Industrial Control Systems
Cyber Emergency Response Team
(NCCIC/ICS CERT)

September 2015

ICSJWG Quarterly Newsletter

—ICSJWG EXPANDING THE COMMUNITY—

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 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 critical infrastructure.

For more information, visit http://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

Contents

Face to Face Meetings Update..... 1
ICS Cybersecurity for the C-Level 2
Cyber Resilience of Building Control Systems Workshop 2
National Cybersecurity Center of Excellence Call for Comments and Collaboration..... 2
What Are Critical Infrastructure Sectors? 3
Spotlight on International 4
Updates From Around ICS-CERT..... 5
Onsite Assessments & Evaluation 6
Cyber Security Evaluation Tool (CSET®) Version 7.0 8
Training with ICS-CERT..... 8
Alerts & Advisories: Feedback and Questions. 10
Homeland Security Information Network (HSIN) Portal 10
ICS-CERT Monitor and Twitter Information 10
ICS-CERT Contact Information 11
Participation is Key! 11
Industrial Control Systems Contributed Content 11
Steering Away From IT Security's "Gold Standard" 11
The ISA99 Committee Meets in Frankfurt..... 13
FERC NOPR on CIP V6: Another Step in the Right Direction 14
How Government Agencies Can Become Secure by Default 18
Protecting Generating Networks with Unidirectional Security Gateways 18

Face to Face Meetings Update

The next Face to Face meeting of the ICSJWG is fast approaching. Taking place in Savannah, Georgia from October 27th to 29th, it will offer presentations on a wide variety of topics and bring together professionals from across the 16 sectors in a variety of roles. This meeting will feature presentations from Director of the National Cybersecurity and Communications Integration Center (NCCIC) John Felker, President of the Technology Association of Georgia Tino Mantella, Independent Security Researcher Marina Krotofil, and Robert Lee from the SANS Institute.

The Meeting will also feature a number of new special sessions. The ICS Village will bring a replica of a typical water plant network setup and with hands-on isolated industrial equipment stations. They will demonstrate commonly found hardware and software that is used in most industries and common security/discovery tools which can be run against these systems. Attendees will have the opportunity to program a PLC, use an ICS protocol fuzzer or just ask questions and push buttons. In addition, there will be special sessions tailored to international partners and the first ISCJWG Vendor Expo. More information regarding the 2015 Fall Meeting can be found at https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG including the Registration Link, Frequently Asked Questions, and Draft Agenda. If you have additional questions, please contact ICSJWG Communications.

ICS Cybersecurity for the C-Level

ICS-CERT, with direction from the ICSJWG, created a new document, "ICS Cybersecurity for the C-Level," in response to growing demand from stakeholders for a concise document that can effectively communicate the need for better ICS cybersecurity practices to the C-Level. This document aims to support that need by providing a succinct overview of basic cybersecurity principles and best practices for ICS-related organizations.

This document provides information regarding two sophisticated malware campaigns, describes key ICS cybersecurity questions and risk management concepts, and details specific services and activities that ICS-CERT can provide to help improve the cybersecurity of the nation's critical infrastructure. This document can be found on ICS-CERT website as well as on the ICSJWG page.

Cyber Resilience of Building Control Systems Workshop

The Federal Facility Facilities Council (FFC), under the auspices of the National Research Council (NRC), part of the National Academies, is sponsoring a two-day "Cyber Resilience of Building Control Systems" Workshop November 17 - 19, 2015, hosted by the Department of Commerce in Washington, DC. The purpose of this workshop is to generate awareness of cyber security vulnerabilities, current and forthcoming guidance, and protection strategies relevant to federal facility stakeholders. Participants can explore state-of-the art technologies and services offered by leading vendors in this rapidly evolving market landscape. The workshop will continue into a third day with optional demonstrations and hands-on training on various tools and strategies.

Workshop BCS cyber resilience topics:

- Global/National Landscape
- Policy and Governance
- Building Control System Vulnerabilities
- Implementing RMF for Federal Facilities
- Federal Landscape
- Federal Cybersecurity Acquisition/Budgeting Requirements
- Government Tools for Discovery & Assessment / Cyber Ranges
- Commercial Landscape
- Continuous Monitoring Solutions
- Tools for Discovery, Assessment
- Training, Equipping and Certifying Facility Cyber Warriors
- View from the Field
- Threat Info Sharing
- Vendor Capability "Fast Pitches" (5 minutes per vendor)
- R&D Roadmap
- Optional Training, Demos - CSET, others TBA

Please save the date if you would like to attend, and forward to your colleagues who may be interested. This is a no-cost event and travel, lodging and per-diem costs will be the responsibility of attendees. Register at: http://sgiz.mobi/s3/0e8622dac0a2. The event will be held at 1401 Constitution Ave NW, Washington, D.C. Please visit the website for more details.

National Cybersecurity Center of Excellence Call for Comments and Collaboration

The National Cybersecurity Center of Excellence (NCCoE) is requesting comments on a draft guide to help energy companies better control who has access to their networked resources, including buildings, equipment, information technology and industrial control systems. The center, part of the US Commerce Department's National Institute of Standards and Technology (NIST), works with IT

developers and providers to help businesses reduce their cyber risk.

The NCCoE at NIST has released a draft of its first energy sector cybersecurity practice guide, *Identity and Access Management for Electric Utilities*. The draft is available for download on the NCCoE website at https://nccoe.nist.gov/projects/use_cases/idam.

The NCCoE collaborated with experts from the energy sector to develop a use case scenario based on day-to-day operations and worked with technology vendors to develop example solutions demonstrating a centralized identity and access management system that would make changing or revoking privileges simple and quick.

The practice guide provides instructions on how to achieve a centralized identity and access management system and includes examples of all the necessary components and installation, configuration, and integration. The guide, which is modular and suitable for organizations of all sizes, also maps security characteristics to guidance and best practices from NIST and other standards organizations, and to North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards.

Comment period closes on October 23, 2015 and the NIST press release for the call for comments may be found at http://www.nist.gov/itl/20150825guide.cfm.

NCCoE is also seeking collaborators to provide products and technical expertise on three projects to help organizations improve their cybersecurity. The projects focus on access control, personal identity verification credentials and mobile devices. Each project will result in an example cybersecurity design that can be used by organizations in multiple industry sectors. The full information is available at NCCoE Seeks Vendors to Develop Model Systems for Controlling Access to IT Assets.

What Are Critical Infrastructure Sectors?

ICS-CERT's mission is to reduce risk to the Nation's critical infrastructure by strengthening control systems security and resilience through public-private partnerships. Critical infrastructure in the US is divided to sixteen sectors and defined in Presidential Policy Directive 21 (PPD 21). ICS-CERT fulfills its mission by: responding to and analyzing control systems-related incidents; conducting vulnerability, malware, and digital media analysis; providing onsite incident response services; providing situational awareness in the form of actionable intelligence; coordinating the responsible disclosure of vulnerabilities and associated mitigations; and sharing and coordinating vulnerability information and threat analysis through information products and alerts. If systems are exposed or not secure, they are vulnerable to attack. These attacks can range from the mundane to the critical and expose both the system owner and their customers to physical risks.

ICS-CERT's mission can be traced down from PPD 21 though the DHS Strategy for Security Control Systems, to build a long-term vision of effective risk management through coordination efforts. Released in 2013, PPD 21 is designed to promote the strength and resilience of US critical infrastructure. It defines the 16 critical infrastructure sectors as: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, and Water and Wastewater Systems.

