SANS | GIAC CERTIFICATIONS

WHITE PAPER

The Industrial Control System Cyber Kill Chain

Michael J. Assante and Robert M. Lee

The Industrial Control System Cyber Kill Chain

Written by
Michael J. Assante and Robert M. Lee

October 2015

Introduction

Cyber attacks on industrial control systems (ICS) differ in impact based on a number of factors, including the adversary's intent, their sophistication and capabilities, and their familiarization with ICS and automated processes. Cyber attackers target systems not in single incidents and breaches but, instead, through a campaign of efforts that enables access and provides sufficient information to devise an effect. A campaign represents the entirety of the operation against the defender organization and its systems. Understanding where an adversary is in his or her campaign can enable defenders to make better-informed security and risk management decisions. Additionally, this knowledge of the adversary's operations can help defenders appreciate the attacker's possible intent, level of sophistication, capabilities and familiarization with the ICS, which together work to unveil the potential impact of the attack on an organization. The authors believe ICS networks are more defensible than enterprise information technology (IT) systems. By understanding the inherent advantages of well-architected ICS networks and by understanding adversary attack campaigns against ICS, security personnel can see how defense is doable. The authors introduce the concept of the *ICS Cyber Kill Chain* to help defenders understand the adversary's cyber attack campaign.

In 2011, Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin created the Cyber Kill Chain™ to help the decision-making process for better detecting and responding to adversary intrusions.[1] This model was adapted from the concept of military kill chains and has been a highly successful and widely popular model for defenders in IT and enterprise networks. This model is not directly applicable to the nature of ICS-custom cyber attacks, but it serves as a great foundation and concept on which to build.

ICS-custom cyber attacks capable of significant process or equipment impact require adversaries to become intimately aware of the process being automated and the engineering decisions and design of the ICS and safety system. Gaining such knowledge enables an attacker to learn the systems well enough to cause predictable effects on systems in a way that circumvents or impacts safety mechanisms and achieves a true cyber-physical attack rather than an attack characterized as espionage, ICS disruption or intellectual property theft. To accomplish such an attack requires adversaries to initiate a two-stage attack against an ICS. The multiple stages, or exaggerated kill chain, provide additional opportunities for defenders to increase the adversary's cost of an attack and to position themselves to detect and disrupt attackers before they reach their goal. To assist personnel in visualizing and understanding an adversary's campaign against ICS, this paper is broken into three parts. The first two parts of the paper introduce the two stages of the ICS Cyber Kill Chain. The third section of the paper uses two case studies to demonstrate the ICS Cyber Kill Chain in action.

[1] Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, Ph.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"
www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

The ICS Cyber Kill Chain: Stage 1

The first stage of an ICS cyber attack is best categorized as the type of activity that would traditionally be classified as espionage or an intelligence operation. It is very similar in nature to attacks covered in Lockheed Martin's Cyber Kill Chain™ and often has the purpose of gaining access to information about the ICS, learning the system and providing mechanisms to defeat internal perimeter protections or gain access to production environments. The phases of the first stage are illustrated in Figure 1.

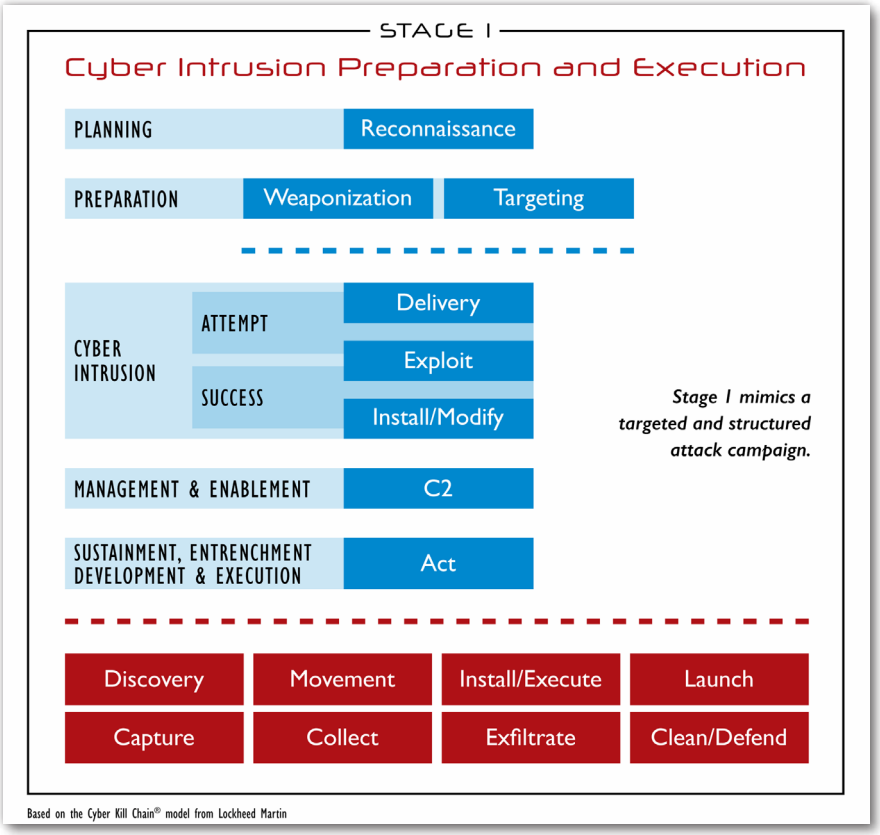

Figure 1. Stage 1: Cyber Intrusion Preparation and Execution

Planning Phase

Planning is the first phase of Stage 1 and includes performing reconnaissance. *Reconnaissance* is an activity to gain information about something through observation or other detection methods. Cyber attack planning and reconnaissance often includes conducting research about the target, usually with open source information-gathering tools such as Google and Shodan, as well as through searches of publicly available data such as public announcements and social media profiles.

