GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

The Perfect ICS Storm

GIAC (GCIA) Gold Certification

Author: Glenn Aydell
Email: graydell@mastersprogram.sans.edu
Advisor: Chris Walker
Accepted: May 15th, 2015

Template Version September 2014

Abstract

As manufacturing Industrial Control System (ICS) architectural designs have evolved from isolated and proprietary systems with physical separation to a layered architecture using more standard IT components to the latest "trend" of Industrial Internet of Things (IIoT); so too have the challenges associated with securing these environments. Stir in a little concept know as Internet off-loading and the environment becomes ripe for a "Perfect ICS Storm". Conflicting concepts of isolation vs convergence and centralized vs distributed lead to a complex array of security concerns. This paper will pull together some of the detection and response challenges which should not be overlooked as the architectural landscape continues to evolve.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

The movie "The Perfect Storm" (Petersen, 2000) tells the story of a fishing vessel (the Andrea Gail) caught at sea in the midst of a storm composed of three weather fronts. This historic weather event created what is considered to be one of the worst storms in modern history. The result of the storm proved catastrophic for the Andrea Gail and its crew. Like the Andrea Gail, many ICS environment appear to be on a collision course with three contrasting forces. Whether or not the ensuing ICS storm proves to be catastrophic will depend greatly on our ability to learn from past mistakes.

While most security professionals are well aware of the ever-changing threats to typical IT assets, until recently (relatively speaking) most thought little of threats to industrial control systems (ICS). These environments were long thought to be proprietary and isolated. Running on expensive, vendor supplied components that encompassed everything from the field device to the human machine interface (HMI), they used technology such as dedicated two wire 4-20mA analog signals to control things like pneumatic valves. Many of these systems predate DOS and have been in service longer than the average cyber security professional has been alive.

Though change was slow and the publicity limited, customer demands for more cost effective and standard ICS solutions were heard. Vendors began offering components more in line with commercial off the shelf IT infrastructure. Although the components became more standard, the lifecycle demands remained extended. Instead of a 3-5 year lifecycle as is common for many standard IT components, the ICS lifecycle demands of 15-20 years led to security challenges that would lay dormant for years.

1.1. The Impact of Stuxnet on ICS Security

In 2010, Stuxnet changed everything in the realm of ICS security. From professional hacker to script kiddy, the world began to take note as the realization began to sink in. Media outlets from Wired (Zetter, 2010) to CNN (Benson, 2010) took note. Those mysterious devices that control things like power plants, robotics, manufacturing plants and even uranium enrichment centrifuges are using the same low cost computers and operating systems as your typical office network.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Hackers (good and bad) who may have never considered the thought that critical ICS components would rely on Windows as an underlying OS suddenly became interested in 'breaking' ICS systems for fun and profit. Researchers looking to improve industrial security, or land big budgets for projects, became interested in identifying vulnerabilities in ICS components and publishing the results. Script kiddies who noticed an increase in 'SCADA' exploit modules within the Metasploit framework (from 7 before Stuxnet to 57 as of this writing), became interested in this 'new' and different world. Opportunistic security professionals, looking for a new revenue stream, became interested in 'branching out' into a new industry created by the media fueled paranoia.

Even with all the hype as vulnerabilities are identified and exploits written, there was still a challenge. What good are exploits without targets? How useful is a Metasploit exploit for a Modicon PLC or a Citect SCADA if you don't know where to use it?

1.2. The Impact of Shodan on ICS Security

Though many individuals and companies have attempted to 'map' the Internet for various reasons, none has had as significant an impact on ICS security as Shodan. (Shodan, n.d.) Shodan is a search engine similar to Google, Bing and Yahoo, the difference being these powerhouse search engines index Internet web content whereas Shodan indexes headers. The Internet is primarily made up of content on sites intended for human consumption. News articles, blogs, images, advertisements and more are examples of the web content intended for user viewing.

The headers, on the other hand are primarily intended for computer consumption. Headers are the identifying fingerprints of systems that support user applications, like a web browser, present the web content. While using a content search engine like Google to search for the term "google", one would expect to find lots of information (web content) related to Google as a company. A Shodan search for "google" would return very different results as any appliance or service with the word "google" in the banner or header would be displayed. Where the content search may reveal the company's recent stock price or the latest news stories, Shodan would reveal the IP address of Google appliances on the Internet. Shodan finds those 'hidden' nuggets of information about the

© 2015 The SANS Institute Author retains full rights.

underlying system services, indexes them and makes them searchable. As a result, our quest to find a Modicon PLC or Citect SCADA to accompany that shiny new exploit is now just as easy as using Google to search for reviews for the latest action movie.