Each sector has a 'Sector-Specific Agency' (SSA) associated with it which indicates the Federal department or agency responsible for providing institutional knowledge, specialized expertise, and any security or resilience programs. ICS-CERT works with all sectors, regardless of SSA to ensure effective coordination and risk management to address vulnerabilities. Also within

each sector there are a variety of organizations available for information sharing, coordination, and learning. Typically these take the form of Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), and various trade organizations. These groups allow individual stakeholder to leverage their scale and achieve better results. Many of the 16 critical infrastructure sectors encompass multiple sub sectors. For example the energy sector covers electric, oil, and gas among other forms of energy. The transportation sector covers trains, shipping, maritime transport. Generally, there are similarities across the subsectors, linking them together topically and technologically.

Critical infrastructure in the US is held primarily by private entities. In some cases, federal, state, or municipal governments may own part of all of an asset, but approximately 85% of our critical infrastructure is owned, operated, and controlled by the private sector. Therefore, collaboration between the government and private sector is key to ensuring the protection of our critical infrastructure and in turn, the homeland.

Spotlight on International

The risks to industrial control systems are not geographically limited. In an interconnected world, cyber risk is global by default. In particular, recent malware campaigns demonstrate that control systems directly facing the Internet get compromised without properly implemented security measures. In addition, supply chain, manufacturing, and markets are all global endeavors. Therefore, a discovered vulnerability in one product may be exploitable in systems around the world. The ubiquitous nature of industrial control systems products means that nefarious actors looking to discover vulnerabilities are more able to analyze products and systems. In many cases, the ability to obtain and study a system is key to exploiting it. Even if a cyber-event doesn't touch US critical infrastructure, the same tactics may be used against the US at a later date. In this inter-connective environment, international engagement is both a strategic necessity and an operational imperative for the DHS cybersecurity mission.

Although US critical infrastructure is held primarily by private entities, this dynamic is not necessarily present in partner countries where a government may play a more forward role in critical infrastructure. Within each country, the responsibility for industrial control systems is handled differently with regard to both scope and organization. The responsibility may be broken out over multiple agencies with each being responsible for different sectors, or a country may choose to define its critical infrastructure to encompass completely different areas of national infrastructure and the economy. The different setup in each country means that when ICS-CERT interacts with international counterparts it is often with a variety of different organizations rather than just the "ICS-CERT" for that country.

In the international community, cyber is playing an ever increasing role, and global organizations have recognized the need to address cyber issues. ICSJWG and ICS-CERT enjoy working with our international partners throughout the community in order to further the conversation around cyber issues. However, the responsibility for securing systems remains on states and the private entities who own the networks. Industrial control systems particularly are just beginning to be explored both from a strategic and tactical perspective.

Much of ICS-CERT's coordination on international engagements is done in tandem with US-CERT in order to benefit from its pre-existing relationships with other CERTs. ICS-CERT's engagement with the international community covers a wide range of activities from meetings and speaking engagements to product development and mutual participation in the Industrial Control Systems Joint Working Group (ICSJWG). This fall the ICSJWG is welcoming back international sessions, particularly designed specifically for international partners. ICS-CERT works with the international

community throughout the year to share information. By engaging with the international community to foster operational collaboration and share information, we improve our collective situational awareness and response to current threats.

Updates From Around ICS-CERT

Notable Incidents

In July, ICS-CERT became aware of a spear-phishing campaign by advanced persistent threat (APT) actors that targeted multiple sectors, including Chemical, Critical Manufacturing, Energy, and Government Facilities. The activity involved emails with links that redirected to web sites hosting malicious files that exploited a zero-day vulnerability that has since been patched in Adobe Flash Player.

In previous incidents occurring in early 2014, the same actors also used various social engineering tactics and social media to perform reconnaissance and target company employees. In one case, the malicious actors used a social media account to pose as a perspective candidate for employment and opened a dialogue with employees of a critical infrastructure asset owner.

The actors asked probing questions and compromised the business network. ICS-CERT worked with the affected entity to confirm that the incident occurred on their business network and was quickly contained. No control systems were impacted.

While the motivations of the APT actors remain unknown, the use of social media and zero-day exploits illustrates a concerted effort to gain access to critical infrastructure networks. In response, ICS-CERT published an alert to the secure portal to consolidate previous campaign indicators with new indicators for network defenders to use. Asset owners/operators can request a portal account by sending an email to ics-cert@hq.dhs.gov.

Focus on: Medical Device Cybersecurity

ICS-CERT might not be the first organization that comes to mind when thinking of medical device cybersecurity. However, Healthcare and Public Health is one of the 16 critical infrastructure sectors, and our work with medical device vendors on software and hardware vulnerability coordination has been increasing over the last 3 years.

Similarities in the underlying embedded hardware and software technologies connect medical device and control system vulnerability exploitation. Programmable logic controllers communicate on a network, have embedded control of processes, and provide human-readable feedback just as, for example, an infusion pump or an MRI does. Vulnerabilities found in a control system device can affect a medical device when standard code libraries are used to develop the embedded operating systems.

ICS-CERT collaborates with the Department of Health and Human Services (HHS), the Food and Drug Administration (FDA), and the National Health Information Sharing and Analysis Center (NH-ISAC). These information sharing relationships are concerned with patient safety rather than regulatory issues and are similar to our relationships with the well-known ES-ISAC (electricity sector) and Water-ISAC (Water and Wastewater Services Sector). Our goal is to provide the same assessment, vulnerability coordination, and incident response services to medical asset owners and operators, as well as device vendors, as we do for those in each of the other 15 critical infrastructure sectors.

Onsite Assessments & Evaluation

The recently released "Industrial Control Systems Assessments FY 2014 Overview and Analysis" provides an overview of all ICS-CERT on-site assessments conducted in FY14. ICS-CERT offers three types of onsite assessments, Design Architecture Reviews (DAR), Network Architecture Verification and Validations (NAVV), and facilitated CSET® Assessments. ICS-CERT uses the National Institute of Standards and Technology's *Recommended Security Controls for Federal Information Systems* (NIST 800-53) as a structured method to group and analyze vulnerabilities found during DAR and NAVV assessments. The NIST 800-53 control family mappings provide a consistent and repeatable methodology for collecting and correlating data to analyze and trend key discoveries at a holistic level. Data collected during these assessments is used to provide recommendations to the asset, and helps ICS-CERT to continually refine its assessment services. All data used by ICS-CERT is protected by Protected Critical Infrastructure Information (PCII) agreements with the asset owner. More information on ICS-CERT assessment services and offerings can be found here or in the full report.

ICS-CERT's stakeholders drive the demand for cybersecurity assessments and, at the request of its partners, ICS-CERT performed a total of 104 assessments in FY 2014. ICS-CERT's partners participate in ICS cybersecurity assessments on a voluntary basis, and stakeholder requests—along with factors such as sector risk profile, specific threat information, the dependence of specific critical infrastructure sectors on control systems, etc.—focus ICS-CERT's assessment activity.

The cyber security risks that organizations face decrease significantly with a strong ICS architectural framework that includes both protective and detective cybersecurity controls, implemented at multiple layers. Similarly, a robust architecture improves the organization's capability to adequately detect and defend against potential threats and exploits. There are several common vulnerabilities that represent significant weaknesses that asset owners should understand and know how to mitigate. These weaknesses, as well as some mitigation suggestions, are introduced below.

Systems and Communications Protection

Without a comprehensive asset inventory of the devices and systems that directly support the OT environment, it can be difficult to establish a cyber-boundary and enforce protective and detective measures. To comprehensively incorporate cybersecurity within the OT architecture, asset owners should establish zones of protection around ICS systems. Understanding the nature of communication flows— including operational ingress/egress points—and protocol hierarchy helps define the logical boundary. It is also imperative to fully understand and define the range of ports and services required for the systems within the ICS environment, as these delineations are necessary for enforcing proper zoning. Without completing this analysis and understanding the required intercommunications at the design onset, existing security and segmentation controls (for example, firewalls, virtual local area networks [VLAN], and access-control lists) can quickly become ineffective, particularly if network paths must be continually opened and modified between devices and network segments. Once asset owners identify and verify the scope of required communication flows, the design of the infrastructure should support both virtual and logical separation of the ICS network, on physically separate devices from the enterprise/corporate network.

