CHAPTER

Industrial Cyber Security History and Trends

3

INFORMATION IN THIS CHAPTER

- Importance of Securing Industrial Networks
- Evolution of the Cyber Threat
- Insider Threats
- Hacktivism, Cyber crime, Cyber terrorism and Cyber war

Securing an industrial network and the assets connected to it, although similar in many ways to standard enterprise information system security, presents several unique challenges. While the systems and networks used in industrial control systems (ICSs) are highly specialized, they are increasingly built upon common computing platforms using commercial operating systems. At the same time, these systems are built for reliability, performance, and longevity. A typical integrated ICS may be expected to operate without pause for months or even years, and the overall life expectancy may be measured in decades. Attackers, on the contrary, have easy access to new exploits and can employ them at any time. In a typical enterprise network, systems are continually managed in an attempt to stay ahead of this rapidly evolving threat, but these methods often conflict with an industrial network's core requirements of reliability and availability.

Doing nothing is not an option. Because of the importance of industrial networks and the potentially devastating consequences of an attack, new security methods need to be adopted. Industrial networks are being targeted as can be seen in real-life examples of industrial cyber sabotage (more detailed examples of actual industrial cyber events will be presented in Chapter 7, "Hacking Industrial Systems"). They are the targets of a new threat profile that utilizes more sophisticated and targeted attacks than ever before. An equally disturbing trend is the rise in accidental events that have led to significant consequences caused when an authorized system user unknowingly introduces threats into the network during their normal and routine interaction. This interaction may be normal local system administration or via remote system operation.

IMPORTANCE OF SECURING INDUSTRIAL NETWORKS

The need to improve the security of industrial networks cannot be overstated. Most critical manufacturing facilities offer reasonable physical security preventing unauthorized local access to components that form the core of the manufacturing

environment. This may include physically secured equipment rack rooms, locked engineering work centers, or restricted access to operational control centers. The only method by which an ICS can be subjected to external cyber threats is via the industrial networks and the connections that exist with other surrounding business networks and enterprise resources.

Many industrial systems are built using legacy devices, and in some cases run legacy protocols that have evolved to operate in routable networks. Automation systems were built for reliability long before the proliferation of Internet connectivity, web-based applications, and real-time business information systems. Physical security was always a concern, but information security was typically not a priority because the control systems were air-gapped—that is, physically separated with no common system (electronic or otherwise) crossing that gap, as illustrated in Figure 3.1.

Ideally, the air gap would still remain and would still apply to digital communication, but in reality it rarely exists. Many organizations began the process of reengineering their business processes and operational integration needs in the 1990s. Organizations began to perform more integration between not only common ICS applications during this era, but also the integration of typical business applications like production planning systems with the supervisory components of the ICS. The

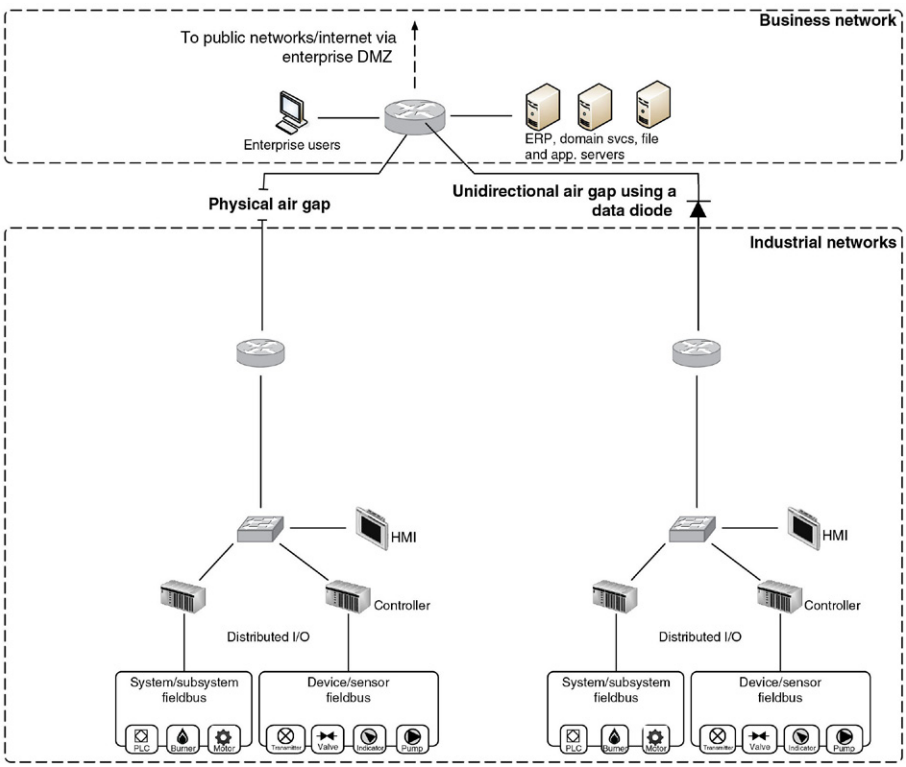

FIGURE 3.1 Air gap separation.

need for real-time information sharing evolved as well as these business operations of industrial networks. A means to bypass the gap needed to be found because the information required originated from across the air gap. In the early years of this integration "wave," security was not a priority, and little network isolation was provided. Standard routing technologies were initially used if any separation was considered. Firewalls were then sometimes deployed as organizations began to realize the basic operational differences between business and industrial networks, blocking all traffic except that which was absolutely necessary in order to improve the efficiency of business operations.