The objective of the Planning phase is to reveal weaknesses and identify information that support attackers in their efforts to target, deliver and exploit elements of a system. The types of information that may be useful to an attacker can include human, network, host, account and protocol information, as well as information about policies, processes and procedures.

Planning and reconnaissance for ICS can also include activities such as researching ICS technical vulnerabilities and features or gaining an understanding of how the process and operating model may be susceptible to exploitation. Passive reconnaissance techniques (often referred to as *footprinting*) can take advantage of the tremendous amount of information available on the Internet to develop information about the target without being observed. Reconnaissance can often include actively mapping a target's publicly or privately accessible attack surfaces, patterning activity and determining versions of operating system software through routine queries.

Attackers can also attempt to hide within the noise of expected Internet traffic and activity. Publicly available information about organizations helps shape the target options available to adversaries, and the one thing defenders do not get to choose is whether their organizations are worth targeting.

Preparation Phase

Preparation is the second phase of Stage 1 and can include weaponization or targeting. *Weaponization* includes modifying an otherwise harmless file, such as a document, for the purpose of enabling the adversary's next step. Many times weaponization is manifested as files, such as PDFs, that have an exploit contained within them. The weaponized document, however, may just take advantage of available features in a malicious way, for example, as macros in Word documents.

Targeting can also take place in the second phase and occurs when the adversary or its agent (such as a script or tool) identify potential victim(s) for exploitation. *Targeting*, in modern military parlance, is the process of analyzing and prioritizing targets and matching appropriate lethal and nonlethal actions to those targets to create specific desired effects. Cyber attackers decide what attack tool or method they will use against the target based on the trade-offs between effort required over some period of time, likelihood of technical success and risk of detection. For example, after reconnaissance an adversary may determine that a virtual private network (VPN) into the environment is the right part of the defender's network to target because it may be the best approach to meet their objectives with the least amount of resource expenditure needed.

Weaponization and targeting can both take place, but both are not required. In the VPN example, the adversary may identify credentials to log in to the network directly and bypass the need for weaponization. Likewise, adversaries can weaponize capabilities to be delivered to a number of targets without specifically targeting any specific one and select a desired target only after they gain initial access.

Cyber Intrusion Phase

To gain initial access requires the third phase of Stage 1, known as the *Cyber Intrusion*. An *intrusion* is any attempt by the adversary, successful or not, to gain access to the defender's network or system. This includes the *Delivery* step, in which the adversary uses a method to interact with the defender's network. For example, a phishing email would be the delivery mechanism for the adversary's weaponized PDF, or the VPN would deliver the adversary directly to the network. The next step, the *Exploit step*, is the means the adversary uses to perform malicious actions. The means may be an exploit for a vulnerability when a PDF or other file opens, or it could be an exploitation of existing accesses to the network, such as using the credentials for a VPN. When the exploitation is successful, the adversary will *install* a capability such as a remote access Trojan. The adversary may also, or instead, *modify* existing capabilities. For example, in newer Windows environments the PowerShell tool provides enough functionality for an adversary that they do not need to rely on malware to perform their intrusion. Defenders should focus is on finding and understanding the threat and should not always assume that the threat is malware-based.

Management and Enablement Phase

With a successful cyber intrusion the adversary moves to the next phase, *Management and Enablement*. Here the actor will establish *command and control* (C2), using methods such as a connection to the previously installed capability or abusing trusted communications such as the VPN. Capable and persistent actors often establish multiple C2 paths to ensure connectivity is not interrupted if one is detected or removed. It is important to note that C2 methods do not always require a direct connection that supports a high frequency of bidirectional communication. Some access to protected networks, for example, may rely on one-way communication paths and require more time to move information out and deliver commands or code in. Attackers often establish C2 by hiding in normal outbound and inbound traffic, hijacking existing communications. In some cases, attackers establish C2 by implanting equipment to establish their own communication bridge.[2] With managed and enabled access to the environment, the adversary can now begin to achieve his or her goal.

[2] For an example of this, see Stephen Hilt's PLCpwn demonstration, in which he embedded a wireless communication channel into a PLC chassis: www.digitalbond.com/blog/2014/02/03/s4x14-video-stephen-hilt-on-plcpwn/

The *Sustainment*, *Entrenchment*, *Development*, and *Execution phase* documents a number of end goals that an adversary might have. In this phase, the adversary *acts*. The complete list of every attacker's actions would be cumbersome; however, common activities include the discovery of new systems or data, lateral movement around the network, installation and execution of additional capabilities, launching of those capabilities, capturing transmitted communications such as user credentials, collection of desired data, exfiltration of that data out of the environment and anti-forensic techniques such as cleaning traces of the attack activity or defending his or her foothold when encountering defenders such as incident responders.

This can be a critical phase for the planning and execution of Stage 2 of the ICS Cyber Kill Chain. A significant amount of information about the ICS and the industrial process, engineering and operations exists in Internet-facing networks such as corporate or enterprise networks. It is vital that defenders assess what information and tools exist in less-protected networks that could aid attackers in an attempt to compromise the ICS. It is also important to note that an attacker may perform Stage 1 against a supplier or partner network to gain necessary information, such as ICS project files delivery paths or an integrator's or vendor's remote access link to the ICS. Stage 1 may be completed when the attacker has successfully compromised the security of an ICS and is able to move on to Stage 2.

Stage 1 most directly maps to what would constitute a breach in traditional IT networks. It is important to highlight that this stage can be bypassed if defenders have Internet-facing ICS components or information about the ICS and process from a successfully compromised third-party. Recent Black Energy2/3 campaigns attempt to exploit susceptible Internet-facing devices.

A significant portion of malware and network intrusions in the community occur during Stage 1 because this is where nation-state-level intelligence and espionage operations are most likely to take place. In addition, it is where criminals are most likely to get information that can be monetized.