Access Control – Information Flow Enforcement

Understanding the communication flows occurring within the ICS network—and conversely those sourced from or destined to the ICS network—is an essential precursor to building a powerful detection and monitoring platform for verifying network traffic and ensuring the integrity and availability of the control process. If devices do not have an operational need to establish a

communications channel, the architecture should support the capability to deny and prevent devices and systems from communicating via a direct or indirect channel. In addition, asset owners should maintain the capability to log and record traffic for systems *attempting* to establish a communications channel, even if explicitly denied. Asset owners should also baseline intra-network traffic in accordance with the operational nature of the control process.

Access Control – Remote Access

The nature of distributed operations, coupled with an observed reduction in the personnel directly responsible for maintaining and monitoring process automation, presents a challenge for real-time monitoring, response, and investigative actions, an important part of control system operations. If not architected properly, remote access can elevate risk and become a catalyst for potentially unauthorized access or nefarious activity. Remote access should not sacrifice security for the sake of convenience. An insecure implementation and use of remote access capabilities can completely invalidate even the best security architecture. Control systems and their supporting systems must never be directly accessible through untrusted networks such as the Internet; they should be protected and sequestered from untrusted (external) networks and systems.

Asset owners should implement multiple defense layers for accessing control system networks from a remote location. Generally, most organizations require their personnel to utilize a VPN technology using encryption to interface with corporate systems and applications when accessing from a remote location. For control systems, the capability to directly interface with supporting systems and components should not be permissible directly from systems housed on the corporate or enterprise network. Rather, asset owners should only allow access through an intermediate system or "jump box" resident within a dedicated Control Systems DMZ. Access to the intermediate system should require a second layer of authentication, which is unique and different from that used to remotely access the corporate environment or corporate systems via VPN. Additionally, to the degree possible, security policy should limit the use of persistent VPN tunnels, and the organization should have the capability to directly control and authorize specific vendors or contractors to initiate remote sessions.

Access Control – Least Privilege

Asset owners should assign roles and permissions to users of the various systems and applications in the automation process based upon the concept of least privilege. Before assigning users' specific permissions, an organization must formally define the roles and responsibilities required to support operational needs. Once user roles and responsibilities are defined, asset owners should review the technologies in place to ensure that the necessary mappings and restrictions can be enforced, tracked, audited, and verified.

Organizations should not allow the unnecessary use of elevated and administrative permissions for daily job functions, and personnel should utilize an account with minimal permissions assigned for normalized operations. If there is a need for use of a privileged account for daily job functions, the organization should harden that system and consider additional defense-in-depth measures to isolate and protect the system. Additionally, logging and monitoring should track user activity and have the capability to provide a record (including timestamp) of user activity occurring on a system or within an application. Asset owners should log, audit, and review changes made by users, including changes pertaining to user mappings, roles, and privilege assignments.

Physical and Environmental Protection

Many asset owners rely upon physical security controls to safeguard and protect key systems utilized in support of the process and automation. If adversaries can exploit a weakness in physical

security, this could lead to risks correlating to both cyber and physical consequences. As many control system environments are widely distributed over a large geographic area, remote sites and locations may not always be physically manned by personnel at all times. It is especially important to enforce both physical and cyber security controls, including monitoring for these environments. If a physical breach were to occur, this could provide a vector for an outsider to gain upstream access back into the core of the control systems infrastructure.

Conclusions

The high-level discoveries and mitigation recommendations outlined in the report should not be used as an all-inclusive focus of an assessment; rather, these areas should be carefully reviewed and encompassed within the scope of an organization's overall cyber security framework, design, and review. Addressing the best practices and recommendations in this report can greatly improve a CI asset owner's overall security posture and heighten awareness of potential threats or cyber-attacks targeting their specific operations. The ICS-CERT Assessments team is currently scheduling future assessments. If you are interested in coordinating an Onsite Assessment, please contact ICS-CERT at ics-assessments@hq.dhs.gov. The full report can be found here.

Cyber Security Evaluation Tool (CSET®) Version 7.0

ICS-CERT has released the latest version of its Cyber Security Evaluation Tool (CSET®), CSET 7.0. New standards include the Cybersecurity Capability Maturity Model (C2M2), Version 1.1, the Department of Defense (DoD) Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) and the National Institute of Standards and Technology Interagency Report (NISTIR) 7628 Volume 1, Revision 1, Guidelines for Smart Grid Cybersecurity.

In addition, the user interface was completely redesigned with a new, more modern look and intuitive interface. Performance updates include increased responsiveness when answering questions, the ability to change the question text size for improved readability, and new encryption functionality.

For additional information on CSET or to download a copy, go to https://ics-cert.us-cert.gov/assessments. To report a problem or request a new feature, go to http://cset.inl.gov

Training with ICS-CERT

Cybersecurity for Industrial Control Systems Online Courses

Introductory courses for ICS-CERT are available online through our Virtual Learning Portal. In addition to "Operational Security (OPSEC) for Control Systems (100W)" which provides a basic overview in order to recognize potential weaknesses in operations, ICS-CERT also maintains the "Cybersecurity for Industrial Control Systems (210W)" online training course. The 201W training course contains modules covering many aspects of cybersecurity for ICS. This course is a web based version of the regional 101 and 201 instructor-led courses which, taken consecutively, will introduce students to the basics of ICS security. This includes a comparative analysis of information technology and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain.

Technical instruction on the protection of ICS using offensive and defensive methods is provided during the course. Upon completion, students will understand how cyber-attacks could be launched, why they work, and mitigation strategies to increase the cybersecurity posture of their control system.

In order to take advantage of these modules and enhance your knowledge of ICS security, simply navigate to: https://ics-cert-training.inl.gov/ and choose Web Based Training.

Cybersecurity for Industrial Control Systems Instructor-Led Courses

ICS-CERT continues to hold regional trainings around the country. Each multiple-day session is designed to allow participants to take Introduction to Control Systems Cybersecurity (101) Lecture, Intermediate Cybersecurity for Industrial Control Systems Part 1 (201) Lecture and Intermediate Cybersecurity for Industrial Control Systems Part 2 (202) including lab, and exercises. The courses help students understand exactly how attacks against process control systems could be launched and to provide mitigation strategies to increase the cyber security posture of their control systems networks. During the sessions, students will review industrial control systems security, demonstrate weaknesses and exploits, and provide an understanding of key issues in cybersecurity related to industrial control systems. In addition, part 2 of the 202 course offers instruction and hands-on application of the concepts presented. This includes, but is not limited to, a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain. So far this year, sessions have been held in Phoenix, Arizona, Salt Lake City, Utah and Oklahoma City, Oklahoma. More information on upcoming sessions, including how to register, can be found at both https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT and https://ics-cert.us-cert.gov/Calendar respectively.

Industrial Control Systems Cybersecurity Training (301) for Fiscal Year (FY) 2015

ICS-CERT 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. They also provide an opportunity for attendees to network and collaborate with other colleagues involved in operating and protecting control systems networks.

- **Day 1**: Overview of DHS ICS-CERT, 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.

