SANS
ICS Attack Surfaces

Dr. Eric Cole
Why Attack Control Systems?

• There are a number of reasons why people attack control systems:
  – Financial gain (or ruin)
  – Corporate espionage
  – Terrorist activities
  – Nation-state espionage and cyber warfare
  – Hacktivism
  – For educational and peer recognition
  – Misguided ethical hacking
How Can We Model Attacks?

• To successfully defend our control systems, we must understand how attackers can attack them
• Attack models help us understand our system's attack surface
  – **Attack Model**: a series of diagrams and/or descriptions of how attackers can attack a system
  – **Attack Surface**: a list of system inputs that an attacker can use to attempt to compromise a system
• The more we can decrease our attack surface, the more resilient our system can become to compromise
High Level Attack Surface

- Attacks on Internet Facing Servers
- Client-Side Attack on Workstations
- Malicious Insiders
- Compromised Servers
- Compromised Field Devices

Networks:
- Internet
- Business Network
- Control Server Network
- Field Device Network

Methods:
- Compromised Remote Access
- Malware on USB Devices
- Physical or Wireless Access
Control Systems Are a Target

www.sans.org/ics

Network Access
- Internet accessible systems are being mapped by EMP or Shodan, or are easily locatable through search engine queries
- Malware can spread vertically through the network by trusted system to system connections or VPN
- It's easy to maneuver undetected throughout a control environment
- There is potential to leverage non-rutable trusted communication paths

Interconnects
- ICS systems can be attacked by exploiting applications that communicate through network segmentation
- Connections to other organizations, plants or systems
- Many ICS environments are susceptible to network-based cyberattacks

Dial-Up
- ICS assets can be remotely accessible through traditional dial-up modems that have little access control protections
- Numerous ICS assets at a location can be accessed through a single dial-up access point with a multiplex device that enables connection to many ICS assets
- Old attack vectors can still be successful in ICS environments

System Management
- Attackers can take advantage of long delays in patching and operating system upgrades
- Attackers can take advantage of systems with no anti-virus, or out of date signatures
- Attackers will leverage default usernames and passwords or weak authentication mechanisms
- Attackers will be difficult to detect due to minimal asset security logging capability
- Attackers will leverage file access techniques to move data in and out of the ICS environment through physical removable media or trusted communication paths attuned for system maintenance

Supply Chain
- Third party vendors, contractors or integrators can be attacked in an attempt to ultimately attack an ICS asset owner or multiple asset owners
- ICS hardware and software can be directly breached or impacted prior to arriving in the production ICS environment

You may not realize it, but your organization's Industrial Control System (ICS) environments are a target for cyber attackers. The ICS automation, process control, access control devices, system accounts and asset information all have tremendous value to attackers. This poster demonstrates the many different ways attackers can gain access to an ICS environment and demonstrates the need for active security efforts and ICS engineer training that will enable informed engineering decisions and reinforce secure behaviors when interacting with an Industrial Control System.

In many cases these are not one off attacks, but are planned for with reconnaissance, multiple attacks and adjustments. These are campaigns that happen over the course of months, and they require system owners and operators to be vigilant and recognize when something is not right.

Governance
- Attackers can leverage the lack of corporate security policies, protected process, asset inventory and standardization that exist in many ICS environments
- Attackers can have greater impacts on ICS environments, as ICS assets are often not considered in the protection phase of security incident response planning and containment approaches
- ICS risk and hazard assessment are not always evaluated with the loss of cyber integrity which can lead to a loss of availability, impacts due to interdependencies and misuse of critical components or functions
- In some sectors ICS assets are often architected or assessed from different perspectives and not always assessed from a security perspective

Social Engineering
- Request for Proposals often contain a wealth of information regarding an ICS environment
- Vendors frequently post information about a project they are working on for an ICS customer
- Employee social media sites often contain technology architecture information and, possibly, images of ICS work environments
- Employee professional bias can provide a helpful map of your ICS
- Publicly available information regarding an ICS asset owned vendor relationships, conference attendance, community participation and domain registrations can all be leveraged against the organization

Physical Security
- Attackers can leverage the physical locations of numerous ICS assets that could be located in remote geographies or are unmonitored, even when little to no physical access controls exist
- ICS assets can be physically stolen or obtained
- ICS assets can be physically stolen or obtained secondhand with access to sensitive information that could be used in planning an attack
- Physical changes or alterations to ICS devices are often difficult to detect

Cyber Actors
- Nation States
- Insiders and other trusted parties (such as contractors / vendors / integrators)
- Criminal Hackers
- Politically motivated attackers (hacktivists)
- Script Kiddies

ICS Security goal. Ensure the safe, reliable and secure operation of ICS environments from procurement to retirement

Abnormal activity or unexplained errors deserve a closer security look
What is an Attack Tree?

