



# ICSJWG QUARTERLY NEWSLETTER

— ICSJWG EXPANDING THE COMMUNITY —

## ***ICS-CERT Updates Vulnerability Disclosure Policy***

ICS-CERT has updated our vulnerability disclosure policy posted on our website at [http://www.us-cert.gov/control\\_systems/ics-cert/disclosure.html](http://www.us-cert.gov/control_systems/ics-cert/disclosure.html). We have modified the policy to state that in the cases where a vendor is unresponsive and /or a reasonable timeframe for remediation cannot be established, we may disclose vulnerabilities 45 days after the initial report, regardless of the existence or availability of patches or workarounds. The policy also includes language that extenuating circumstances, such as active exploitation, threats of an especially serious nature, or situations that require changes to an established standard may result in earlier or later disclosure. Other factors include:

- whether the vulnerability has already been publicly disclosed;
- the severity of the vulnerability;
- potential impact to critical infrastructure;
- possible threat to public health and safety;
- immediate mitigations available;
- vendor responsiveness and feasibility for creating an upgrade or patch; and
- vendor estimate of time required for customers to obtain, test and apply the patch.

We appreciate the time and dedication that you all spend in working to secure your products and we feel that this policy will have very little impact on you and other responsive vendors who already have a working relationship with ICS-CERT.

Current/existing timeframes will not be affected or changed as a result of the new policy. It is our goal that this alignment and update will enable us to more effectively address vulnerability information with vendors who are not responsive to vulnerability discovery and remediation.

## ***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/](http://www.us-cert.gov/control_systems/icsjwg/)*

## **Contents**

<i>ICS-CERT Updates Vulnerability Disclosure Policy.....</i>	<i>1</i>
<i>ICSJWG 2012 Fall Meeting Update.....</i>	<i>2</i>
<i>ICSJWG 2012 Fall International Partners Day.....</i>	<i>2</i>
<i>ICS-CERT Monthly Monitor and Twitter Announcement.....</i>	<i>3</i>
<i>Advanced Training Events Scheduled for Fiscal Year (FY) 2012.....</i>	<i>3</i>
<i>ICSJWG Subgroup Status.....</i>	<i>4</i>
<i>Homeland Security Information Network (HSIN) Portal.....</i>	<i>5</i>
<i>Participation is Key!.....</i>	<i>6</i>
<i>Industrial Control Systems Contributed Content .....</i>	<i>6</i>
<i>CSSP Contact Information .....</i>	<i>16</i>

## **ICSJWG 2012 Fall Meeting Update**



Come to Colorado in 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). Attendees will be able to discuss the latest initiatives impacting the security of industrial control systems and will have the opportunity to interact with colleagues and peers who may be addressing the threats and vulnerabilities to their systems.

There is no cost to attend the ICSJWG Fall Meeting. 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 agenda details! [http://www.us-cert.gov/control\\_systems/icsjwg/2012/fall/index.html](http://www.us-cert.gov/control_systems/icsjwg/2012/fall/index.html)

### **ICSJWG 2012 Fall International Partners Day**

The inaugural ICSJWG International Partners Day was such a success that future meetings with our international partners will continue to be coordinated with the biannual ICSJWG meetings. The second ever ICSJWG International Partners Day will be held on Thursday, October 18, 2012 in Denver Colorado.

More than a dozen countries sent representatives to attend the inaugural event and we expect a similar turnout in Denver. To view the agenda and other details of the International Partners day check out the site! [http://www.us-cert.gov/control\\_systems/icsjwg/international-partners/2012/fall/agenda.html](http://www.us-cert.gov/control_systems/icsjwg/international-partners/2012/fall/agenda.html)

## ***ICS-CERT Monthly Monitor and Twitter Announcement***

ICS-CERT releases its Monthly Monitor Newsletters in order to inform the control systems cybersecurity community of the latest activities that have occurred over the past month. The Newsletter can be accessed at [www.ics-cert.org](http://www.ics-cert.org) along with our other Control Systems Advisories and Reports.

Also, please also follow ICS-CERT on Twitter at @ICSCERT to get the latest news involving ICS-CERT activities.

### ***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.

The training events for FY13 are under consideration. Please monitor the [CSSP training calendar](#) for details to be posted in the coming weeks.

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 each course will be sent out and posted to the following website - [http://www.us-cert.gov/control\\_systems/cscalendar.html](http://www.us-cert.gov/control_systems/cscalendar.html). Please monitor the site periodically, since 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](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@hq.dhs.gov](mailto:icsjwg@hq.dhs.gov) or contact the co-chairs directly.