ICS Cybersecurity (301) training is scheduled for each month throughout the rest of the calendar year. All course dates are subject to change but the current schedule for ICS Cybersecurity (301) training events is:

- November 16-20, 2015
- December 7-11, 2015

- Keep an eye on http://ics-cert.us-cert.gov/Calendar for more upcoming dates

There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant. As the date scheduled for the 301 Training gets closer, a link for registration will be made available on the public facing web page. Please monitor our page at http://ics-cert.us-cert.gov/Calendar for scheduled sessions of interest and for any possible changes to specific training dates. Register by clicking on the link provided for that session using the registration link found at the appropriate date. Registration is open approximately two (2) months before the start of a class. Due to high demand, classes are limited to a maximum of two (2) individuals per company per event. Each training session accepts a limited number of international partner registrations. Class sizes are limited to approximately 40 persons and fill quickly – so early registration is encouraged. Should you register and then need to cancel, a notification may be sent to CSSP_Training@hq.dhs.gov with as much advanced notice as possible so that others who may be on a waiting list may be contacted with the opportunity to attend the course.

Alerts & Advisories: Feedback and Questions

As with any malicious and targeted cyber activity, ICS-CERT requests feedback and reporting if your organization has been targeted. Reporting your cyber events and incidents to ICS-CERT helps the community at large have a better understanding of the activity occurring across sectors and the techniques/indicators of compromise (IOCs) being used. ICS-CERT will protect and anonymize your information and only share the technically relevant information (such as IOCs) with partners that have a need to know.

ICS-CERT publishes alerts to provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks and advisories that provide timely information about current security issues, vulnerabilities, and exploits. These notifications are available on the ICS-CERT website under Information Products.

If you, or a member of your organization has a question regarding these products and what they mean for your organization please contact ICS-CERT at ics-cert@hq.dhs.gov. If you have an ICS incident or software vulnerability to report, please go to http://ics-cert.us-cert.gov and scroll to the bottom of the page to the “I Want To” selections.

Homeland Security Information Network (HSIN) Portal

HSIN is the information sharing tool chosen by ICSJWG for the membership. Reference materials may be uploaded for the use of the members. Those that are interested in obtaining an account should send an email to ICSJWG.Communications@hq.dhs.gov with your name, company, contact information, and critical infrastructure sector. Having an account is useful for participants to review posted materials on the portal.

ICS-CERT Monitor and Twitter Information

ICS-CERT releases its Monitor Newsletters in order to inform the control systems cybersecurity community of the latest activities. The Monitor can be accessed at http://ics-cert.us-cert.gov/ along with other Control Systems Advisories and Reports. The latest Monitor Newsletter covers July/August 2015.

The official Twitter account has more and more followers every month. If you want the latest news involving ICS-CERT activities, follow them @ICSCERT.

ICS-CERT Contact Information

ICS-CERT encourages you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting information is available at http://www.dhs.gov/report-cyber-risks and at the bottom of the ICS-CERT webpage.

Other important contact information:

Website Address: http://ics-cert.us-cert.gov/

ICS-CERT Email: ics-cert@hq.dhs.gov

Phone: 1-877-776-7585

Participation is Key!

Your participation and input are critical to the overall mission of the ICSJWG in coordinating cybersecurity efforts to secure industrial control systems across the nation's critical infrastructure.

Face-to-face meetings and webinars designed to move the nation forward in our cybersecurity posture both rely on your input and volunteer participation. General suggestions and input, webinar ideas, and newsletter articles may be made at any time at ICSJWG.Communications@hq.dhs.gov.

Industrial Control Systems Contributed Content

ICSJWG is now accepting contributions and upcoming event announcements from the community pertaining to control systems cybersecurity for the December Quarterly Newsletter. If you want to submit an article or an upcoming ICS-related event announcement for the December Newsletter, please email ICSJWG.Communications@hq.dhs.gov and we will take your submission into consideration for publication. The deadline for submissions for the December Newsletter is **December 16, 2015**. This edition and past editions are also located on HSIN at http://go.usa.gov/FnyY.

Also, thank you to all members who contributed content to the Quarterly Newsletter! The following articles were 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 are provided as is, with no warranties, and should be confirmed and tested prior to implementation.***

Steering Away From IT Security's "Gold Standard"

By: Paul Feldman, Board Director, Industry Advisor

For the first decade of industrial control-system cybersecurity, IT security practices were held up as the gold standard for control system security. Yes, certain IT practices amounted to constant, aggressive change to "keep up with the bad guys," such as constant updates to anti-virus signatures and security updates. While these practices were recognized as a poor fit for the engineering change control discipline fundamental to safety and reliability, IT experts kept telling us that if we could just somehow *invent* a way to apply standard IT security practices to control systems, then all would be well.

This expert consensus is shifting. The IT "gold standard" has been found inadequate to the

needs of protecting control systems. How can this be? Well, let's look at what is the "IT way." IT security starts at the perimeter with a layer or three of firewalls between the open Internet and the corporate network. These firewalls are assumed to be porous; after all, they forward messages from the Internet into the corporate network, including millions of email messages each day for large organizations, and a comparable number of Web pages. Some of these messages contain attacks. Firewall vendors and security practitioners do what they can to filter out the attacks, but no filter is perfect. Some attacks get through.

Inside the network perimeter, what do we find? Software: countless computers running all manner of software, including security software. The problem is that all software has bugs and some bugs are security vulnerabilities. In practice then, all software can be hacked, even security software. For proof of this, we need look only as far as every security software vendor's website and count the security updates posted last month.

All of this is why the pinnacle of every modern, defense-in-depth, "gold-standard" IT security program is intrusion detection. We put "eyes on glass," we pit "our experts against theirs," we assume we have been compromised and we systematically hunt down the equipment our attackers have taken over. We isolate that equipment, erase it and restore it from a pre-compromise backup.

Control system security is different

How does this work for control system security? Firewalls at the control system perimeter are just as porous as firewalls at the corporate perimeter. Firewalls are routers after all, routers with filters. Firewalls forward messages from less-trusted networks into control-system networks, and the filters do what they can to separate "bad" messages from "good" messages. No filter is or can ever be perfect, though. From time to time, all control-system firewalls forward attacks into control-system networks.

Inside every control system network, we find just as much software as we find in corporate networks. Control systems generally have a little less security software deployed than do IT systems, and they are generally a little more out of date than are IT systems. This means that just like IT systems, control-system software can be hacked; the interior of control system networks is generally an even softer target than the interior of IT networks. At first glance then, all the preconditions seem identical, and so intrusion detection systems seem just as essential to ICS networks as to IT networks.

The problem with intrusion detection is that it takes time. In June of 2015, Tripwire published survey results of 400 critical infrastructure executives and IT professionals: 86 percent of the respondents were confident that they could detect a compromised equipment on their control-system networks within a week of the compromise. Other studies suggest this confidence is misplaced. A 2014 Ponemon study showed that the average time from infection to detection was 170 days, and a 2014 Verizon study showed that the average time from infection to remediation was 200 days.

Whether the time to detect and remediate compromised equipment is a month, or a week, or an hour is immaterial. For all of that time, however long it is, a remote attacker has control of equipment on our reliability-critical and safety-critical control-system networks. Control system practitioners always regard such unauthorized operation of their equipment as an unacceptable risk. The IT "gold standard" has failed control-system security practitioners. Control-system security must be based on a much more thorough foundation of attack protection than is possible on IT networks.

Revising control-system security standards

Control-system security standards are being revised and updated all over the world, and are evolving away from this IT approach to security. For example, France's 2014 ANSSI regulations for control-system security identify three types of control-system networks, depending on the societal

impact of the networks. Class 1 networks are expendable; society suffers minimally when such a network is compromised. Class 2 networks are important to society, and the compromise of class 3 networks has serious consequences. For class 2 networks, ANSSI states that connections to less-trusted networks "should be unidirectional" toward the less-trusted system. For class 3 networks, "The interconnection of a class 3 ICS with an ICS of a lower class shall be unidirectional towards the latter." The recently-updated NIST 800-82r2, NERC CIP V5 and V6 standards, and IEC 62443-3-3 all position unidirectional gateways within control-system defense-in-depth programs, as well.