Joshua Wright has a saying that goes something like this: "Vulnerabilities will remain until tools exist to expose them." (personal communication, 2011) He used this saying in the context of WiFi vulnerabilities, but it applies in this case as well. Shodan is not a tool to expose the vulnerabilities in the underlying ICS software, but rather the architectural design flaws that put the systems containing the vulnerability at greater risk. It exposes a 'security through obscurity' mindset that depends heavily on hiding assets in plain sight. Shodan revealed many ICS devices with little or no security controls (more on this later) connected directly to the Internet. Although this practice violates even the most basic layered architectural design, it points to a trend that Joshua Wright voices regarding WiFi security – humans are prone to repeat past mistakes.

Some like to quote Einstein as defining insanity as doing the same thing over and over and expecting different results. Although this quote cannot be directly attributed to Einstein, it does appear to fit the field of cyber security. Often convenience wins out over security leading to unintentional risk.

2. Layered Architecture

Layered architectural design is a key component of secure IT infrastructure. The concept of segmenting environments into different levels of trust is incorporated into even the most basic home use router. When applied to the corporate environment, breaking the concepts down into inbound and outbound communication makes them easier to visualize. The direction of the communication is from the standpoint of the client. A workstation within company 'A' traversing the corporate network to access the Internet hosted portal of company 'B' would be considered 'outbound' for company 'A' and 'inbound' for company 'B'.

2.1. Inbound Communication

Since Internet hosting became popular, the concept of layered network architecture for inbound communication has been essential. Firewalls are installed to

© 2015 The SANS Institute Author retains full rights.

protect Internet facing web servers. The web servers present end users with information they receive from application servers. The application servers turn raw data pulled from backend database servers into usable information by manipulation and contextualization of the data. The entire environment is protected from the office network by another firewall (see figure below).

No traffic is allowed to circumvent predefined pathways. In this approach, the database servers contain the "high valued" data and are considered the primary target of interest. The data housed on these servers is never directly exposed to the Internet, but rather retrieved by an application server and presented through a web interface.

This layered network approach creates known points of intersection and communication. These well-known and predictable pathways led to better control over data flow allowing intrusion detection and response to focus on key components and traffic patterns.

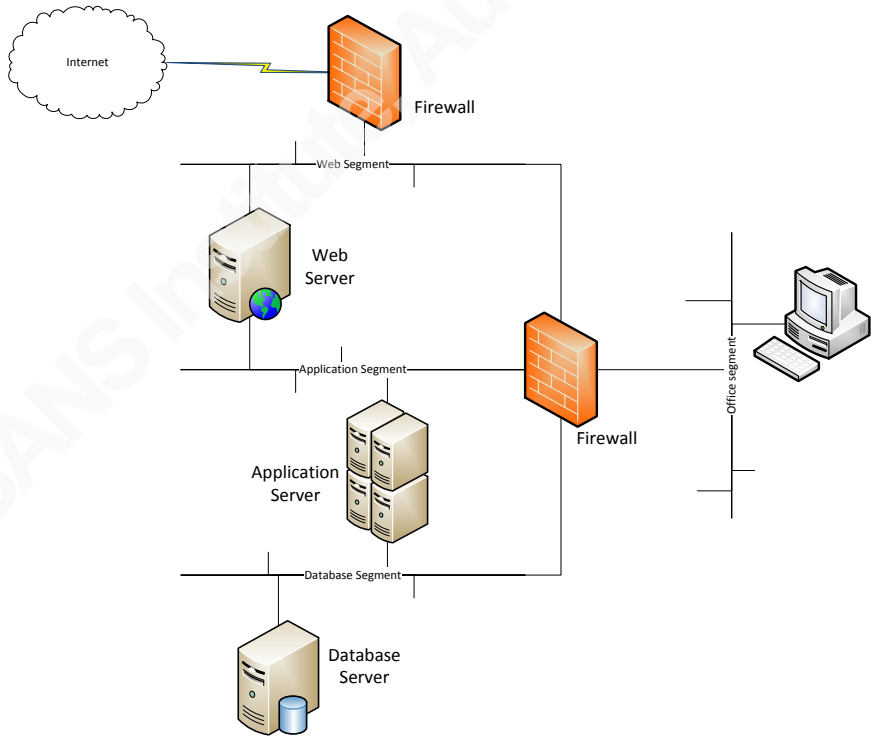

Figure 2-1 - Simple Web Hosting Layered Architecture

© 2015 The SANS Institute Author retains full rights.

2.2. Outbound Communications

For many years, outbound traffic was viewed by organizations as relatively benign. Aside from the requirements of HR departments to restrict employee access to "inappropriate" Internet content, the traffic was not considered a significant concern to the overall security of the corporation. Over time, this changed as companies realized the "weakest link" in securing the environment is not the perimeter, but rather the end user. Attack campaigns began focusing on users with great success. Legal departments became concerned as they realized a compromised internal workstation could be used to attack others that could expose the organization to legal liability for damages caused by the compromised company asset (O'Reilly, 2013). This led to changes in outbound infrastructure designs which included the incorporation of multiple detection and defensive layers such as intrusion detection systems (IDS); application layered proxies; DNS segregation and logging; botnet detections systems; and other components positioned at the company's perimeter or Internet aggregation points to address the rise of these user targeted attacks.

