MAKING SENSE OF INDUSTRIAL CYBER SECURITY

Abstract

Industrial cyber security is currently not well understood nor widely practiced by engineers in the manufacturing and process industries. Increasingly, manufacturing and process control computer systems are being connected to business, commercial and enterprise networks that in turn are connected to the Internet. Process control systems may also contain computers with Internet connections, or modems for remote access. These connections with the outside world provide the means for attackers to penetrate the systems and cause harm. The potential also exists for manipulation of control systems by people acting from inside a company.

Presently, it is likely there are more people trying to break into computer systems than trying to prevent intrusions. Fortunately, most potential intruders have not yet targeted manufacturing and process control systems. However, that could change quickly.

This article explains and defines industrial cyber security and the vocabulary used, identifies threats and vulnerabilities for computer systems, describes techniques and methods used by adversaries in attacking them, and identifies cyber security protective measures that can be implemented.

Introduction

Since the events of September 11, 2001, the chemical process industries have invested considerable effort in developing approaches to manage the risks of terrorism and other deliberate criminal acts against facilities, called *malevents* in this article. For manufacturing and process facilities, protection is needed against such malevents as:

- Release of hazardous materials
- Diversion or theft of hazardous materials
- Contamination of products
- Interruption of production
- Damage to facilities resulting in impacts on the economy and the infrastructure of society

Adverse consequences to be avoided include employee and public fatalities, injuries and health effects, environmental impacts, damage to the economy and the infrastructure of society, and loss of public confidence.

The American Chemistry Council has published “Site Security Guidelines for the US Chemical Industry”(1) and the Center for Chemical Process Safety has developed “Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites”(2). These efforts are focused on assisting facilities in deciding what protective

measures should be taken. Protective measures can be categorized as *secureguards*, which protect against access to facilities and processes, and *safeguards* which provide protection from harm[3]. These protective measures can be subdivided into the categories of personnel, physical, information, and cyber security.

Personnel security deals with such issues as screening and controlling personnel, maintaining good labor relations, and taking appropriate actions on termination. *Physical security* involves measures such as protective barriers, area lighting, surveillance systems, guards and guard dogs, intrusion detection systems and alarms, access controls, and vehicle control. *Information security* addresses the control of written, verbal and electronic information. There are established approaches that can be applied to deal with most of these issues[4,5]. This is not so for industrial cyber security.

Manufacturing and process plants contain a variety of computer systems. In particular, they are used for control. Historically, these control systems have been kept separate from business computer systems but increasingly they are being connected through networks. This is driven by the need to communicate process information to business groups and the opportunity to intervene in manufacturing processes through an intranet or the Internet ("Net" for short) using distributed control systems. Enterprise-level software such as ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), PLM (Product Lifecycle Management) and manufacturing management software such as MES (Manufacturing Execution System) all use information from the plant floor. Traditional, hard-wired control systems are also being replaced by network architectures.

Connection of process control systems to other networks and provisions for remote access expose them to penetration. Current control systems were not designed with public access in mind, often have poor security, and are vulnerable to attack. Much of the technical information needed to penetrate these systems is readily available. There is evidence that al Qaeda terrorists have investigated the availability of software and programming information for systems that run power, water, transport and communications in the US[6]. Furthermore, the Net was not designed with security in mind. It is a massive network with many software flaws. People can easily remain anonymous and cover their tracks by weaving a trail through multiple systems. Any link to a site on the Net is a potential two-way street. Connecting control systems to networks or providing dial-up access without protections is like leaving the doors of your house unlocked. There may not be a problem immediately, but eventually the house will be burglarized or vandalized.

These issues also affect other types of computer systems including communications, access control, inventory control, power, transportation, and financial systems, all of which are increasingly linked to the Net. They can be attacked from within a facility or externally. The Net also provides the means for attacks from outside the country. This makes possible information warfare (infowar) and more broadly cyber warfare. These

threats are changing the nature of conflict as fundamentally as other technologies have in the past including gunpowder and nuclear weapons.

Cyber Security Explained

The cyber prefix is used to mean computer. For example, cyberspace is the non-physical terrain created by computer systems. *Cyber security* is an established discipline for commercial and business computer systems. Historically, people have attacked computers for the information stored there and the value of the information. Therefore, cyber security typically has focused on the protection of information or data so it cannot be read, compromised or destroyed. Since the nature of computer attacks has changed over the years as technology and opportunities have evolved, cyber security for process plants needs to be defined more broadly to include a range of malicious acts that could be perpetrated through access to a computer system.

Industrial cyber security can be defined as the protection of manufacturing and process control computer systems, and their support systems, from threats of:

- Cyber attack by adversaries who wish to disable or manipulate them.
- Physical attack by adversaries who wish to disable or manipulate them.
- Access by adversaries who want to obtain, corrupt, damage, destroy or prohibit access to valuable information. This is an aspect of information security. Note that a cyber attack may be mounted to obtain sensitive information to plan a future physical or cyber attack.

