Control Systems Security Program/ ICS-CERT

June 2012 Issue

# ICSJWG QUARTERLY NEWSLETTER

— ICSJWG EXPANDING THE COMMUNITY —

## ICSJWG 2012 Spring Meeting Report

The ICSJWG 2012 Spring Meeting was a great success! We thank all of the engaged participants who presented and supported the panels. The number of people in Savannah was at a record high and we are encouraged by the significant number of first-time attendees. We appreciate the input and discussions during the entire event. The continued contributions of industry and government professionals ensure that our mutual efforts to secure control systems will be successful. The presentations continue to illustrate and enhance the collaborative partnership fostered between federal agencies/departments and private asset owners/operators of industrial control systems.

Presentations with speaker release forms and the final agenda are posted to the ICSJWG site at http://www.us-cert.gov/control_systems/icsjwg/presentations/spring2012/agenda.html.

## ICSJWG International Partners Day

The inaugural ICSJWG International Partners Day was a tremendous success thanks to the knowledgeable contributors and active participants. More than a dozen countries sent representatives to attend this event. Many of the participants traveled thousands of miles to attend the event and all attendees were encouraged by the eagerness and commitment exhibited by their international peers to improve the security of industrial controls systems around the world.

The success of this inaugural event ensures that future International Partner Day events will continue to be hosted by the ICSJWG.

The final International Partners Day agenda and presentations may be found at http://www.us-cert.gov/control_systems/icsjwg/international-partners/agenda.html.

## About the ICSJWG

***The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC). The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure and key resources (CIKR) sectors between federal agencies and departments as well as private asset owner/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the facilitation and collaboration of the industrial control systems stakeholder community in securing CIKR.***

***For more information, visit http://www.us-cert.gov/control_systems/icsjwg/***

## Contents

*ICSJWG 2012 Spring Meeting Report... 1*

*ICSJWG International Partners Day..... 1*

*ICSJWG 2012 Fall Meeting Update..... 2*

*International Highlight Article - MPCSIE..... 2*

*Advanced Training Events Scheduled for Fiscal Year (FY) 2012..... 3*

*ICSJWG Subgroup Status..... 4*

*Homeland Security Information Network (HSIN) Portal..... 5*

*Participation is Key!..... 6*

*Industrial Control Systems Contributed Content..... 6*

*Blocking Malware Attacks on Programmable Logic Controllers of Industrial Control Systems..... 6*

*Defense in Depth is Key to Process and SCADA Security..... 7*

*ICS and SCADA Security Myth: Protection by Firewalls..... 12*

## *ICSJWG 2012 Fall Meeting Update*


Come to Colorado this October! The ICSJWG 2012 Fall Meeting will be held at the Grand Hyatt Denver on October 15 – 18, 2012. The ICSJWG Fall Meeting is open to all members interested in learning about cybersecurity issues facing the nation's critical infrastructure control systems. This is an excellent resource for government professionals (federal, state, local, tribal, and international); control system vendors and systems integrators; research, development, and academic professionals; and owners and operators (management, engineering, production, and IT). Meeting attendees will be able to discuss the latest initiatives impacting security of industrial control systems and will have the opportunity to interact with colleagues and peers who may be addressing the risks of threats and vulnerabilities to their systems.

There is no cost to attend the meeting sessions or any associated meetings and training. Travel, accommodations, meals, beverages, and other incidental expenses are the responsibility of the meeting participants and will NOT be covered by ICSJWG or the Control Systems Security Program (CSSP). Check out the ICSJWG site for meeting information and stay tuned for upcoming ICSJWG 2012 Fall Meeting announcements and "Call for Abstracts" information! http://www.us-cert.gov/control_systems/icsjwg/

## *International Highlight Article - MPCSIE*

In July, members of the Meridian Process Control Security Information Exchange (MPCSIE) will receive a questionnaire intended to help identify milestones, near-term goals, and key agenda items for in-person meetings to be held in the fall. The completed questionnaires will be due in August. Responses and feedback will be analyzed by the MPCSIE Working Group Program Office and used to develop the agenda and path forward. Members of MPCSIE should be on the lookout for the questionnaire and additional information by July 27, 2012.

## *Advanced Training Events Scheduled for Fiscal Year (FY) 2012*

CSSP is currently offering advanced cybersecurity training sessions at the Control Systems Analysis Center located in Idaho Falls, Idaho. These sessions provide intensive hands-on training in protecting and securing control systems from cyber attacks, including a realistic Red Team/Blue Team exercise that is conducted within an actual control systems environment. It also provides an opportunity for attendees to network and collaborate with other colleagues involved in operating and protecting control systems networks.