• An attack tree is a logical way to string multiple attacks together to accomplish some greater attacker goal
• Attack trees are always subjective and usually focused on a specific risk
• Detail can vary depending on need
• Efforts to exhaustively model all attacks and all risks often fail because attacks and risks are often innumerable
• Sometimes control systems are exposed to the public Internet
  – Often by ignorance
  – Sometimes by mistake
  – Occasionally by valid business reason

• These systems can be found through a number of different methods
  – Port scanning
  – Google searches (aka Google Hacking)
  – Shodan searches
ICS Technology Trends

- Decentralized monitoring and control tasks with greater local accessibility
- Continued replacement/consolidation of cables/wires and new installation use of wireless networking on plant floor
- Proliferation of connections from the ICS environment
- Supplier provided security quality (progressive companies) and selling features (low adoption)
- Cloud services for optimization and analytics
- More embedded devices and new suppliers
- Discovery of Internet facing architectures
Rise of Embedded Systems
Attack Surfaces
Human Machine Interfaces (HMIs)

- Can be traditional indicator and switch based
- Can be serial interface based
- Can be network based
  - Most modern HMIs are now web interfaces
  - Some leverage web services to a user front-end
  - Some older ones may use RPC calls
- If we can gain access of the HMI, we can often control the system
Social Engineering

• The art of manipulating humans to do what you want with a combination of logic and emotion
  – Convincing the help desk you need your password reset (at least the person you are pretending to be)
  – Getting a field technician or engineer to insert a USB drive into their field laptop (to infect their laptop with a Trojan)
  – Gaining physical access to guard protected locations
  – Convincing a group of managers or engineers to open an e-mail attachment or click on a web link

• SE is often used to enhance other technical attacks
Phishing and Spear Phishing

• Phishing is the process of sending an attack to a large number of individuals
  – Attacks are more general and sent to a larger variety of targets
  – The more it is sent to, the more will fall victim
• Spear Phishing is similar, but instead it targets a small number of people
  – Attacks are very specific and convincing, often modified for each target
  – More effort is spent to increase the odds that the target will fall victim
Non-directed Worm

Conficker worm was found on multiple energy ICS. The Internet spreading worm found its way in to generation plants.

Details:
- North America
- CY 2008
- Multiple infections
- Difficult to remove

Source: Electricity sector incident reporting

Conficker Infections
Stuxnet

• Discovered in June 2010
• Targeted Iran's nuclear facilities
• Attacked Siemens Step-7 software to reprogram PLCs
• Best write-up on Stuxnet:
  – http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf
Default and Weak Passwords

- Many HMIs are protected by a password
- Default passwords are usually found in the vendor documentation
- If HMI passwords are shared among many users, it is often based on company terms
- Weakly chosen passwords can be easy to guess with fuzzing techniques, also known as brute force or dictionary attacks
Web-based Attacks

- Many modern HMIs are now web-based
- Common web vulnerabilities affect them and may even affect non-web based applications:
  - Authentication Bypass
  - Weak Session Management
  - SQL Injection (SQLi)
  - Cross Site Scripting (XSS)
  - Cross Site Request Forgery (CSRF)
  - Local and Remote File Inclusions (LFI & RFI)
• Authentication bypass can happen in a number of different ways
• Often it is a developer that forgets to require every web page from verifying the user is logged in
• If the attacker knows the right request to send and the application doesn't verify the requester is logged in for that request, that request works without authentication
• Once you give an application a username and a password, the application usually gives you a secure cookie with a session token
• Your browser must send this cookie back to the server for every request so the server knows who you are
• If the attacker can obtain your cookie or guess its contents, they can hijack your session
Default Configurations

- All systems come with default settings to help administrators configure the systems
  - Default admin username and password
  - Default running services
  - Default security settings
- These defaults can easily be found in system documentation from the vendor
- Attackers use this documentation to learn potential weaknesses in specific systems
Many systems use "admin" or "administrator" as the default user with a preset password
  – These are easy to find in system documentation
  – Often easy to find with Google
  – Sometimes already included in security tools