The problem is that—regardless of how justified or well intended the action—the air gap no longer exists, as seen in Figure 3.2. There is now a path into critical systems, and any path that exists can be found and exploited.

Security consultants at Red Tiger Security presented research in 2010 that indicates the current state of security in industrial networks. Penetration tests were performed on approximately 100 North American electric power generation facilities, resulting in more than 38,000 security warning and vulnerabilities.[1] Red Tiger was then contracted by the US Department of Homeland Security (DHS) to analyze the data in search of trends that could be used to help identify common attack vectors

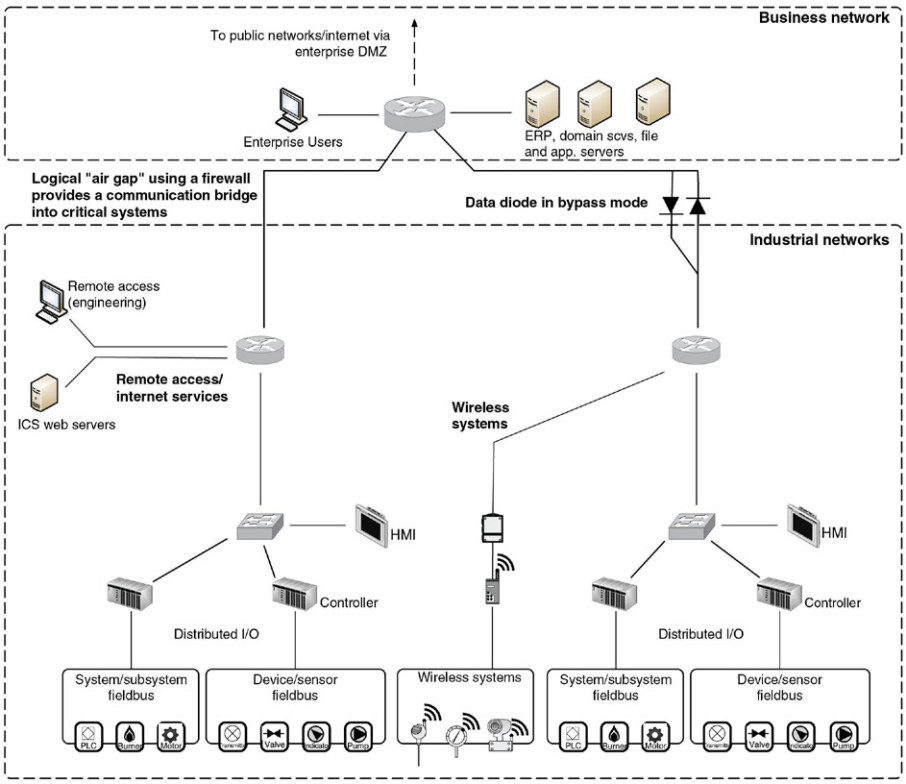

FIGURE 3.2 The reality of the air gap.

and, ultimately, to help improve the security of these critical systems against cyber-attack.

The results were presented at the 2010 Black Hat USA conference and implied a security climate that was lagging behind other industries. The average number of days between the time a **vulnerability** was disclosed publicly and the time the vulnerability was discovered in a control system was 331 days—almost an entire year. Worse still, there were cases of vulnerabilities that were over 1100 days old, nearly 3 years past their respective "zero-day."[2]

What does this mean? It says that there are known vulnerabilities that can allow hackers and cyber criminals entry into control networks. Many of these vulnerabilities are converted into reusable modules using open source penetration testing utilities, such as **Metasploit** and Kali Linux, making exploitation of those vulnerabilities fairly easy and available to a wide audience. This says nothing of the numerous other testing utilities that are not available free-of-charge, and that typically contain exploitation capabilities against zero-day vulnerabilities as well. A more detailed look at ICS exploitation tools and utilities will be discussed in Chapter 7, "Hacking Industrial Systems."

It should not be a surprise that there are well-known vulnerabilities within control systems. Control systems are by design very difficult to patch. By intentionally limiting (or even better, eliminating) access to outside networks and the Internet, simply obtaining patches can be difficult. Actually applying patches once they are obtained can also be difficult and restricted to planned maintenance windows because reliability is paramount. The result is that there are almost always going to be unpatched vulnerabilities. Reducing the window from an average of 331 days to a weekly or even monthly maintenance window would be a huge improvement. A balanced view of patching ICS will be covered later in Chapter 10, "Implementing Security and Access Controls."