Cyber attacks on control systems can be targeted at specific systems or subsystems and can target multiple locations simultaneously from a remote location. Computer systems are subject to attack by various groups including:

- Thrill-seeking, hobbyist or alienated hackers who gain a sense of power, control, self-importance, and pleasure through successful penetration of computer systems to steal or destroy information or disrupt an organization's activities. Often they have been motivated by the fame and notoriety they gain in the community of hackers and/or the media.

- Disgruntled employees or other insiders who damage systems or steal information for revenge or profit.

- Terrorists for whom hacking offers the potential for low cost, low risk, but high gain attacks.

- Professional thieves who steal information for sale.

- Adversary nations who use the Net as a military weapon.

Cyber threats can originate externally, for example, from terrorists, saboteurs, and hackers, as well as internally from employees, contractors and other insiders who desire to cause harm. Data on cyber attacks indicate that about 70% of actual attacks are made by insiders[7]. Insiders usually have legitimate reasons to use the computer system but they may misuse their privileges or impersonate higher-privilege users. Outsiders may use the Internet, dial-up lines, partner networks linked to your network, or physical break-ins to access a computer system.

The term *hacker*, or alternatively*, cracker*, has been used pejoratively to mean individuals who gain unauthorized access to computer systems. “White hat” is used to describe a hacker who identifies a security weakness in a computer system or network but, instead of taking advantage of it, exposes the weakness to allow the system's owners to fix it. White hat hackers don't break the law, commit any offense, or engage in any malicious activity as part of their hacking. The term is now commonly used by security consultants who offer hacking/penetration testing as part of their services. "Black Hat" is used to describe malicious hackers who cause harm or break laws as part of their hacking *exploits* (attacks on a computer system, especially one that takes advantage of a particular vulnerability offered by the system). “Grey Hat" hackers commit actions that are not malicious but their hacking methods may cross legal or ethical lines. These terms come from old Western movies, where the “good guys” often wore white hats and the "bad guys" wore black hats.

Computer systems that need to be considered are those used for manufacturing and process control, safety systems operation, facility access, information storage, and networks. Locations that need to be protected include computer rooms, server rooms, control rooms, motor control centers, rack rooms, and telecommunications rooms.

Not all cyber events are malicious. They can also be caused by accident. People may make mistakes such as incorrectly entering data, using the wrong data, accessing the incorrect system, mis-programming systems, using conflicting software, inadvertently introducing software or hardware infected with malicious software, etc.

Types of Attack

Attackers may have specific objectives or they may simply want to penetrate a system. In the latter case they may cause harm deliberately or inadvertently as they explore the system. Possible forms of attack include the following:

Theft, Corruption, Damage or Destruction of Information

Electronic data can be obtained by hacking into a computer system or by theft of computer storage media. Attackers may gain access to a computer system to cause harm, or they may intercept data during transport across a network or between computers to read or corrupt it. Intercepted information may be delayed, replayed,

altered, or reordered to produce a damaging effect.

Denial of Service (DoS)

In this type of attack, no information is stolen but users are prevented or inhibited from accessing services or a host is crashed. This is done to cause damage or for perverse entertainment. DoS attacks usually involve overloading a resource such as disk space, network bandwidth, memory, or input buffers. Many DoS attacks exploit limitations in the suite of TCP/IP protocols used for communications between computers on the Internet and many intranets.

Manipulation

Computers are used to control process equipment such as pumps, valves, and motors. It is this type of equipment that can be manipulated by cyber or physical attack on computer control systems. Examples of manipulation include:

- Opening/closing valves
- Starting/stopping equipment
- Disabling alarms
- Changing set points for such process parameters as pressure, temperature, and level
- Overriding alarm and trip settings
- Misdirecting material transfers
- Disabling Safety Instrumented Systems (SIS)
- Disabling Visual Display Units (VDU)
- Forcing operators to take actions

Loss of Control

This type of attack results in the process neither being under the control of the operators or attackers. This is like a “Hail Mary” pass in football. The attackers gamble that anything they do to interfere with the control system will result in an adverse consequence. However, unless disabled by the attackers, safeguards will likely shut the process down.

Shutdown

This type of attack results in shutdown of the facility. Forms of attack include:

- Overloading the system
- Cyber instruction to shut down
- Physically disabling the computer system
- Forcing operators to shut down
- Cutting cables

- Disabling utilities and support systems including backups

Vulnerabilities in Computer Systems

Computer systems are especially susceptible to attack when they contain vulnerabilities that allow easy cyber or physical access by unauthorized users. Computer systems are composed of hardware, software and peopleware (the people who use them) and all may contain vulnerabilities.

Vulnerabilities of computer systems can be categorized as providing access, or facilitating access or misuse. They include those shown below.