- **Day 1:** Welcome, overview of DHS CSSP, a brief review of cybersecurity for industrial control systems, a demonstration showing how a control system can be attacked from the internet, and hands-on classroom training on Network Discovery techniques and practices.

- **Day 2:** Hands-on classroom training on Network Discovery, instruction for using Metasploit, and separation into Red and Blue Teams.

- **Day 3:** Hands-on classroom training on Network Exploitation, Network Defense techniques and practices, and Red and Blue Team strategy meetings.

- **Day 4:** A 12-hour exercise where participants are either attacking (Red Team) or defending (Blue Team). The Blue Team is tasked with providing the cyber defense for a corporate environment and with maintaining operations to a batch-mixing plant and an electrical distribution Supervisory Control and Data Acquisition (SCADA) system.

- **Day 5:** Red Team/Blue Team lessons learned and roundtable discussion.

Below are the available advanced training events scheduled for the calendar year:

- **October 8-12**: Industry Partners

There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant.

As scheduled advanced training gets closer, an invitation along with a link to register for the course will be sent out and posted to the following website - http://www.us-cert.gov/control_systems/cscalendar.html. Please monitor the site periodically, as this schedule is updated as new courses are confirmed.

Register by clicking on the link provided on our webpage - http://www.us-cert.gov/control_systems/cscalendar.html. Registration is open approximately 2 months before the start of a class. Due to high demand, class size is limited to approximately 40 people with a maximum of 2 individuals per company per event. Classes fill quickly, so early registration is encouraged. Notification of cancellation is appreciated, with as much advance notice as possible so that others who wish to take the course can do so.

## *ICSJWG Subgroup Status*

Below is an update on the progress of the ICSJWG subgroups. If you would like to become a member of any of the subgroups, send an email with your contact information to icsjwg@dhs.gov or contact the co-chairs directly.


- **Roadmap to Secure Industrial Control Systems Subgroup**
  *GCC Co-Chair: Perry Pederson (Perry.Pederson@nrc.gov)*
  *SCC Co-Chair: Tim Roxey (Tim.Roxey@nerc.net)*

  The Roadmap subgroup has taken the first version of the *Cross-Sector Roadmap for Cybersecurity of Control Systems* to private, public, and government contacts within all Critical Infrastructure and Key Resources (CI/KR) sectors where it has been well received. Currently, activity is focused on developing a metrics plan to include in the next version of the document in order to make the Roadmap more robust.

- **Vendor Subgroup**
  *GCC Co-Chair: Marty Edwards (Marty.Edwards@dhs.gov)*
  *SCC Co-Chair: Eric Cosman (ECCosman@dow.com)*

  The Vendor subgroup revealed progress with all three of its subcommittees. First, the Improve Communications Subcommittee presented its final report and Tier-1 and Tier-2 recommendations to the ICSJWG leadership during the Spring Meeting and formally sunset. Secondly, the Vulnerability Disclosure Subcommittee presented the final draft of the Vulnerability Disclosure paper, which provides a consensus-based foundation for ICS vendors and integrators working to develop a vulnerability disclosure policy. The paper was approved by the Vendor Subgroup in June and will be posted to the DHS website soon.

  Lastly, the Cross-Vendor Subcommittee presented a draft position paper outlining the current landscape and direction that the ICS community should take to improve control systems security. The lead authors have been identified for the remaining five sections of the paper and the subcommittee intends to complete and present a final report during the ICSJWG Fall Meeting in October.

- **Workforce Development Subgroup**
  *GCC Co-Chair*: Keri Nusbaum (*Keri.Nusbaum@dhs.gov*)
  *SCC Co-Chair*: Michael Glover (*M.Glover@prime-controls.com*)

  The Workforce Development subgroup is currently working to map standards' requirements and Knowledge, Skills, & Abilities (KSAs) and consolidating these with the National Initiative for Cybersecurity Education (NICE) Framework. This will allow a comprehensive look at the state of the workforce and help develop alternatives which impact education and the application of expertise in all sectors involved with our nation's CI/KR.

- **Research & Development Subgroup**
  *GCC Co-Chair: Doug Maughan (Douglas.maughan@dhs.gov)*
  *Acting SCC Co-Chair: Zach Tudor (Zachary.tudor@sri.com)*

  The R&D subgroup met during the Spring Meeting in Savannah and discussed a variety of topics related to R&D requirements and plans including current DHS Science and Technology research projects as well as opportunities with industrial control systems security funded research projects. The subgroup is currently developing a re-occurring meeting schedule and is actively looking for an individual to fill the open Sector Coordinating Council (SCC) Co-Chair position on a permanent basis. If you are interested in this position please submit your request to icsjwg@dhs.gov.