To be fair, many elements of the IT gold standard are still applicable to control system security; it is the emphasis that is shifting. The top priorities on control system networks are not availability or integrity after all, but safety and reliability.

The ANSSI classification is instructive. The control networks most important to society must be protected unidirectionally, but there are no such demands of networks French society considers expendable. Few businesses operating large industrial sites, though, will regard their industrial operations as expendable to the business, however expendable society may deem those operations.

With this new understanding of control-system security being codified in updated standards and advice, we all need to start asking, "Which of our operations are expendable enough to be protected by firewalls?"

The ISA99 Committee Meets in Frankfurt

The ISA99 committee on industrial automation and control systems (IACS) cybersecurity held a series of working meetings in Frankfurt Germany on June 23-25, 2015. In addition to current members of the committee several external stakeholders and interested parties attended the meeting to learn more about the committee and to offer their input on recent developments and current priorities.

The purpose of the meetings was to review recent developments, collect additional feedback on several of the fundamental concepts and reaffirm plans for several documents in the ISA/IEC-62443 series of standards. Individual sessions focused on topics ranging from general summary of the current status of the committee work products to reviews of the status of specific standards. The agenda also included time for individual work and task groups to continue work on their respective work products.

Fundamental Concepts

There are several fundamental concepts that form the basis for the ISA/IEC-62443 series. Each of these concepts is introduced in the planned second edition of the ISA/IEC-62443-1-1 standard, and further detailed and applied in the remaining standards in the series. In the course of the Frankfurt meetings those present reviewed several of these concepts and reaffirmed their importance as key elements of the series. Any inconsistencies across the standards were noted and will be addressed in subsequent editions.

Life Cycles

The design, development, implementation and operation of industrial control systems take place in the context of set of intersecting lifecycles, each addressing a specific set of activities and involving particular contributors.

The product development life cycle is primarily the responsibility of the product or system

supplier. Integration and commissioning is the focus of system integrators and operation and maintenance is the responsibility of the asset owner.

Collectively these life cycles provide the context for the gathering of requirements and the subsequent development of secure products, systems and solutions.

Document Status

Several documents in the ISA/IEC-62443 series have been formally published or are about to be released to the committee for comment or vote. Recent publications include:

- 62443-2-3: Patch Management in the IACS Environment
- 62443-2-4: Requirements for IACS Solutions Providers

Documents that have recently been circulated for review and comment include:

- 62443-4-1: Product Development Requirements
- 62443-4-2: Technical Security Requirements for IACS Components

Finally, the following draft documents have been or will soon be issued to the committee for review and approval:

- 62443-1-3: System Security Metrics
- 62443-3-2: Security Risk Assessment and System Design

Implications for Stakeholders

The stakeholder community for the ISA/IEC-62443 standards includes suppliers, integrators and asset owners across a broad range of industries. Each of these groups have different levels of interest in and applicability for the various types of standards in the series.

Those with interest in learning more about the information contained in the 62443 standards will soon have available several new drafts for re-view and comments, as well as completed and published standards and reports in areas such as risk assessment and patch management.

It is possible to apply these standards now, both to the design and configuration of industrial control systems, as well as to their regular operation and maintenance. Assistance in such application is available in the form of a series of training courses available from ISA.

As the full set of normative requirements and informative guidance be-comes available the attention of the committee will begin to shift to the development of additional tools such as metrics and use cases. The will be also become valuable resources to those applying the standards.

More Information

Detailed notes from the meeting are available for review on the committee web site, at:
http://isa99.isa.org/Public/Meetings/Committee/201506-Frankfurt/Committee-Meeting-Notes.pdf

---

FERC NOPR on CIP V6: Another Step in the Right Direction

By: Joseph J. Januszewski, III, CISSP

With the Notice of Proposed Rulemaking (NOPR) issued in RM15-14-000 on July 16, 2015, the Federal Energy Regulatory Commission (FERC) made five broad changes in the critical infrastructure protection (CIP) Reliability Standards in the Bulk Electric System (BES). Four address various areas of the CIP version 5 Standards, and one proposes seven new Standards for CIP version 6. FERC proposes to approve the following critical infrastructure protection (CIP) Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training),CIP-006-6 (Physical Security of BES Cyber

Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments),and CIP-011-2 (Information Protection).

The four over-arching goals that permeate the proposed CIP version 6 Standards are to:

(1) eliminate the "identify, assess, and correct" language in 17 of the CIP version 5 Standard requirements;
(2) provide enhanced security controls for Low Impact assets;
(3) provide controls to address the risks posed by transient electronic devices (e.g., thumb drives and laptop computers); and to
(4) address the need for a NERC definition for the term "communication networks."

Based upon this NOPR, there still appears to be several broad technical areas to address, which include:

- the question of the level of use of commercially-available encryption schemes to protect control information and data,
- the level of risk associated with transient cyber assets, and;
- whether the concept of "Low Impact BES Cyber Systems" is realistic in the current threat landscape.

The Impact of Encryption in Real-Time Systems (RTS)

The question of the level of control data latency while using encryption continues to be an outstanding issue. It begs a further question: has a real-time or near-real-time objective evaluation been conducted in this area?

Is the comparison of a web server farm belonging to a major media provider, or that of a large database-driven application server with communications over TCP/IP using digital certificates *fair* with regard to that of comparatively low-volume, low-latency traffic? Granted, high levels of control and data information may cross links, however, many network latency models deal with multimedia "Web-based" traffic levels, but relatively fewer connections occur. A closer approximation may be made with various examples performed using financial market data, which occurs in sub-second time resolutions. [1] Other challenges, for instance, legacy controls and systems, complicate the matter. The concept of an "Internet of Things" focuses on the use of the global Internet and its communication protocols as an underlying infrastructure for access and communication. In addition to economies of scale gained by using common devices and software across an expansive framework, this also provides the means and platforms to attack network entities using the existing infrastructure. The need to keep information confidential and the integrity of control of various industrial control systems is vital to various aspects of critical infrastructure.

Protecting the Environment from Transient Cyber Assets

The protection of transient electronic devices in the BES is vital, the tired example of Stuxnet now seeming trite, notwithstanding. If these devices are not under the same level of protection as auditable BES Cyber Assets, then should they be permitted inside the security perimeter? To do so creates a potential "Trojan Horse" scenario. Drawing from a case study which impacted another sector, the attack on Point-of-Sale (PoS) systems belonging to a major department store chain through the network access used by an HVAC contractor exposed the entire operating infrastructure of that retailer to attack. [2]

While the NERC Petition regarding the Protection of Transient Devices requests NERC to re-examine its processes and procedures using its six security elements, one must ask if existing procedures would protect systems from the original Stuxnet attack vector, if it had been used to target BES Cyber Assets and Systems rather than controllers used for nuclear centrifuges.

As noted in the author's previous article, "Industrial Control Systems in the Power Sector Under FERC Order 791", published in the December 2013 issue of the ICSJWG Quarterly Newsletter, the 30-day exemption of a transient Cyber Asset to be considered a BES Cyber Asset is in the author's view, a potential invitation to attack. There is the potential for a "Transient Cyber Asset", being connected for 30 consecutive calendar days or less to not be considered a BES Cyber Asset, however, the reality is that it only takes a few minutes (or less) to transfer malware at USB 3.0 or Bluetooth throughput capacities from device to device. In

many industries, a support engineer's laptop has long been considered the least-trusted device in the environment. While CIP-010-2, Requirement R4 aids in this regard, Low Impact systems are not included in the Requirement. Zero-day attacks are especially troublesome in this area, if they cannot be subjected to safeguards such as "traditional antivirus hardening". [3]

CIP-010-2, Section 4, Requirement R1 indicates that "Part 1.1.5 requires entities to list all applied historical and current patches." Just for the Microsoft Windows 7 operating system, commonly used in desktop environments, as of September 2015, 105 security updates had been issued. [4] Perhaps a better method of listing updates for documentation purposes would be to indicate the date of last update and then list the individual patches that, due to environmental issues and software conflicts, could not be installed. The list would likely be shorter (for the sake of auditability), which could also more readily point to potential security issues.