Vulnerabilities that Provide Access

Connection to the Net: Manufacturing and process control systems increasingly are being interfaced with business or enterprise networks. These networks in turn usually connect to the Net. Thus attackers can reach a manufacturing or process control system through other networks and possibly manipulate it to cause harm.

Wireless networks: Most wireless networks do not implement any form of reliable security, enabling access by anyone. For example, WiFi is being used increasingly in process control, often without security features enabled.

Dialup access: Often manufacturing and process control systems provide modem connections for use by process engineers for troubleshooting and by vendors for system support and maintenance. These modems could be accessed by attackers. Furthermore, outside users may follow lower security standards and practices in using the computer system. Sometimes modems are installed without authorization and the hosts may have remote control software installed such as pcAnywhere without any security enabled. This represents an open door to the systems connected to the host.

Intranet connected to manufacturing and process control systems: Provides insiders with remote access from anywhere within the company.

Local Area Network (LAN) connected to manufacturing and process control systems: Provides insiders with remote access from anywhere within the site.

Links to vendor or customer networks: Some companies connect their networks to those of vendors or customers for convenience and efficiency of operations and in so doing provide another means for access by attackers.

Unattended workstations: People may leave their workplace for a break or lunch after logging on. If the workstations are not secured, insiders will have access to the computer system. Unsecured consoles left unattended overnight also are at risk.

Backdoors (also called trapdoors): These are undocumented ways of gaining access to a program, or an entire computer system. The backdoor is written into the program by the programmer and is often known only by the programmer. However, others may discover or be informed of the presence of the backdoor. Backdoors may also be installed by attackers once they have penetrated a system so they can gain future access without going through login procedures.

Location of control rooms and stations: Proximity to the plant perimeter or location in remote areas may facilitate attacks.

Physical protection of computer hardware, peopleware and support systems: Attackers may be able easily to gain access to control rooms and stations and the people who know how to operate them. They may also be able to access network cabling systems and support systems.

Vulnerabilities that Facilitate Access

Weak passwords and poor password management: People often choose a password that is common, mundane or easy to remember and is therefore easily guessed or cracked by attackers. Some users even choose “password”, their username, or empty passwords. In manufacturing and process control systems, default passwords sometimes remain in use after commissioning the system. When multiple passwords are required of users, often they will use the same one. An attacker who obtains the password then has access to multiple systems. Users may employ the same passwords on weakly protected home computers or unsecure Internet services as on work computers. Those easily obtained passwords could be used to access secure systems. It is not unusual to see passwords on scraps of paper at work stations and insiders may look for them. Also, user accounts and passwords for terminated employees may not have been removed. Sometimes passwords are empty, or not set. This provides the opportunity for an attacker to enter their own.

Flaws, or holes, in application, operating system or other software: Often programs are complex and contain many lines of code making them susceptible to bugs and security vulnerabilities. Flaws in operating systems and applications may allow penetration by attackers. Patches (software bug fixes) may be available but may not always be installed. Some users may not find out about them. Others may have delayed installing a patch because they often cause other processes in a network to break down, or they may cause safety and operational problems. Prioritization of patch installation is difficult because no one knows which vulnerabilities will actually be exploited by attackers. Furthermore, patch installation and testing for a large number of computers may require considerable time and effort and the resources may not be available to install the large numbers of patches issued. Attackers will often try to discover which versions of software are being used so they can see if patches that correct known vulnerabilities remain uninstalled.

Weaknesses in network protocols: For example, TCP/IP was designed to guarantee delivery of data regardless of the path and time taken and without verification of the authenticity of the source. Attackers can exploit these design features to capture data during transmission, and modify the routing and authentication process.

System default configurations: Most systems are shipped with default, easy-to-use configurations which usually also means easy-to-break-into. Unfortunately, systems are often used as-is without changing the defaults.

Use of commercial-off-the-shelf (COTS) software: Such software is vulnerable because it is usually developed in an environment where there is a lack of a security culture.

Open architecture systems: These systems use off-the-shelf components and conform to approved standards and specifications that are public. Increasingly, users prefer open and standardized architectures which allow mixing and matching products from different manufacturers. However, they may make the system susceptible to penetration by attackers who can more easily identify weaknesses in an architecture they can examine for vulnerabilities. On the other hand, vulnerabilities are not likely to go unnoticed for long with so many developers reviewing and refining the source code. For closed systems the opposite is true. Since only a small group of people will ever see the source code, it is possible for vulnerabilities to go unnoticed for years, but it should be harder to find those vulnerabilities. This issue applies both to hardware and software. It is particularly an issue for open-source operating systems.

Trust relationships: Networks establish relationships of trust between machines on the network. However, attackers may use trust relationships to exploit networks by compromising one machine in order to access others freely. Networks are only as secure as their weakest link and most networks have fewer defenses from inside attacks.

Multiple connected networks: Hackers may penetrate one network that has weak security and use it to access higher security networks to which it is connected.