### ➤ **Roadmap to Secure Industrial Control Systems Subgroup**

*GCC Co-Chair: Perry Pederson ([Perry.Pederson@nrc.gov](mailto:Perry.Pederson@nrc.gov))*

*SCC Co-Chair: Tim Roxey ([Tim.Roxey@nerc.net](mailto:Tim.Roxey@nerc.net))*

The Roadmap subgroup is actively communicating the availability of 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 generally 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. To that end, a subcommittee has been formed which will look at the scope of the document, capturing sector-specific information regarding security posture and making the metrics sections more robust and reflective of what is currently being done throughout the community. The Subgroup will have an update during the Denver Meeting regarding the development of the Maturity Model, the status of goals included in the Roadmap document and reaching out about the ICS Cross-Sector security posture.

### ➤ **Vendor Subgroup**

*GCC Co-Chair: Marty Edwards ([Marty.Edwards@dhs.gov](mailto:Marty.Edwards@dhs.gov))*

*SCC Co-Chair: Eric Cosman ([ECCosman@dow.com](mailto:ECCosman@dow.com))*

The Vendor subgroup finalized and published the [Vulnerability Disclosure paper](#), which provides a consensus-based foundation for ICS vendors and integrators working to develop a vulnerability disclosure policy. Also, the Cross Vendor Subcommittee is finalizing a draft of the Cross-Vendor position paper for discussion during the ICSJWG Fall Meeting in Denver. The paper outlines the current landscape and direction that the ICS community should take to improve control systems security. Lastly, the Vendor subgroup is considering several new topics for further consideration, including: interactive remote access; the importance of timely patching; and how to improve, deprecate, or replace systems that can no longer be patched.

### ➤ **Workforce Development Subgroup**

*GCC Co-Chair: Keri Nusbaum ([Keri.Nusbaum@dhs.gov](mailto:Keri.Nusbaum@dhs.gov))*

*SCC Co-Chair: Michael Glover ([M.Glover@prime-controls.com](mailto:M.Glover@prime-controls.com))*

The Workforce Development subgroup is currently revising the scope of the overall work to include requirements, Knowledge, Skills, & Abilities (KSAs) from multiple sources including the NICE Framework, the NERC CIP and ISA99 and tailoring those specifically to industrial control systems. The subgroup is actively developing a plan to reach out to other subgroups to help define requirements. During the Denver Meeting, the subgroup will update the status of current deliverables and will have a working meeting to develop additional details for products under development.

➤ **Research & Development Subgroup**

*GCC Co-Chair: Doug Maughan ([Douglas.maughan@dhs.gov](mailto:Douglas.maughan@dhs.gov))*

*Acting SCC Co-Chair: Zach Tudor ([Zachary.tudor@sri.com](mailto:Zachary.tudor@sri.com))*

The R&D subgroup met in July and September to discuss a variety of topics related to research and development requirements as well as making revisions to the subgroup's charter. The R&D subgroup will meet during the ICSJWG Fall meeting in Denver to finalize the charter and provide status updates on a variety of R&D projects and requirements.

### ***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@hq.dhs.gov](mailto:icsjwg@hq.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@hq.dhs.gov](mailto:icsjwg@hq.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@hq.dhs.gov](mailto:icsjwg@hq.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 December Quarterly Newsletter. If you want to submit an article for the December Newsletter, please email [icsjwg@hq.dhs.gov](mailto:icsjwg@hq.dhs.gov), and we will take your submission into consideration for publication. The deadline for submissions for the December Newsletter is **December 10, 2012**.

Past ICSJWG newsletters are located on the CSSP website [http://www.us-cert.gov/control\\_systems/icsjwg/index.html](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 September 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.

---

## ***Securing Systems Based Upon Insecure Platforms***

*By: Joseph J. Januszewski, III, CISSP, CHSP, CNA*

It has been said many times, however, it appears that the advice is worth repeating: *a holist approach to security is required*. Borrowing an analogy from the culinary arts, security must be baked-in, it **cannot** be a topping. Computer security experts continue to echo similar mantras, although somehow, security doesn't make it to the bottom of the balance sheet. In its purest form, the bottom line is money. However, there exist overlooked components of the bottom line that include the reputation of a company and its brands, shareholders, and its financial security, not to mention the health and safety of its employees, customers and the surrounding communities. In the security realm, on the other hand, the bottom line is a set of processes, procedures, equipment and software configured in a manner based upon solid risk assessment designed to protect the proprietary information of those companies, and in many instances, lives.

SCADA systems, controllers, and host systems that comprise what we term "control systems" require several layers of security including hardening of the operating system, whether general-purpose or application-specific, patches applied to software, as well as network security, provisions for secure remote access, etc. An example of a recent advertisement for a utility management system based upon a commonly available general-purpose database introduces the need for software updates for both the application software and for the operating system of the server (or servers) that the database management system and the application are running on. However, it requires other security

measures as well: back-ups, a secure operations area with disaster recovery procedures, and an off-line disaster location with data replication procedures, to name just a few of the considerations that must be made. Losing some or all of the equipment at a site doesn't have to mean also losing all of the operational and institutional knowledge maintained there.