The Risk of Low Impact BES Cyber Systems

In another area of critical infrastructure, an analogy can instructional. Recent announcements in various news outlets of the compromise of Department of Defense unclassified email systems [5] and computers within the food court inside the Pentagon [6] question the value of classifying systems as "low-risk", strictly from a security standpoint determined within a vacuum, and ignoring the environment in which they operate – and potential connectivity to systems of higher levels of security (and risk!) Parallels can be drawn in the Bulk Power System with respect to Low Impact BES Cyber Systems, as well as elsewhere in other critical industries. Concerns regarding the potential to "overly prescribe" controls point to an anachronistic basis of security protocol design. Can a networked system classified as "Low Impact" *truly* be isolated from the remainder of the environment so not to provide a vector for an attack into more critical areas? In many instances, the answer appears to be a resounding "No."

Cyber Assets, Perimeters and External Routing

"These malware campaigns [targeting supply chain vendors] represent a new type of threat to the reliability of the bulk electric system where malicious code can infect the software of industrial control systems used [in bulk electric system operations] by responsible entities."[7]

Evaluating the efficacy of security of industrial controls is a concern. Unlike an information technology system, many industrial controls cannot be "tested" or "exercised" in place, requiring the use of simulations and table-top exercises to estimate their effectiveness and range of operations. An attempt has been made to align the security controls for industrial control systems through the security process adopted by the National Institute of Standards and Technology under the Federal Information Security Modernization Act (FISMA) of 2014. [8]

"We are concerned, however, that the limited applicability of the proposed standard, i.e., BES Cyber Assets within the same Electronic Security Perimeter but located outside of a Physical Security Perimeter, results in a reliability gap . . . [W]e propose to direct that NERC modify Reliability Standard CIP-006-6 to require physical or logical protections for communication network components between all bulk electric system Control Centers." [7]

An overall risk-based approach is required for determining a reliability gap with regard to the Electronic Security Perimeter and the Physical Security Perimeter. A remote telecommunications link to a switchyard located a distance from a plant or a control center may very well be considered outside of the Physical Security Perimeter of that plant or center as viewed in a historical context. However, in terms of a holistic approach, which does not yet appear to be taken in some areas of security, the Electronic Security Perimeter in many (if not most!) instances encompasses an area larger than the Physical Security Perimeter. By simply considering the network connectivity from the control center(s) to outlying resources (switchyards, substations, plants, distribution centers, AMI, etc.), the Physical Security Perimeter can be much, much larger than first considered. Such a wide increase in scope needs to be considered as back-haul data connectivity providers and service level agreements with them may have to be evaluated from a cybersecurity standpoint.

"Low Impact External Routable Connectivity" [7]

This begs the question: When is externally-routable connectivity to a control system "low-impact"? This term appears to be an oxymoron that requires more clarification.

Conclusion

Anyone who questions the inclusion of the analysis of access to HVAC controls and department store and cafeteria Point-of-Sale systems in this discussion needs to look no farther than CIP-006-6 to understand that historically lower-risk non-control systems, such as those found in the supply chain still both pose risk, as well as to create potential attack vectors that can impact the security of control systems.

Is it possible that in all areas of critical infrastructure, that we have been forced by recent events and attacks to move beyond the posture of questioning whether we should, in fact, be addressing even "minimal risk"? The ancient Greek tale of Achilles illustrates that the size and accessibility of a vulnerability does not necessarily correlate to a system's fatally weakest point. Therefore, it is very well possible that by not providing further protections, and by maintaining rigidity that prevents adequate defenses in a rapidly-changing environment, that the infrastructure will remain vulnerable.

_____

Author's Note: This article is an informed opinion, and is not intended to provide procedural guidance under FERC or NERC policies.

_____

References

[1] Stonebraker, M., Çetintemel, U. & Zdonik, S. The 8 Requirements of Real-Time Stream Processing. Retrieved from http://cs.brown.edu/~ugur/8rulesSigRec.pdf

[2] Vijayan, Jaikumar. (2014, Feb. 7) "Target attack shows danger of remotely accessible HVAC systems". Retreived from http://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html

[3] North American Electric Reliability Corporation, "Cyber Security — Configuration Change Management and Vulnerability Assessments" (CIP-010-2), Nov. 2014.

[4] Microsoft Security Bulletin Summary for September 2015. Published: September 8, 2015. Retrieved from https://technet.microsoft.com/en-us/library/security/ms15-sep.aspx

[5] Whitlock, C. & Ryan, M. (2015, August 6) U.S. suspects Russia in hack of Pentagon computer network. The Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/us-suspects-russia-in-hack-of-pentagon-computer-network/2015/08/06/b80e1644-3c7a-11e5-9c2d-ed991d848c48_story.html

[6] Klimas, C. (2015, September 8) Pentagon food court computers hacked, exposing employees' bank information. The Washington Examiner. Retrieved from http://www.washingtonexaminer.com/pentagon-food-court-computers-hacked/article/2571606

[7] UNITED STATES OF AMERICA FEDERAL ENERGY REGULATORY COMMISSION. 152 FERC ¶ 61,054. 18 CFR Part 40 [Docket No. RM15-14-000]. (2015, July 16) Revised Critical Infrastructure Protection Reliability Standards.

[8] NIST Special Publication 800-82, Revision 2. (2015, May) Guide to Industrial Control Systems (ICS) Security. http://dx.doi.org/10.6028/NIST.SP.800-82r2

North American Electric Reliability Corporation, "Cyber Security — Security Management Controls" (CIP-003-6), Nov. 2014.

North American Electric Reliability Corporation, "Cyber Security — Personnel & Training" (CIP-004-6), Nov. 2014.

North American Electric Reliability Corporation, "Cyber Security — Physical Security of BES Cyber Systems" (CIP-006-6), Nov. 2014.

North American Electric Reliability Corporation, "Cyber Security — System Security Management" (CIP-007-6), Nov. 2014.

North American Electric Reliability Corporation, “Cyber Security — Recovery Plans for BES Cyber Systems” (CIP-009-6), Nov. 2014.
North American Electric Reliability Corporation, “Cyber Security — Information Protection” (CIP-011-2), Nov. 2014.

How Government Agencies Can Become Secure by Default

By: Tempered Networks

Description: Faced with aggressive state-sponsored cyber threat actors, the expanding Industrial Internet of Things (IIoT), and increasing budget scrutiny, government agencies need a new approach to improve security, efficiency, and resiliency for critical infrastructure.

This article is attached in order to maintain consistent formatting.

Protecting Generating Networks with Unidirectional Security Gateways

By: Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Most electric-sector security practitioners are aware of unidirectional gateway technology and its advantages over firewalls in one circumstance or another, but many are still unclear as to what a unidirectionally-protected "big picture” network looks like. In this article, we describe the network architecture deployed routinely to protect power plant control networks.

This article is attached in order to maintain consistent formatting.

How Government Agencies Can Become Secure by Default

Leveraging the Host Identity Protocol (HIP) to address the fundamental vulnerabilities of IP communications

Faced with aggressive state-sponsored cyber threat actors, the expanding Industrial Internet of Things (IIoT), and increasing budget scrutiny, government agencies need a new approach to improve security, efficiency, and resiliency for critical infrastructure.