Lack of awareness by people: Users of computer systems may be unaware of cyber security issues. This lack of awareness represents an opportunity for attackers to take advantage of system vulnerabilities.

Gullibility of people to social engineering: Ruses or ploys are often used by attackers who prey on the trusting nature of people who willingly may provide sensitive information needed to penetrate a system in the mistaken belief they are helping someone for legitimate reasons. Information such as passwords, software used, hardware configuration, etc. may be obtained this way. The technique involves more psychology than engineering.

Poor account management: If there are no privileged accounts established, all users

have access to all functions. Open accounts of employees who have left the company are vulnerabilities.

Vulnerabilities that Facilitate Misuse of Computer Systems

Susceptibility to malicious software (malware): Malware is designed specifically to damage or disrupt a system and is loaded onto and run on a computer without the user's knowledge or approval. It performs malicious actions such as using up the computer's resources, damaging files, and possibly shutting down the system. Malware includes viruses, worms, trojan horses, logic bombs and spyware (see later section).

Use of portable Personal Computers (PCs): It is not uncommon for employees or contractors to use portable PCs at home and at work. Home use can lead to infection with malware that subsequently can be introduced into an otherwise secure work system.

Availability of information: Information on hardware and software design from vendors and companies can be used to penetrate and manipulate control systems.

Mistakes during installation and maintenance of computer systems: These can create security weaknesses in systems that are not part of the intended design.

Attack Techniques and Tools

Attackers exploit the vulnerabilities described in the previous section using a variety of techniques and tools. Hackers originally were individuals with highly specialized and esoteric knowledge of computer systems. Consequently, they were few in number. However, some of these early hackers decided to make their knowledge available to others through the development and distribution of software packages that provide hacking tools. Some of these packages rival commercial software in their design and are essentially point-and-click applications. A number of them provide suites of hacking tools. Their availability has significantly increased the number of people capable of performing sophisticated hacking. The hacking community spends considerable time probing computer networks for vulnerabilities and will actually publicize them, for example, through chat rooms on the Net.

The term *script kiddie* is used to describe a person, usually not technologically sophisticated, who employs such hacking tools randomly to seek out a specific weakness without really understanding what they are exploiting because the weakness was discovered by someone else. A script kiddie is not looking to target specific information, or a specific company, but rather uses knowledge of a vulnerability to scan the entire Net for a victim with that vulnerability.

Similarly, the term *packet monkey* is used to describe someone who intentionally inundates a network with traffic resulting in denial of service. Packet monkeys usually employ tools created and made available on the Net by hackers.

Once an attacker has penetrated a system, they will probably try to obtain *root access* that provides unrestricted access to the system. Various techniques are used by attackers. They can be categorized as reconnaissance, preparation, penetration, and attack (see Table 1) and include those described below:

Reconnaissance

IP address scan: Attackers may surf the Net looking for possible targets, for example, they may scan random IP addresses looking for specific holes and exploit any they find. Alternatively, attackers may target specific facilities.

Internet research: A key piece of information for an attacker is the identifier or address of a target on a network. Each computer on a TCP/IP network has a unique IP address that is used to route messages. Tools are available to assist them in detecting, identifying and obtaining information about other users. Resources are available on the Net that provide information about domain names and their registrars (Internet Network Information Center), IP addresses assigned to an organization (American Registry for Internet Numbers), etc.

Literature search: Attackers will also use other resources to collect information about targets such as web sites, newsletters, news releases, newspaper and magazine articles, etc.

Dumpster diving: Attackers may search through trash for information such as company directories, organization charts, etc. that can assist an attack. Care must be exercised to ensure that computer equipment that is sent for sale or disposal is sanitized so that no sensitive information remains stored on it.

Social engineering: Attackers may use ruses or ploys to obtain information useful for accessing computer systems, for example, remote access numbers, instructions for performing tasks with the computer system, and information about the operation of the computer system.

Ping sweep: This is a form of scanning. It is also known as an ICMP (Internet Control Message Protocol) sweep. A ping sweep is used to determine which of a range of IP addresses correspond to live hosts. Ping is a program that determines whether a specific IP address is accessible by sending a packet (called an ICMP ECHO request) to the specified address and waiting for a reply. A ping sweep sends messages to multiple hosts. Live hosts respond with an ICMP ECHO reply. Firewalls can be configured to block ping requests from outside sources.

Port scan: A series of messages are sent by an attacker to a computer to determine which network services are provided by the computer. Each network service is associated with established port numbers. For example, Port 80 is used for HTTP communications. In a port scan, a message is sent systematically to each port. The response indicates if the port is in use, or *open*. Open ports can be used to exploit known vulnerabilities of the computer system. Port scanning effectively identifies doors to a computer that can be used to penetrate the system. Software packages are available to perform this scanning. There are various types of port scans. For example, a vanilla scan attempts to connect to all ports, a strobe scan attempts to connect only to selected ports, and a sweep scans the same port on a number of computers.

