are prime targets for both crooks and nation-state actors.

According to a Forrester study, 56% of organizations using SCADA/ICS reported a breach in the second half of 2018 through the first half of 2019. Only 11% indicate they have never been breached.

In many cases, attackers exploit vulnerabilities affecting industrial control systems (ICS). For this reason, it is interesting to analyze which issues were disclosed in 2019 and potentially exploitable in attacks in the wild.

116 Unique Types Of Flaws

ICS security firm Dragos analyzed 438 ICS vulnerabilities that were reported in 212 security advisories in 2019, and revealed that 26% of advisories are related to zero-day flaws. This circumstance is worrisome because attackers exploiting zero-day vulnerabilities in their attacks could have had a significant likelihood of success.

The experts classified the issue in 116 unique types of flaws, most of the flaws discovered in 2019 were improper input validation, stack-based buffer overflow, cross-site scripting (XSS), the use of hard-coded credentials and uncontrolled resource consumption (i.e., DoS) issues.

Vulnerabilities Deep Within

The experts revealed that 77% of the assessed vulnerabilities were residing deep within a control system network; the flaws only affect products that belong on engineering workstations, human-machine interface (HMI) systems, operator panels, industrial network equipment and field devices themselves. The researchers pointed out that their exploitation requires some existing access to a control systems network.

According to the experts, only 9% of advisories were related to flaws in products associated with border systems (e.g., data historians, OPC servers, cross-domain web applications and VPN services). Their exploitation could potentially allow attackers to move from the IT to the OT networks.

Most of the advisories (roughly 75%) are related to vulnerabilities that could be exploited from the network, while the remaining flaws could be only exploited by attackers with local or physical access to the targeted machine.

The experts also analyzed the potential operational impact on industrial control processes for each issue focusing on the loss of view and the loss of control.

50% of advisories are related to vulnerabilities that could cause both a loss of view and a loss of control, while 5% of advisories could only cause a loss of view (but no loss of control) via exploitation and 2% could result in a loss of control.

The risk of attacks exploiting the flaws related to the advisories issued in 2019 is very high: 26% of them had no patch available when the initial advisory was disclosed and 76% of the advisories which had no patch did not offer mitigation advice.

SCADA attack surface

Before introducing the most common ICS/SCADA threats, let us understand the architectures of SCADA systems and how the internal components interact with each other.

The main components of a SCADA system are:

- A human–machine interface (HMI) is the component responsible for data presentation to a human operator. It consists of a console that allows the operator to monitor and control the process
- Remote terminal units (RTUs) are microprocessor-controlled electronic devices that interface the sensors to SCADA by transmitting telemetry data
- The supervisory system is responsible for data acquisition and for control activities on the process
- Programmable logic controllers (PLCs) are the final actuators used as field devices
- Communication infrastructure connecting the supervisory system to the remote terminal units
- Various process and analytical instrumentation

In a real attack scenario, hackers could target one of the above components with different techniques and means. Malware, for example, could be used to infect the supervisory system or the HMI by exploiting known vulnerabilities in the underlying OS. Malware might infect the system through a USB stick or a network interface.

Most common ICS/SCADA security issues and threats

Legacy Software

One of the biggest problems for ICS/SCADA systems is that they often run on legacy software that lacks sufficient security. Most of this type of software doesn't implement security fundamentals such as user/system authentication and data integrity checking features, allowing attackers to carry out a broad range of attacks against the ICS components.

Networking Issues

It is very common to find internet-facing ICS/SCADA systems that are not properly protected and hosted on a misconfigured network. In many cases, firewalls employed as a defense measure for the industrial networks fail to detect/block malicious activity launched by external attackers, allowing them to access the OT systems.

In some cases, SCADA systems are connected to unaudited dial-up lines, or operators of the industrial environment have wrongly configured remote-access servers that could give attackers a path to access to the OT network as well as the corporate LAN.