By Tempered Networks Q

Escalating Threat Levels

The intensity of cyber attacks and the growth of machine-to-machine (M2M) communications, driven by the emergence of the Industrial Internet of Things (IIoT), has radically changed the security environment from what it was just five years ago. IP networks have become the global backbone of commerce and communications. This introduces many new challenges for any organization using IP networks for business operations, but it is particularly important for many federal government agencies that help protect the nation's most valuable infrastructure and information.

In this new era of state-sponsored hacking and profit-driven cyber crime, agencies are also facing a much tougher budgetary environment than ever before. Significant federal government breaches of critical infrastructure have already proven that existing cyber security efforts are not adequate. The ability to safeguard the nation's critical infrastructure will depend on deploying a more effective and cost-efficient solution.

A new cyber-security approach is needed to address the fundamental vulnerabilities of IP-based communications. A solution that cloaks critical infrastructure from attackers' visibility can stop attacks before they start, providing federal agencies with a cost-effective and incredibly secure defense-in-depth model for protecting critical assets.

Understanding the Challenges

Today, government agencies are trying to balance the need for security with increased appropriations scrutiny. The congressional hearings over the massive theft of more than 20 million federal employee records from the Office of Personnel Management (OPM) is just one recent example of officials being forced to justify how they are using information technology funding to protect sensitive data and assets.

> **"19 of 24 major federal agencies have reported deficiencies in information security controls. Inspectors general at 23 of those agencies cited information security as a major management challenge. How many headlines of serious data breaches will it take to implement the steps necessary to protect ourselves?"**
>
> Senator John Boozman, R-Ark., during a Senate Appropriations Committee on Financial Services and General Government hearing on the massive OPM data breaches

Congressional appropriators have made it clear that they want to understand how cyber-security budgets will be spent differently from the ways that led to past breaches. The conclusion is that traditional approaches to security are insufficient, and government organizations are looking for fundamentally stronger protection against new threats that are increasing in volume and sophistication.

Vulnerable endpoints are increasing the attack surface

Within federal government agencies, flat networks provide interoperability, flexibility, and perceived management efficiency. However, these flat networks give hackers a larger surface to attack and more opportunities to penetrate the broader network. This is true across the full range of agencies, from the U.S. Department of Homeland Security (DHS) and the Department of Defense (DoD) to the General Services Administration (GSA) and the Food and Drug Administration (FDA). And the attack surface is only increasing with the number of unconventional things connecting to networks—whether it's tracking sensors, IP cameras, HVAC systems, water pumps, or other devices. In addition, integrating new equipment or consolidating facilities, such as those within military bases, disrupts the network every time devices or systems are added or removed, making the network more brittle and vulnerable to attacks.

75 % **of IT security professionals believe that mobile endpoints have been the target of malware at their organization over the past 12 months**

Ponemon Institute, 2015 State of the Endpoint Report

Cost and complexity work against security

Solving cyber-security problems has historically meant adding more budget to purchase more firewalls, which then requires even more budget for technical staff to maintain. However, with increased appropriations scrutiny, the expansion in the volume and sophistication of attacks, and the huge growth in the number of devices being protected, this approach is simply unrealistic. Firewalls are costly to procure and costly to manage, since they require ongoing, complex, and manual configurations performed by skilled security resources. Add to that the fact that every time something changes, more intervention is required, and the total cost of ownership rises. The more complex a system becomes, the greater the opportunity is for breach or malware penetration into the larger or distributed network.

95 % **of all security incidents involve human error.**

IBM Study, 2014 Cyber Security Intelligence Index

Legacy systems are especially vulnerable

Federal agencies use many applications and devices that have a very long useful life—such as weapons systems, aircraft controls, medical device platforms, and utilities infrastructure—that are still critical to the organization. Yet many of these systems predate what are now considered standard security methods. In some cases these vulnerable assets—many of which are mobile—can be protected with firewalls, yet that comes with complexity and cost. Additionally, these systems often exist in environments where the personnel maintaining the systems do not have the specialized technical expertise to manage a complex firewall configuration.

> **"Let's not just throw money at it—let's get value and security. It's OPM today, and it will be another agency tomorrow, so we need to make sure our cyber shields are up."**
>
> Senator Barbara Mikulski, D-Md., during a Senate Appropriations Committee on Financial Services and General Government hearing on the massive OPM data breaches

Defining a New Approach to Security

Federal agencies will need to identify and implement new strategies to solve the problems that previous security solutions have been unable to handle. Creating a successful model starts with defining the principles that are needed to overcome the challenges faced.

Operational efficiency and scalability are critical

Minimizing operating cost is essential to implementing an appropriate cyber-security solution because it allows organizations to be more agile. Today's firewalls and many other security systems involve tremendous operational complexity, and in most cases require specialized, ongoing skills. However, in many civilian environments, and particularly in military situations, equipment must be maintained by personnel without specific IT expertise. In addition, the sheer number of devices being protected is skyrocketing with the Industrial Internet of Things (IIoT). Successful security solutions must allow for massive scalability at a reasonable cost and be easy to manage by non-IT personnel.

Security must target the attacker's process

Using a kill chain model (Figure 1) to map the course of advanced persistent threats (APTs), today's sophisticated hacker begins with a reconnaissance phase, scouting out the target system to find vulnerabilities.

(Figure 1)

Figure 1: Kill chain model

1. **Recon:** Probing and harvesting information
2. **Weaponize**: Coupling a specific exploit with a backdoor into a deliverable payload
3. **Deliver**: Deliver the weaponized bundle via channel (e.g. email, web, USB)
4. **Exploit**: Exploit a vulnerability to execute code on victim's systems
5. **Install**: Install malware on identified asset(s)
6. **Command/Control**: Command channel for remote manipulation
7. **Action**: Ex-filtrate content/objective

There are several places along the kill chain where an attack can be stopped or mitigated, however, the most efficient and effective place is at the reconnaissance stage. Cloaking assets is a highly effective and secure means of preventing attacks because it renders the attacker unable to see or identify the protected assets. With cloaking, the attack is stopped before it can advance to any further phases (Figure 2).

(Figure 2)

Host Identity Protocol (HIP): A New Trust Model

The root cause of most TCP/IP architecture challenges stem from the fact that IP addresses are used in two places: identifying the traffic and identifying the host. When originally developed, the priority was on connectivity rather than security, as end users and endpoints are assumed to be mutually trusting. It was never designed to be secure, and consequently we're left with a protocol that is incredibly reliable, yet completely insecure from the start.

Using the Host Identity Protocol (HIP), this trust model can be reversed. Developed by the Internet Engineering Task Force (IETF) to address the vulnerabilities created by the dual use of IP addresses, HIP is an IETF workgroup-specified alternative to traditional encryption methodologies. It has been in development since the mid-90s in coordination with a collection of large companies, including Ericsson, Verizon, Yokogawa, Boeing, Shell, and others.

The next significant change in IP communications

Recognized by the IETF community as the next big change in IP infrastructure, HIP separates the identity of a host from its location by replacing IP addresses with cryptographic identity addresses. HIP effectively decouples the transport layer from the network layer, and allows the upper layers of the stack to use a Host Identity (HI) in their socket APIs instead of an IP address. HIP establishes secure communications between cryptographic HIs and binds local and remote application interfaces to these identities (Figure 3).

Using cloaking to stop attacks before they start

HIP can be used to create a security platform that "cloaks" critical systems and endpoints by establishing secure communications between cryptographic identities. HIP-based security appliances (physical or virtual) are deployed in front of critical infrastructure to create private, encrypted overlay networks. Starting with zero trust, the platform allows users to whitelist devices for explicitly trusted and encrypted communications between security appliances. Devices that sit behind the security appliances are invisible and undetectable from the underlying network.