Many operations personnel are under the impression that a control system is *just another application running on the network*. From a network-centric model, this may appear to be true, but most systems typically protected by network administrators aren't responsible for keeping critical infrastructure up and running. A "blip" may be inconvenient when office workers are trying to access the Internet or the office printer, but can be catastrophic if a control system ceases to function and an assembly line comes to a halt, costing thousands of dollars in lost product, or worse: resulting in health, safety and environmental issues. For worst-case scenarios, we need to look no farther than Three Mile Island, or Fukushima Daiichi. Keeping in mind that the cause of neither example was a network-based issue, the former was the result of the failure of at least one control system, and the latter was a catastrophic failure on various levels, including control system failures due to power loss at the site. However, there are several examples of industrial site accidents involving automation that have resulted in several injuries and deaths in just the past twelve months at manufacturing facilities in the Mid-Atlantic region, alone. We must remind ourselves that a loss of situational awareness CAN be deadly.

When computer systems used as terminals in control rooms of nuclear power plants have game software installed on them, or allow their users unfettered access to the Internet<sup>1</sup>, it is apparent that someone *still* isn't getting the message that security can mean the difference between life and death. Computers used for controlling systems, especially in a nuclear power plant, should have several layers of protection between them and the Internet. Beyond the obvious danger of distracted employees in a control room of a power plant, what access did that give to computers from the global Internet into the control room of the power plant? Worms, rogue networks searching for new "zombie" systems, key-logging of command and access codes – the possibilities are myriad... and frightening.

Many people (some of whom are members of the control system community) decry air-gaps as viable security measures. While air-gaps didn't protect centrifuge control systems from Stuxnet, I would argue that a single border firewall is just as worthless, or that a good password scheme is just as worthless (not hard-coded three-letter passwords as we have seen used in practice), or that a policy against USB drives in the workplace is just as worthless, or that a biometric access system is likewise just as worthless, alone. The truth is, that without defense-in-depth (an established model that is valid, but apparently, the value of which is still not recognized) and regular sanity checks on the true access levels and mechanisms by which every system in a secure environment operates and can be potentially compromised, no **one** security measure will *ever* be adequate.

## Bibliography

<sup>1</sup> "NOTICE OF VIOLATION AND PROPOSED IMPOSITION OF CIVIL PENALTY - \$140,000, NRC INVESTIGATION REPORT 4-2010-064 - RIVER BEND STATION". U.S. Nuclear Regulatory Commission. January 5, 2012. EA-11-159, Docket: 50-458.

## **Thwarting Large Scale ICS Reconnaissance and Attacks**

*By: David A. Kruger, Senior Architect; Mitch Tanenbaum, Chief Technical Officer;  
Dan Kruger, Chief Executive Officer*

### **Synopsis**

Industrial Control Systems (ICS) run our country's critical infrastructure and industrial base. Authentication of users, devices, and applications and the protection of control communications are limited in the existing critical infrastructure. In many cases ICS are connected to the Internet and/or to business networks that are connected to the Internet. Connection to the internet combined with weakness or absence of built-in ICS security mechanisms makes ICS vulnerable to extensive remote reconnaissance and code injection. Vulnerabilities in families of ICS devices operating in multiple locales create the possibility of multiple serial or simultaneous attacks across the industrial infrastructure. Additionally, interconnected ICS and business networks provide attack vectors to each other; *one cannot be secured without securing the other.*

It is not possible to immediately secure ICS because there are, conservatively, hundreds of millions of inadequately secured digital ICS devices in the United States. The scale of the task necessitates prioritization; the most cyber-vulnerable systems with the greatest potential for disruption or destruction need to be secured soonest.

Wholesale replacement of hundreds of millions of inadequately secured ICS devices is not feasible. Practical solutions must be engineered that can be added to existing ICS with minimal disruption. Solutions must be economically attractive.

The solution proposed applies the technology described in our white paper “Radically Simplifying Cybersecurity” to ICS. We encourage you to read it before continuing.

### **Definitions**

*Industrial Control Systems (ICS):* ICS control electrical power generation and transmission; water and wastewater facilities; smart electric and water meters; chemical plants; refineries; oil and gas pipelines; offshore oil rigs; manufacturing; dams, locks, and canals; Internet data centers; rail and street traffic controls; prison doors and gates; building HVAC systems; boilers; elevators; and more. The number of digital ICS devices in the U.S. conservatively numbers in the hundreds of millions.