Similar to the inbound design, these revisions to outbound network designs create known communication channels allowing intrusion detection and response to focus these channels to identify and react to suspicious activity.

2.3. Defense in Depth Strategy

One key to a layered defense is the concept of "defense in depth". This concept can be a little confusing as some view defense in depth and layered network architecture as synonyms. A solid defense in depth strategy would include a layered network architecture; however, this would make up only one component of the overall defense in depth strategy. "20 Critical Security Controls for Effective Cyber Defense" (SANS Institute - Critical Security Controls) offer a good representation of a solid defense in depth strategy. The strategy can be summarized as:

- Know what you wish to protect – know your assets and who is authorized to access them.
- Prevent what you can – where feasible, implement cost effective controls to prevent attacks.

© 2015 The SANS Institute Author retains full rights.

- If you can't prevent, detect – where circumstances preclude the implementation of prevention controls, implement cost effective detection countermeasures.
- If you can't detect, react – where circumstances prohibit the implementation of detection countermeasures, implement cost effective reactionary compensating controls.
- If you can't react, recover – where circumstances prevent the implementation of reactionary measures, implement cost effective recovery countermeasures.
- If you can't recover, rethink defense strategy – where circumstances prevent the implementation of recovery countermeasures, rethink the defense strategy.

2.4. Kill Chain Model

One approach in the area of layered defense involves a concept known as a kill chain model (Martin, n.d.). This model breaks down an attack into a sequence of logical stages:

- reconnaissance => identification of target(s) and vulnerabilities
- weaponization => coupling of exploit with remote access functionality
- delivery => transmission of 'weapon' to target environment
- exploitation => activation of the 'weapon' in target environment
- installation => installation of persistent access tools
- command/control => communication to attacker's control environment
- objective actions => attacker's objective achieved

These stages make up a 'chain' of events required for the successful achievement of the attacker's objective. Breaking the chain prevents the attacker's objective from being met. This model allows for the creation of an active defense or action matrix to detect, deny, disrupt, degrade, deceive, or destroy the attack. Within the model it becomes important to identify the links in the chain where the defensive strategy can be most effectively implemented.

2.5. Standard IT vs ICS

Many of these concepts were developed to secure standard IT environments with a focus on protecting data. How do standard business IT and ICS differ?

As the use of standard IT components grew within the ICS environment, so too did the misconception that IT and ICS had the same security requirements. Two

© 2015 The SANS Institute Author retains full rights.

interesting differences between standard 'office' IT and ICS emerged: (1) the view of the CIA triad and (2) the physical consequences of a security failure.

Though exceptions exist, most standard IT environments view the CIA triad in the order of confidentiality, integrity and availability. A two hour delay in accessing email once a month during the regularly scheduled IT maintenance window as patches are applied to the email servers may be inconvenient to an end user, but in most cases would not significantly disrupt the business. The users irritation of having patches pushed down to a workstation and forcing a reboot during working hours is seen as a minimal and acceptable level of disruption for typical IT environments to ensure the security of the environment as a whole.

The same cannot always be said for ICS environments. In most cases, ICS views the CIA triad in exactly the opposite order (availability, integrity, confidentiality). Eric Cosman is well known for his work in the area of ICS security. He put it best by asking the question: "Would you want a pilot locked out of the controls of the plane or have the system reboot while in the middle of trying to land?" In many industries, the operators of the ICS are managing "controlled explosions". Disruptions in these environments can have a very serious impact and not just on data. (personal communication, 2014)

This leads to the second difference, the physical consequences of a failure. ICS environments influence the physical world. The NIST Special Publication 800-82 Rev 1 – "Guide to Industrial Control System (ICS) Security" (Stouffer, Falco, & Scarfone) cites multiple intentional and unintentional incidents involving ICS. Two noteworthy incidents taken directly from the document are:

> **Worcester Air Traffic Communications[4].** In March 1997, a teenager in Worcester, Massachusetts disabled part of the public switched telephone network using a dial-up modem connected to the system. This knocked out phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. Also, the tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress. The attack also knocked out phone service to 600 homes and businesses in the nearby town of Rutland.
>
> **Maroochy Shire Sewage Spills[5].** In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a two-month period, the disgruntled rejected

© 2015 The SANS Institute Author retains full rights.

> employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.

These two intentional acts highlight the adverse impact ICS can have on the "real" world.

