BEST PRACTICES IN AUTOMATION SECURITY

By:

Murray McKay, Principal Application Engineer, Siemens Industry, Inc.

ABSTRACT

Historically, automation systems have relied on "security through obscurity" to avoid computer attacks. Those days are gone. While the number of actual attacks on automation systems has been small, the tools needed to conduct these attacks are now loose in the "wild", and the potential losses from an attack are large. Requirements for MIS and MES integration with the control system, as well as program backup and maintenance activities eliminate the possibility of security through lack of connectivity.

With careful system design and security-aware practices, security risks can be controlled. Network design complying with the ISA-99 recommendations places barriers between external threats and your control system. Proper configuration of security options on control system equipment can erect further barriers to attacks. Creation of, and adherence to operating policies can limit threats from non-network sources.

INTRODUCTION

An automation system includes all the plant equipment and facilities required to safely and reliably operate a production process according to the recipe and parameters selected by plant managers. The automation system is not just the specialized computers used to compute control responses, but also includes everything required to receive production targets from sales and scheduling, all the infrastructure required to keep the automation system running, and everything required to route production reports to management, logistics, and accounting operations. This includes, but is not limited to, PLC's, DCS systems, SCADA systems, RTU's, intelligent networked devices, sensors, actuators, monitoring and diagnostic systems, networks, wire, power, cabinets, wireways, and communications infrastructure.

Historically, the focus of control engineers has been to create and maintain systems that had maximal availability with high data integrity. Confidentiality was not considered to be a concern because the data were located within a company-controlled plant air-gapped from the outside world. Security was accomplished by locks on the plant doors and guards at the gates. Even if someone were to gain physical access to the system, the tools, methods, and procedures used were so specialized that no-one outside the control engineering community would be able to make much sense of what they were seeing. Security was accomplished by physical perimeter security, air-gapping, and "security through obscurity".

In order to maximize system availability, no changes were made to a working automation system that were not prescheduled for a plant outage, or required by an equipment failure. This included all operating system updates and security patches. Passwords and other access barriers were disabled or minimized to allow easy access by maintenance technicians. Remote access portals were added, often without the knowledge or approval of IT departments, to allow remote monitoring and troubleshooting by plant engineering and vendor personnel. Engineering station PC's were kept turned on and logged into control systems with the programming software to allow fastest possible troubleshooting access to the system. Any software or hardware items that might add possible points of failure or slow the operation of the automation system were minimized or removed, including firewalls, virus scanners, activity logs, and other security hardware and software. These practices all were done for the best of reasons: to insure maximal availability of the controlled processes in a low security threat environment.

In the last few years, the security threat environment to control systems has substantially changed. "State of the Art" hackers and malware can penetrate most counter-measures, and attackers are now

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

aware of the possibilities of attacking control systems. The days of "Security by Obscurity" are now over. Systems are now easier to attack because nearly all systems are directly or indirectly connected to public networks. In most cases, air-gaps are an illusion. The consequences of a successful cyber-attack on an automation system can be severe, and include loss of production, loss of trade secrets, physical damage to the plant, and injury to personnel. With this change in the threat environment, the practices required to maximize system availability must also change to incorporate defensive measure against hackers and malware.

DEFINITION OF THREAT

In order to design an automation system to be "hardened" against security threats, a definition of these threats is required. Threats may be classified by the characteristics of the attacker, the characteristics of the attack, the goal of the attack, and the system vulnerabilities that the threats target.

Attackers may be characterized as:

- Hobbyists" – break into systems for fun and glory. Difficult to stop, but consequences are low
- Professional hackers – break into systems to steal valuable assets, or on a contract basis. Very difficult to stop, consequences usually financial. May be hired to perform theft, industrial espionage, or sabotage
- Nation-States and NGO's – break into systems to gather intelligence, disable capabilities of opponents, or to cause societal disruption
- Malware – automated attack software. Intent ranges from building botnets for further attacks, theft, or general disruption. Ranges from easy to stop to moderately difficult to stop.
- Disgruntled employees

Malware attacks are easier to stop than human directed attacks because malware attack software methods can be analyzed and detected by readily available commercial security software. This does not make them less of a threat, but makes them a more manageable threat.

The main differences between hobby hackers, professional hackers, and state-level cyber warriors are the level of funding, and the reasons for the attack. All hackers are more difficult to stop than malware because the hacker can dynamically respond to the specific defenses that are employed. The higher the level of funding of the hacker, the more likely that new, not previously characterized attack methods will be utilized.

Insider attacks by disgruntled employees are a form of attack that is different in characteristics than attacks by outsiders, and requires different strategies to counteract. Insiders are likely to attack systems that they already have detailed knowledge of and may have privileged access to. Insiders are less likely to be using "hacker" techniques, as they are neither known nor needed by the insider.