## *Homeland Security Information Network (HSIN) Portal*

HSIN is the information sharing tool used by ICSJWG subgroup members. All subgroup members can stay abreast of upcoming meetings through the calendars and subgroup reference materials in HSIN (e.g., charters, meeting minutes, agendas, etc.).

In addition, the "Alert Me" feature notifies users of changes to the portal, which eliminates the need for users to constantly log in to find out if updates have been made. Alerts can be sent immediately, daily, or weekly. To sign up for alerts, click on the "Alert Me" link on the left-hand side of the ICSJWG homepage and choose your delivery option. ICSJWG subgroup members who still need access to HSIN can send an email to icsjwg@dhs.gov to request an account.

- **If you do not currently have a HSIN account**, please provide your name, company, contact information, critical infrastructure sector, and ICSJWG subgroup affiliations to icsjwg@dhs.gov.

At this time, DHS is not able to grant non-U.S. citizens or those residing outside of the U.S. and its territories access to the HSIN portal. The owners of the HSIN portal are reviewing sharing agreements concerning information posted to the site. Until that process is complete, international user accounts will be on hold. ICSJWG Communications will contact all international members immediately if there are new developments.

## Participation is Key!

Your participation and input is **critical** to the success of these subgroups and to the overall mission of the ICSJWG in coordinating cybersecurity efforts to secure industrial control systems across the nation's critical infrastructure. Please email the co-chairs or icsjwg@dhs.gov to get involved with one or more of the subgroups.

## Industrial Control Systems Contributed Content

ICSJWG is now accepting contributions from the community pertaining to control systems security for the September Quarterly Newsletter. If you want to submit an article for the September Newsletter, please email icsjwg@hq.dhs.gov, and we will take your submission into consideration for publication. The deadline for submissions for the September Newsletter is **September 10, 2012**.

Past ICSJWG newsletters are located on the CSSP website http://www.us-cert.gov/control_systems/icsjwg/index.html and in HSIN https://cs.hsin.gov/C10/C1/ICSJWG/Document%20Library/Forms/AllItems.aspx?RootFolder=%2fC10%2fC1%2fICSJWG%2fDocument%20Library%2fICSJWG%20Newsletters%2fICSJWG%20Quarterly%20Newsletter&View=%7b6F252F6A%2d18EB%2d447A%2d96D4%2d106024729AB9%7d.

Also, thank you to all members who contributed content for the June Quarterly Newsletter! The following content was submitted by members of the ICSJWG for publication and distribution to the ICSJWG community. Content and opinions are those of the authors and do not represent DHS opinions, endorsements, or recommendations. The advice and instructions provided in the contributed content should be confirmed and tested prior to implementation.

---

## Blocking Malware Attacks on Programmable Logic Controllers of Industrial Control Systems

*By: Alan Morris, Morris and Ward*

In mid-2010 Stuxnet malware in showed that the write-*always* memories of PLC could be changed, when at the nuclear enhancement plant in Natanz, Iran, Stuxnet changed the programming stored on the memories of the PLCs so as to cause the destruction of 1,000 uranium refining centrifuges, putting a halt to Iran's nuclear program. From 2005 to 2010 we had been working with write-*once* storage media for purposes of our patent for write-once, monitored media. We recognized the vulnerability of the PLC memories, as corroborated in the 2010 Symantec Dossier explanatory reports about the Natanz event. Our patent, which issued in 2010, is dedicated to digital storage on write-once monitored media. The patent claims apply to write-once, monitored storage media, as, for example, the media that ought to be utilized as memories for PLCs.

Write-once memories for PLCs will block malware, for once written-to, i.e., programmed, write-once memories cannot be written-to again. Ideally, the PLC that incorporates provision for interchangeable, preprogrammed write-once memories would be a modernized PLC having an exterior connection slot for the memory. But there are millions of extant PLCs with write-always, corruptible memories. Instead of replacing these extant PLCs, it will be far less costly to have fabricated an add-on, side-mount box having an external connection slot. The box would mount on the rack next to the PLC, with the necessary wiring accomplished in the back-plane.

Critical facilities such as nuclear plants, power plants, refineries, hydroelectric dams, electric grids, etc., all have their programming tightly controlled. For these facilities there would be ample time for programming of the needed new write-once memory.

Discrete manufacturing requires memory reprogramming for every new configuration of the production line, and the production line can change every few hours or every few days. However, with proper planning, a few hours' time would allow a needed new write-once memory to be prepared.