To compound the problem, many ICS components are "not secure"; but that's not the real concern. According to Dale Peterson of Digital Bond, they are "insecure by design". (Peterson, 2011) The underlying communication for many ICS protocols assumes the operating environment is trusted. When these environments were completely isolated island networks, this practice was considered acceptable. As lines begin to blur between IT and ICS, the level of trust of the environment decreases, which exposes fundamental flaws in the underlying protocols. Throw into the mix the extended lifecycle of ICS (15 to 20 years) as compared to standard IT lifecycle (3 to 5 years) and we see a 4 to 5 factor rate of change related to technology used in these two environments. To put it into perspective, many of these "insecure by design" components are likely to still be in use, long after Windows 10 is end of life.

2.6. Contrasting ICS Systems

It is clear that IT and ICS differ, but what about ICS within different industries? ICS is a generic terms that incorporates many different components (similar to Metasploit's use of the term 'SCADA'). ICS is used in many different industries - from small municipal water treatment facilities to the national power grid; from a facility blending paint to the manufacturing of pharmaceuticals; from local traffic lights to air traffic control; from manufacturing vinegar to cracking natural gas; from mixing cement to drilling for crude oil. This is only a short list of examples but with such vastly different use cases, ICS security is difficult to generalize. The threat to an environment depends heavily on outside influences. A small water company operating a remote PLC controlling a floodwater overflow valve in the foothills of sparsely populated region will face different threats than a nuclear power plant near a large city. This does not mean the consequences of a failure would be any less tragic, but the impact and the resources required to defend differ significantly.

© 2015 The SANS Institute Author retains full rights.

With so many different industries represented by the term ICS, it would be impossible in such a brief document to cover all views. As such, the focus herein will be with respect to manufacturing.

2.7. The Purdue Model

For manufacturing, one of the most commonly referenced architectural models is referred to as the "Purdue Model" (Purdue Research Foundation, 1989). This model finds its origin in the publication "A Reference Model For Computer Integrated Manufacturing (CIM)" prepared by the CIM Reference Model Committee of the International Purdue Workshop on Industrial Computer Systems and first published in 1989. This CIM reference model was originally intended to open the door to automation through computer integrated manufacturing for *automatable* functions.

With respect to modern manufacturing, the Purdue Model has taken on a life of its own. A Google image search reveals a plethora of differing perspectives and representations of the model. The model has also been the basis for other publications such as ISA-95 and has greatly influenced industry standards like IEC62443.

As it relates to this writing, the Purdue Model is being viewed primarily from a security perspective with a focus on a layered network architecture. As a result, the Internet connected ICS components discussed within the earlier Shodan section represent a violation of this basic layered architecture approach.

2.8. Recommended Defense in Depth Model

In 2009, the US Department of Homeland Security published the "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies" (US Department of Homeland Security, 2009). This document expanded on the foundation set forth by the Purdue Model and provided additional security considerations including the recommended architecture shown below.

© 2015 The SANS Institute Author retains full rights.