THE EVOLUTION OF THE CYBER THREAT

It is interesting to look at exactly what is meant by a "cyber threat." Numerous definitions exist, but they all have a common underlying message: (a) unauthorized access to a system and (b) loss of confidentiality, integrity, and/or availability of the system, its data, or applications. Records dating back to 1902 show how simple attacks could be launched against the Marconi Wireless Telegraph system.[3] The first computer worm was released just over 25 years ago. Cyber threats have been evolving ever since: from the Morris worm (1988), to Code Red (2001), to Slammer (2003), to Conficker (2008), to Stuxnet (2010), and beyond. When considering the threat against industrial systems, this evolution is concerning for three primary reasons. First, the initial attack vectors still originate in common computing platforms—typically within level 3 or 4 systems. This means that the initial penetration of industrial systems is getting easier through the evolution and deployment of increasingly complex and sophisticated malware. Second, the industrial systems at levels 2, 1, and 0 are increasingly targeted. Third, the threats continue to evolve, leveraging successful techniques from

past malware while introducing new capabilities and complexity. A simple analysis of Stuxnet reveals that one of the propagation methods used included the exploitation of the same vulnerabilities used by the Conficker worm that was identified and supposedly patched in 2008. These systems are extremely vulnerable, and can be considered a decade or more behind typical enterprise systems in terms of cyber security maturity. This means that, once breached, the result is most likely a *fait accompli*. The industrial systems as they stand today simply do not stand a chance against the modern attack capability. Their primary line of defense remains the business networks that surround them and network-based defenses between each security level of the network. Twenty percent (20%) of incidents are now targeting energy, transportation, and critical manufacturing organizations according to the 2013 Verizon Data Investigations Report.[4]

NOTE

It is important to understand the terminology used throughout this book in terms of "levels" and "layers." Layers are used in context of the Open Systems Interconnection (OSI) 7-Layer Model and how protocols and technologies are applied at each layer.[5] For example, a network MAC address operates at Layer 2 (Data Link Layer) and depends on network "switches," while an IP address operates at Layer 3 (Network Layer) and depends on network "routers" to manage traffic. The TCP and UDP protocols operate at Layer 4 (Transport Layer) and depend on "firewalls" to handle communication flow.

Levels on the other hand are defined by the ISA-95[6] standard for the integration of enterprise and production control systems, expanding on what was originally described by the Purdue Reference Model for Computer Integrated Manufacturing (CIM)[7] most commonly referred to as the "Purdue Model." Here the term Level 0 applies to field devices and their networks; Level 1 basic control elements like PLCs; Level 2 monitoring and supervisory functions like SCADA servers and HMIs; Level 3 for manufacturing operations management functions; and Level 4 for business planning and logistics.

Incident data have been analyzed from a variety of sources within industrial networks. According to information compiled from ICS-CERT, the Repository for Industrial Security Incidents (RISI), and research from firms including Verizon, Symantec, McAfee, and others, trends begin to appear that impact the broader global market:

- Most attacks seem to be opportunistic. However, not *all* attacks are opportunistic (see the section titled "Hacktivism, Cyber Crime, Cyber Terrorism, and Cyber War" in this chapter).
- Initial attacks tend to use simpler exploits; thwarted or discovered attacks lead to increasingly more sophisticated methods.
- The majority of cyber-attacks are financially motivated. Espionage and sabotage have also been identified as motives.
- Malware, Hacking, and Social Engineering are the predominant methods of attack amongst those incidents classified as "espionage." Physical attacks, misuse, and environmental methods are common in financially motivated attacks, but are almost completely absent in attacks motivated by espionage.[8]

- New malware samples are increasing at an alarming rate. New samples have slowed somewhat in late 2013, but there are still upwards of 20 million new samples being discovered each quarter.[9]
- The majority of attacks originate externally, and leverage weak or stolen credentials.[10] The pivoting that follows once the initial compromise occurs can be difficult to trace due to the masquerading of the "insider" that occurs from that point. This further corroborates a high incidence of social engineering attacks, and highlights the need for cyber security training at all levels of an organization.
- The majority of incidents affecting industrial systems are unintentional in nature, with control and software bugs accounting for the majority of unintentional incidents.[11]
- New malware code samples are increasingly more sophisticated, with an increase in rootkits and digitally signed malware.
- The percentage of reported industrial cyber incidents is high (28%), but has been steadily declining (65% in the last 5 years).[12]
- AutoRun malware (typically deployed via USB flash drive or similar media) has also risen steadily. AutoRun malware is useful for bypassing network security perimeters, and has been successfully used in several known industrial cyber security incidents.
- Malware and "Hacking as a Service" is increasingly available, and has become more prevalent. This includes an increasing market of zero-day and other vulnerabilities "for sale."
- The number of incidents that are occurring via remote access methods has been steadily increasing over the past several years due to an increasing number of facilities that allow remote access to their industrial networks.[13]

The attacks themselves tend to remain fairly straightforward. The most common initial vectors used for industrial systems include **spear phishing**, **watering hole**, and **database injection** methods.[14] Highly targeted spear phishing (customized e-mails designed to trick readers into clicking on a link, opening an attachment, or otherwise triggering malware) is extremely effective when using Open Source Intelligence (OSINT) to facilitate social engineering. For example, spear phishing may utilize knowledge of the target corporation's organization structure (e.g. a mass e-mail sender that masquerades as legitimate e-mail from an executive within the company), or of the local habits of employees (e.g. a mass e-mail promising discounted lunch coupons from a local eatery).[15] The phishing emails often contain malicious attachments, or direct their targets to malicious websites. The phished user is thereby infected, and becomes the initial infection vector to a broader infiltration.[16]