The push for increased productivity, using extensive network connectivity to the ICS, would not degrade the ultimate malware security provided by the write-once memories of the PLCs.
By messenger, the new write-once preprogrammed memory would be taken from the control room to the designated PLC, and inserted into the connection slot of the add-on box. At that point, the control room operator would confirm that the new memory inserted is the correct selected memory by monitoring, through cable connection, using a checksum program. All connections between the memory, the PLC, and the control room would be alarmed, as well as the memory itself as inserted into the connection slot.

The technology described is of low cost and is readily implemented.

---

## *Defense in Depth is Key to Process and SCADA Security*

By: Eric Byres, Tofino Security, Belden Inc.

Cyber security is becoming increasingly important for the modern SCADA and industrial control system (ICS). Without security, the reliability and safety of the entire industrial process can be at risk.

Unfortunately, good security doesn't just happen. It needs to be designed into the system, using proven security strategies and processes.

One of the foundation strategies is *defense in depth* – the idea that effective security is created by layering multiple security solutions, so that if one is bypassed, another will provide the defense.
The Defense in Depth strategy is not something unique to ICS/SCADA security. In fact, it is not even unique to cyber security. It is a military strategy that has been around since days of the Romans. If you search the Internet, the first definition you will find is the military one on Wikipedia:

*Defense in depth (also known as deep or elastic defence) is a military strategy; it seeks to delay rather than prevent the advance of an attacker, buying time and causing additional casualties by yielding space. Rather than defeating an attacker with a single, strong defensive line, defence in depth relies on the tendency of an attack to lose momentum over a period of time or as it covers a larger area.*

Countless battles have been lost because the law of "defense in depth" has been ignored. Carl von Clausewitz, a Prussian soldier and military theorist during the Napoleonic era stated: "*If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere*." So let's explore this idea and begin by looking at a military disaster where defense in depth was not used.

**The End of the Great War Led to a Fortress Mentality**

Let's travel back in time to France in November 1918. World War I, the greatest war the world has ever seen, has just ended and France is reeling from the devastation. The conflict has killed over one million French citizens, wounded a further four million and destroyed much of the countryside of eastern France. A fierce debate begins to rage - "*how should France ensure that another invasion of their beautiful country by the German armies never occurs again*?"

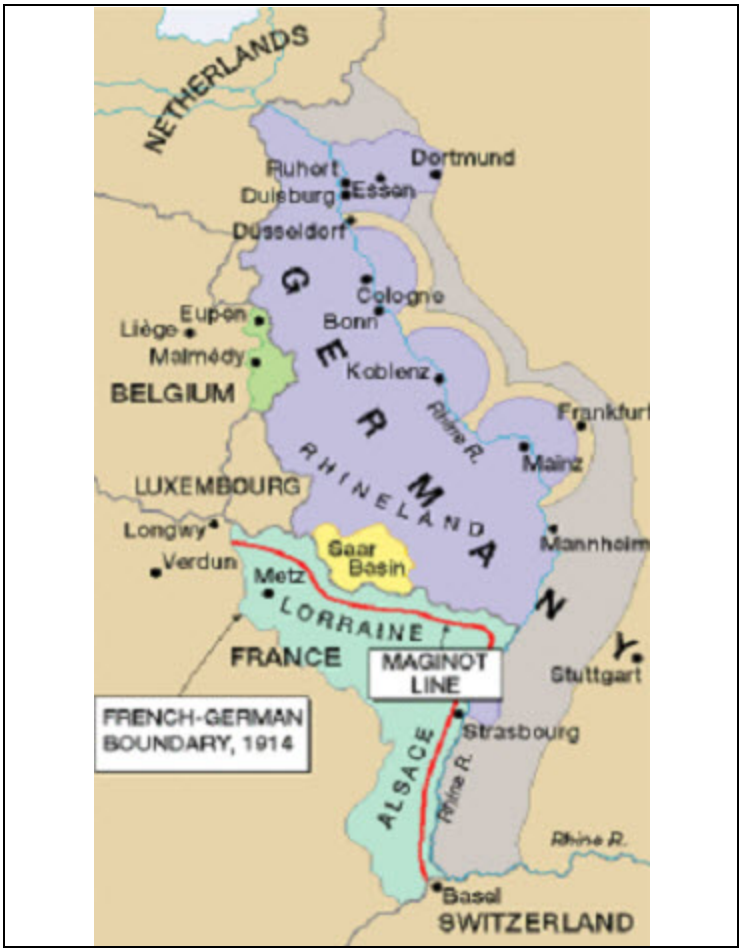
While there are a number of opposing ideas on how to achieve this, the one that prevails is to build a defensive line of fortresses along the border with Germany. Thus, between 1930 and 1936, the French government pours approximately three billion francs into building 400 miles of fixed concrete fortifications known as the Maginot Line. Everyone in France feels secure knowing that their country was safe behind the massive barrier of concrete and guns.