In many cases, there is significantly more value, depending on the attacker's current goals, in performing espionage than in perpetrating an actual attack that would include the destruction or manipulation of systems. Enjoying sustained access provides the opportunity for attackers to initiate follow-on actions later if they align with national security or military goals and/or criminal objectives. Therefore, it is important to identify and remediate adversary intelligence efforts—even if there is no immediate danger or business impact.

What makes performing an ICS cyber attack so different from a traditional IT cyber attack is that ICS components are shaped by the underlying engineering and process and are designed in unique ways and configurations that require the attacker to have extensive knowledge to impact them in a meaningful and designed way. Additionally, in a properly architected ICS, there are many layers of systems and detection sensors that an adversary has to traverse in Stage 1 to gain access to the ICS components. Unfortunately, directly connecting an ICS to the Internet significantly undermines the inherent advantages that a properly architected ICS has with regard to security.

To continue to take advantage of these inherently defensible architectures, defenders must be careful in the design choices they make and how they integrate systems. For example, integrating safety systems into the same network as operations significantly reduces the effort an adversary has to expend to fully compromise the system.[3] It also gives the defenders less opportunity to identify and remediate the attack. This loss of opportunity to defend coupled with a simultaneous increase in value to the attack accounts for a significant decrease in ICS security. With a properly architected ICS, even environments that do not traditionally have security designed into them, which can be a significant problem, are not easy to impact in a meaningful and predictable way. This problem is visualized in Stage 2 of an ICS attack.

[3] For a look at the integration of safety systems, see: www.designnews.com/author.asp?section_id=1386&doc_id=278253&itc=dn_analysis_element&dfpPParams=ind_182,industry_machinery,kw_50,aid_278253&dfpLayout=blog

It is in Stage 2 that the attacker must use the knowledge gained in Stage 1 to specifically develop and test a capability that can meaningfully attack the ICS. Unfortunately, due to sensitive equipment it is possible that Stage 1 adversary operations could lead to an unintended attack. This is a significant risk for a nation-state cyber operation because such an attack may be perceived as intentional and have unforeseen consequences. For example, an attempt to actively discover hosts on an ICS network may disrupt necessary communications or cause communication cards to fail. Simple interactions with ICS applications and infrastructure elements may result in unintentional outcomes. This activity would still be contained within Stage 1 and be an unintended effect in the Act step. Intentional attacks take place in Stage 2 and are described in Figure 2.

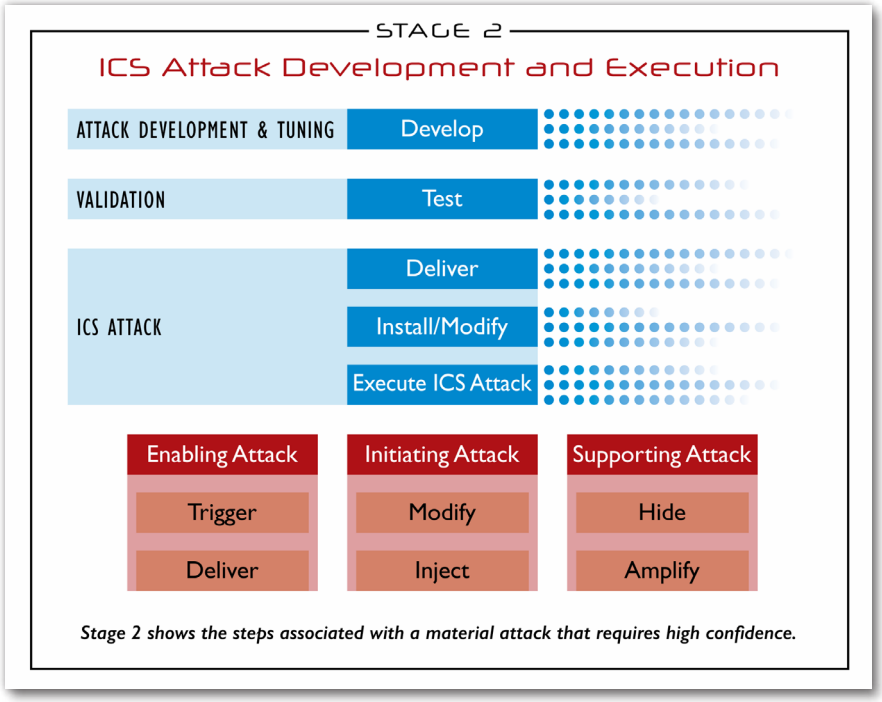

Figure 2. Stage 2: ICS Attack Development and Execution

Attack Development and Tuning

Stage 2 begins with the *Attack Development and Tuning phase*, in which the aggressor develops a new capability tailored to affect a specific ICS implementation and for the desired impact. This development will most likely take place through exfiltrated data. Only brazen attackers that have a very low opinion of the ability of the system owner and operator ability to observe their actions will experiment and develop their attack through live in-production testing. Therefore, under normal conditions, the adversary's development and tuning is especially difficult to detect. There may also be significant lag between Stage 1 and Stage 2 operations due to the need for prolonged development and testing time.

Validation

Once an adversary has developed a capability, the next phase is the *Validation phase*. Here, the attacker must *Test* his or her capability on similar or identically configured systems if the capability is to have any meaningful and reliable impact. Even simple attacks, such as increased network scanning for the denial of service to systems, need a level of testing to confirm that the scanning can deny service to the systems. However, for more significant impacts, significant testing may occur in which the adversary may acquire physical ICS equipment and software components. While it is difficult for most defenders to have insight into the ICS vendor community, various government organizations can utilize their sources and methods to identify unusual acquisitions of such equipment that may indicate a Stage 2 attack for an already established Stage 1 operation.

ICS Attack

Ultimately, the last phase is the *ICS Attack*, in which the adversary will *deliver* the capability, *install* it or *modify* existing system functionality, and then *execute* the attack. The attack may have many facets (preparatory or concurrent attacks) that fall into the attack categories of *enabling*, *initiating* or *supporting* to achieve their ultimate effect. These may be necessary to trigger conditions needed to manipulate a specific element of the process, initiate changes in process set points and variables or support the attack over time by such tactics as spoofing state information to fool plant operators into thinking everything is normal.