Attacks may be characterized as:

- Denial of service – operations disrupted by huge number of nuisance messages on network, slowing or blocking legitimate network traffic
- Storage modification – causes computer to run attacker's program
- Memory modification – replaces pieces of running program with attacker's program
    - Memory Injection
    - SQL injection
- "Man-in-the-Middle" – attacker impersonates trusted computer, inserting itself as a middleman between trusted partner computers, modifying the messages between them to accomplish the attacker's goals
- Network monitoring – watches messages between computers to gain information about system
- Escalation of privilege – gives attacker administrative privileges on system
- Phishing attacks – convincing users to unknowingly install malware by clicking on links, bypassing outward-directed firewalls

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

- Social engineering – attackers exploit trusting, helpful impulses of plant personnel to gain information used to bypass defenses.
- Physical modification or sabotage of control equipment

Denial of service attacks disrupt automation systems by saturating communications channels, keeping legitimate messages from being processed in a timely manner. Denial of service attacks can occur intentionally, such as when the MyDoom virus attacked the SCO Group's web site[1], or by miscoding of malware such that its infection mechanism traffic grows too rapidly, such is in the Morris worm.[2] In automation systems, denial of service attacks can lead to Human/Machine Interface (HMI) systems being unable to communicate with the control computers to issue control commands, or the control computers being unable to communicate with remote Input/Output (I/O) devices. The result will be that the process will either run incorrectly, or will automatically shutdown. The main strategy for preventing denial of service attacks on an automation system is to use firewalls and switches to keep all non-required network traffic off from the control system networks.

Storage modification is a technique where an attacker modifies the copy of a program kept on permanent storage such as a hard drive, so that the program will perform an attacker-assigned task the next time the program is executed, instead of the task intended by the user. Most viruses and worms use storage modification techniques as one of their attack mechanisms. Strategies for defeating storage modification attacks include implementing authentication and security mechanisms on file accesses, and using scanning programs such as virus scanners and whitelisters to detect and/or prevent unauthorized storage modification.

Memory modification is a technique where an attack modifies a program that is already running in memory, hijacking it to perform the attacker's tasks instead of the user's intended tasks. Memory modification techniques often take advantage of inadequate input checking on user input fields in software, allowing unexpected input values to change the contents of memory areas. For example, inputting a string longer than the buffer allocated to accept user input can, if not checked, write over the program memory that contains the return address for the current function, allowing an attacker to execute code embedded within the input string.[3] Another type of memory modification attack exploits input fields that are used to construct database queries, specifying input in such a way as to change the function of a query. For example, on a logon page of a website, if a user input fields supply values for the variables varUserName and varPassword that are used in the SQL statement:

```
SELECT * FROM users WHERE name = '" + varUserName +
"'AND password = '" + varPassword + "'";
```

If the input fields are not rigorously checked, and the user inputs a value of "XX'; DROP TABLE users; --", the resulting SQL command will delete the users table from the system.[4] The strategy for defending against memory modification attacks employs input field value testing to prevent unwanted values, and to check sizes to prevent buffer overflows.

Man-in-the-Middle attacks are used to assume a trusted role in a communications network. They have been used in spoofing IFF systems, stealing from banks, and loading attacker code into a PLC. In the Stuxnet worm, a communications driver DLL was replaced using a storage modification attack. The attacker's DLL passed legitimate commands between PLC programming software and the PLC, but added commands to modify the program, and modified the responses from the PLC to hide the changes from the programming software. In a reported aircraft IFF spoofing attack, IFF challenge responses were recorded at one location, and then played back at another to fool a defense system. The main strategy for defeating man-in-the-middle attacks is to use protocols that include encrypted authentication mechanisms, and include time and sequence information to keep recorded challenge/response sequences from being valid. Encrypted domain authentication using strong encryption protocols, instead of computer-level (workgroup) authentication with their weaker encryption reduces systems' vulnerability to man-in-the-middle attacks.

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

Network monitoring is using passive surveillance software to record normal network traffic, and use this information to identify the key devices on the network, identify vulnerabilities of the system, and even break encryption protocols to determine passwords, access codes, etc. Network monitoring is especially easy where wireless communications are implemented, as the attacker does not even need to be within the security-controlled area of the plant to access the network traffic. Even where wireless communications are not used, routers and switches that are insufficiently protected can be hacked to send network traffic to an attacker. Network monitoring is a technique used mainly by hackers, not malware or disgruntled insiders. It is very difficult to detect and stop. The primary defense strategy against network monitoring is to encrypt network traffic using strong encryption protocols, and to keep networks well partitioned so that network traffic is only visible to those devices that need access to it.

Escalation of Privilege is an attacker technique that exploits bugs in the operating systems to gain administrative / root privileges once user-level access is gained to a system. Attackers usually need administrative privileges to gain access to their targets, or to make the changes they want to the target systems. Defensive strategies against Escalation of Privilege attacks include:

- Giving users only the minimum privileges they need to do their jobs, to make the attacker's task as difficult as possible
- Keeping operating systems patched to latest revision to close known escalation of privilege mechanisms
- Keep attackers from getting user-level access to automation systems

Phishing attacks use email and websites that pretend to be from trusted parties, but instead are used to get users to install malware or to tell the attacker private information such as user id's and passwords. Examples of phishing attacks are:

- Email that pretends to be from a bank, asking the user to update their account information, and helpfully providing a link to the update page. However, instead of leading to the bank website, the link leads to a website owned by the attacker that looks like the bank's website. The user is prompted to log in, providing user id and password. The attacker then uses the user id and password to access the victim's bank account and empty it.
- Advertisements on legitimate websites that use malware to infect unprotected viewers of the advertisement.
- Emails with offers for great products at low prices, if only we will click on the link.
- "I Love You" virus

The key feature of phishing attacks is that they persuade users to give up information or install malware. Phishing attacks are effective because most firewalls are designed and configured to prevent undesired information and content on the unprotected side of the firewall from accessing systems on the protected side of the firewall, but no nothing to prevent systems on the protected side from accessing undesired information and content. Attackers can't batter down the firewall with unsolicited information, but they can persuade users to request malware be downloaded which firewalls allow by default. Defense strategies against phishing attacks are user training, network partitioning (separating email systems from control systems, for example), and well-configured firewalls.