Then on May 10th 1940, Hitler attacks France. While a German decoy force sits opposite the Line, Hitler's second Army Group cuts through Belgium, the Netherlands and the undefended Ardennes Forest. These troops completely bypass the Line; within a week Nazi troops are deep inside France, and a month and half later France surrenders. The Line is only marginally involved in the fighting. What went wrong? The Line certainly achieved the task it was intended to do, namely preventing a direct assault against France's eastern border.

But France's strategic use of the Line was poor. As originally designed, the Maginot Line was supposed to be only part of a larger multilayered plan, involving other defenses and the French Army.

Instead, the mere existence of the Line gave French authorities a false sense of security. They based their entire defense strategy on this single solution, resulting in a quick and embarrassing defeat at the hands of the Nazis.

*Photo of the Maginot Line fortifications*




*Map of the Maginot Line*

**A Single Method of Defense Leads to a Single Point of Failure**

In the words of several historians "The Maginot Line did not fail France, but the 'Maginot mentality' did cause her defeat." It was the belief that a single very strong defence was good security. Basing a security design on hiding behind a single monolithic solution is known as the Bastion Model. It results in the possibility of a single point of failure. With the inevitable help of Murphy's Law, this single point will eventually either be bypassed (like the Maginot Line) or will experience some sort of malfunction. When it does, the system will be left wide open to attack.

In the same way, industrial security designs that assume all evil traffic will flow through a single choke point are succumbing to the same dangerous set of beliefs. Depending on a single firewall or data diode is building a security solution based on a single point of security failure. Only a proper defense in depth design, where the control devices and systems are both individually and collectively hardened, can provide reliable security for the plant floor.

**Defense in Depth - A Proven Security Strategy**

Clearly the Maginot Line is an example of what not to do when designing a security strategy. But what is an example of good security? For this, we will look at security in a bank and see what we can learn.

Ever wonder what it is that makes a typical bank so much more secure than a home or convenience store? It's not because banks have stronger steel doors or armed guards. Those help a bit, but are quickly offset by the fact that a bank's adversaries (i.e. professional bank robbers) are also better armed and more determined than the typical house burglar.

The first reason is that a bank employs *multiple security measures* to maximize its security. For example, to name a few defenses, a typical bank has steel doors, bulletproof windows, security guards, room sized safes, security boxes, alarm systems, cameras and security-trained tellers. Even more important, not only are there more defensive layers at a bank, but each layer is designed to address a specific type of threat at the point where it is employed. For example, bank doors are effective, but simple security devices. They are either locked or unlocked. They either grant or deny access to customers on an all-or-nothing basis – regardless of what a visitor looks like or how the visitor behaves.

One layer up is the security guards – they perform access control to 'clean' the general flow of people into the bank. They ensure that access to the bank is for people who have a legitimate need to be there and will 'behave' within expected norms. They regard each visitor based on specific criteria, such as, not wearing a mask, suspicious behaviour, acting erratically etc.

At yet another level, the tellers, security box keys, passwords, etc. keep these pre-screened customers from accessing other accounts or information. Rather than worrying if a visitor should or should not be in the bank, the tellers and passwords present a different layer of security: account security. These measures 'filter' what account access individual customers are allowed, based on who they are.

**More than Just another Layer**
The bank analogy points out three important aspects of Defense in Depth:

1. Multiple layers of defense. Do not rely completely on a single point of security, no matter how good it is.
2. Differentiated layers of defense. Make sure that each of the security layers is slightly different. This ensures that just because an attacker finds a way past the first layer, they don't have the magic key for getting past all the subsequent defenses.
3. Context and threat specific layers of defense. Each of the defenses should be designed to be context and threat specific.

This last point is the most subtle and perhaps the most important. Going back to the bank example, note that banks do not simply have additional security guards at every level. Banks understand that threats come in different flavors, ranging from the desperate drug addict with a gun, to the sophisticated fraud artist. Thus for the banks, each defensive layer is optimized to deal with a specific class of threats.

| Technology Layer | Example Solution | Defence Against |
|---|---|---|
| Network Security | Firewall | •Network Scans<br>•Malformed Packets<br>•Unacceptable Connection<br>•Denial of Service Attacks |
| Platform Security | Anti-virus software | •Known worms |
| Application Security | Account and Role Access Control | •Disgruntled Employees<br>•Inappropriate Access |

*Table of Layer Technologies that Contribute to Defense in Depth*

**Designing for the Threat**

So what does this have to do with security on the plant floor? Like the bank, the SCADA/ICS system can be exposed to a variety of different security threats, ranging from disgruntled employees, to computer malware, denial of service attacks and information theft. Each needs to be considered and defended against.