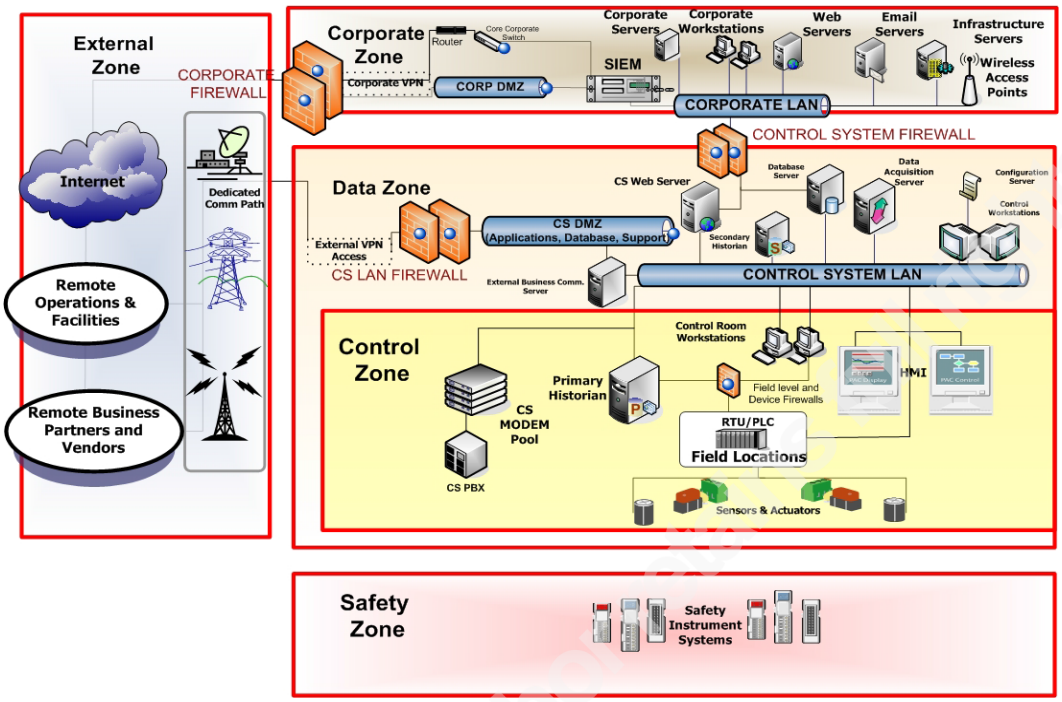

Figure 2-2 - Complete ICS Layered Architecture (US Department of Homeland Security, 2009)

By incorporating multiple layers of defense and detection between external threats and the components making up the ICS, the model strives to reduce the risk of compromise by limiting exposed services.

2.9. Military Analogy

The concept of 'defense' brings to mind a military setting. Some of the most vivid and entertaining of these settings are brought to life through books and movies. To highlight the importance of a defense in depth model, it is often easies to compare 'virtual' concepts in cyber security to 'real' concepts in warfare.

2.9.1. Components of Defense

Drawing on this visualization concept, we can take some of the defensive components of war and map them to similar representations of cyber defense.

- Spies => threat intelligence feeds – These assets represent the first line of defense. The intelligence gathered will influence policy and alert the kingdom/company of emerging threats.
- Outposts => IDS – These assets would help detect the approaching threat and trigger actions necessary to keep the kingdom/company safe.

© 2015 The SANS Institute Author retains full rights.

- Intelligence agency => Logging and SIEM tools – These assets would correlate the data into usable and actionable information to aide in the planning of the defense.
- Countrymen => end users awareness training – The well informed community keeping a keen eye out for suspicious behavior can help detect threats early enough to react making them valuable to the defense of the kingdom/company.
- City Gates => firewalls or other aggregation points – These assets serve to funnel traffic into defensible areas.
- Trained military => trained security professionals – These assets are constantly training for battle to ensure the best opportunity for victory.
- Country => office network – This would be the where most of the citizens spend the majority of their time supporting the kingdom/company.
- Castle => manufacturing network – This would represent the core functions of the kingdom where the most important supporting assets reside.
- Crown Jewels => ICS – These assets would represent the most value to the kingdom/company. If these are lost, the kingdom may fall.

Though this is fun, the mappings are subjective and it's not a very fair or realistic analogy. It does however help visualize the importance of different layers of defense all working together to compensate for the shortfall of other components to create a mesh of protection.

2.9.2. Speed of Attacks

In warfare, it would take months or even years to assemble an army to initiate an assault. In the cyber battlefield, things can happen at a much faster pace. A cyber attack can traverse the entire kill chain, from reconnaissance to objective achieved, as quickly as it takes for a user to click on a malicious link. This abbreviated defensible window makes it very important to put as many layers as possible between the attacker and the ICS. The more isolated the target is from the attacker, the more likely one of the layers of defense will detect the attack before harm is done.

3. Industrial Internet of Things (IIoT)

The Internet is obsessed with the "Internet of Things" (IoT). The concept of everything from the smallest home appliance to the most extravagant home security system being "connected" with the ability to communicate and share data brings to mind

© 2015 The SANS Institute Author retains full rights.

the making of a scary science fiction movie where machines take over the world. But this is no movie; it's quickly becoming a potential reality.

3.1. IoT vs IIoT

With the popularity of IoT comes the misconception that IoT and IIoT serve similar functions but with more "industrialized" tolerances. Industrialized usually refers to a more rugged design capable of withstanding extreme conditions or capable of being used in incendiary area classification ratings. But these minor distinctions are not the primary differentiating factors between IoT and IIoT. Like the comparison of standard IT to ICS, IIoT tends to be positioned in areas with "real" (physical world) consequences. Where IoT devices typically rely on the ability to communicate with each other and the Internet, IIoT components primarily focus on communicating within a fairly closed community of devices. An analogy can be drawn between the isolated environment legacy ICS components resided in and the architectural expectations for modern IIoT deployments. (Nagaraj, 2014)

3.2. Benefits

The benefits of IIoT depend heavily on the industry. As it relates to manufacturing, reliability and predictive maintenance are two driving forces. The ability to monitor real-time data from equipment, compare that data with similar components, trend key indicators for signs of wear, predict failures and schedule preventative maintenance before the failures occur, offer the potential for significant savings. Having a system automatically trigger the creation of work orders and ordering necessary replacement parts could alleviate mistakes and reduce scheduled down time. In an environment where profits are measured by the second as opposed to by the day, eliminating unplanned outages or reducing scheduled down time, can have a profound impact on profitability.