The complexity of launching an attack is determined by the security of the system, the process being monitored and controlled, the safety design and controls, and the intended impact. For example, a simple denial of service that disrupts the ICS is significantly easier to achieve than manipulating the process in a designed way or being able to attack the system and have the option of re-attacking as illustrated in Figure 3. The attacker ultimately needs to manipulate the process to do significant harm, including reliable or predictable physical destruction, damage of equipment under control or process elements, or modification, including manipulation of formulas, recipes and mixtures.

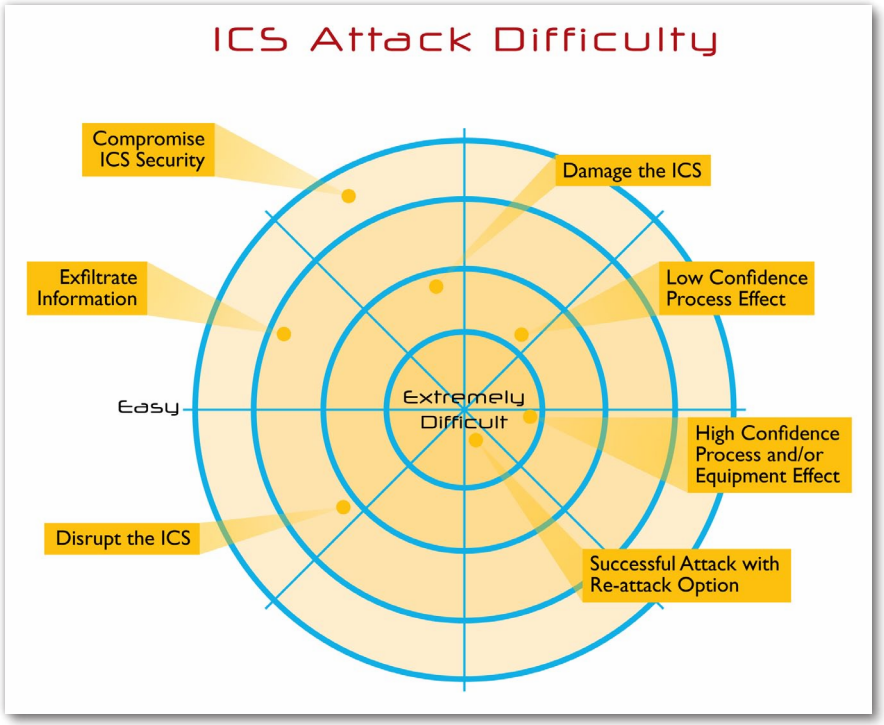

Figure 3. ICS Attack Difficulty Scale

Although there are various ways to attack an ICS environment, the most common methods to achieve functional impact fall into three categories: loss, denial and manipulation. They include a loss of view, denial of view, manipulation of view, denial of control, loss of control, manipulation of control, activation of safety, denial of safety, manipulation of safety and manipulation of sensors and instruments (see Figure 4).

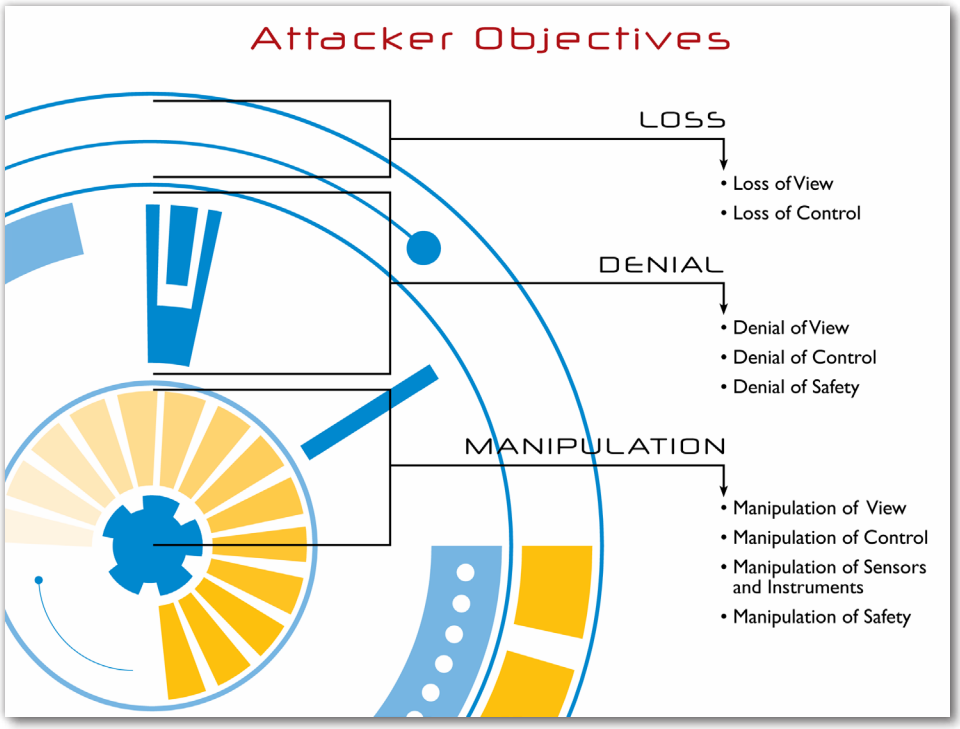

Figure 4. Attacker Objectives

There is an inherent contrast in impacts between IT and operations technology (OT) that operate an ICS. As an example, denial of service to an IT system may be extremely significant to a business process, whereas in ICS the manipulation of sensors or the process is more disturbing because it could lead to the failure of safety systems designed to protect human life or induce the process to injure personnel.