ICS include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Master and Remote Terminal Units (MTU and RTU) and Intelligent Electronic Devices (IED), that is, all digital devices used to control physical processes. Additionally, ICS include servers, desktops, digital testing equipment, laptops, tablets, removable drives, memory cards, smartphones, cameras, printers and all other digital devices and storage media that may be permanently or temporarily connected to the ICS network. ICS networks use many communications methods, including wire, multiple types of radio transceivers, telephone, cable and optical fiber.

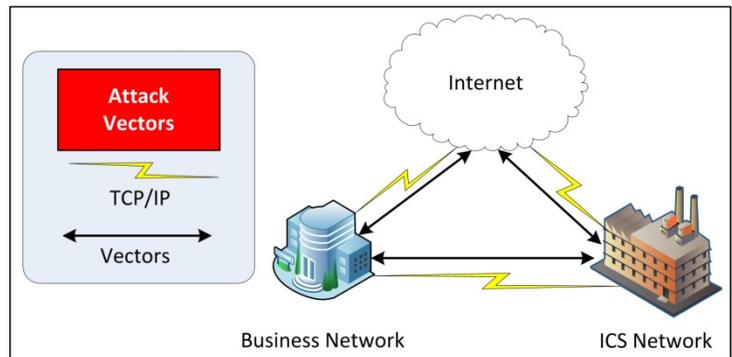
*Business Networks:* As used in this white paper, business networks include devices and applications people use for human interaction and information sharing. Business networks are the portion of an organization's networks that are *not* ICS.

## A Growing Threat

Following the June 2012 reports that the Flame and Stuxnet<sup>1</sup> malware was a joint U.S.-Israeli cyber attack, public concerns about retaliatory cyber attacks on U.S. critical infrastructure and increased risk of protracted nation-state cyber warfare are increasing.<sup>2, 3</sup> Cyber attackers, using skills honed by long practice in exploiting business networks, are now beginning to turn their attention to ICS. Attacks are on the rise.<sup>4, 5</sup>

Business networks interconnected with ICS are penetrated frequently. A casual glance at the daily news confirms that industrial espionage, wholesale leaks of classified information, intellectual property piracy, cyber sabotage, and identity theft are rampant.<sup>6, 7</sup> ICS and business networks provide attack vectors to each other. This is critical; if ICS security and business network security are approached as separate problems, that separation will limit real risk reduction and will likely impart a false sense of security. *Securing either requires securing both.*

**Exhibit 1**



## Prioritizing Defense Implementation Based on Degree of Cyber-Vulnerability

The degree of cyber vulnerability is based on six factors:

### 1. The initial attack vector: remote or proximate.

1.1. **Remote attacks** can be launched from a distance using IP networks. Remote attacks are particularly worrisome because a skilled attacker has little reason to fear identification, much less retribution.

1.2. **Proximate attacks** can be launched when a person (wittingly or unwittingly) physically connects a device or storage media to an ICS or interconnected business network, or positions monitoring or signal injection equipment on or near wireless ICS communication links.

### 2. The number of available attack vectors and targets. Every TCP/IP-connected digital device, operating system (OS), application, transmission path, digital communication and file

#### Footnotes

<sup>1</sup> The Washington Post, Ellen Nakashima, Greg Miller and Julie Tate, June 19, 2012, "U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say."

<sup>2</sup> Financial Times, June 26, 2012, "Telling the truth about cyberwarfare."

<sup>3</sup> The New York Times, Misha Glenny, June 24, 2012, "A weapon we can't control."

<sup>4</sup> U.S. Department of Energy, March 2012, "Technology Security Assessment for Capabilities and Applicability in Energy Sector Industrial Control Systems," Pacific Northwest National Laboratory, March 2012, PNNL-21313.

<sup>5</sup> 2009-2011 ICS-CERT Incident Response Summary Report, U.S. Department of Homeland Security.

<sup>6</sup> ZDNET, Emil Protalinski, March 28, 2012, "FBI: U.S. losing hacker war."

<sup>7</sup> Security Testing, Jamie Saine, March 28, 2012, "You are losing the battle with hackers. Yes, you."

has multiple attack vectors (paths to the target) and attack surfaces (that which can be attacked). Every time a device is booted, a user logs in, an application is launched, an email or an ICS control message is sent, a website is browsed, a file is manipulated, or a device is connected, attack vectors are opened and attack surfaces are exposed. Serial networks offer some, but significantly fewer attack vectors and surfaces.

3. **Ease of cyber reconnaissance.** Using the Internet, remote cyber attackers can conduct large-scale cyber reconnaissance of Internet-facing ICS devices using known search utilities such as Shodan<sup>8</sup> and ERIPP<sup>9, 10</sup> to create maps of unsecured or inadequately secured ICS devices. Simple identification tools can discover device location, function, make, model and communications protocol. It is likely that covert as well as overt IP search engines are currently mapping US ICS vulnerabilities.