4. Internet Off-loading

With the migration to cloud services and the rapid expansion of Internet hosted media and e-learning, the question of bandwidth has become a considerable concern. When a home user can purchase outrageous Internet access speeds for less than a gym

© 2015 The SANS Institute Author retains full rights.

membership, they start to expect similar throughput capabilities from the office network. Unfortunately as costs for Internet access continues to fall, the cost for dedicated or MPLS circuits remain high. Adding to the challenge, Microsoft's O365 offering increases the demand and dependency on Internet based services. As companies begin considering their options, the concept of Internet Off-loading begins to build a case.

To better understand the challenge, we should examine a typical company. In a typical multi-office company, branch offices are connected to a central office via dedicated or MPLS circuits. These leased lines are managed and the security of the data 'guaranteed' by the service provider. The central office would be connected to the Internet with sufficient bandwidth to accommodate the entire company's needs. All Internet traffic from every branch office would traverse the dedicated connection to the central office before accessing the Internet. When the majority of traffic flowing over these dedicated links was for communication to internal resources such as an ERP or logistics system, this design was reasonable.

There has been a steady shift in business network traffic. Where once the most traffic was destined for internal resources; the majority of the traffic is now destined for the Internet. Internet bandwidth demands over dedicated WAN links have begun impacting internal business applications. This has brought to light the concept of Internet Off-loading.

Instead of increasing bandwidth on expensive dedicated WAN circuits, installing low cost Internet access at branch office locations can alleviate the need to backhaul Internet traffic. By only using the dedicated WAN links for internal traffic, WAN congestion caused by Internet-bound traffic can be reduced. This would allow for more cost effective use of the internal network.

5. Bringing Things Together in "The Perfect ICS Storm"

We'll set the stage by laying out a fictitious company named Acme Manufacturing Corporation. Acme manufactures multiple products in over 300 international locations. Acme has deployed a defense in depth strategy following the SANS 20 Critical Controls as well as layered network architecture similar to the DHS

© 2015 The SANS Institute Author retains full rights.

recommendations to protect the ICS environment. Inbound (hosted) applications residing in Acme's DMZ follow a layered network design with web application firewalls, HIDS and NIDS deployments. Outbound traffic is funneled through two Internet breakout points protected by application layer proxies requiring user authentication, inline malware and botnet detection services, split DNS with query logging enabled. All logs are centralized in an enterprise SIEM. All current ingress/egress Internet points consist of a DMZ sandwiched between firewalls where full packets are captured for both directions. There is no direct Internet access and no default route to the Internet. Internal traffic destined for non-internal IP address space is routed to a honeypot for analysis. The company's Internet breakout points are registered to Acme.

Acme did not deploy all their security architecture and detection/defensive layers in a single project. These layers evolved as the threat landscape changed. The environment is now relatively stable. Acme's security team is proficient and therefore priority incidents are at a minimum. The success is commendable, but sometimes success in the security field leads to complacency.

Acme management is proactive and the savings surrounding IIoT appear substantial. With the migration to O365 and the high cost of MPLS circuits, Internet off-loading could create additional savings. The decision has been made to move forward with both initiatives. The infrastructure and security teams are being asked to implement and secure the technologies.

5.1. IIoT Challenges

Acme's use case for IIoT involves predictive maintenance for rotating equipment. Management is interested in monitoring all rotating equipment and feeding the data to the manufacture's cloud-based analytics engine. The infrastructure and security teams will need to address two issues: (1) how will the communication from a field instrument to an Internet-based cloud service impact their interpretation and implementation of a layered network architecture and defense in depth model; (2) how will the unauthenticated outbound traffic from the IIoT devices impact their ability to attribute Internet activity to individual users?

© 2015 The SANS Institute Author retains full rights.

5.2. Internet Off-loading Challenges

Internet off-loading offers potential benefits, but those benefits come at a cost. Multiple layers of detection and defense exist at Acme's Internet breakout locations. It would be cost prohibitive to replicate these layers at every manufacturing location. Acme's infrastructure and security teams will need to identify compensating controls for the lost detection and defense layers Internet off-loading will create.

5.2.1. Internet routing challenge

Acme makes use of the private IP address space for internal devices. Internal routing tables include only internal networks. Site routers have a default route to a central router. The central router routes all non-internal traffic to a honeypot. By implementing Internet off-loading, the defensive technique will be less effective. Manufacturing site will maintain internal routing tables, but with their default route pointing to the Internet there is no way for the security team to distinguish between valid and suspicious traffic.

5.2.2. Proxy challenges

Acme's current Internet architecture takes advantage of clusters of active proxies in the DMZ of each Internet access location. Proxy logs are forwarded to Acme's SIEM tool for correlation, analysis and long term achieving. A central policy is used to implement HR requirements regarding internet activity tracking and content filtering. Acme has decided the implementation of a proxy at every manufacturing location would not be cost effective, so they will need to evaluate other options for addressing benefits provided by the proxy infrastructure.