The ICS community, as a whole, does not fully understand the extent of the possibilities available to an attacker. The scenarios of power grid failure and dam overflows are commonly discussed, but other impacts, such as the release of deadly chemicals, degrading manufacturing goods slowly over time or financial loss due to unusable product resulting from modified mixtures, are other concerning scenarios.[4] It is, therefore, essential that IT and OT security personnel, as well as national policy makers, fully engage the engineering community to uncover the scenarios that could be harmful at various facilities to help them understand the potential achievable goals of an adversary. The industry must approach the problem of ICS attacks as they do equipment prognostics. It is not a matter of *if* it will fail, but *when* it will fail, and the community must complete the necessary assessment, engineering and instrumentation tasks to plan for and deal with the potential for attacks on the best terms.

Another effective way to understand ICS attacks, as well as visualize the ICS Cyber Kill Chain, is to review case studies of ICS targeted intrusions and attacks.

[4] For a discussion on nontraditional attack scenarios on ICS, see the blog post by Patrick Coyle on attacking a solution polymer chemical process: https://ics.sans.org/blog/2015/08/14/ics-cross-industry-learning-cyber-attacks-on-a-solution-polymer-chemical-process

Case Studies Examined with the ICS Cyber Kill Chain

Analyzing previous intrusions into ICS networks provides validation and insight into the ICS Cyber Kill Chain as a workable model for defenders. The ICS community historically lacks visibility into their networks and suffers from having sparse forensic evidence and data following compromises. For this reason, it is not feasible to properly identify and extract every piece of evidence from these case studies. However, understanding them at a high level is sufficient.

It is important to understand the layout and structure of a typical ICS network. We use the Purdue Reference Model, shown in Figure 5, to illustrate the architecture of an ICS network.

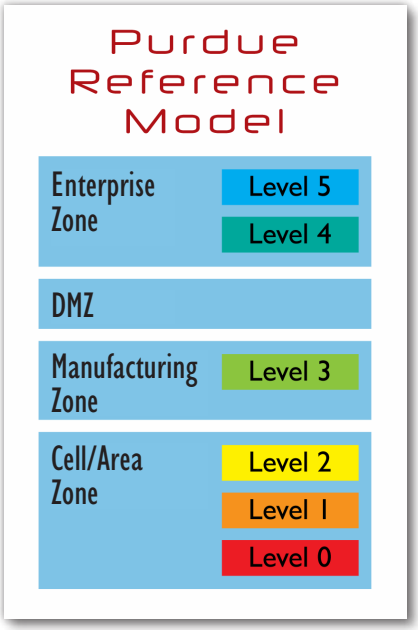

Figure 5. High-Level Purdue Model

In the following case studies, the Purdue Model will illustrate the architectural level at which the ICS was impacted, and the ICS Cyber Kill Chain will demonstrate the phases the adversary completed in their campaign.

Havex

The Havex malware, used in a campaign against ICS to gather sensitive data and network architecture information from thousands of sites around the world, was a remote access Trojan that was originally used for general-purpose espionage and evolved into a criminal tool set.[5] It was also adapted to target ICS by including new code and modules specific to ICS environments.[6] From publicly available information, it has been determined that the campaign took place over the course of at least three years.[7]

The actors behind Havex utilized multiple methods to get the Havex malware onto defenders' networks. Three of the most common were the following:

- Sending spearphishing emails with a malicious file attached
- Infecting ICS vendor websites with malware and compromising ICS defenders when they visited those websites (known as a *watering hole* technique)
- Providing a trojanized version of ICS software installers that infected the host system when staff ran the installer

[5] "Havex Hunts for ICS/SCADA Systems," F-Secure, 23 June 2014: www.f-secure.com/weblog/archives/00002718.html

[6] "ICS-ALERT-14-176-02A," ICS-CERT, 27 June 2014: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A

[7] "Dragonfly: Cyberespionage Attacks Against Energy Suppliers," Symantec Security Response, 7 July 2014: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

These multiple methods of compromise highlight that adversaries remain flexible and are not bound by a single technique for delivery and intrusion when conducting a campaign. The observed techniques indicate the attackers were successful in their planning phase of identifying weaknesses to exploit, such as the general trusting nature of engineers and inherent trust and reliance on the ICS supply chain. Additionally, it offers three intrusions to map against the ICS Cyber Kill Chain.

In the first intrusion, the spearphishing email, the adversary would have first performed reconnaissance to determine good targets and tailor the phishing emails. Next, the actors performed *weaponization* by combining a file with an exploit and attaching it to the spearphishing email. Specific *targeting* took place to choose which people would receive the email. The email itself was the delivery mechanism, and when the user opened the file attached to the email, it *exploited* the system to *install* the Havex malware. Then, the Havex malware attempted to communicate with one of hundreds of *C2* servers. Havex then scanned the environment to discover ICS components, collect the information and exfiltrate it to the C2 server for the adversary to gather. The phishing email-based intrusion mostly impacted the external network. This method was less likely to provide specific information about the ICS, except in cases where organizations kept engineering files on the business network.

The second intrusion, the infected websites, followed the first intrusion closely but used other methods to carry out Stage 1. Note, the intrusion against the ICS vendor websites had its own kill chain, and the adversary's efforts were to enable an intrusion against ICS networks. The kill chain against the ICS networks would have needed *reconnaissance* to identify what ICS networks were desired and what ICS vendors they used. From there, the vendor websites were the subject of the *weaponization*, with the intent of *targeting* the ICS networks that used those vendors. The delivery mechanism in this scenario was the Internet connection using the HTTP protocol to access the web page.

The websites were weaponized using exploits from a common penetration testing framework known as *Metasploit*.[8] The re-used exploits against known vulnerabilities acted as the *exploit* to allow the adversary to then *install* Havex into the environment, where it established its C2 and completed the same actions observed in the first intrusion. This intrusion had a higher chance of gaining access into the ICS because of the engineers and operators that were visiting the vendor websites. This intrusion mostly impacted the DMZ of ICS networks, but it was able to gain access deeper into the ICS for those organizations that did not utilize the Purdue Model or a defense-in-depth–styled architecture.