In addition, sophisticated surreptitious monitoring and reporting malware (such as Flame) that can access ICS from interconnected business networks can provide comprehensive ICS and business network information that identifies technical and human vulnerabilities, enables the injection of attack code and reveals operational patterns that can be used to optimize timing of attacks. Malware such as Gauss can steal personal or company information at the same time it is performing reconnaissance.

4. **Attack repeatability.** Repeat attacks can be based on the vulnerability's particular device types, applications, exploitation methods, organizational policies (or the lack thereof) and geography. Malware can be easily copied, as can be step-by-step instructions for delivering the malware to the target. Previously successful ICS exploits are currently being published<sup>11</sup>; this practice enables future attacks to be repeated by less sophisticated attackers. Large scale vulnerability mapping in conjunction with repeatability creates the potential to stage multiple serial or simultaneous attacks. (Stuxnet worked by repeatedly exploiting known vulnerabilities for a family of devices.)
5. **The risk of identification and reprisal.** Anonymity is arguably the greatest ally of the cyber attacker. Skilled attackers are unlikely to be identified by technical means, and lack of identification thwarts reprisal. Surveillance and attacks can be launched from compromised computers unbeknownst to the computer's owner.
6. **The communications protocol of the ICS target: routable (TCP/IP) or non-routable (serial).**

6.1 Ease of remote management, increased span of control, the sophistication of control applications and the desire for increased capacity in the wiring plant have driven large-scale implementation of TCP/IP-based routable networks in ICS.<sup>12,13</sup> The very capabilities that

---

<sup>8</sup> Washington Post, Robert O'Harrow Jr., June 3, 2012, "Cyber search engine Shodan exposes industrial control systems to new risks."

<sup>9</sup> ICS-ALERT-11-343-01—Control System Internet Accessibility, U.S. Department of Homeland Security, December 9, 2011.

<sup>10</sup> ICS-ALERT-12-046-01—Increasing Threat to Industrial Control Systems, U.S. Department of Homeland Security, February 15, 2012.

<sup>11</sup> The Register, Dan Gooden, March 22, 2012, "Dozens of SCADA exploits, proof-of-concept code published."

<sup>12</sup> Eric Byres, P.E., Dan Hoffman, Ph.D., 2006, "The myths and facts behind cyber security risks for Industrial Control

make routable connectivity desirable also make it vulnerable.

6.2 Serial networks are vulnerable to attack, but their non-routable nature generally requires (at some point) physical proximity for a direct attack. However, serial networks can be attacked via routable networks by compromising TCI/IP-connected controllers which control non-routable serial networks.

## Priorities

The consequences of an attack on less vulnerable portions of an ICS can be as devastating as an attack on highly vulnerable portions of an ICS. The less vulnerable must be secured; however, securing the most vulnerable soonest reduces overall risk fastest.

### First Priority: Remote IP Cyber Reconnaissance and Attack

ICS are most vulnerable to remote cyber attacks via portions of the ICS that use the routable TCP/IP protocol and that are either directly connected to the Internet or all-too-easily-exploited business networks.

Reconnaissance is easy to moderately difficult and can be conducted on a very large scale. Large numbers of targets can be identified. The scope of potential attacks is, frankly, enormous. Attacks are highly repeatable. Remote attackers are at little risk of identification and reprisal. This form of reconnaissance and attack is also *cheap*. Economics are strongly in favor of the attacker.

### Second Priority: Proximate IP Reconnaissance and Attack

Proximate attacks require that one or more individuals (witting or unwitting) spend at least some time physically proximate to the target to perform reconnaissance, plant devices, install software or monitor operational patterns. Proximity creates much higher risk of detection, capture, identification and reprisal. Reconnaissance and targeting scope are smaller. Attacks are less repeatable.

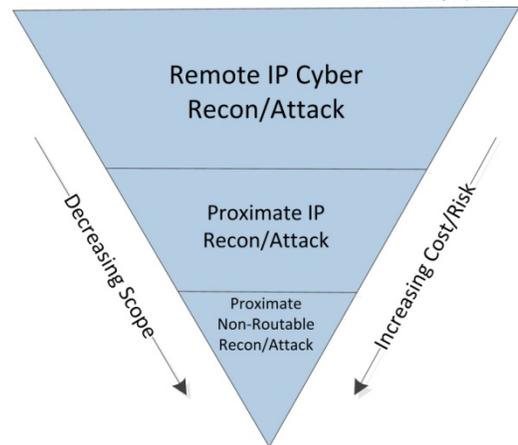
### Third Priority: Proximate Reconnaissance and Attack on the Nonroutable Network

This form of attack will often require sustained proximity to the target by a witting attacker and significant real-world knowledge of the target environment. It is the riskiest, smallest scale, least repeatable and most expensive form of cyber attack.