For example, a boundary firewall can act like the bank guard, so that network messages using specified protocols are either permitted or denied access into the control network. This is ideal for keeping the bulk attacks out, particularly the average IT worm or the common denial of service attack.

Deeper into the control system, more sophisticated SCADA-aware firewalls, such as the Tofino Security Enforcer, can observe the traffic beyond the obvious protocol types. This allows defenses based on the behaviour and context of the systems using these protocols on the control network. For example, if an operator station computer suddenly starts trying to program a PLC, then perhaps a worm like Stuxnet or a disgruntled employee is at work. This attack needs to be immediately blocked and alarms raised to prevent serious risk to the system.

Finally, servers and controllers with a robust security implementation can act like a well-trained bank teller. After a user successfully connects to a server or controller, the security configuration ensures they only get access to the specific applications and data they are supposed to have access to. Attempts to access other services or data should be blocked and logged.

As with the steel doors, the bank guard and the teller example, the perimeter firewall providing the boundary security, the SCADA/ICS firewall providing the internal security and the server providing the application security are an essential team. For example, a firewall can block millions of randomly malformed messages directed at a control system as part of a Denial of Service (DoS) attack. At the same time, an ICS/SCADA deep packet inspection module and user authentication checks can prevent an individual or worm already inside the corporate network from making changes that might risk property or lives.

**Providing Reliable Security for the Plant Floor**

Depending on a single defence, such as a perimeter firewall, is building a security solution based on a single point of failure. Make sure that your facility has a proper Defense in Depth design where the network, control devices and systems are collectively hardened - thereby providing reliable security for the plant floor. Using security technologies designed for industrial defence in depth make this a goal that any organization can achieve.

---

## *ICS and SCADA Security Myth: Protection by Firewalls*

*By: Andrew Ginter, Waterfall Security Solutions*

In this article I am going to talk about a fairy tale. This tale doesn't have princes or frogs in it, but instead it deals with SCADA and industrial control system security. The existence of a "firewall" between control system networks and the rest of the world has been one of the most enduring fairy tales in the field of SCADA/ICS security. The idea is that**,** in a properly designed system, there is a logical barrier between the control network and the business network. Since unauthorized information cannot cross such a firewall, bad things like hackers and worms can never get into critical control systems. From this, a corollary flows:

"Companies that get worms in their systems obviously have not configured the proper firewall and deserved to be infected."

The real problem with the firewall concept is not the technology. The issue is that a firewall misleads companies into a false sense of security, making it a very dangerous fairy tale indeed. Even if there really is no logical connectivity, there is still good old-fashioned "sneakernet." There's either malicious or unintentional misuse by an operator who does get in. There's piggy-backing on vendor-recommended "essential" connections - isn't that how Stuxnet propagated through firewalls in search of its target networks? There's drive-by downloads, piggy-backing on VPNs and stealing passwords. So there are all sorts of ways for a cyber attack to cross that mythical firewall.

So obviously no, the protection is not there anymore. And even if you think it's there, it's probably a sound best practice to assume that it isn't and put host security controls in place to protect against that potential attack anyway. Better safe than sorry. With a little knowledge, one can do a Google or Shodan search on a SCADA or PLC and find multiple examples of systems that are supposed to be inaccessible behind multiple layers of firewalls and never supposed to be connected to the world online and vulnerable to attack.

Firewalls do not and should not exist. Patching vulnerabilities won't make systems secure. Standards and regulations are here to stay. The threat will surpass our ability to tolerate it long before we can re-engineer and re-deploy every vulnerable system. These are all just facts, and ignoring them is just as dangerous as ignoring corrosion on high-pressure pipes. Many of those who still rally to the defense of firewalls are folks with experience and intellect beyond question. They have spent more time applying those weighty assets to these issues than virtually anyone else, and their opinions cannot be disregarded. Experience and brilliance, however, do not always lead to correct conclusions.

**This Is, Of Course, Nonsense**

The above rants are cut-and-pasted from publications by well-known security experts, arguing against air gaps. I have substituted "firewalls" for "air gaps" and substituted words illustrating vulnerabilities of firewalls rather than illustrating vulnerabilities of air gaps. Pretty much every argument which has been made against air gaps can also be made against firewalls, and quite a few more besides.