The third intrusion was the most creative. It placed a trojanized version of ICS software installers on vendor websites.[9] *Reconnaissance* would have to take place in much the same way as it did in the second intrusion. In this case, though, it was the installer that was the subject of the *weaponization*, with the intent of *targeting* ICS networks employing those types of ICS software. The *delivery* mechanism, the *exploit*, *install*, *C2* and related actions occurred just as they did in the other intrusions. The difference in this scenario, though, was that even well-architected networks that only allowed Internet access from the business network or DMZ were subject to Havex being present in lower zones of the Purdue Model. This delivery technique may have evolved from initial attempts to defeat planned security controls, such as perimeter protections, by relying on engineers to physically transport files from Internet-facing computers into the production ICS network. The *Exploit*, *Install*, *C2* and *Act* steps in this case took place internal to the ICS networks. The majority of reported infections took place in the supervisory level, where engineers and operators would have been accessing systems such as engineering workstations and human machine interfaces (HMIs). The adversary undoubtedly gained great data from this third intrusion. Because of that, it was the most observed intrusion method.[10]

[8] "Energetic Bear – Crouching Yet," Kaspersky Labs: https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf

[9] "Energetic Bear – Crouching Yet"

[10] "Energetic Bear – Crouching Yet"

Case Studies Examined with the ICS Cyber Kill Chain
(CONTINUED)

To date, the security research community has not observed evidence of follow-on actions by the Havex actors. The authors believe Havex can be characterized as a generally successful Stage 1 ICS attack. To date, there has been no documented evidence of Stage 2 activity. A representation of the ICS Cyber Kill Chain for Havex mapped to the Purdue Model for the three intrusions is diagrammed in Figure 6.

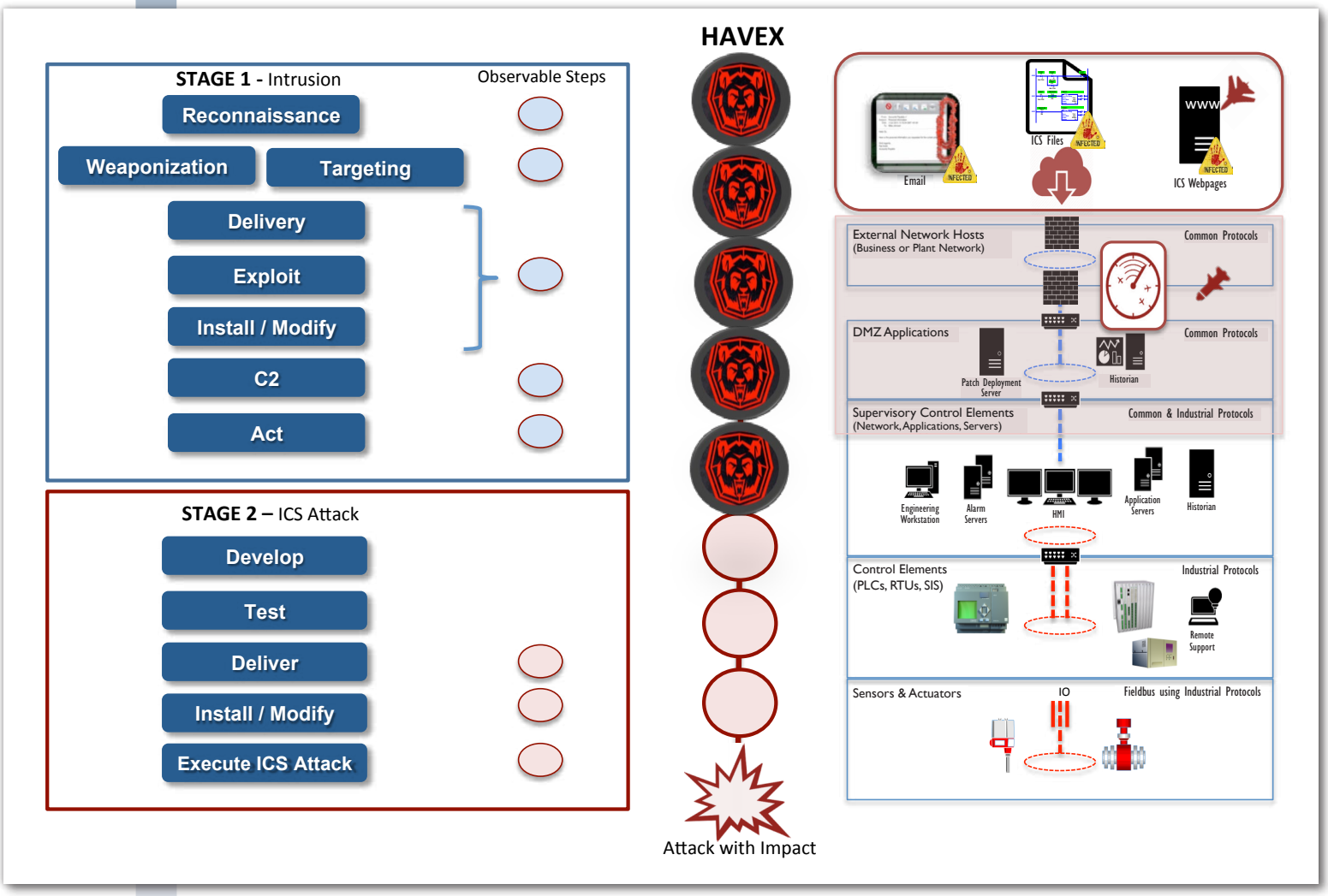

Figure 6. Havex Compared to the ICS Cyber Kill Chain and the Purdue Model

Stuxnet

The Stuxnet malware, which has been reported to have physically destroyed centrifuges at the Natanz facility in Iran, serves as a great case study of an attack that took place over Stage 1 and Stage 2 of the ICS Cyber Kill Chain.[11] Stuxnet was mostly observed in 2010; however, it was a campaign that may have taken place over a number of years, with earliest estimates around 2006 and 2007.[12] Over that period of time, the actor went to a significant amount of effort to create a highly targeted attack that was able to physically destroy specific centrifuges. This intelligence-gathering period is best understood through Stage 1 of the ICS Cyber Kill Chain.