## Constraints and Requirements

Since wholesale replacement of ICS components is not economically viable, a practically implementable solution must deal with the real-world constraints:

**Exhibit 2**



Systems.”

<sup>13</sup> Joseph Weiss, July 30, 2010, “Protecting Industrial Control Systems from electronic threats” (Kindle Location 624).

### Exhibit 3

Constraints	Solution Requirement
ICS devices and applications are a mixture of ages, brands, makes, models, communication protocols and communication media.	Make applicable across a broad range of devices and applications.
Few devices were designed to support security. Little or no provision was made in their original design for device, user or application authentication.	Provide a method of authenticating devices, users and applications.
ICS use readily discoverable, unencrypted communication protocols.	Encrypt control communications.
ICS operate in real-time mode (exception: historical data).	Implement authentication and encryption with minimal increases to bandwidth requirements and latency.
Data stored in ICS Historians can be manipulated.	Provide a method of authenticating devices, users, applications and data that assures the validity of data in the Historian.
Many ICS digital devices do not have the compute power or headroom to operate additional software.	Provide implementations external to existing equipment.
Many ICS devices are “brittle”. Minor software changes such as updates or patches can fail a system.	Provide implementations that can be updated without system failure and risk to authentication.
Many ICS devices provide insufficient audit data.	Provide a method for enabling manufacturers to add audit data external to devices. (Support Security Information and Event Management (SIEM), intrusion detection (IDS), etc.)
Interconnection of ICS networks with business networks is the norm.	Provide a common or interoperable security solution for ICS and business networks.
Cybersecurity professionals with the skills to implement and administer secure ICS are in short supply. <sup>14, 15</sup>	Place most of the intelligence in the security solution. Reduce the technical skill required to install and configure the solution.

### Point Solutions Fall Short

Integrating a collection of “point” solutions, that is, partial solutions offered by multiple manufacturers, is a less-than-practical option. Interoperability between point solutions provided by competing manufacturers cannot be assured, and ICS device manufacturers are not likely to provide business network solutions (and vice versa). Plant owners would be required to purchase multiple solutions from different manufacturers at significant cost. Integrating disparate point solutions into a cohesive ICS and business network solution would be an extraordinarily complex undertaking. It would require personnel resources currently in short supply and would take too long. A common, vendor-neutral security architecture is the practical requirement.

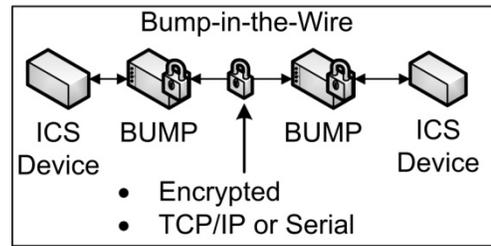
<sup>14</sup> National Defense, Eric Beidel and Stew Magnuson, "Government, Military Face Severe Shortage Of Cybersecurity Experts", March 2011

<sup>15</sup> Washington Post, Alexander Fitzpatrick. "Cybersecurity experts needed to meet growing demand", May 29, 2012

## Continuously Challenged Authentication

Exhibit 4

External implementations can be accomplished using Bump-in-the-Wire (BitW or, simply, BUMP). BUMPs are a software/hardware solution that can be attached to the communications port of currently installed devices and can provide required computing capability without altering installed devices.