Ever since the recent burst of rants against air gaps by well-known authors, I have heard nothing but confusion from practitioners. "Such-and-such-an-expert said firewalls are stronger than air gaps, so we're deploying firewalls everywhere." Well firewalls are far from perfect, and lead a false sense of security just as often as do air gaps. Should we abandon firewalls as well? Should we put all of our PLCs and HMIs right out on the Internet, to be certain that nobody develops a false sense of security?

This is, of course, nonsense. No security process or technology is perfect: not air gaps or firewalls, not patching or long passwords, not anti-virus or whitelisting, and not intrusion detection or SIEMs. As my martial arts instructor is fond of pounding into us students: for every defence there is an offence, and for every offence there is a defence. If the point we want to make is that there are no silver bullets, should we be out there poking holes in one security technology after another? Will "myths of anti-virus" be the next trend in headlines? Will "fairy tales in patching" be the headline after that? How much confusion must we sow?

**Stop Confusing Us**

I have spoken to the authors of several of these rants and every one of them maintains they are not trying to confuse practitioners. They are merely trying to point out how one or another "silver bullet" is vulnerable, and so practitioners really should be practicing defence-in-depth, both of security process and of security technology, for all of their equipment. This is a fine sentiment, but this "fairy tale rant" tactic is fatally flawed. The message practitioners are taking from these rants is that they should deploy weak approaches to security to avoid being seduced by strong approaches. ICS security practitioners surely have enough problems without us confusing them this way.

If the security experts of the world want to help matters, we should undertake to educate practitioners as to what is the spectrum of threats we face, what specific, modern threats each practice or technology addresses, and how thoroughly each threat is addressed.

**Walking the Walk**

Lest I be accused of doing no more than the experts I criticize, let me offer up an alternative to firewalls: unidirectional security gateways. Beyond the "false sense of security" nonsense, the "air gap" articles point out that modern control systems must routinely transfer a fair amount of information to business systems in order to control the costs of the physical process they control. Unidirectional gateways support that one-way data movement without introducing the attack opportunities which firewalls do. Better yet, in the vast majority of cases, the gateways are seamless replacements for firewalls - no redesigning of networks or application integration technologies is necessary. Even better, and perhaps counter-intuitively, the technology supports a variety of remote support and central management strategies as well.

And for the corner cases? The "air gap" rants make much of the dangers of USB sticks when any data must be moved back into a protected network. Let's look at those dangers. Which modern-day threats propagate via USB sticks and how can we combat them?

- High-volume, organized-crime-authored, worms, viruses, and botnets? These attacks propagate via USB sticks, yes, and anti-virus systems do a fair job of catching high-volume threats. Application-control/whitelisting solutions do even better. Stand up "media cleansing" stations with defences like these installed and use them habitually on your mobile media.

- Insiders on the business WAN? They don't attack with USB sticks because they aren't authorized to physically enter the secure ICS server room and touch the equipment.

- ICS insiders? Are they really going to use USB sticks if they have passwords and access to the hardware? No - they'll use their passwords. Or hammers.

- Advanced Persistent Threats? These adversaries do not use USB sticks - they use spear phishing or conventional web/SQL attacks to pass through firewalls, and manual remote control to propagate once they are inside. Unidirectional gateways defeat both of these attacks.

- Stuxnet? Yes, Stuxnet propagated via USB sticks, but if you recall, it punched through firewalls like they weren't there as well. And once Stuxnet stopped being a highly-targeted, under-the-radar threat and went high-volume, anti-virus vendors put signatures out for it and that was the end of Stuxnet on AV-protected networks. Today, both whitelisting and AV solutions catch Stuxnet in a heartbeat.

In fact, sending absolutely everything through your firewalls and banning USB sticks entirely is dangerous. Do you really want your firewalls to pass every kind of rarely-needed data through to your control network? I submit that a well-practised system of screening USB keys through a handful of different vendors' whitelisting and anti-virus systems is a better way to address USB threats than any firewall can be. After all, firewalls make you complacent about removable media. Then, when you really need to use a USB stick, you are out of practice and prone to error.

**Looking Forward**

Security practitioners: if you can't use air gaps because you have too much data which must move routinely, use unidirectional gateways. If you can't use the gateways for whatever reason, use firewalls with absolutely minimal data movement configured. *Do not configure holes through your firewalls* for every last bit, of every kind, of diverse, low frequency data that you will ever need. Always have a powerful, *well-practiced* system of media cleansing available, using at least one application control/whitelisting solution, and one or more anti-virus solutions.