Phishing attacks are a form of "Social Engineering". Social Engineering is a practice of exploiting the helpful, trusting nature of people to gain access to private information or systems. Another example of social engineering is to pretend to be the assistant of a company officer, confess to having made a mistake that will get you fired unless you can fix it, and all you need to fix it is to know the password to a particular computer system. With good acting skills, an attacker, basically a "Con Man", can persuade people to give out information that can be used to access automation systems other valuable data. The main defense against social engineering attacks is training personnel to recognize and counter such attacks.

Control systems are usually optimized for system availability, not security. Product trends in last decade have been towards easier and more open network access, reducing historical "air gap" security.

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

- Control sensors and actuators frequently have no security features at all, but will supply their information and take commands from any device that correctly addresses them and communicates with the correct protocol
- Field control devices (PLC's, motion controllers, DCS nodes, RTU's, etc) usually have some security features such as passwords, but these features are underutilized
- HMI devices must have control capability over field control devices in order to be useful. Most HMI's can be remotely modified, to allow control engineers to modify their programs. These features can be disabled, but usually are not.
- HMI and field control device communications are seldom encrypted
- SCADA systems use commercial off-the-shelf (COTS) computers and operating systems, so inherit the vulnerabilities of these systems.
- PC's functioning as elements of a control system frequently do not have the software regularly updated to close security vulnerabilities. This is because changing the software to close security holes often changes the behavior of the system, causing the control system to malfunction. However, this also makes them more vulnerable to cyber attacks.
- Some older control system software is incompatible with security software such as virus scanners.
- Control systems are usually connected to plant operations networks for MIS/MES data acquisition.
- Control systems are frequent connected to the internet, for remote access and troubleshooting.
- Control system PC's are often used for office functions, such as email access. This makes them vulnerable to phishing attacks
- Programming terminals frequently have administrative privileges, detailed knowledge of the control system, and are not kept updated with latest security patches.

The trend to greater connectivity of automation systems is a good thing: processes can run more efficiently with lower cost. However, the design of automation systems has not yet incorporated the trends in information technology to greater security to counter the increasing security threat. The emphasis on keeping automation systems always available, the need for cost control, and a culture of "if it's not broke, don't fix it" has led to automation systems that have life cycles of a decade or more. Computer and IT technology tends to change substantially every three years or so. The result is that automation systems are employing computers and software that are far behind the state of the art, and often have large number of known security vulnerabilities.

SELECTION OF DEFENSES

A variety of automation security defenses are available, but none are effective against all types of attackers or attacks. A combination of security policies, practices, devices, and software must be employed to slow or stop cyber attacks.

- Virus Scanners
  Virus Scanner software can recognize known malware and attack mechanisms by identifying patterns in the code. Virus scanners usually include simple intrusion detection systems, watching for suspicious activity on ports and web browsers. Virus scanners are effective against the known universe of malware, and are required in automation systems for that purpose. However, hackers test exploits against all major virus scanners, and change pattern if detected. For this reason, virus scanners are usually ineffective against hackers. Virus scanners must be updated frequently be able to recognize new malware patterns.

- Firewalls
  Firewalls block communication from unauthorized sources, or of unauthorized types. They are key to keeping unwanted internet traffic off from an automation system. However, a firewall is only as effective as its configuration. The default firewall configuration blocks incoming data requests, but does not block outgoing data requests and incoming responses. This makes poorly configured firewalls vulnerable to phishing attacks. Configuring firewalls is not an easy

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

task, and is not a skill set that most control engineers possess. Network architecture can complicate firewall configuration: a poorly partitioned network requires very complex firewall rules. Firewall rules should be reviewed whenever a change is made to any network device, to make sure that they are still appropriate. It is also important to remember that Firewalls are software, so have their own vulnerabilities and may require software updates.

- Whitelisting
  Virus Scanners block programs that are recognized as malware according to a "blacklist" of malware pattern definitions. Whitelisters come from the other direction, blocking all programs that are not specifically added to a "whitelist" by an authorized user. In principle, this would prevent all malware from running on a computer making use of whitelisting. Whitelisting software often also includes memory protection mechanisms to block memory modification attacks. In practice, whitelisting is effective against most storage modification attacks and some classes of memory modification attacks. Whitelisting is not effective against some other attacks, such as SQL injection and man-in-the-middle. Whitelisting software must allow a mechanism for software updates that can leave an opening for escalation of privilege attacks.