Scanning is noisy, sending out many packets, and is subject to detection. Therefore, attackers will try to conceal their scanning activities by using decoy IP addresses or fragmenting IP packets to evade intrusion detection systems and penetrate firewalls. There is no way to stop port scanning while a computer system is connected to the Net because accessing a Net server opens a port.

Operating system scan: Attackers can scan to identify the operating system in use on a computer to help them determine holes that may exist. Invalid input deliberately sent to the system by an attacker elicits a different, signature response for each system.

Account scan: Attackers can scan for accounts with no passwords, default accounts that have not been removed, etc. which can then be used to access the system.

War dialing: This involves scanning large numbers of telephone numbers to find modems that provide access to computer systems. Software hacking tools are available for war dialing. Attackers look for unsecure modems that allow access to the computer systems to which they are connected. Modems are often installed on computers without proper authorization and security precautions.

War driving: This is cruising streets using a rig of hardware and software to search for access points (APs) to wireless networks. Typically, a portable PC or personal digital assistant (PDA) is used with a wireless LAN card installed, usually with an external antenna connector, omni-directional antenna and pigtail connector, and possibly an amplifier. A GPS device, possibly connected to the PC or PDA, is used to record the specific geographic location. Both freeware and commercial war driving software are available and they are capable of determining if the AP is secured. There are web sites that are used by war drivers to upload locations of APs they discover.

Preparation

Cracking Passwords: Many computer systems are protected by passwords and attackers have developed several approaches for obtaining them. Social engineering is used, for example, by calling someone and pretending to be another employee in order

to persuade them to part with their password. Attackers are also aware that people often choose a password that is easy to remember and is therefore easily guessed (called a *weak* password). Password cracking tools are used by attackers. Dictionary attacks break passwords by trying every word from dictionaries and word lists of common passwords and names. Brute force attacks try all possible combinations of characters using trial and error rather than intellectual strategies.

Theft of passwords: Insiders may look for scraps of paper at work stations with passwords written on them.

Shoulder surfing: Passwords of users logging on may be observed by others standing nearby.

Elevation of Privilege: Unprivileged users may gain privileged access. Insiders may be able to elevate their access privilege level.

Penetration

Sniffing: A sniffer is a program or device that monitors data traveling over a network. Sniffers provide a form of eavesdropping. They can be used for legitimate network management as well as for stealing information. Sniffers can collect usernames, passwords, e-mails, files, etc. Encrypted passwords obtained this way may need to be cracked unless the attacker can use a replay attack and use the encrypted form. Some protocols actually use clear-text passwords that are not encrypted as they pass from client to server. Sniffing of an un-encrypted password may lead to penetration of another system where the same password is used in encrypted form.

Switched networks provide segmentation that prevents every system on the network from seeing all packets and so provides a measure of protection. Encryption provides another layer of protection.

Spoofing: Attackers impersonate a trusted host to gain unauthorized access to a system. There are different ways this can be done.

Identity spoofing: Attackers employ the username and password of a legitimate user to masquerade as the user and illegally access a system.

IP spoofing: An attacker must first use a variety of techniques to find an IP address of a trusted host, disable it, and then modify the packet headers they send to a target so it appears they are coming from the trusted host. IP spoofing is possible because the source address that is sent with each packet is not actually used for routing. It is used only when the target responds to the source. IP spoofing is a blind attack because the attacker will never see the responses of the target which are sent to the trusted host where they will be discarded. Routers and firewalls can offer protection against IP

spoofing so long as the host is outside the network.

Attack

Smurfing: A smurf attacker sends ping requests with the forged source address of an intended victim to an Internet Broadcast Address that broadcasts all received messages. The return address of the request is spoofed to be the address of the attacker's victim. All the hosts receiving the ping request reply to the victim's address instead of the real sender's address. The victim is swamped with replies causing denial of service.

Zombie: This is a computer that has been implanted with a daemon that puts it under the control of an attacker without the knowledge of the computer owner. A *daemon* is a process that runs in the background and performs a specified operation at predefined times or in response to certain events. Zombies are used by attackers to launch DoS attacks.

Pulsing zombie: This is a form of DoS attack known as a *degradation*-of-service rather than *denial*-of-service. The pulsing zombie attacks with irregular small bursts of traffic to a single target from multiple sources over an extended time period. Pulsing zombie attacks are more difficult to detect and trace because they are slow and gradual and do not immediately appear to be malicious.

Malicious Data: This is information input to a program that can cause the program to take action it would not otherwise be capable of taking to cause harm. Many applications do not check the validity of input data. This enables attackers to add characters at the end of an input field or enter data when a selection should be made from a pre-defined list. These flaws in software input routines can be used by attackers to cause buffer overflows and lock up or crash a computer. They can even be used to cause the program to run code supplied by the attacker.