The payloads (the malware itself) range from freely available kits, such as Webattacker and torrents, to commercial malware, such as Zeus (ZBOT), Ghostnet (Ghostrat), Mumba (Zeus v3), and Mariposa. Attackers prevent detection by antivirus and other detection mechanisms by obfuscating malware.[17] This accounts for the large rate at which new malware samples are discovered. Many new samples are code variants of existing malware, created as an evasion against common detection

mechanisms, such as anti-virus and network intrusion protection systems. This is one reason that Conficker, a worm initially discovered in 2008, remained one of the top threats facing organizations infecting as many as 12 million computers until it began to decline in the first half of 2011.[18,19]

Once a network is infiltrated and a system infected, malware will attempt to propagate to other systems. When attacking industrial networks, this propagation will include techniques for pivoting to new systems with increasing levels of authorization, until a system is found with access to lower integration "levels." That is, a system in level 4 will attempt to find active connectivity to level 3; level 3 to level 2, and so on. Once connectivity is discovered between levels, the attacker will use the first infected system to attack and infiltrate the second system, burrowing deeper into the industrial areas of the network in what is called "pivoting." This is why strong defense-in-depth is important. A firewall may only allow traffic from system A to system B. Encryption between the systems may be used. However, if system A is compromised, the attacker will be able to communicate freely across the established and authorized flow. This method can be thought of as the "exploitation of trust" and requires additional security measures to protect against such attack vectors.

APTs AND WEAPONIZED MALWARE

More sophisticated cyber-attacks against an industrial system will most likely take steps to remain hidden because a good degree of propagation may be needed to reach the intended target. Malware attempts to operate covertly and may try to deactivate or circumvent anti-malware software, install persistent rootkits, delete trace files, and perform other means to stay undetected prior to establishing backdoor channels for remote access, open holes in firewalls, or otherwise spread through the target network.[20] Stuxnet, for example, attempted to avoid discovery by bypassing host intrusion detection (using zero-day exploits that are not detectable by traditional IDS/IPS prior to its discovery, and by using various autorun and network-based vectors), disguised itself as legitimate software (through the use of stolen digital certificates), and then covered its tracks by removing trace files from systems if they are no longer needed or if they are resident on systems that are incompatible with its payload.[21] As an extra precautionary measure, and to further elude the ability to detect the presence of the malware, Stuxnet would automatically remove itself from a host if it were not the intended target once it had infected other hosts a specific number of times.[22]

By definition, Stuxnet and many other modern malware samples are considered "Advanced Persistent Threats" (APT). One aspect of an APT is that the malware utilized is often difficult to detect and has measures to establish persistence, so that it can continue to operate even if it is detected and removed or the system is rebooted. The term APT also describes cyber campaigns where the attacker is actively infiltrating systems and exfiltrating data from one or more targets. The attacker could be using persistent malware or other methods of persistence, such as the reinfection of systems and use of multiple parallel infiltration vectors and methods, to ensure broad and consistent success. Examples of other APTs and persistent campaigns against

industrial networks include Duqu[23,24], Night Dragon[25], Flame[26], and the oil and natural gas pipeline intrusion campaign.[27,28]

Malware can be considered "weaponized" when it obtains a certain degree of sophistication, and shows a clear motive and intent. The qualities of APTs and weaponized malware differ, as does the information that the malware targets, as can be seen in Tables 3.1 and 3.2. While many APTs will use simple methods, weaponized malware (also referred to as military-grade malware) trend toward more sophisticated delivery mechanisms and payloads.[29] Stuxnet is, again, a useful example of weaponized malware. It is highly sophisticated—the most sophisticated malware by far when it was first discovered—and also extremely targeted. It had a clear purpose: to discover, infiltrate, and sabotage a specific target system. Stuxnet utilized multiple zero-day exploits for infection. The development of one zero-day requires considerable resources in terms of either the financial resources to purchase commercial malware or the intellectual resources with which to develop new malware. Stuxnet raised a high degree of speculation about its source and its intent at least partly due to the level of resources required to deliver the worm through so many zero-days. Stuxnet also used "insider intelligence" to focus on its target control system, which again implied that the creators of Stuxnet had significant resources and that they either had access to an industrial control system with which to develop and test their malware, or they had enough knowledge about how such a control system was built that they were able to develop it in a simulated environment.

The developers of Stuxnet could have used stolen intellectual property—which is the primary target of the APT—to develop a more weaponized piece of malware. In other words, a cyber-attack that is initially classified as "information theft" may seem relatively benign, but it may also be the logical precursor to weaponized code. Some other recent examples of weaponized malware include Shamoon, as well as previously mentioned Duqu and Flame campaigns.

Details surrounding the Duqu and Pipeline Intrusion campaigns remain restricted at this time, and are not appropriate for this book. A great deal can be learned from

Table 3.1 Distinctions Between Common APT and Weaponized Malware

APT Qualities	Weaponized Malware Qualities
Often uses simple exploits for initial infection	Uses more sophisticated vectors for initial infection
Designed to avoid detection over long periods of time	Designed to avoid detection over long periods of time
Designed to communicate information back to the attacker using covert command and control	Designed to operate in isolation, not dependent upon remote command and control
Mechanisms for persistent operation even if detected	Mechanisms for persistent operation or reinfection if detected
Not intended to impact or disrupt network operations	Possible intentions include network disruption

Table 3.2 Information Targets of APT and Cyber War

APT Targets	Weaponized Industrial Malware Targets
Intellectual Property	
Application code	Certificates and authority
Application design	Control protocols
Protocols	Functional diagrams
Patents	PCS command codes
Industrial Designs	
Product schematics	Control system designs and schematics
Engineering designs and drawings	Safety controls
Research	PCS weaknesses
Chemicals and Formulas	
Pharmaceutical formulas	Pharmaceutical formulas
Chemical equations	Pharmaceutical safety and allergy information
Chemical compounds	Chemical hazards and controls

Night Dragon and Stuxnet, as they both have components that specifically relate to industrial systems.

