



# Control Systems Are a Target



[www.sans.org/ics](http://www.sans.org/ics)

## Network Access

- Internet accessible systems are being mapped by ERIPP 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 is very easy to maneuver undetected throughout a control environment
- There is potential to leverage non-routable 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 Man in the Middle Attacks

## 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 connections 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- Attackers can take advantage of systems with no anti-virus, or out-of-date signatures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
- Attacks 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 utilized 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.



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**

[www.securingthehuman.org](http://www.securingthehuman.org)

## Governance

- Attackers can leverage the lack of corporate security policies, procurement language, 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 preparation 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 a compliance perspective 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
- Engineer professional bios can provide a helpful map of your ICS
- Publicly available information regarding an ICS asset owners' vendor relationships, conference attendance, committee 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
- 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 Hacker
- Politically motivated attackers (hacktivists)
- Script Kiddies