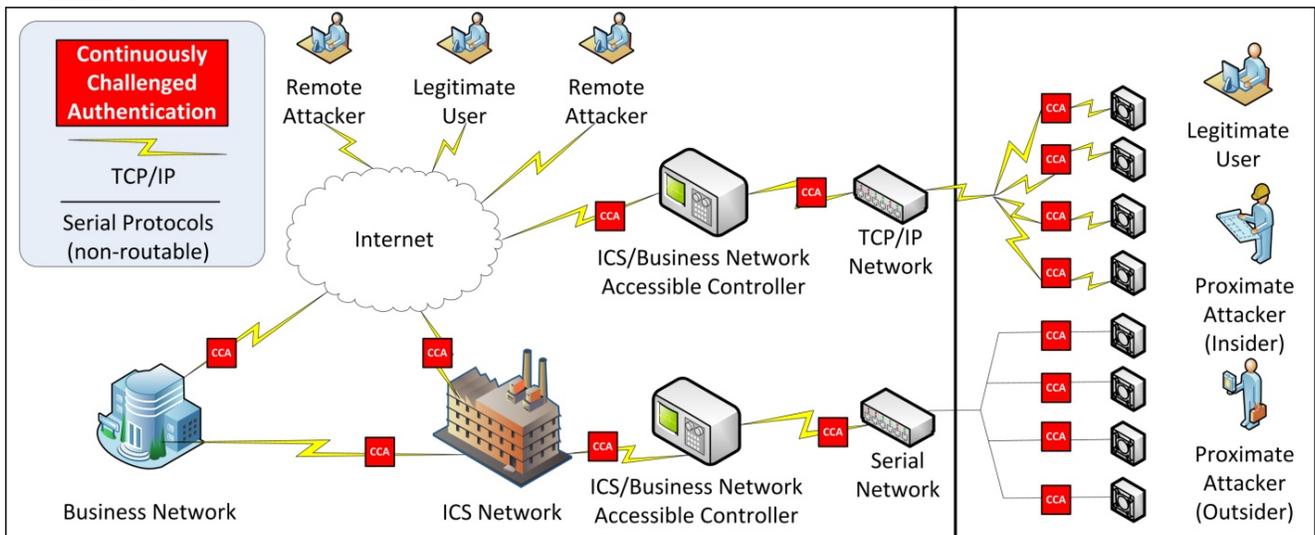


Each ICS input and output is a control message—a discrete information object sent from device to device or user to device. Given the real-time operations, reducing vulnerability requires that devices, applications, users, and control messages are continuously challenged to authenticate their participation in the ICS network.

In practical terms, ICS attacks are based on injecting false information for a long enough period of time to alter a physical process. Continuously challenging authentication (CCA) and rejecting control messages that cannot be authenticated make it possible to thwart attacks from entering the ICS network or to reduce their duration to below the time required to damage physical systems.

- ICS devices must be authenticated to the CCA-enabled networks, either by being connected to a BUMP that authenticates their endpoints or by authenticating themselves directly.
- Either method (authenticating the BUMP or the device) must be applied using a well-controlled provisioning, change management, and operations process.

Exhibit 5



CCA can be implemented on serial networks but first requires manufacturer-specific engineering. There are current BUMP-based point solutions which demonstrate that extending CCA to serial devices can be accomplished, but they are necessarily point solutions.

## Defense-in-Depth

Defense in depth is a practical necessity; no one defense can stop all attacks. Perimeter defenses,

reactive defenses such as SIEM and IDS, application whitelisting, OS hardening, and others all have critical roles to play. CCA thwarts attacks from *inside* the perimeter and provides vital audit data for intrusion detection and performing post-incident analysis.

## Conclusion

ICS operators, ICS device manufacturers, services firms (firms that engineer and manage solutions installation), insurers and regulators are all stakeholders in securing ICS. ICS operators need the lowest-cost, least-disruptive solution. ICS device manufacturers need a business opportunity large enough for them to invest and scale to needed production levels. Services firms need solutions that can be implemented with available technical resources. Insurers need reduced and predictable risk. Regulators need solutions that enable securing ICS quickly with minimal political pushback. A vendor-neutral solution that can be applied quickly, with minimal operational disturbance and at low relative cost, is the most likely to satisfy stakeholders and to be implemented in the least time.

---

## Grid Security: Where is the prevention?

By: Paritosh Tripathi

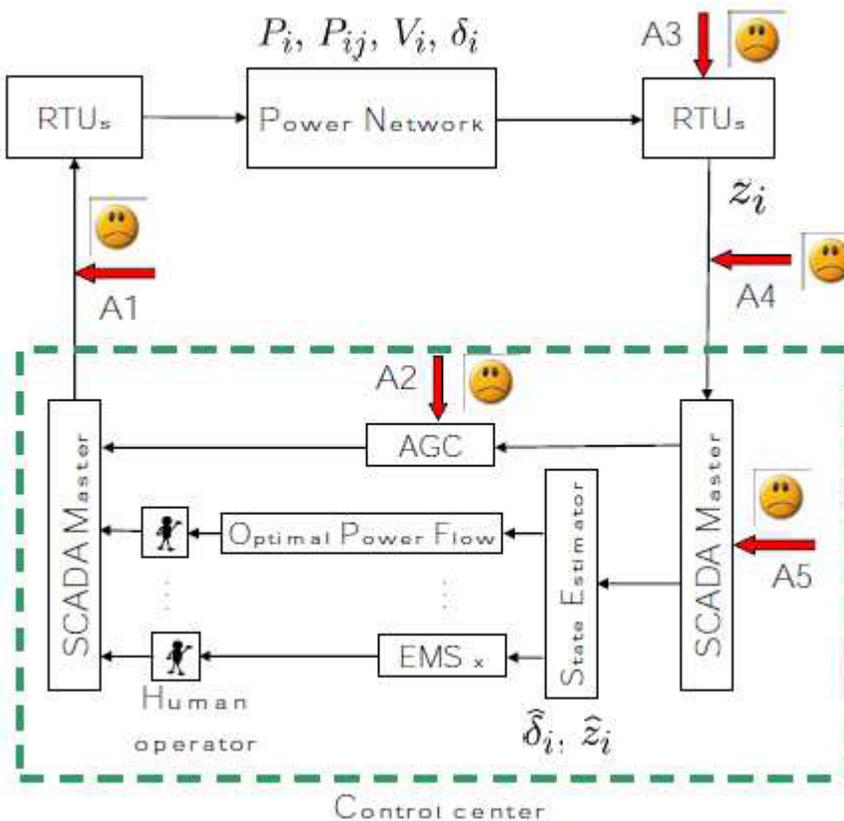
The recent event of the grid collapse in India which was described as the biggest in the history of the world, the question that becomes obvious is, if we could have prevented such a collapse at the first place? But before that the other important question that we have to answer is what could have triggered such a collapse? Was it a human error? Was it a mechanical/device failure? Was it an insider/outsider attack? I feel it's a hard one to answer. Unless the investigators come up with a formal report, it is hard to tell what could have lead to such a failure.