Night Dragon

In February 2011, McAfee announced the discovery of a series of coordinated attacks against oil, energy, and petrochemical companies. The attacks, which originated primarily in China, were believed to have commenced in 2009, operating continuously and covertly for the purpose of information extraction,[30] as is indicative of an APT.

Night Dragon is further evidence of how an outside attacker can (and will) infiltrate critical systems once it can successfully masquerade as an insider. It began with SQL database injections against corporate, Internet-facing web servers. This initial compromise was used as a pivot to gain further access to internal, intranet servers. Using standard tools, attackers gained additional credentials in the form of usernames and passwords to enable further infiltration to internal desktop and server computers. Night Dragon established **command and control** (C2) servers as well as **Remote Administration Toolkits** (RATs), primarily to extract e-mail archives from executive accounts.[31] Although the attack did not result in sabotage, as was the case with Stuxnet, it did involve the theft of sensitive information, including operational oil and gas field production systems (including industrial control systems) and financial documents related to field exploration and bidding of oil and gas assets.[32] The intended use of this information is unknown at this time. The information that was stolen could be used for almost anything, and for a variety of motives. None of the industrial control systems of the target companies were affected; however, certain

cases involved the exfiltration of data collected from operational control systems[33]—all of which could be used in a later, more targeted attack. As with any APT, Night Dragon is surrounded with uncertainty and supposition. After all, APT is an act of cyber espionage—one that may or may not develop into a more targeted cyber war.

Stuxnet

Stuxnet is largely considered as a "game changer" in the industry, because it was the first targeted, weaponized cyber-attack against an industrial control system. Prior to Stuxnet, it was still widely believed that industrial systems were either immune to cyber-attack (due to the obscurity and isolation of the systems), and were not being targeted by hackers or other cyber-threats. Proof-of-concept cyber-attacks, such as the Aurora project, were met with skepticism prior to Stuxnet. The "threat" pre-Stuxnet was largely considered to be limited to accidental infection of computing systems, or the result of an insider threat. It is understandable, then, why Stuxnet was so widely publicized, and why it is still talked about today. Stuxnet proved many assumptions of industrial cyber threats to be wrong, and did so using malware that was far more sophisticated than anything seen before.

Today, it is obvious that industrial control systems are of interest to malicious actors, and that the systems are both accessible and vulnerable. Perhaps the most important lesson that Stuxnet taught us is that a cyber-attack is not limited to PCs and servers. While Stuxnet used many methods to exploit and penetrate Windows-based systems, it also proved that malware could alter an automation process by infecting systems within the ICS, overwriting process logic inside a controller, and hiding its activity from monitoring systems. Stuxnet is discussed in detail in Chapter 7, "Hacking Industrial Control Systems."

Advanced Persistent Threats and Cyber Warfare

One can make two important inferences when comparing APT and cyber warfare. The first is that cyber warfare is higher in sophistication and in consequence, mostly due to available resources of the attacker and the ultimate goal of destruction versus profit. The second is that in many industrial networks, there is less profit available to a cyber-attacker than from others and so it requires a different motive for attack (i.e. socio-political). If the industrial network you are defending is largely responsible for commercial manufacturing, signs of an APT are likely evidence of attempts at intellectual theft. If the industrial network you are defending is critical and could potentially impact lives, signs of an APT could mean something larger, and extra caution should be taken when investigating and mitigating these attacks.

STILL TO COME

Infection mechanisms, attack vectors, and malware payloads continue to evolve. Greater sophistication of the individual exploits and bots is expected, as well as more sophisticated blends of these components. Because advanced malware is expensive to develop (or acquire), it is reasonable to expect new variations or evolutions of

existing threats in the short term, rather than additional "Stuxnet-level" revolutions. Understanding how existing exploits might be fuzzed or enhanced to avoid detection can help plan a strong defense strategy. It is important to realize the wealth of information available in the open-source community. Tools like the Metasploit Framework by Rapid7 offer the ability to alter exploits and payloads to avoid detection, as well as transport this code between different mechanisms (DLL, VBS, OCX, etc.).

What can be assumed is that threats will continue to grow in size, sophistication, and complexity.[34] New zero-day vulnerabilities will likely be used for one or more stages of an attack (infection, propagation, and execution). The attacks will become more focused, attempting to avoid detection through minimized exposure. Stuxnet spread easily through many systems and only fully activated its entire payload within certain environments. If a similar attack was less promiscuous and more tactically inserted into the target environment, it would be much more difficult to detect.