- Intrusion Detection Systems
  Intrusion Detection Systems (IDS) are used to detect attacks, so that countermeasures can be employed. Physical intrusion detection systems employ cameras and sensors to detect and record access to protected physical systems such as the plant floor or cabinets containing automation equipment. Network intrusion detection systems monitor network traffic for "abnormal activity" and log any that they find. To be effective, an intrusion detection system must encode detailed knowledge of what activity is "normal" for a particular network. Commonly, there is no-one available to set up the IDS who has this knowledge, so IDS's either have too relaxed rules, so do not detect intrusions, or have too strict rules so generate too many false alarms. IDS's usually detect high speed attacks, but less effective against slow, stealthy attacks. IDS's usually report intrusions via log files, but reviewing log files is usually a very low priority for automation system engineers.

- Passwords / Identification
  Passwords and other identification mechanisms are the most commonly employed information security mechanism, being used in nearly all computer systems and automation devices. However, password mechanisms have a key flaw: people are not good at remembering them. In addition, many automation and networking devices employ a small set of passwords tied to a permission level, not to a user. Permission level passwords are usually shared by all personnel who require that permission level, so soon become common knowledge. To simplify configuration and maintenance tasks, passwords are frequently left at the vendor default value, so are common knowledge. Passwords are frequently maintained at a computer or device level, so that changing passwords when personnel change is very difficult and time consuming. Even when effective password mechanisms are available, such as in a Windows domain, most users chose passwords that are common words or personal information (child names, phone numbers, etc.) that is discoverable by web searches and social engineering. The bottom line is that passwords are not a highly effective defense, but give some protection. Centralizing password maintenance and implementing a role-based authentication mechanism can increase the security provided by passwords.

  The idea behind role-based authorization is to give each user only the system permissions needed to accomplish the tasks that the user is authorized to perform, and no others. This limits what an attacker can access if a computer is compromised. To be effectively employed, a centralized user administration system (such as a Windows Domain) must be used with role-based authentication, as the users and roles will change over time. Some automation devices and systems support centralized role-based authentication: others do not. The utility of role-based authentication depends on the devices and systems that are used an automation system. In general, the more complex the automation system, the more it can benefit from a role-base

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

authentication system. However, ongoing maintenance of the user list is required for role-based authentication, and reliable communication with the centralized authentication server(s) as well as a fallback mechanism for local authentication if communications are lost is required for role-based authentication in an automation environment. Escalation of privilege attacks are specifically designed to circumvent role-based authorization systems. This limits its effectiveness, and makes it dependent on installing latest security patches.

- Certificate-based authentication
  Certificate-based authentication is a way of using encryption to positively identify what computer and/or user is making a request. The intent of this is to prevent "man in the middle" attacks, and to block all requests from non-authorized sources. Certificate-based authentication is much more secure than common practice, which is to accept any computer presenting the correct address and computer name as that computer. Hackers attack certificate-based authentication systems by either breaking the encryption (possible, but very difficult for modern encryption algorithms), obtaining a certificate from a trusted authority (as was done with Stuxnet), or by hacking a trusted computer then using its certificate. Once an attacker compromises a trusted system, he can use the certificate owned by that system gain the trust of other systems.

- Data Encryption
  Data sent over a network can be seen by devices on the network. This may include valuable data such as credit card information, passwords, etc. Encryption makes data readable only by systems that have the encryption key to decrypt the data. Data encryption on networks is effective against network monitoring attacks because it makes the data unintelligible to attackers. Encrypting data on a storage media can make the data inaccessible to unauthorized persons if the media is lost or stolen, and makes storage modification attacks more difficult. Like certificated-based authentication, attackers try to defeat data encryption by gaining access to the encryption and decryption keys. Encryption keys are usually installed on computer systems, so compromising a computer can give an attacker encryption keys to access network and storage data.

- Virtual Private Network
  Another use of Certificate-based authentication and encryption is to create Virtual Private Networks (VPN). A VPN uses encryption and certificate-based authentication to establish a secure communications channel between two or more computers, even over a non-secure communications mechanism such as the Internet. VPN's share the same strengths and limitations of encryption based systems: they are effective against network monitoring and "man in the middle" attacks, but if a single trusted computer is compromised, access to all other computers on the VPN can be gained by the attacker.

- "Data Diode" systems
  "Data Diodes" are proprietary systems that implement unidirectional data flow. Proxies are used on the source network to collect data and forward it to a proxy on the destination network. Only pre-configured communications may pass between proxies. In principle, Data Diodes act as 100% effective firewalls since only the pre-specified data may pass through them. However, Data Diodes violate basic Ethernet specifications and protocols, so may not work with all systems, and require configuration and maintenance whenever data exchange needs change. Like firewalls, they are only as good as their rule sets. Unlike firewalls, they have no direct data path in hardware between the source and destination networks, so even hacking the data diode system is unlikely to allow an attacker access to the source network.