5.2.3. DNS query log challenges

Within Acme's current infrastructure, all internal DNS queries are logged. These logs are forwarded to a SIEM tool which detects and alerts on queries to Internet hosts. Since all Internet traffic uses a proxy, all Internet DNS queries should originate from the proxy only. Any internal attempt to resolve an Internet host is investigated as suspicious. With this configuration Acme can identify misconfigured hosts, applications that are not proxy aware as well as malicious traffic. Moving forward with Internet off-loading will render this defensive technique less effective. Clients will need the ability to resolve

© 2015 The SANS Institute Author retains full rights.

Internet hosts. As a result, the identification of valid and suspicious DNS internal queries becomes more challenging.

5.2.4. Inline malware and botnet detection capabilities

Acme's security team considers APTs and botnets a serious concern. As a result Acme implemented inline malware and botnet detection capabilities. Being inline allows these appliances to help detect suspicious patterns in Internet bound traffic. A live feed subscription to the vendor's IOC signature database takes advantage of expertise beyond Acme's own security staff. The ability to add custom IOCs provide the security team flexibility to incorporate threat information for other sources to quickly react to emerging threats. This technology is cost prohibitive to deploy to every location. Alternatives will need to be found to address gaps in the security architecture as Internet off-loading renders these appliances less effective to Acme.

5.2.5. Advanced traffic analysis (full packet capture)

Acme found itself involved in an incident requiring forensic investigation of traffic patterns. At the time they were unsuccessful in recreating the necessary evidence so Acme implemented a full packet capture system at both Internet egress points. These captures are kept to aide in future investigations. With Internet off-loading, the security team will need to find cost effective alternatives for supporting future investigations.

5.2.6. IDS

With all user Internet traffic funneled through two known egress points, Acme has been able to implement a solid IDS infrastructure. The management overhead of deploying IDS sensors at every manufacturing location is cost prohibitive. Acme's security team is investigation other options.

5.2.7. Firewalled egress

Acme's current Internet egress points are protected by a DMZ sandwiched between two firewalls. It would not be cost effective to replicate this environment at every location, but Acme will be implementing a single firewall at each Internet egress. The firewall appliance selected bundles some advanced capabilities that may be called upon to address some security gaps. Transparent proxy with content filtering and

© 2015 The SANS Institute Author retains full rights.

IDS/IPS capabilities are the most promising options; but by clustering these detection and defense layers into a single platform, Acme is not achieving the full benefit of the defense in depth concept.

5.2.8. Attribution challenges

One of the challenges of incident response is the ability to quickly identify suspicious traffic and attribute that traffic back to a given source. With the sophistication of the attacker campaigns increasing, organizations can struggle to keep up with the latest indicators of compromise (IOC). As a result, many times malicious traffic may be detected by someone outside the organization before the organization is even aware of it. As command and control (C&C) servers are infiltrated or taken offline by officials, owners of infected systems attempting to communicate with these C&C servers are identified. Having an organization's Internet address space attributable to the organization makes it easier for officials to notify them of the compromise. With Internet off-loading, address space is attributable to an ISP instead of a specific company. This makes the identification and notification more difficult. For example, the ICS-CERT reported roughly 300 known Havex infected systems within the United States. Of these 300 infections, less than 2% of the infected individuals or companies were identified and notified of the infections. How might this impact the company's legal liability?

5.3. Combining IIoT and Internet Off-loading

Like the military analogy of placing the crown jewels as far away from the attacking army as possible, security professionals should strive to keep the ICS as far away from the attackers as possible. The architectural and communication requirements of these two technologies have the potential to chip away at a well thought out defense in depth architecture and unintentionally move the ICS closer to the attacker. If we tie this back to the kill chain model, one of the links in the attack chain is a communication path from the attacker to the target. As IIoT and Internet off-loading blur the lines between intranet and Internet traffic, so to do the lines (or layers) of defensive between the attacker and the target. The more these layers are eliminated, the more difficult the task of protecting the target becomes, especially as attacks evolve. Reliance on a single

© 2015 The SANS Institute Author retains full rights.

protection, regardless of the technology or architecture, will expose the ICS to risk. Whether that risk is acceptable will depend on the process controlled by the ICS.

6. Conclusion

IIoT and Internet off-loading can have a significant impact on the profitability of an organization. Unfortunately they can also have a significant impact on the security landscape as well. IIoT, Internet off-loading and ICS are not mutually exclusive. There may be environments where these three can coexist without a significant increase in the risk to the organization. Where the most costly result of an attack is the loss of data, it may be easier to blend all three.