The actors behind the Stuxnet campaign may have performed reconnaissance to identify potential paths to the Natanz facility. However, experts have speculated that there may also have been a physical component to the reconnaissance to gain such intimate data about the facility.[13] It is always important to consider the impact of the physical security component, as well as geopolitical tensions. For example, the Iranian uranium enrichment program at Natanz was of significant concern for various countries in the world, and the purpose and location of the Natanz facility was publicly leaked by a dissident group in 2006.[14] That, along with other non-cyber data, likely significantly contributed to the actor's *planning* and *reconnaissance* efforts. Additionally, the Natanz facility reportedly had an air-gapped network that did not allow for using traditional methods to compromise the ICS over network connections. Instead, it could have been an insider threat that, knowingly or unknowingly, compromised the network through the use of an infected engineering laptop or removable media device, such as a USB.

The *weaponization* would have been the malware's code combined with the exploits that were placed onto the laptop or removable media. The removable media or laptop then acted as the *delivery* mechanism to *exploit* the Natanz network. Then, Stuxnet installed itself on various versions of Windows systems and repeated the exploit and *install* phases, compromising a number of systems until it could activate Internet access and reach out to the attacker's C2 servers.

[11] "To Kill a Centrifuge," Ralph Langner, November 2013: www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

[12] "Duqu and Stuxnet Not the Only Malicious Programs Created by the Responsible Team," Kaspersky Lab's Virus News, 29 December 2011: www.kaspersky.com/about/news/virus/2011/Kaspersky_Lab_Experts_Duqu_and_Stuxnet_Not_the_Only_Malicious_Programs_Created_by_the_Responsible_Team

[13] "The Real Story of Stuxnet," David Kushner, 26 February 2013: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[14] "As Crisis Brews, Iran Hits Bump in Atomic Path," William J. Broad and David E. Sanger, 5 March 2006: www.nytimes.com/2006/03/05/international/middleeast/05iran.html?pagewanted=all

This version of Stuxnet, at the time, may not have had any ICS-specific payload. The gathering of information about the environment and exfiltration of that to the C2 servers or by other means were the material actions that took place in the Stage 1 *Act phase*. Investigators believe a large amount of data was collected over many years, so that the adversary knew the ICS and its network as well as, if not better, than the engineers and operators on site.[15]

During the second stage of the ICS Cyber Kill Chain, the attacker developed and tested an update to the Stuxnet malware that would impact the ICS. Once the capability was ready, the attacker delivered it to Natanz. There are a number of methods that could have been the delivery mechanism, but the engineering workstation or USB method is the most common theory. Additionally, the attack had provisions to continually deliver and install itself throughout the environment until it found its appropriate targets: One updated sample of Stuxnet would move throughout the network, find older versions of the malware that did not have the newly developed ICS attack modules, and have those older versions update to the newer version of Stuxnet. Once Stuxnet was on the correct targets, a WinCC SIMATIC server connected to specific Siemens controllers with other specific conditions, it then performed the *Execute ICS Attack phase*. The impact of this attack was the modification and manipulation of the process and systems to force the centrifuges being controlled into physically destroying themselves.

[15] "W32. Stuxnet Dossier," Nicolas Falliere, Liam O Murchu and Eric Chien, February 2011: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Case Studies Examined with the ICS Cyber Kill Chain
(CONTINUED)

In the Stuxnet campaign there is a completed two-stage ICS attack that led to the highly tailored and impactful manipulation of the process to cause physical destruction. The campaign ultimately reached all layers of the Purdue Model and represents a worst-case scenario of a completed ICS Cyber Kill Chain against a victim. The attack is mapped to the Purdue Model and illustrated in Figure 7.