Security experts: stop trashing one approach to security after another. Start recommending strong alternatives, and position them correctly within defence-in-depth strategies. Consistently add value through reasoned analysis. If you must point out limitations of one technology, explain clearly, either stronger alternatives, or compensating measures, to include in security programs.

Stop confusing security practitioners. Start teaching them.

---

## *Ensuring a "Whole Company" Response: Strengthening Corporate Cyber Incident Response Relationships through Exercises*

*By: Adam Bulava*

The increasing frequency, scope, and complexity of cyber attacks against the private sector underscores the need for a more robust organizational cyber incident response capability. As corporate crisis managers continue to make a concerted effort to integrate "all-hazards" into their emergency response and continuity planning, the inclusion of cyber threats presents certain challenges due to their unique attack vectors, widespread impacts, and complex mitigation requirements. Companies seeking to allocate already-stretched security dollars to strengthen their overall emergency preparedness are finding it difficult to balance traditional incident response needs with those necessitated by a cyber intrusion. At the crux of this challenge lies the critical role IT staff play during a suspected or confirmed breach of company systems. As evidenced in previous high-profile breaches, including the 2011 Sony Play Station 3 breach, a fundamental communications gap often exists between IT personnel and other critical incident response elements within an organization. As a result, companies are able to successfully mitigate the technical impacts of a cyber incident but often fail to achieve a successful "whole company" response. However, carefully designed private sector cyber exercises can help bridge this corporate communications gap.

In today's exercise environment, if a company conducts a cyber exercise it is often technical in nature and involves the IT department investigating a potential system breach, working to contain the breach, and perhaps conducting comprehensive forensics – all according to defined protocols and procedures. Other corporate cyber exercises might aim to test or validate specific response plans, addressing continuity of operations or disaster recovery procedures primarily handled by crisis managers. Both of these types of exercises hold immense value, but should not be thought of as an all-encompassing gauge of cyber preparedness. Separate from these "exercises of validation" exist another category of exercises, namely "exercises of discovery." These exercises seek to involve the broader response elements of a corporation and address not only the technical mitigation of a cyber attack but also key internal and external communications processes vital to a successful "whole company" response.

Exercises of discovery can help illuminate gaps and shortfalls in an organization's cyber incident response operations by examining key areas of conjunction between IT and other corporate response elements, to include (for example):

- The need for mutual understating between IT personnel and crisis managers regarding their respective roles and available resources during events caused by cyber disruption;
- The need for IT leaders to be able to communicate key incident impacts and recommended courses of action to senior executives using non-technical language;
- The existence of clear communications channels between IT and external affairs to ensure customer messaging is accurate, appropriate, and clear; and
- Mutual awareness between the IT and legal department regarding the legal implications/restrictions involved in hiring a third-party vendor to help support forensics.

Planning for such an exercise typically requires several weeks to a few months in order to be successful. At the outset of the planning process, companies should form an exercise design team comprised of representatives from key corporate incident response elements (e.g., IT, legal, HR,

external affairs, crisis management, senior leadership, etc.) who can collaborate to develop and reach consensus on exercise goals and objectives.
These goals and objectives should directly promote an in-depth exploration of the "whole-company" response to a cyber attack. Also, the exercise scenario should be realistic and should drive exercise discussion among *all* players. There is little need for a company to spend an exorbitant amount of money in attempts to make the exercise interactive or highly-operational. In fact, a successful cyber exercise typically involves a half or full-day, facilitated "tabletop" discussion among key players, working through a well-constructed scenario aimed at achieving clear objectives.

Ultimately, one of biggest challenges in the exercise planning process is gaining senior leadership buy-in for such an effort. Unfortunately, as evidenced in the real-world, senior leaders typically do not give cyber threats due consideration until a significant incident at their organization requires them to do so. However, if the exercise is designed in such a way that it serves as the guiding component of a company's regular business impact/risk analysis process, this may lend increased significance to the effort and highlight the potential negative impacts and cascading effects a cyber disruption can have on an organization.

---

## *CSSP Contact Information*

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an e-mail to icsjwg@hq.dhs.gov.

The CSSP and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at https://forms.us-cert.gov/report/.

In addition, the ICS-CERT Monthly Monitors are published on HSIN as appendices to the ICSJWG newsletter and can be found here http://www.us-cert.gov/control_systems/ics-cert/.


Other important contact information:
Website Address: http://www.us-cert.gov/control_systems/
ICS-CERT Email: ics-cert@hq.dhs.gov
Phone: 1-877-776-7585
CSSP Email: cssp@hq.dhs.gov