In early 2011, additional vulnerabilities and exploits that specifically target ICSs were developed and released publically, including the broadly publicized exploits developed by two separate researchers in Italy and Russia. The "Luigi Vulnerabilities," identified by Italian researcher Luigi Auriemma included 34 total vulnerabilities against systems from Siemens (FactoryLink), Iconics (Genesis), 7-Technologies (IGSS), and DATAC (RealWin).[35] Additional vulnerabilities and exploit code, including nine zero-days, were released at that time by the Russian firm Gleg as part of the Agora+ SCADA exploit pack (now called the SCADA+ pack) for the Immunity CANVAS toolkit.[36] Today, Gleg consistently offers regular updates to the SCADA+ exploit pack often including ICS-specific zero days.[37] Tools like CANVAS and Metasploit will be covered further in Chapter 7 "Hacking Industrial Systems."

Luckily, many tools are already available to defend against these sophisticated attacks, and the results can be very positive when they are used appropriately in a blended, sophisticated defense based upon "Advanced Persistent Diligence."[38]

DEFENDING AGAINST MODERN CYBER THREATS

As mentioned in Chapter 2, "About Industrial Networks," the security practices that are recommended in this book are aimed high, because the threat environment in industrial networks has already shifted to these types of advanced cyber-attacks, if not outright cyber war. These recommendations are built around the concept of "Advanced Persistent Diligence" and a much higher than normal level of situational awareness because the APT is evolving specifically to avoid detection by known security measures.[39]

Advanced Persistent Diligence requires a strong **defense-in-depth** (DiD) approach, both in order to reduce the available attack surface exposed to an attacker, and in order to provide a broader perspective of threat activity for use in incident response, analysis, remediation, restoration, and investigation. The APT is evolving to avoid detection even through advanced event analysis, making it necessary to examine more data about network activity and behavior from more contexts within the network.[40]

The application of traditional security recommendations is not enough, because the active network defense systems, such as stateful firewalls, are no longer capable of blocking the same threats that carry with them the highest consequences. APT threats can easily slide through these legacy cyber defenses, and is why new technologies like **next-generation firewalls** (NGFW), **unified threat management** (UTM) appliances, and ICS protocol aware intrusion protection systems (IPSs) can be deployed to perform deeper inspection into the content that actually comprises the network communications.

Having situational awareness of what is attempting to connect to the system, as well as what is going on within the system is the only way to start to regain control of the network and the systems connected to it. This includes information about systems and assets, network communication flows and behavior patterns, organizational groups, user roles, and policies. Ideally, this level analysis will be automated and will provide an active feedback loop in order to allow information technology (IT) and **operational technology** (OT) security professionals to successfully mitigate a detected APT.

INSIDER THREATS

One of the most common pitfalls within manufacturing organizations is the deployment of a cyber security program in the absence of a thorough risk assessment process. This often leads to the commissioning of security controls that do not adequately represent the unique risks that face a particular organization, including the origin of their most probable threats—the insider. It is essential to have a clear definition of exactly what is meant when someone is called an "insider." A commonly used definition of an insider is an individual who has "approved access, privilege, or knowledge of information systems, information services, and missions."[41] This definition can be expanded to the unique operational aspects of ICS to include a wide range of individuals[42]:

- Employees with direct access to ICS components for operation
- Employees with highly privileged access for administration and configuration
- Employees with indirect access to ICS data
- Subcontractors with access to specific ICS components or subsystems for operation
- Services providers with access to specific ICS components or subsystems for support.

It is easy to realize that there are many viable pathways into a secure industrial network through what could be thought of as "trusted connections" or trusted relationships that are not commonly identified on system architecture and network topology diagrams. Each one of these trusted insiders has the ability to introduce unauthorized content into the ICS while masquerading as a legitimate, authorized, and often time's privileged user. The security controls deployed in these cases are typically not designed to detect and prevent these inside attacks, but are focused

more heavily on preventing traditional attacks that are expected to originate on external, untrusted networks. A common symptom of this approach is the deployment of firewalls between the business and industrial networks where the deployed rules are designed to only aggressively block and log "inbound" traffic from the business network with little or no monitoring of "outbound" traffic from the industrial networks.

The Repository of Industrial Security Incidents (RISI) tracks and updates a database of ICS cyber events and publishes an annual report that includes a yearly summary along with cumulative findings. The 2013 report showed that of the incidents analyzed, only 35% originated from outsiders.[43] If the primary defenses are based on protecting from external threats, then it can be expected to only mitigate 1/3 of the potential threats facing the ICS!

Many organizations find it difficult to accept the fact that their industrial security program needs to include controls to protect the system from the actual users and administrators. The reason is not that they do not understand the risk, but that they do not understand or accept that an employee could intentionally cause harm to the system or the plant under their control. In most cases, the event is the result of an "unintentional" or "accidental" action that is no longer directed at any particular employee, but rather on the overall security policies deployed within the architecture. According to RISI, 80% of the analyzed cyber events in ICS architectures were classified as "unintentional" in nature.[44]