Malware: These are programs that are loaded onto a computer without the users knowledge and run without their approval. They perform malicious actions such as using up the computer's resources, damaging files and possibly shutting the system down. There are various types of malware:

> *Virus*: A code segment that replicates by attaching copies of itself to other executable programs, or hosts. The copy of the virus is executed when a user executes the new host program. Viruses arrive attached to other files. They may include an additional payload that triggers when specific conditions are met. For example, some viruses display a text string on a particular date. Antivirus software is available to screen for and remove the best-known viruses. A *macro virus* is encoded as an application macro embedded in a document and executes each time the document is opened. Once a macro virus is introduced

into a system, it can embed itself in all future documents created with the application. A *friends and family virus* replicates itself by using an infected machine to send out email messages, either to people in the machine's address book or by replying to incoming messages.

Worm: A self-replicating program that is self-contained and does not require a host program. Worms make copies of themselves, for example, using e-mail or another transport mechanism, and the copies execute without any user intervention. Worms commonly use network services to propagate to other host systems.

Trojan Horse: A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. They can be used to allow remote penetration of firewall.

Logic bomb: (also called *slag code)* Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising action under circumstances such as the lapse of a certain amount of time or the failure of a user to respond to a program command. In effect, it is a delayed-action computer virus or Trojan horse. Logic bombs may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects. Some logic bombs can be detected and eliminated before they execute through a periodic scan of all computer files, including compressed files, with anti-virus software.

Spyware: Software that covertly gathers user information through the user's Net connection without their knowledge or permission. Spyware transmits that information, in the background, to someone else. It can monitor user activity on the Net, gather password information, monitor keystrokes, scan the hard drive, snoop other applications, read cookies, etc. Spyware is similar to a Trojan horse in that users unwittingly install it when they install something else. Spyware applications are typically bundled as a hidden component of programs that can be downloaded from the Net. Spyware can lead to system instability or crashes since it uses system memory and resources.

Cyber Security Measures

Various measures can be taken to counter cyber attacks (see Table 2). They can be categorized as providing prevention, detection or mitigation of threats and include the following:

Authentication

This is a preventive measure. Authentication is the process of proving the identity of a

user or a computer before being granted access. Typically, the entity whose identity is verified reveals some secret knowledge to the verifier. For users, it generally involves a user name and password. Computers usually pass a code. Authentication verifies identity, but it says nothing about access rights. It is usually the first step of a two-step process in which the second step is authorization. Authorization allows the user access to different resources based on the user's identity.

Authentication is normally based on something the user knows, e.g. passwords; something the user possesses, e.g. token, smart card, digital certificate; or something the user is, e.g. biometrics or a digital signature.

Passwords: A secret word or phrase that gives a user access to a particular system, program or file. Unfortunately, a single computer user may need many passwords for e-mail, Web sites and connecting to office systems. Passwords suffer from the weaknesses of either being easy to guess or difficult to remember. Password management programs provide policies and procedures that:

- Define rules for password selection (note that rules can serve as guidelines for attackers). Passwords are needed that cannot be cracked by brute-force methods within the expected lifetime of the password.
- Educate users on how to choose passwords
- Ensure new users fully understand and apply the rules
- Require users to change passwords periodically
- Run validity checks on passwords as they are entered and reject those that are not in compliance
- Routinely run a cracker on password files and require any that are cracked to be changed immediately

Password lock-out is often used so that after, say three tries, the user is locked out of the system for a certain time period.

Token: A device that can replace or augment passwords. A token is the size of a credit card and displays a constantly changing ID code. A user first enters a password and then the card displays an ID that can be used to log onto a network.

Smart Card: Similar to a token in size and purpose but with an embedded microprocessor. They help authenticate a person's identity when plugged into a computer slot or swiped through a reader.

Digital certificate: An encrypted electronic file used to verify that a user sending a message is who they claim to be, and to provide the receiver with the means to encode a reply. Digital certificates are issued by a Certificate Authority (CA), a trusted third-party organization or company. The CA guarantees the identity of the owner of the certificate and digitally signs the certificate to provide assurance of its authenticity.

Biometrics: Authentication techniques that rely on measurable human physical characteristics that can be automatically checked, for example, fingerprints, hand geometry, voice recognition or retinal analysis.

Digital signature: A digital code attached to an electronically transmitted message that uniquely identifies the sender and verifies that the message has not been altered since it was sent. Digital signatures support *non-repudiation*, or proof of the integrity and origin of data so that it cannot subsequently be refuted.

Prevention

Vulnerability Scanning: This is the identification of system vulnerabilities using software that seeks out known security flaws. Scans can be run on networks connected to the Net or internal networks to assess the threat of rogue software or malicious employees.

War dialing: The same technique used by attackers to identify unsecured dial-up modems is also used by system administrators to identify unauthorized modems so they can be removed or secured. It can also identify rogue modems that have been installed for malicious purposes. War dialing should be performed on a regular basis.

