Originally appeared in:
October 2014, pgs 65-66.
Used with permission.
HYDROCARBON PROCESSING

HP Bonus Report | Cyber Security

L. NEITZEL and R. MIXER,
Emerson Process Management, Round Rock, Texas

What to do about ICS cyber security threats?

Stuxnet, Shamoon, Heartbleed, Energetic Bear, and other cyber-security attacks keep coming with no end in sight. No one wants their industrial control system (ICS) to be the next target. So, what are the biggest threats to ICSs (**FIG. 1**) and what can be done about them?

One such ICS threat is allowing access from the Internet. Attacks from the Internet generally follow a common pattern. First, the attacker probes Internet facing access points of the plant's IT system to find a bug that it can exploit to download executable code (malware). Using the downloaded code, this process is repeated, with the attacker hopping from node to node until the desired target, which may be an ICS node, is reached.

Defense strategies. Internet threats can be mitigated through a well maintained defense-in-depth strategy. Three concepts are key to this strategy:

1. The demilitarized zone (DMZ)
2. Separate user domains for the plant IT system and the ICS
3. Up-to-date security patches and anti-malware updates for both the plant IT system and the ICS.

The DMZ is a buffer zone between the plant network and the ICS through which all traffic to the ICS must pass. It should be protected on both sides by firewalls with restrictive rule sets. Maintaining separation between the ICS domain and the plant IT domain, without defining trusts between them, means that plant users must have separate credentials in the ICS to gain access to it. Therefore, if a plant workstation is infected, the malware cannot use the user identification and password under which the infected software is running to gain access to the ICS. Finally, security patches fix bugs that can be exploited, and anti-malware updates protects the ICS from known malware.

Closely related to Internet attacks are remote access attacks in which a remote workstation or laptop that is authorized to connect to the ICS, such as through a virtual private network (VPN), becomes infected.

The strategy for countering this type of threat complements the defense-in-depth strategy for Internet access. Instead of directly connecting to the ICS, the remote computer first establishes a secure connection to the DMZ and then creates a separate connection to the ICS from there.

To establish these connections, the user should supply a one-time or short-lived user identification and password that has been created just for this access. This prevents malware from discovering and reusing these credentials. Similarly, the firewalls that support these connections should restrict access to only authorized workstations at authorized times.

Malware threat. Another avenue of attack is portable media; such as USB sticks, SD cards, DVDs, smart phones, cameras, and anything that has similar storage capabilities. This media can contain malware embedded in files such as pictures, PDF documents, and executables. Even officially marked ICS software DVDs can pose a threat because these markings are easily reproduced.

Generally, attackers try to fool legitimate users into carrying infected portable media past physical security perimeters into the ICS, and then opening a malware file, thus infecting the ICS. Often, the infection is able to connect back to the attacker, effectively bypassing firewall rules designed to prevent an external attacker from initiating communications to the ICS. Once connected, the malware can download additional malware and/or leak sensitive ICS information.

To protect against portable media attacks, portable media ports should be locked at all times. If this is not possible, they should be unlocked only for short periods when their use is authorized, and then only authorized media should be permitted. Users should never be allowed to use their own portable media. When used, portable media should be scanned for malware, and ICS workstation patches should be kept current to fix bugs that undetected malware could exploit. In addition, firewalls

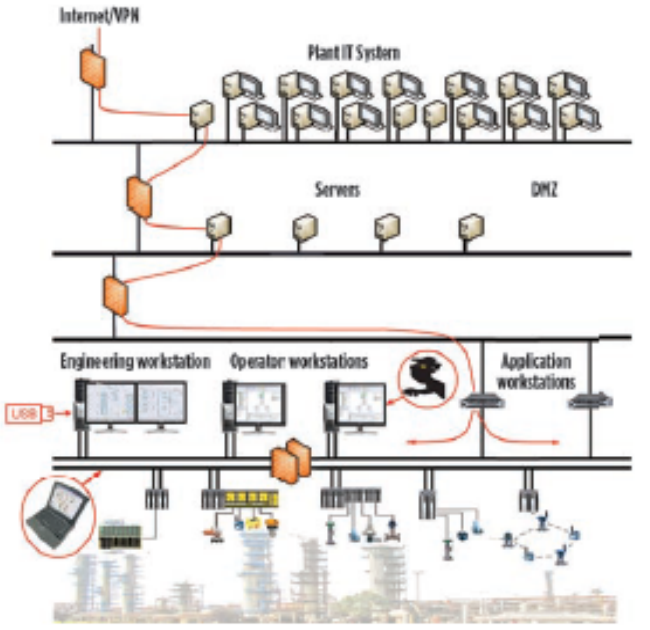

FIG. 1. Primary hacker attack avenues usually involve workstation vulnerabilities, laptop computers or Internet access.

should be configured to prevent malware from initiating communications back to the attacker. Finally, all installation media should be obtained through a verified channel.

Front line. The first line of defense against unauthorized devices is to have formal procedures for connecting devices to the network and then periodically examining the network for new devices. Using locked cabinets for switches and routers and physically disabling unused ports provides an additional level of protection. Using switches that can be configured to both disable unused ports and allow connection of only authorized MAC addresses offers even more protection. Finally, workstation-based firewalls and other host-based firewalls, static IP addresses, and static address resolution protocol (ARP) tables are more technical measures that can be used to make communications for unauthorized devices difficult.

One of the often overlooked threats to ICS, and IT systems as well, is the disgruntled employee. It is often not clear what to do about this threat because the employee has legitimate access to the system. A first protective step is to make sure that all employees are able to only access the resources they need, such as files, the registry, and desktop menus. Also, user accounts should be kept up-to-date. They should be disabled, deleted or updated when the employee's status changes (i.e., when he or she resigns or is reassigned).

If the ICS supports it, a second person to authorize sensitive operations should be required. If you are using Windows, User Access Control (UAC) can help in this regard. Sensitive operations can be set up to require elevated privileges, and UAC can be configured to intercept standard user requests for these operations and then prompt the user for additional credentials.

Another deterrent is notifying employees that all security-related actions and events are logged, including theirs. In addition, intrusion detection systems (IDSs) can be used to provide alerts when suspicious or irregular activities are detected. If disgruntled employees believe that they will be caught, they are less likely to harm the ICS.

Addressing the threats discussed here is a great place to start when hardening an ICS from attacks. A full cyber security threat assessment will help identify other pertinent security risks. HP

LEE NEITZEL is a senior engineer at Emerson Process Management in Austin, Texas. He has been involved in security and network standards for more than 30 years. He has worked on IEEE 802, FDDI, Fieldbus Foundation, and OPC standards. He is currently the IEC project leader for integrating the WIB "Process Control Domain – Security Requirements for Vendors" specification into the IEC 62443 and the ISA-99 security standards.

ROB MIXER is a security architect at Emerson Process Management in Austin, Texas. He has been designing high-security network products and systems for more than 15 years. He has worked on threat modeling for mission-critical systems, security management policies, and incident responses. His technology focus areas are trustworthy computing, security design patterns and applied cryptography.