This should in no manner diminish the importance of maintaining diligence with trusted individuals with granted access to industrial networks who could in fact initiate intentional attacks. Even fully vetted insiders could be pressured to initiate an attack through bribery or blackmail. The widespread deployment of remote access techniques has increased the need for heightened awareness and appropriate controls resulting from more individuals allowed access to industrial networks from potentially insecure locations and assets. Remote access is a leading point of entry for cyber events, with approximately 1/3 of the events originating via remote connections.[45] An example of this occurred in 2003 when a contractor's Slammer-infected computer connected via a Virtual Private Network (VPN) connection to his company's network that had a corresponding secure site-to-site connection to a nuclear power generating station's business network. The worm was able to traverse the two VPNs and eventually penetrate the firewall protecting the industrial network and a safety monitoring system that was disabled by the worm. The plant engineers responsible for the system that was targeted did not realize that a patch for the bug was available six months earlier.[46]

HACKTIVISM, CYBER CRIME, CYBER TERRORISM, AND CYBER WAR

The risk against industrial networks, especially those that support critical infrastructures (local, regional, or national), has increased steadily in the past years. This can be attributed in part to an increase in cyber security research of industrial control

systems resulting from the global awareness of ICS security following the disclosure of Stuxnet, as well as the easy availability of tools, such as ICS-specific exploit packages within both open-source and commercial penetration testing tools, such as Metasploit and CANVAS. Figure 3.3 depicts the year-over-year disclosure counts as logged in the Open Source Vulnerability Database (OSVDB)[47] and shows a significant increase in disclosures beginning in 2010. To remotely breach an industrial network and execute a targeted cyber-attack, the attacker still requires a certain degree of specialized knowledge that may not be as readily available. Unfortunately, this logic—while valid—is too often used to downplay the risk of a targeted cyber-attack. Of the more than 700 SCADA vulnerabilities listed in the OSVDB, most involve vulnerabilities of devices that are *not* typically used in highly critical systems. On the other hand, over 40% of those vulnerabilities have a Common Vulnerability Scoring System (CVSS) score of 9.0 or higher. The debates will continue.

What it comes down to is simple: There are vulnerable industrial systems, and because these systems are vulnerable, anyone willing to perform some research, download some freely available tools, and put forth some effort can launch an attack. With a minimal amount of system- and industry-specific training, the likelihood of a successful attack with moderate consequences is significantly increased. The real question is one of motive and resources. While the average citizen may not be motivated enough to plan and execute an attack on critical infrastructures, there are hacktivist groups who are highly motivated. While the average citizen may not have the resources to craft a targeted payload, develop a zero-day exploit to penetrate network defenses, steal digital certificates, or execute targeted spear-phishing campaigns, all

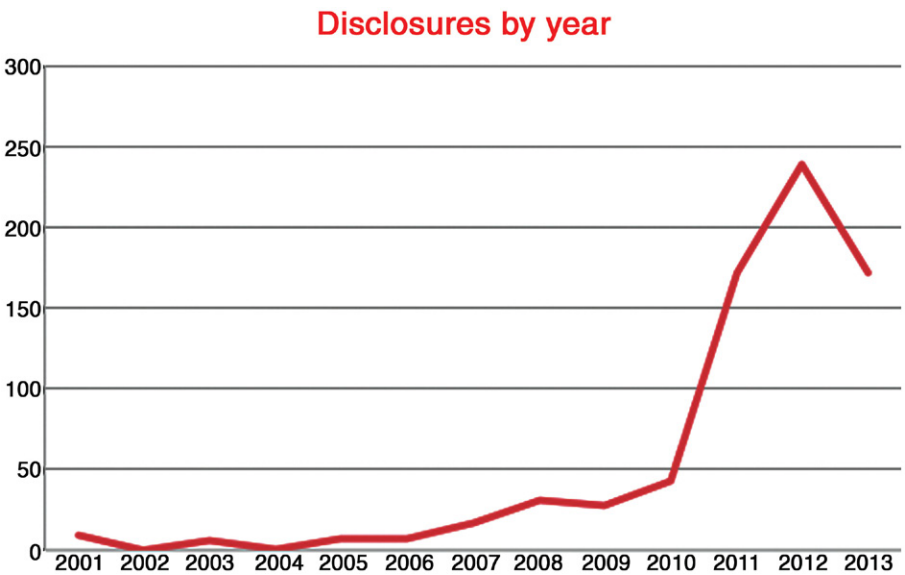

FIGURE 3.3 ICS vulnerability disclosures by year (2001–2013).

of these services are available for hire—anonymously. In a report by McAfee Labs, the use of digital currencies to anonymously buy and sell illegal products and services is becoming more prevalent, fostering an enormous digital black market. Cyber Crime and Cyber Terrorism are no longer isolated to organized syndicates and terrorist groups, but are now services available for hire. A fully weaponized attack against critical infrastructures at any level no longer needs to be military, because it can be mercenary—bought as a service, online.

Taking into consideration the possibility of "hacking as a service" from potentially very large and capable anonymous entities, the known vulnerability data (which is compelling on its own) becomes an almost moot argument. The real attacks are far more likely to involve the unknown, using zero-day exploits and highly sophisticated techniques.

SUMMARY

Industrial networks are both vital and vulnerable—there are potentially devastating consequences in the event of a successful cyber incident. Examples of real cyber incidents have grown progressively more severe over time, highlighting the evolving nature of threats against industrial systems. The attacks are evolving as well, to the point where modern cyber threats are intelligent and adaptable, difficult to detect and highly persistent. The intentions have also evolved, from information theft to industrial sabotage and the actual disruption of critical infrastructures. Combined with a rise of criminal cyber services that are becoming increasingly available via anonymous systems and that are paid for with anonymous digital currencies, this trend is worrisome, and should send a clear message to owners and operators of critical infrastructures to improve cyber security wherever and whenever possible.