Default Configuration

Threat actors always attempt to exploit devices that still use factory settings, which are well known to the hackers. Factory settings, including default passwords, allow the attackers to compromise a device and easily enumerate and compromise other OT systems in the same network.

Most common ICS/SCADA security issues and threats

Unencrypted Communications

Almost any legacy ICS and industrial protocol does not use encryption to protect communication, allowing threat actors to eavesdrop on the traffic in order to capture authentication credentials and carry out man-in-the-middle attacks. Attackers could leverage unencrypted communication protocols to target ICS, HMI and workstations delivering malicious code — for example, by pushing rogue updates that are able to compromise these components.

DDoS Attacks

Threat actors could attempt to sabotage OT systems by launching DDoS attacks on vulnerable unpatched systems that are exposed online and improperly protected. It could be very easy for hackers to locate these systems by using specific search engines like Shodan. The popular search engine allows attackers to retrieve all the information that could be used to find a potential target exposed online.

The disconcerting news is that most OT systems exposed online lack proper authentication mechanisms and, in many cases, are not updated.

Malware

Threat actors continually specifically design malware that compromises ICS systems and interferes with their operations. Additionally, ICS systems are often exposed to other threats that are not specifically designed to target this family of devices.

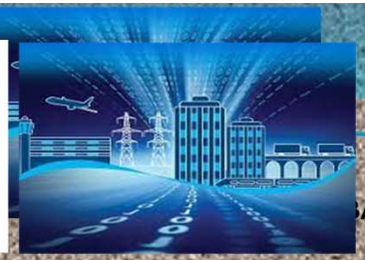
Most common ICS/SCADA security issues and threats

Web Application Attacks

Threat actors are increasingly targeting OT systems that are exposed online via their web interface. Hackers attempt to carry out web applications attacks to exploit vulnerabilities (e.g., SQL injection, cross-site scripting in the interface of OT components such as human-management interfaces and programmable logic computers).

Command Injection and Parameters Manipulation

ICS systems may be targeted with command injection attacks that allow attackers to execute arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are caused by the lack of validation of user supplied data.



BACHELORS: INFRASTRUCTURE IN NATIONAL SECURITY INTELLIGENCE

Defending SCADA Systems

We have described the SCADA attack surface and the most common issues and threats related to industrial control devices. It is time to explore the ways to defend them from attacks.

Organizations using ICS/SCADA systems in their infrastructure have to keep their systems up to date by applying security patches and updates released by the vendors. Operators of critical infrastructure have to deploy security measures that can defend against cyberattacks, some of them are based on the National Institute of Standards and Technology's NIST's guide to ICS security.

Defending SCADA Systems

Below is a short list of recommendations to secure ICS/SCADA systems:

- Use virtual patching to help manage updates and patches. Patch management is critical in industrial systems where the deployment of an update could cause downtime. Virtual patching can help manage vulnerabilities and prevent cyberattacks when it is not possible to immediately apply the patches
- Implement network segmentation to prevent the spread of malware and lateral movements of the attackers once they have compromised the target network. By segmenting the network, it is possible to drastically minimize the exposure of sensitive information
- Separate the ICS network from the corporate network, using adequate security measures like firewalls in order to prevent the lateral movement of attacks from one to another
- Prevent the use of untrusted removable devices that could be used as attack vectors by threat actors
- Manage authorization and user accounts. Experts recommend monitoring and assessing the authorizations and accesses to SCADA systems. Monitor the creation of administrator accounts by third-party vendors
- Protect engineering workstations connected to SCADA for device programming and control adjustments with endpoint protection
- Employ strict policies to regulate how devices can connect to SCADA networks. Deploy secure remote access methods such as Virtual Private Networks (VPNs) for remote access
- Restrict the roles of transitory SCADA nodes to a single purpose. Having a single purpose for transitory nodes lowers the chances of unknowingly exposing these nodes or having them accessed by unauthorized users.
- Using a web application firewall (WAF) to scan and patch vulnerable web applications
- Remove, disable or rename any default system accounts