Encryption: This is the transformation of data into a form that is unintelligible without a deciphering mechanism using a process called cryptography. Encryption is the most effective way to protect information. A key or password is needed to decipher (decrypt or read) encrypted data. Un-encrypted data is called clear or plain text while encrypted data is called cipher text. Encrypted messages can sometimes be broken by cryptanalysis, or code breaking, although modern cryptography techniques are virtually unbreakable.

There are two main types of encryption, symmetric and asymmetric (also called public-key). Symmetric encryption uses the same key for both encryption and decryption while asymmetric encryption uses a pair of keys. Pretty Good Privacy is an example of an asymmetric encryption scheme.

E-gap and air gap: Both terms are used to mean an intermediate hardware device that allows the shuttling of data only to/from another network without information such as TCP headers and system operating software commands. The lack of this information limits actions by attackers. Air gap is also used to mean the physical separation of a network from other networks and the Net.

Secure modems: Modem policies control the purchase and installation of modems and telephone lines and ensure personnel are aware of, understand and implement it. They should require management approval of all new modem installations and connections. Modems can be secured by employing modem firewalls and strong passwords, implementing a modem configuration standard, removing information that may be

useful to attackers from the login screen, limiting the number of login attempts before disconnection, disabling auto-answer where it is not needed, enabling event logging for all incoming connections and regularly reviewing the logs possibly in real time, enabling the dial back option, activating modems only when needed, using a different range of phone numbers for modems than regular phones, periodically changing dial-up access numbers, and placing any dial-up servers in a DMZ with a firewall protecting the internal network.

Wireless Technology: Security should be enabled on wireless APs. Similar safeguards can be used as for modems. Frequency hopping spread spectrum technology can also be used. It changes the carrier frequency several times per second and requires another radio set to exactly the same pattern which is based on a user-selected key and is virtually impossible to reproduce[8].

Honeypot: This is a Net-attached server that acts as a decoy, luring in potential attackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that they are being tricked and monitored. Most honeypots are installed inside firewalls so that they can better be controlled, though it is possible to install them outside firewalls. A firewall in a honeypot works in the opposite way to a normal firewall. Instead of restricting what comes into a system from the Net, the honeypot firewall allows all traffic to come in from the Net and restricts what the system sends back out.

By luring an attacker into a system, a honeypot serves several purposes. The administrator can watch the attacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be eliminated. The attacker can be caught and stopped while trying to obtain access to the system. By studying the activities of attackers, designers can better create more secure systems that are potentially invulnerable to future attackers. Attacks on honeypots also act as warnings of attacks to come.

Account management program: Privileged accounts should be used. They should employ minimum necessary access privileges. The accounts of employees who leave the company must be terminated. Accounts maintenance should be performed.

Lock-outs and time-outs: Screen saver passwords and program time-outs can help protect unattended workstations.

Physical and Personnel Security: Computers and their support systems and personnel must be protected from physical attack in the same way as other facility assets[3-5]. This poses some challenges in today's distributed computing environment using networks. Equipment is located in many places. There are control rooms, control stations, workstations, consoles, computer rooms, rack rooms, server closets/rooms, etc.

Suitable physical protection for all must be considered. Guards, surveillance, access controls, hardening of buildings and rooms, bolting equipment in place, secure locations, physical intrusion detection, personnel screening, security policies and procedures, and other methods should be considered. Measures that may have already been taken to protect against natural disasters and accidents may help with security, for example, fire and flood protection.

Education: Ensuring that facility personnel are appropriately oriented and trained in security matters is a vital part of a cyber security program. Personnel must be aware of social engineering, the need for proper password use, etc.

Access Control

Various methods are available. They are prevention countermeasures.

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. They are frequently used to prevent unauthorized Net users from accessing private networks connected to the Net, especially intranets. Firewalls employ a rule set that configures the firewall to pass/block information. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the rule set. There are several types of firewall techniques. In practice, many firewalls use two or more techniques in concert.

A firewall is considered a first line of defense in protecting information. For greater security, data can be encrypted. Firewall logs provide a history of blocked connections and can be used to determine who invaded the network and what damage was done. They can be set to collect as little or as much information as the systems administrator wants, but if the information is never examined, there is no point in logging it. Most firewalls offer user-defined alerts that can send email or pager messages when suspicious activity is detected. Unfortunately, firewalls have weaknesses. Administrators enable service ports such as HTTP, Telnet and FTP to allow desired traffic to pass. The firewall does not perform content checking on the data passing though enabled ports and attacks through these ports are not preventable.

Bastion Host: This is a gateway between an inside network and an outside network. It is the only host computer that can be addressed directly from the outside network. A bastion host is designed as a security measure to defend against attacks aimed at the inside network. Depending on a network's complexity and configuration, a single bastion host may stand guard by itself, or it may be part of a larger security system with different layers of protection.