Securing industrial networks requires a reassessment of your security practices, realigning them to a better understanding of how industrial protocols and networks operate (see Chapter 4, "Introduction to Industrial Control Systems and Operations" and Chapter 5, "Industrial Network Design and Architecture"), as well as a better understanding of the vulnerabilities and threats that exist (see Chapter 8, "Risk and Vulnerability Assessments").

ENDNOTES

1. J. Pollet, Red Tiger, Electricity for free? The dirty underbelly of SCADA and smart meters, in: Proc. 2010 BlackHat Technical Conference, Las Vegas, NV, July 2010.
2. Ibid.
3. The Open-Source Vulnerability Database (OSVDB) Project, ID Nos. 79399/79400. <http://osvdb.org> (cited: December 20, 2013)
4. 2013 Data Breach Investigations Report. Verizon.
5. Microsoft. KB 103884 "The OSI Model's Seven Layers Defined and Functions Explained," <http://support.microsoft.com/kb/103884> (cited: December 21, 2013).

6. International Society of Automation (ISA). Standards & Practices 95. <http://www.isa-95.com/subpages/technology/isa-95.php> (cited: December 21, 2013).
7. Purdue Enterprise Reference Architecture (PERA), "Purdue Reference Model for CIM." <http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html> (cited: December 21, 2013).
8. Verizon report.
9. McAfee Labs. McAfee Labs Threat Report: Third Quarter 2013. McAfee. 2013.
10. Verizon Report.
11. Repository of Industrial Security Incidents (RISI). 2013 Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems, June 15, 2013.
12. Ibid.
13. Ibid.
14. Ibid.
15. J. Pollet, Red Tiger, Understanding the advanced persistent threat, in: Proc. 2010 SANS European SCADA and Process Control Security Summit, Stockholm, Sweden, October 2010.
16. J. Pollet, Red Tiger, Understanding the advanced persistent threat, in: Proc. 2010 SANS European SCADA and Process Control Security Summit, Stockholm, Sweden, October 2010.
17. Ibid.
18. Microsoft. Microsoft Security Intelligence Report, Volume 12, July-December 2011.
19. Threat Post. Move Over Conficker, Web Threats are Top Enterprise Risk. <http://threatpost.com/move-over-conficker-web-threats-are-top-enterprise-risk/99762> (cited: December 20, 2013)
20. J. Pollet.
21. N. Falliere, L.O. Murchu, E. Chien, Symantec. W32.Stuxnet Dossier, Version 1.1, October 2010.
22. Ibid.
23. Budapest Univ. of Technology and Economic. Duqu: A Stuxnet-like malware found in the wild, v0.93. October 14, 2011
24. Symantec. W32.Duqu: The precursor to the next Stuxnet, v1.4. November 23, 2011
25. McAfee. Global Energy Cyberattacks: "Night Dragon." February 10, 2011
26. Symantec. Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East, May 28, 2012. <http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east> (cited: December 20, 2013)
27. ICS-CERT, U.S. Dept. of Homeland Security. Monthly Monitor, June/July 2012.
28. ICS-CERT, U.S. Dept. of Homeland Security. ICSA-12-136-01P, Gas Pipeline Intrusion Campaign Indicators and Mitigations, May 15, 2012.
29. N. Falliere, et al.
30. McAfee.
31. Ibid.
32. Ibid.
33. Ibid.
34. Ibid.
35. D. Peterson, Italian researcher publishes 34 ICS vulnerabilities. Digital Bond. <http://www.digitalbond.com/2011/03/21/italian-researcher-publishes-34-ics-vulnerabilities/>, March 21, 2011 (cited: April 4, 2011).

36. J. Langill, SCADAhacker.com. Agora+ SCADA Exploit Pack for CANVAS <http://scadahacker.blogspot.com/2011/03/agora-scada-exploit-pack-for-canvas.html>, March 17, 2011. (cited: December 20, 2013)
37. J. Langill, SCADAhacker.com. Gleg releases Ver 1.28 of the SCADA+ Exploit Pack for Immunity Canvas, October 8, 2013. (cited: October 8, 2013)
38. D. Peterson, Friday News and Notes. <http://www.digitalbond.com/2011/03/25/friday-news-and-notes-127>, March 25, 2011. (cited: April 4, 2011)
39. Ibid.
40. US Department of Homeland Security, US-CERT, Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, Washington, DC, October 2009.
41. M. Maybury, "How to Protect Digital Assets from Malicious Insiders," Institute for Information Infrastructure Protection.
42. M. Luallen, "Managing Insiders in Utility Control Systems," SANS SCADA Summit 2011, March 2011.
43. Repository of Industrial Security Incidents (RISI), "2013 Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems," June 15, 2013.
44. Ibid.
45. Ibid.
46. Security Focus, "Slammer worm crashed Ohio nuke plant network," August 19, 2003, <http://www.securityfocus.com/news/6767>, (cited: January 6, 2014).
47. Open-Source Vulnerability Database (OSVDB) Project. <http://osvdb.org/search?search[vuln_title]=scada>. (cited: January 1, 2013)