The grid is about generation, transmission and distribution. The systems view of grid contains elements like buses, generators, loads, transformers, lines, circuit breakers etc. When many such elements combine, in a geographically dispersed setting, it constitutes the grid. Such systems (grid) depend on SCADA for their proper functioning. SCADA stands for Supervisory Control and Data Acquisition. SCADA based networks follow a simple sounding but complex logic that of acquire information, making decisions based on information acquired and passing the same decision to the entities involved so as to keep the system stable, efficient and viable. How does it do that? By something called State Estimators, the decision making body. Its job is to maintain a virtual picture or state of whole system using the acquired/estimated parametric values from RTUs. As the expansion of SCADA suggests there are two important aspect to it, one data acquisition from remote sites generally referred as Remote Terminal Unit (RTU) using sensors and the other supervisory control that happens at the Master Terminal Unit (MTU) and is about passing commands to RTU/s for either data acquisition or for changing certain parameters in the grid. This communication between MTU and RTUs happen over industrial communication protocols such as DNP3, ModBus etc. This qualifies it as a cyber-physical system.

Until some years back the exchange of information between MTU and RTU/s was done in an obscure manner and thus did not get much attention from the security community. Though the philosophy of SCADA remains intact the way information is now being shared using IT over IP and the abuse that it can go through is what is making the security community bothered. When we talk about securing such systems, we should be differentiating when we are talking about the security of IT and when the security of SCADA. In a cyber-physical system IT security has to complement

SCADA security as it alone is not enough to stop attacks. Application white-listing, access control, anti-virus, IDPS, cryptographic primitives is the way to look at solving the problem (without burdening the system). The only issue that remains is that attackers are/will still find their ways into grid (Stuxnet though an old example but still applicable).

If I now look at an attacker's perspective (SCADA viewpoint), his objective is to somehow feed bad information to the SE. By doing this, it will achieve its purpose of destabilizing the grid and the associated knock-on effects (cascading etc). Though there are bad data detection algorithms to detect inexact data but recent published works have demonstrated that these algorithms can be by-passed, and that is of some concern. The picture below shows some attack points on SCADA. The picture is taken from Vikings Project in EU.



There are lots of solutions out there in market but I still feel that when it comes to prevention, it is hard to stand-up and say we will prevent a collapse.

Issues with prevention system development:

- Lack of SCADA Test-bed: There are some in USA and Europe, but I am still to find one in Asia. The reason for this seems to be because of
  - Test environment using bulk power system components and control software is costly
  - A grid is too complex to be set up with analog scaled down models
  - One cannot test developed security solutions directly on real power system

A SCADA simulator can help us in bridging the Cyber-Physical divide by bringing in the Physical system inside the Cyber domain. We already have tools for power system modeling. We can use them and by building wrapper software above them to represent

MTU, RTU and communication protocol set-up. This can be of huge help to small security groups spread across the globe.

- Lack of solutions which can help the state estimator in making more informed decisions.
- It will be hard for utility companies to trust security solutions completely. With the kind of affect a false positive can have on such system, it's very unlikely that utility companies can entrust a prevention mechanism completely.
- Lack of trust in upgrades that happen time to time in software community, whether OS or otherwise.
- The real-time nature of some of these systems means that the alerting mechanism has to be much faster than typical SCADA cycles

---

### **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](mailto: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/](http://www.us-cert.gov/control_systems/ics-cert/).



Other important contact information:

Website Address: [http://www.us-cert.gov/control\\_systems/](http://www.us-cert.gov/control_systems/)

ICS-CERT Email: [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov)

Phone: 1-877-776-7585

CSSP Email: [cssp@hq.dhs.gov](mailto:cssp@hq.dhs.gov)