DeMilitarized Zone (DMZ): Also called a perimeter network. This is a separate network added between a protected internal network and an outside environment. It contains systems that are not trusted, for example, devices accessible to Net traffic, such as

Web, FTP, SMTP, and DNS servers that can be accessed by anyone on the Net. Bastion hosts are placed in the DMZ with a firewall on one or both sides. Various DMZ architectures are possible. Web servers can be placed in their own DMZ since often they pose the greatest security risks. Web, application and database servers can also be placed in separate DMZs arranged serially to provide greater security. The use of different DMZ designs also improves security through diversity.

Virtual Private Network (VPN): This is an emulation of a secure private network using a public network such as the Internet. The VPN implements authentication, integrity checking to confirm data was not altered during transit, and encryption to provide data confidentiality.

Detection

Anti-Malware: This is software that scans incoming files and searches hard disks for malicious software such as viruses and removes any that are found. Most programs include an auto-update feature that enables the program to download profiles of new viruses as they are discovered.

Intrusion Detection System: An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Mitigation

Incident response: This covers stopping an intrusion that has been detected and securing the system. Preservation of evidence is usually important to allow a later investigation and possibly facilitate legal action. Organizations may have a team of first responders. There are well-established procedures that can be followed.

Incident investigation: Usually involves specialized computer forensics performed by qualified individuals. Companies offer services in this area.

Data Recovery: Salvage of data stored on damaged media may be possible. There are a number of software products that can help recover data damaged by a disk crash and there are companies that specialize in data recovery.

Conclusions

Many of the hacking techniques and countermeasures described in this article have been developed to protect information stored in computer systems (IT cyber security). These methods have applicability for industrial cyber security, although some of the countermeasures described may require care to avoid compromising safety or

operability. For example, in IT cyber security it is not uncommon to provide password lockout (e.g. after three attempts) but this may not be feasible for process control. For safety systems, password protection may not be acceptable.

Undoubtedly, new hacking methods will be developed, particularly for control systems when their vulnerabilities are discovered by the hacking community. There are many people actively looking for weaknesses in standard operating systems, applications and protocols. Once found, the knowledge is spread rapidly. This calls for vigilance by operators of manufacturing and process control computer systems to stay ahead of the hacking community and other attackers. Unfortunately, there is a lack of awareness of cyber threats and the risks involved. Security measures are often not considered until a company or others in the same industry have been attacked.

Protection of computer systems from cyber attack is a constantly changing field. As new exploits are devised, suitable countermeasures will need to be developed. There is a ongoing war between the community of hackers and systems administrators with no end in sight. Manufacturing and process control computer systems will also require new types of countermeasures to address the special issues they pose.

Protection of manufacturing and computer control systems requires a collaboration between IT personnel and controls systems engineers. Unfortunately, these groups have not always had the best of relationships owing to conflicts in their goals and a lack of mutual understanding. This historical animosity must be overcome if facilities are to provide the protection their control systems need.

This article has explained and defined industrial cyber security. Descriptions have been provided of the threats and vulnerabilities faced by manufacturing and computer control systems, techniques and methods used by adversaries to attack computer systems, and cyber security protective measures that can be implemented.

References

1. Site Security Guidelines for the US Chemical Industry, American Chemistry Council, October 2001.

2. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, August 2002, Center for Chemical Process Safety.

3. P. Baybutt, “How Can Process Plants Improve Security?”, Security Management, p. 152, November, 2002.

4. P. Baybutt, “Process Security Management Systems: Protecting Plants Against Threats”, Chemical Engineering, p. 48, January, 2003.

5. P. Baybutt and V. Ready, “Protecting Process Plants: Preventing Terrorist

Attacks and Sabotage", Homeland Defense Journal, Vol. 2, p. 1, February, 2003.

6. "Al Qaeda Studies Cyberattack Systems", Infotech, September, 2002.

7. CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2001.

8. M. Young, "Building Security Into Your Wireless Network", Intech, September 1, 2002.

Table 1. Techniques Used By Attackers.

CATEGORY	TECHNIQUES
Reconnaissance	IP address scan Internet research Literature search Dumpster diving Social engineering Ping sweep Port scan Operating system scan Account scan War dialing War driving
Preparation	Cracking passwords Theft of passwords Shoulder surfing Elevation of privilege
Penetration	Sniffing Identity spoofing IP spoofing
Attack	Smurfing Zombie Pulsing zombie Malicious data Malware

Table 2.Cyber Security Measures.

CATEGORY	MEASURES
Authentication	Password Token Smart card Digital certificate Biometrics Digital signature
Prevention	Vulnerability scanning War dialing Encryption E-gap Secure modems Wireless technology Honeypot Account management Lock-outs and time-outs Physical and personnel security Education
Access control	Firewall Bastion host Demilitarized zone Virtual Private Network Air gap
Detection	Anti-malware Intrusion Detection System (IDS)
Mitigation	Incident response Incident investigation Data recovery