- Software updates
  Attackers exploit bugs and oversights in system software to gain unauthorized access to systems and data. System software manufacturers regularly publish updates to remove known vulnerabilities. Installing these updates closes security vulnerabilities, especially to storage modification, memory modification, and privilege escalation attacks, but may also "break"

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

automation systems by changing the way that system services work or are configured. In an automation environment, this makes installing updates problematic. To reduce the probability that software updates will cause operation problems, updates should be tested by automation vendors for compatibility prior to being installed in an automation system. This requires a detailed software update management system be implemented, as the default settings from operating system vendors do not take into account this compatibility testing and approval process. Because of the product life cycle differences between automation systems and system software vendors, software is frequently in use in automation systems long after system software vendors stop supporting and updating the software. This makes older automation system vulnerable to attackers. Attackers circumvent software update defenses in two ways: they reverse engineer updates to identify vulnerabilities they may not have known about, and take advantage of the time delay between an update being available and its being installed to attack systems using the newly identified vulnerabilities. This is a particular problem with automation systems, as vendor compatibility testing adds a longer delay time.

- Physical Access control
  Attackers who can gain physical access to an automation system can bypass network-based defensive measures (e.g. firewalls, IDS, etc.) to effect the operation of the controlled process. This can be as simple as disconnecting or moving wires, or as complex as adding logic bombs to the control programs. Physical access to the control system can also allow attackers to find password logs, copy reports, and steal hard drives. Locks, cameras, and physical intrusion detection can deter or prevent physical access attacks. Facility access controls (guards, fences, and gates) can complicate physical access attempts by non-insiders. Disgruntled employees will usually have authorizations to access automation systems, but using physical access monitoring to automatically log who had access when can identify those causing mischief.

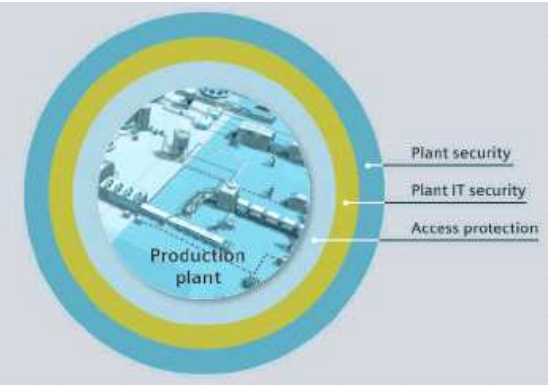
- Media Access Control
  In addition to network and physical attacks, hackers can use malware residing on storage media to attack systems. In the Stuxnet worm, contractor USB memory sticks were employed as a vector to infect automation systems[5]. A common hacker technique is the “flash drive drop”, where a pre-infected USB flash drive is mailed to a person within a targeted company, or even left in a public place where it might be found, such as a site lobby. If used, the USB drive can infect computers with malware that “phones home” with what information it finds, and opens a gateway for a hacker to access the infected computers.[6] USB, CD-ROM, etc. ports are available on nearly all computers, so the opportunity for a user to insert infected media exists. Virus scanners are effective against known media-based attacks, but are ineffective if not up to date, or if new malware agent is used.

  To defend against removable media vectored attacks, the first line of defenses is good media control policies implemented by a trained workforce. Media access control software attempts to automatically enforce media access control policies. This software is available for some computer platforms, but not for all. For platforms where media access control is not available, company policy can be effective in policing media access vulnerabilities. These policies are only effective if users are well trained about how to recognize and report Phishing and Social Engineering attack techniques, and the need to verify the integrity of any removable media device before inserting it into any computer system.

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

	Denial of Service	Storage Modification	Memory Modification	Man in the Middle	Network Monitoring	Escalation of Privilege	Phishing	Social Engineering	Physical Sabotage
Virus Scanners		☑	☑			☑	☑		
Firewalls	☑			☑	☑				
Whitelisting		☑	☑				☑		
Network Intrusion Detection	☑			☑			☑		
Passwords / Identification		☑	☑			☑			
Certificate-based authentication				☑			☑		
Role-based authorization		☑	☑			☑	☑	☑	
Data Encryption		☑			☑				
VPN				☑	☑				
Data Diode		☑	☑	☑	☑	☑	☑	☑	
Software Updates		☑	☑			☑			
Physical access control								☑	☑
Media access control		☑				☑			
User Training		☑	☑			☑	☑	☑	☑

No single defensive measure is effective against all attacks. To provide effective defense against cyber attacks a combination and layering of defensive measures must be employed.



The relative lack of security features in today's automation devices and software, combined with the lifecycle difference between automation systems and other system software means that defenses integral to the automation system are likely to be insufficient to prevent attacks: what is needed is one or more additional layers of security which act as a hard shell around the automation system. These added layers are not directly involved in the automation system, so do not have the same availability

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

requirements as the automation system. This means that they can more easily and inexpensively be modified and/or replaced to keep them up to the state of the art for cyber defenses.

The degree to which an automation system needs to be protected is a trade-off between the potential cost and impact of a successful attack and the cost of implementing defensive measures. For example, the level of defenses required by critical infrastructure, such as power plants, is vastly different from that required by a small concrete plant. While the risk of an attack in any given time period is low, the level of capability that exists for conducting attacks makes the likelihood of an attack occurring at some point very large. Most attacks will be made by automated malware, which relatively inexpensive measures can defeat. Human hackers are much more difficult to stop: the objective in automation system security defenses is to slow and complicate their task sufficiently that they either give up and find a softer target, or the defender is alerted to the attack and can take active countermeasures like disconnecting the control system from external networks.