Implementing IIoT or Internet off-loading alone in a low risk ICS industry would be difficult in and of itself. Combine either with the inherent risk of a manufacturing process with potential health or environmental consequences and the challenge increases significantly. Care should be taken to evaluate the total cost of ownership over the lifecycle of the technology; taking into consideration how technology changes may compound the challenges of securing the environment. It is important to know the assets and processes being secured to better evaluate an acceptable risk appetite for the organization and the surrounding community. Careless attempts to implement these (or other) technologies into a high risk manufacturing process can lead to disaster.

A storm is coming to the ICS world. Whether or not it turns out to be "The Perfect ICS Storm" will depend greatly on how organizations address the challenges of securing these new technologies. If we as security professionals are not vigilant in the pursuit of sound security practices with a defense in depth mindset, the ICS environment may suffer the same fate as the Andrea Gail. As tragic as that story was and without minimizing the suffering to those who lost loved ones, the impact on human life was minimal. If security professionals resort to valuing convenience over security and fail to protect the ICS from the impending storm, the results may not be so insignificant. Entire cities without power or clean water or cloud of HCL gas blanketing small towns bring to mind apocalyptic visions and mass panic.

Glenn Aydell

© 2015 The SANS Institute Author retains full rights.

In the ICS world, two areas of concern must be accounted for when designing a plant: (1) loss of visibility and (2) loss of control. New technologies like IIoT and Internet off-loading can introduce blind spots or create gaps in the organizations overall security architecture. These challenges must be accounted for with acceptable compensating controls before the decision to move forward with any new technology is made.

Another misinterpreted Einstein quote relates to training the mind to think as opposed to simply learning facts. The actual quote was talking about a college education, but the abridged version can hold true for security professionals. As with any security related topic, ICS relies heavily on technology; however, technology is not enough. Highly skilled security professionals with the ability to learn every aspect of the technology are not enough. The key to winning the battle of ICS security is the ability for security professionals to become educators; not necessarily in the formal sense, but as an ambassador for security within the organization. Gone are the days where security professionals can simply sit on the sideline waiting for an opportunity to play Monday quarterback. "I told you so" is no longer acceptable when you realize what is actually at stake.

Glenn Aydell

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

References

US Department of Homeland Security, (October 2009), *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

Purdue Research Foundation, *A Reference Model for Computer Integrated Manufacturing (CIM)*, Copyright © 1989 Purdue Research Foundation, ISBN 1-55617-225-7

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011, March). *Cyber Kill Chain®* · Lockheed Martin. Retrieved from http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

National Security Agency. (n.d.). *Defense in Depth*. Retrieved from https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Peterson, D. G. (August). *PLC's: Insecure By Design v. Vulnerabilities* « Digital Bond's SCADA Security Portal. Retrieved from (Peterson, 2011)

Stouffer, K., Falco, J., & Scarfone, K. (n.d.). *NIST Special Publication 800-82 Revision 1*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

Nagaraj, V. (2014, February 25). *The Industrial IoT isn't the same as the consumer IoT* - O'Reilly Radar. Retrieved from http://radar.oreilly.com/2014/02/the-industrial-iot-isnt-the-same-as-the-consumer-iot.html

Bradford, K. (2014, February 4). *The Industrial Internet of Things - The opportunity no one is talking about*. O'Reilly Radar Retrieved from http://radar.oreilly.com/2014/02/the-industrial-internet-of-things.html

Oberlaender, M. (2015, January 26). Norse – *IoT / IoE: If It Has an IP Address, It Can Be Hacked*. Retrieved from http://blog.norsecorp.com/2015/01/26/iot-ioe-if-it-has-an-ip-address-it-can-be-hacked/

Petersen, W. (Director). (2000). *The Perfect Storm* [Motion picture]. USA.

Shodan. (n.d.). Retrieved from https://www.shodan.io/

SANS Institute - Critical Security Controls. (n.d.). Retrieved from https://www.sans.org/critical-security-controls/

© 2015 The SANS Institute Author retains full rights.

Zetter, K. (2010, November 15). Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage | WIRED. Retrieved from http://www.wired.com/2010/11/stuxnet-clues/

Benson, P. (2010, November 18). Computer virus Stuxnet a 'game changer,' DHS official tells Senate - CNN.com. Retrieved from http://www.cnn.com/2010/TECH/web/11/17/stuxnet.virus/

Wright, J. (Instructor) (2014 March 7) SEC 617: Wireless Security. SANS 2011 Orlando, Lecture conducted from SANS Institute, Orlando, FL.

O'Reilly, D. (2013, April 2). How you may have inadvertently participated in recent DDoS attacks - CNET. Retrieved from http://www.cnet.com/how-to/how-you-may-have-inadvertently-participated-in-recent-ddos-attacks/

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.