Username is rarely changed

Password is frequently still set to default

This main administrator account often becomes a shared account among admins
Many control systems, especially master servers, support multiple different protocols

- ICS protocols for monitoring and control
- User interfaces for administrative configuration
- Protocols for remote system updates

Default configurations usually have all available services running
• Installation documentation often provide initial examples using unsecure protocols to simplify install instructions
  – Telnet and FTP instead of SSH and SFTP
  – HTTP instead of HTTPS
• This leads ICS operators to lean towards these insecure protocols
Default Security Settings

• When ICS systems have advanced security configurations, these usually must be configured before use
  – Cryptographic key expiration and renewal
  – Enhanced encryption capabilities
  – Administrator roles with access to all assets
  – Device to device authentication

• Sometimes these features can't be used due to vendor incompatibilities

• Sometimes these features aren't enabled because of concerns with control process interference
Traffic Capture and Data Extraction

• An attacker can capture and analyze our control network traffic if:
  – The attacker can gain access to the network transmitting that traffic
  – The control traffic is not encrypted
  or
  – The attacker can gain control of a system that is sending/receiving traffic, encrypted or not

• Encryption only helps with the first
Wireless Attacks

• When ICS communications are transported wirelessly, the following should be assumed
  – Denial of service attacks are much easier and near impossible to defend against
  – Network capture is possible, regardless of RF frequency used or use of hopping technologies
  – Attacker has at least a limited ability to communicate on the wireless network

• Security defenses should be focused primarily on the higher level network protocol
Physical Access and Control

• Remote field devices are often placed in locations with limited physical protections
  – Fences and locks are easily defeated
  – Video cameras, if present, are not often monitored
  – Any alerts raised require hours and sometime days for personnel to respond

• Physical access to field devices often allows manual control of the control signals

• Of greater concern is an attacker’s ability to leverage physical access on one device for remote access on another device, or even access to the master server
Technician Interfaces

• Many field devices provide local interfaces for field technicians to troubleshoot or manually override the control device
• Field technician interfaces may or may not have authentication protections
• If present, many authentication defenses can be defeated or bypassed with physical access
• Simple password protection on interfaces often uses universal passwords on all devices
Next Steps to Securing ICS
The SANS Industrial Control Systems Team is working to develop a curriculum of focused ICS courseware to equip both security professionals and control system engineers with the knowledge and skills they need to safeguard our critical infrastructures. The entry level course in the SANS ICS Curriculum is ICS 410 – ICS Security Essentials.

This course provides students with the essentials for conducting security work in Industrial Control System (ICS) environments. Students will learn the language, the underlying theory and the basic tools for ICS security in industrial settings across a diverse set of industry sectors and applications. This course will introduce students to ICS and provide the necessary information and learning to secure control systems while keeping the operational environment safe, reliable, and resilient.
### Course topic areas:

<table>
<thead>
<tr>
<th>Day one</th>
<th>Day Two</th>
<th>Day Three</th>
<th>Day Four</th>
<th>Day Five</th>
</tr>
</thead>
<tbody>
<tr>
<td>History &amp; overview of ICS</td>
<td>Overview of attacks</td>
<td>The security infrastructure</td>
<td>IP Behavior</td>
<td>Security foundations</td>
</tr>
<tr>
<td>Field components</td>
<td>Attacks on HMIs &amp; applications</td>
<td>Security policies &amp; templates</td>
<td>Industrial communication protocols</td>
<td>Risk assessments and auditing</td>
</tr>
<tr>
<td>Network components</td>
<td>Attacks on workstations &amp; servers</td>
<td>Service packs, patches, and backups</td>
<td>Perimeters</td>
<td>Password management</td>
</tr>
<tr>
<td>Communication paths &amp; telecommunications</td>
<td>Attacks on network communications</td>
<td>Auditing &amp; automation</td>
<td>Wireless</td>
<td>Incident handling</td>
</tr>
<tr>
<td>Industry models &amp; ICS drivers/constraints</td>
<td>Attacks on remote devices &amp; embedded systems</td>
<td>Operating Systems</td>
<td>Cryptography</td>
<td>ICS resources</td>
</tr>
<tr>
<td>Physical security &amp; safety</td>
<td>Security tools</td>
<td>Embedded system security</td>
<td>Standards</td>
<td></td>
</tr>
</tbody>
</table>
Upcoming Events

SANS Asia Pacific ICS Security Summit Dec 2-7 in Singapore
Register: https://www.sans.org/event/asia-pacific-ics-security-summit-training
THANK YOU