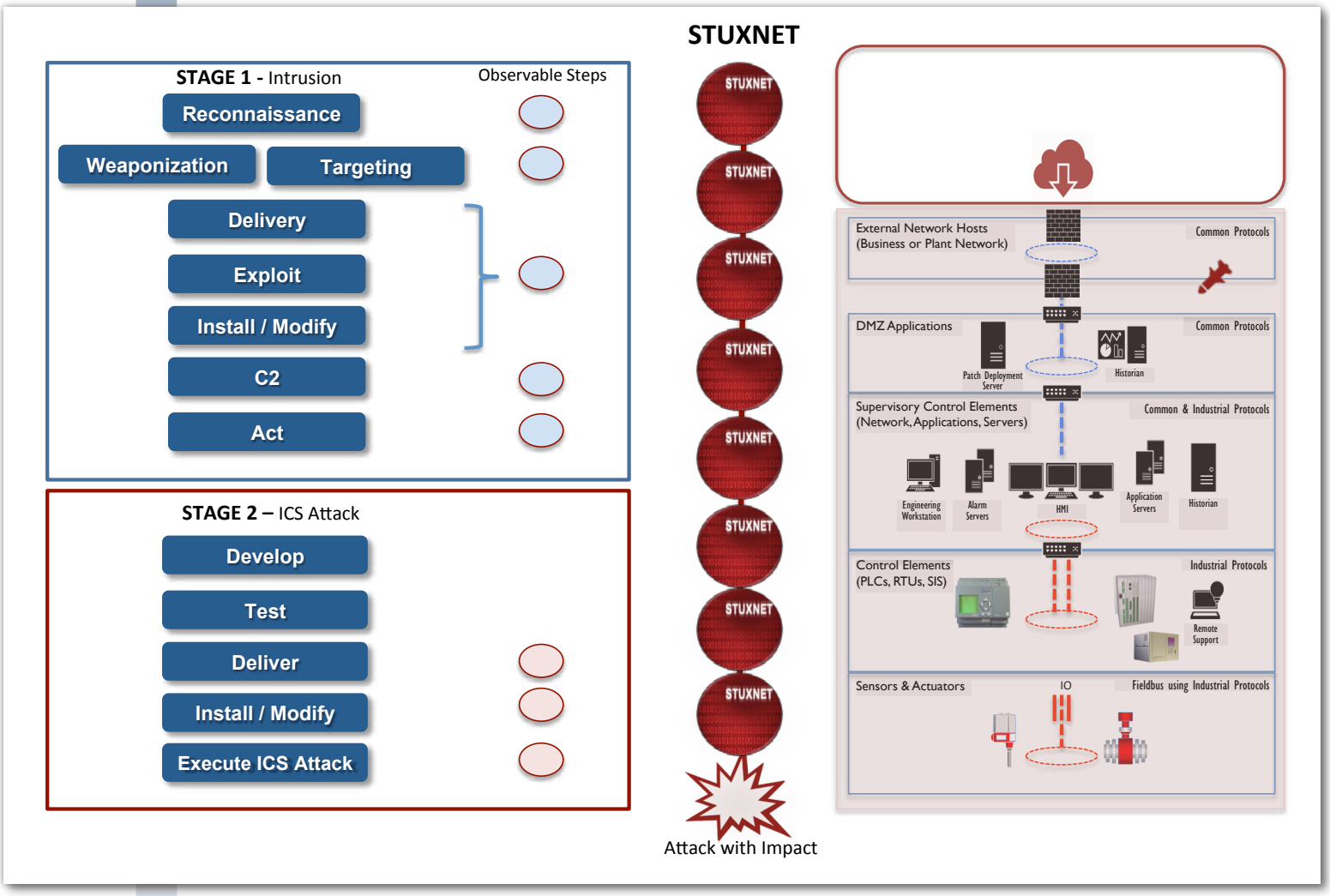

Figure 7. Stuxnet Compared to the ICS Cyber Kill Chain and the Purdue Model

Conclusion

The ICS Cyber Kill Chain is a model that builds upon the traditional understanding of a cyber kill chain and tailors it to adversary attacks on ICS. The model provides defenders an opportunity to better understand the phases of an adversary's campaign into an ICS to identify opportunities for detection, remediation and defense. These opportunities for success also highlight that ICS networks are more defensible than traditional IT networks and stress the importance of maintaining this defensible architecture through actions such as limiting the integration of safety systems with operations networks and removing ICS components from direct Internet access.

There are a growing number of models for ICS defenders to apply against the concepts revealed in the ICS Cyber Kill Chain. For example, the Sliding Scale of Cyber Security[16] added a nuanced discussion to resource investments and defender actions that can be implemented to protect the safety, security and reliability of operations. Models mapped to this sliding scale, such as the Active Cyber Defense Cycle[17] and Defense in Depth concepts, are all vital for defense.[18] With these emerging models and with the appreciation of the adversary's ICS Cyber Kill Chain, ICS security personnel can learn a great deal and leverage their knowledge to advance the security of the ICS community.

Follow us on Twitter for additional updates:
https://twitter.com/SANSICS
https://twitter.com/robertmlee
https://twitter.com/assante_michael

[16] "The Sliding Scale of Cyber Security," Robert M. Lee, August 2015: www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

[17] The Active Cyber Defense Cycle is the subject of the SANS ICS515 course, "Active Defense and Incident Response": www.sans.org/course/industrial-control-system-active-defense-and-incident-response#__utma=195150004.1660189780.1433250549.1443043898.1443051215.56

[18] The ICS Cyber Kill Chain and the models for defense mapped to the Sliding Scale of Cyber Security are included in the 2015 SANS ICS "Sliding Scale of Cyber Security" poster: https://ics.sans.org/resources/ics-security-resource-poster

About the Authors

Michael Assante is currently the SANS lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security and co-founder of NexDefense, an Atlanta-based ICS security company. He served as vice president and chief security officer of the North American Electric Reliability (NERC) Corporation, where he oversaw industrywide implementation of cybersecurity standards across the continent. Prior to joining NERC, Michael held a number of high-level positions at Idaho National Labs and served as vice president and chief security officer for American Electric Power. Michael's work in ICS security has been widely recognized, and he was selected by his peers as the winner of Information Security Magazine's security leadership award for his efforts as a strategic thinker. The RSA 2005 Conference awarded him its outstanding achievement award in the practice of security within an organization.

Michael has testified before the U.S. Senate and House and was an initial member of the Commission on Cyber Security for the 44th Presidency. Before his career in security, he served in various naval intelligence and information warfare roles, and he developed and gave presentations on the latest technology and security threats to the chairman of the Joint Chiefs of Staff, director of the National Security Agency and other leading government officials. In 1997, he was honored as a Naval Intelligence Officer of the Year.

Robert M. Lee is a SANS certified instructor and the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. He is also the CEO and founder of the critical infrastructure cybersecurity company Dragos Security LLC, where he has a passion for control system traffic analysis, incident response and threat intelligence research. Robert is a non-resident National Cyber Security Fellow at New America, focusing on policy issues relating to the cyber security of critical infrastructure, and a PhD candidate at Kings College, London. For his research and focus areas, he was named one of Passcode's Influencers and awarded EnergySec's 2015 Cyber Security Professional of the Year.

Robert obtained his start in cyber security in the U.S. Air Force, where he served as a cyber warfare operations officer. He has performed defense, intelligence and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as Control Engineering and the Christian Science Monitor's Passcode and speaks at conferences around the world. Lastly, Robert, is author of the book SCADA and Me and the weekly web-comic www.LittleBobbyComic.com