All feasible defensive measures should be employed around the automation system. In this context, feasibility includes both technical possibility and cost justification. The strategy is to make access to critical systems sufficiently difficult so that the hacker either abandons the effort, or is detected before critical systems can be accessed. Any countermeasure has weak points where an attacker can try to get though, but with multiple counter-measures, attacks not stopped by one defense may be stopped by another

Once in place, defensive measures should be regularly reviewed to see if they are adequate to achieve the desired security level in the face of changing security threats. Just as the security threat level now is substantially different than it was just a few years ago, the types and target of cyber attacks will change in the future. Static defenses, once obsolete, change from deterring attacks to attracting attacks due to being an easy, known target.

To accomplish an effective layering of defenses, networks must be segmented into functional “zones”, with firewalls between all zones. The intent of this segmentation is to limit what information and target choice is available to an attacker should a computer be compromised by an attack. Different security zones will have different communications needs, so will employ different firewall rules and other security measures. Even within a company intranet, different security zones should consider all other zones to be potentially compromised, so should implement firewall rules blocking all but required traffic between zones. The objective here is to detect and stop attacks on one zone before they can spread to other security zones.

For example, a SCADA system network firewall may block all email and http traffic, since neither web browsing nor email are usual control system requirements, keeping most phishing attack vectors out of the automation system. On the other hand, the company business operations network will need to allow both http and email traffic to accomplish business tasks. Email and web browsing may be needed by control engineers to research and diagnose problems, but a workstation in the control room that is connected only to the business operations network, not the control network, can accomplish this task without endangering the automation system.

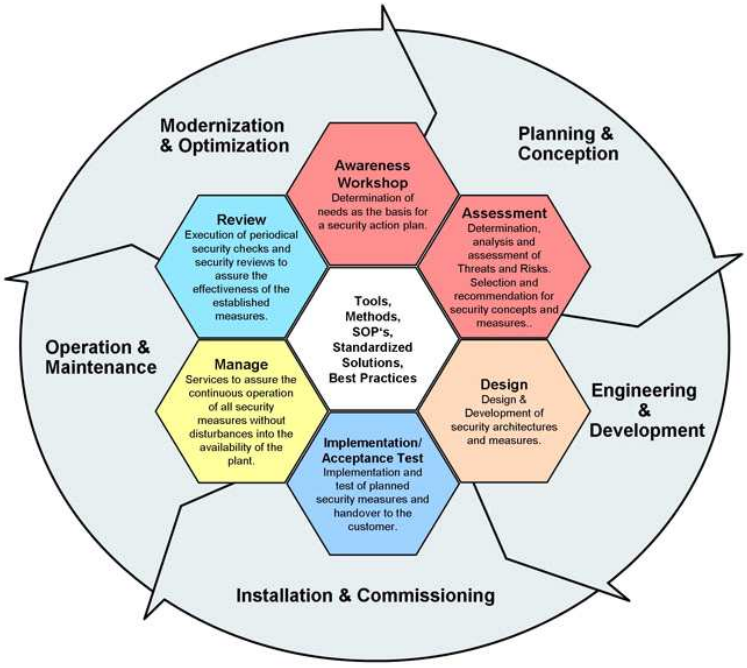
Since, given enough time, a determined attacker can compromise almost any system, Intrusion detection methods must be employed so that the attack can be detected and blocked. Without an intrusion detection system, you usually will not know if your systems are compromised. Virus scanners are insufficient as intrusion detectors, as they only detect certain types of attacks with known software and attack patterns. If a single computer on your network is compromised, an attacker can use it as a base of operations to attack other computers on your network, or to use your resources to attack others. Even if your systems are not damaged, this could make your systems evidence in a criminal case, disrupting your business.

Centralized administration of computers, users, and software must be employed to prevent a mis-configured computer from opening a vulnerability to attack. The objective here is not to make things

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

more difficult for users, but to insure that all users have implemented a consistent, well thought out defense strategy. Administration of computers is not the primary task of most people within a company. The computer is a tool to accomplish the tasks that are peoples' jobs. Most of these users will make a good-faith effort to comply with company policy, but their expertise levels will vary enough so that someone will leave security vulnerabilities open. If security settings are left to users, disgruntled or malicious employees will be able to compromise your computer systems by exposing vulnerabilities. In order to implement a reasonably secure system, the tasks of configuring and updating the computers must be automated, and administered by people whose job and expertise is to make sure it is done correctly. In addition to the consistency argument, security mechanisms employed by centralized systems tend to be much stronger than those used in distributed systems.

Security is a continuous process that must be regularly reviewed and revised.



Process of Implementing and maintaining a secure Control System:

1. Implementation of an effective and comprehensive security management for the technology, the engineering process and the production process.
2. The interfaces to office IT and Internet / Intranet are subject to clearly defined regulations – and are monitored accordingly.
3. PC based systems (HMI, engineering and PC based controllers) are protected by anti-virus software, white-listing and integrated security mechanisms.
4. Protection of the control level - by security functions which are automatically activated and integrated into the automation devices, such as IP hardening - by security functions that have to be activated by the programmer – e.g. setting up of access passwords
5. Monitoring of the entire communication with systems for intrusion detection and intelligent partitioning of the network using firewalls.

RECOMMENDED PRACTICES

A security system is only as strong as its weakest links. To ensure that all vulnerabilities are covered, a systematic implementation of security measures is required. The starting point for this is to review and revise company polices for all security procedures. An excellent starting point for this is the Cyber Security Evaluation Tool (CSET), available from the U.S. Dept. of Homeland Security at http://www.us-cert.gov/control_systems/satool.html. Writing of policies is a necessary start, but for them to be

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

effective, all personnel must be trained in the policies, and the policies must be rigorously enforced. Personnel will set their priorities to be in line with those they see from management. If cyber security is given a high priority in attention and funding, they will make carrying out the policies a high priority. If the policies are just paper documents, given no particular attention or funding, then implementing the policies will be given a low priority.

When automation systems are designed, methodologies such as those described in the ISA-99 standards are a good starting point. There are various other standards that also adequately cover the design and period review of security systems, and commercial tools that assist with this process. These may be overkill for small manufacturing processes, but should be rigorously followed where significant public safety or critical infrastructure threats exist. These standards are not perfect, but fall into the category of "consensus standards", and may have some legal weight in questions of liability or negligence.

Physical access control to all automation system equipment should be implemented. This access control should both keep out unauthorized personnel, and keep track of when and by whom equipment was accessed. This can be as simple as having to sign out a key, or as complex as using biometric access control devices.

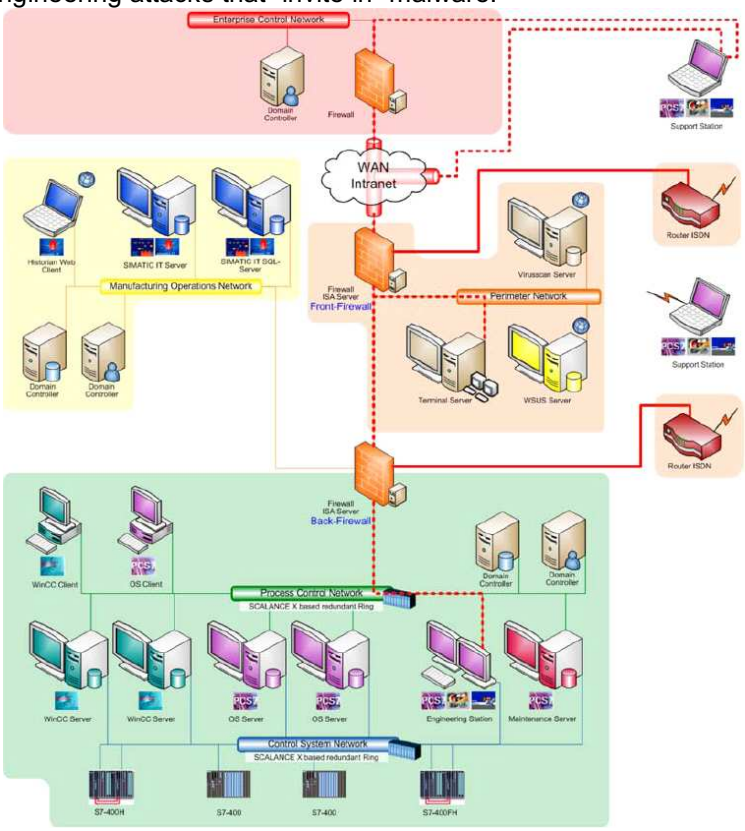
To make sure that defensive measures are implemented in a consistent manner, centralized computer configuration and authorization control should be utilized in any system where more than two or three computers are interconnected. This should include such features as

- Windows Domains which include strong authentication and encryption protocols, and allow for role-based authentication using user groups.
- Enterprise level virus scanners, which can be configured to manage their own updates, pushing updates to appropriate subsets of the automation system computers at appropriate times. The virus scanners should be configured to check only local resources on each computer, to prevent performance degradation due to multiple checks on by different computers. The virus scanners should be configured to scan only changes normally, with full system scans done in periods when the process is not running.
- Control vendor software such as Siemens' Simatic Logon can allow Windows Domains to administer user rights in programming and HMI software, enforces central administration of role-based authentication. Wherever possible, such software should be utilized.
- Software Updates must be actively managed by a central server such as Windows Server Update Services. This allows detailed control of exactly which updates are applied, and control of when the updates are applied so that the automation tasks are not disrupted.
- Users can be given only permissions appropriate to their tasks and only on the computers required to accomplish their tasks. This role-based authentication will require that each user is given unique credentials, instead of using shared credentials. This approach takes more management and maintenance, but allows credentials to be changed when personnel roles change, and allows tracking of exactly who make what change to automation and computer systems.
- Change all default passwords on all automation, networking, and computer equipment. If the equipment does not support a centralized role-based authorization mechanism, passwords should be recorded in a physically secured log so that the equipment can be if the original configuring person is not available, such as in a 3:00 AM equipment failure causing a process shutdown.
- Enable all auditing features available that do not unacceptably degrade the system performance. Windows and other computer systems have extensive auditing capabilities that can be used for attack detection, but they frequently are not enabled. These auditing functions should be enabled, and group policies put in place to automatically enable them on all computers in the domain. Communications trace and performance management functions are also available, but they frequently cause noticeable performance degradation, so these should usually only be run on systems where performance is not an issue.

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

Integral to system security is maintaining the ability to fully recover from equipment failure, or attacks causing loss of information. To do this, backups of all configuration and runtime data must be regularly made and stored completely offline. This ensures that you have something to restore if a system is found to be compromised. Backups should be run automatically whenever possible, to avoid user inattention or error.

Networks must be partitioned into security cells, with each cell containing only computers and devices that are working closely together to accomplish a task. Where security cells must interconnect for data sharing, the interconnection must be made at a single logical point (there may actually be more than one interconnection where redundant devices are used). Each interconnection should be done via a firewall configured to allow only the data required for the sharing tasks through in either direction. Functions not central to a security cell's purpose should not be allowed access to the security cell. This especially applies to web browsing and email in control system networks, as these functions tend to be targets of phishing and social engineering attacks that "invite in" malware.



Where physically separated components of an automation system must work closely together, such as where a process in one building is used as raw material for a process in a different building, VPN's should be implemented to create a single security cell that spans the process. The encryption and authentication used in the VPN allow the separate components to pass data securely through other security cells. The firewalls on the security cells will have to be configured to allow the VPN pass-through between the specified devices. The VPN should be configured as tightly as possible, so that unauthorized devices are not allowed to join the VPN without prior, manual configuration and authorization steps.

When possible, data encryption should be employed between automation devices. Encryption is not supported by all devices, but is available in nearly all computers, and can be implemented transparently to the control applications that are exchanging data. The encryption will add a little bit of overhead to the system, but will make passive monitoring attacks much less effective. Similarly, whenever possible,

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

device programs and configurations should be stored in an encrypted form to prevent unauthorized access.

Once configured, networks should be "locked down" by disabling all unused ports on switches, routers, etc. Many network devices can detect and cause SNMP traps or other notification mechanisms when network changes occur on individual ports, or to the configurations of the network devices. These mechanisms should be enabled, and the notifications logged. This information can be useful in both detecting intrusion attempts, and in helping to diagnose network hardware and configuration problems.

Intrusion detection systems should be employed within each security cell. To develop rule sets for the IDS, the traffic on each security cell will have to be analyzed and characterized. Part of this will have been necessary to properly configure the firewalls. Where the IDS functions well (no missed suspect activity, and few false positives), real-time notification of IDS detected problems should be implemented. However, at a minimum, IDS results should be logged and the logs regularly reviewed.

In addition to the IDS logs, operating system and firewall logs should be enabled and reviewed. This process may be simplified by implementing a log server for the security cell, where all log files are collected and combined. The shared clock from the domain server should simplify combining log files.

Configuration and program files for all automation devices should be regularly compared with master copies to verify that no unauthorized changes have been made.

Where remote access to a security cell is required, implement a mechanism that requires manual intervention by an operator to enable remote access. This can be as simple as a mechanical timer switch attached to the power of the remote access routing device. Including a manual step in authorizing remote access forces an attacker to use both social engineering and network attacks to be successful, and causes the access attempt to be noticed and verified.

Sooner or later, a process disturbance will happen that may have been caused by an attack, equipment failure, raw material quality problems, weather, or some other cause. Often, the root cause of the problem will not be immediately apparent. Having a response plan in place to deal with automation system disturbances can greatly simplify and speed up your response to problems, as you will have spent energy ahead of time thinking about the possibilities and coming up with decision trees to help diagnose the problem quickly.

REFERENCES

Siemens Information on Industrial Security
- www.Siemens.com/industrialsecurity

Industrial Control System Security Standards
- ISA 99 standards www.isa.org
- NIST publications http://csrc.nist.gov/groups/SMA/fisma/ics/index.html
- IEC 62443 www.iec.ch

Homeland Security – News, Tools, and Emergency Response
- http://www.us-cert.gov/control_systems/ics-cert/

[1] "Security firm: MyDoom worm fastest yet", CNN January 28, 2004, http://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/

[2] Spafford ,Eugene H., "The Internet Worm Program: An Analysis", Purdue Technical Report CSD-TR-823 1988

978-1-4673-0285-2/12/$31.00 © 2012 IEEE

[3] Erickson, Jon, “Hacking: the art of exploitation”, pp. 23-30, No Starch Press 2003

[4] “2011 Industrial Control Systems Cybersecurity Advanced Training Manual”, Network Exploitation p. 9, Department of Homeland Security

[5] Falliere, Nicolas, Murchu, Liam O, and Chien, Eric, “W32.Stuxnet Dossier”, version 1.4 Febuary 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[6] Scher, Rod, “Protect Your Company, Social engineering and your employees”, Sandhills Publishing Company 2011, http://www.social-engineer.org/wiki/archives/NewsArticles/ProtectYourCompany.pdf

978-1-4673-0285-2/12/$31.00 © 2012 IEEE