This technology originated in the defense and aerospace industry, where state-sponsored attacks happen on a regular basis and the cost of downtime is more than $1 million per hour. Leveraging HIP makes the platform secure by default, providing a cloaking technology for federal agencies' critical infrastructure and high-value endpoints, including non-traditional devices that cannot protect themselves (e.g. cannot run endpoint security). Trust is baked in, rather than relying on bolted-on components to become secure.

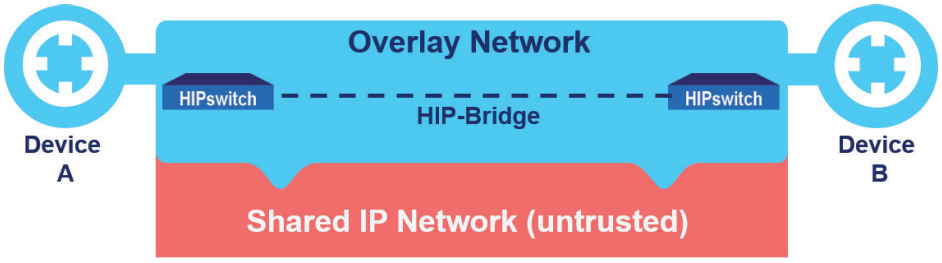


Figure 3: HIP-based security appliances create a mutually-authenticated, certificate-based Encapsulating Security Payload (ESP)-protected bridge between each other. Device packets are encrypted (AES-256) and encapsulated, therefore resistant to denial-of-service (DoS) and man-in-the-middle (MitM) attacks.

Automated orchestration

Simplicity and scalability are integral to this unique approach. An orchestration engine facilitates centralized governance and minimizes errors. Through drag-and-drop functionality, a user interface enables easy coordination and configuration of distributed security appliances. IT departments can maintain centralized governance while compartmentalizing control and access to designated departments or operations team. By automating much of the configuration process, operational expenses are significantly reduced, as is the risk of manual human error, a leading cause of security incidents.

Delivering Benefits to Federal Agencies

This fundamentally new approach to cyber security can immediately help federal government agencies improve their security posture and provide the efficiencies that are needed to protect critical infrastructure in today's environment.

Doing more with less

There is a clear mandate for federal agencies to accomplish more with fewer resources even as requirements to improve security increase. Many of the critical assets that require cyber-security protection are in locations where it is not practical for highly skilled security personnel to be present. This approach provides a solution that is simple enough to operate that non-IT military personnel, such as a sailor on a warship, can do it. In civilian environments where security personnel with knowledge of specialized systems are aging and retiring, the solution offers a means to enable standard operations personnel to manage critical infrastructure security.

Preservation of legacy investments and long-lived infrastructure

The HIP-based solution provides a cost-effective way to protect any device or system. Legacy and long-lived systems—such as HVAC, fuel pumps, and generators—that would be expensive or impractical to put behind a firewall can be protected without complex configurations and on a completely vendor-agnostic basis. The solution also works over any network—including cellular, WiFi, wired Ethernet, and/or satellite communications networks, so existing networks can be fully leveraged.

Stronger security through cloaking and micro-segmentation

Any device or endpoint that is whitelisted on the protected overlay network is concealed through cloaking—malware or network breaches cannot detect infrastructure that resides behind the securityappliances. Cloaking key systems makes attack reconnaissance much more difficult to accomplish, providing a way to shut down attacks at the beginning of the kill chain.

In alignment with DHS ICS-CERT recommended practices, network segmentation involves partitioning the network into smaller networks (micro-segmentation through private overlay networks). The NIST Guide to ICS Security (Revision 2) advises organizations to partition one large ICS network into multiple ICS networks, where the partitioning is based on factors such as management authority, uniform policy and level of trust, functional criticality, and amount of communications traffic that crosses the domain boundary.

This new approach goes above and beyond segregating and inspecting communications, adding availability, integrity, and confidentiality (encryption) protection as critical data and information traverse the control systems network. Micro-segmentation of the network also enhances security by providing the ability to constrain administrators' access to only the specific segment(s) of the network they are responsible for.

Security at scale

Federal agencies of any size can use this solution to implement hardened security that protects critical infrastructure without the tedious complexity that is typically associated with configuring and managing firewalls, VPNs, VLANs, etc. For example, an agency like NASA that has a broad range of equipment, such as power and cooling devices from many different manufacturers, can protect the full array of critical assets with one solution. By segmenting and isolating critical infrastructure, IT staff can give operations personnel compartmentalized access and control of high-value assets while maintaining centralized governance and without running the risk of compromising the shared network.

The Next Step Forward

Facing today's significant challenges, federal agencies are looking for cost-efficient and highly effective cyber-security controls for federal information systems. Defense-in-depth cyber-security practices must incorporate new methods that have security "baked in" from the start and that are sustainable for long-term protection and management.

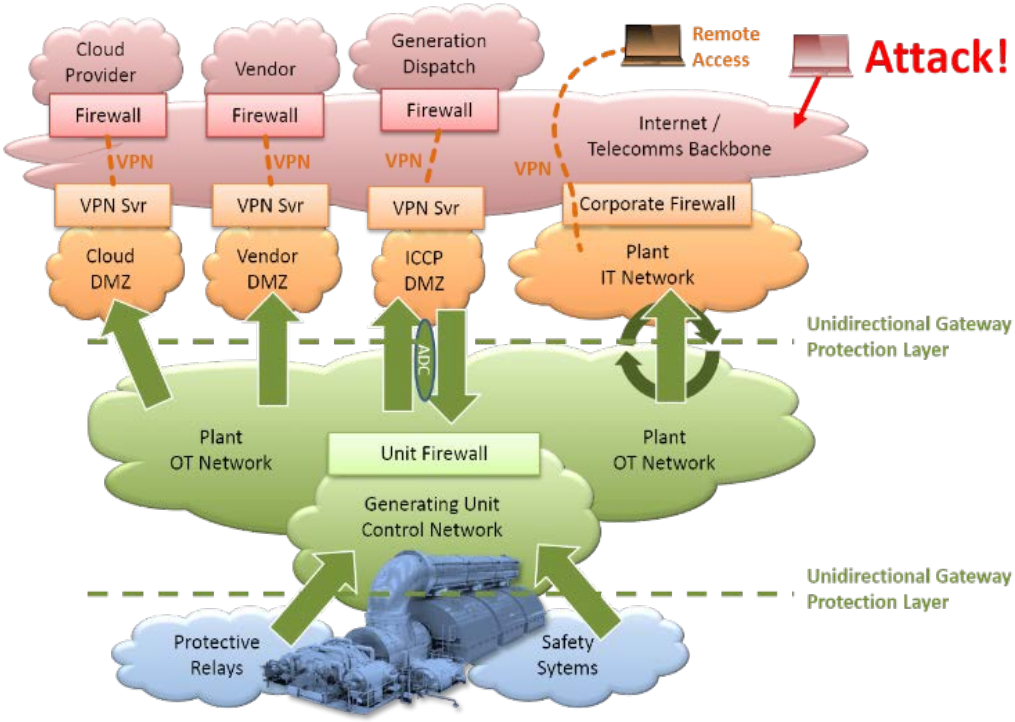
By leveraging a new trust model based on HIP, departments and agencies can comply with increased mandates and guidelines for cyber security—regardless of size or degree of cyber-security risk or sophistication. Federal agencies can leverage existing infrastructure and immediately create cloaked overlay networks that protect specific infrastructure and endpoints within the network. If malware or a network breach occurs on the underlying network, threat actors are thwarted in performing reconnaissance on protected infrastructure, as devices behind the security appliances are invisible except to explicitly trusted peers within a specific overlay network.

Operations and field teams can manage local control of connectivity and networking needs, while central IT retains control of cyber-security compliance, oversight, and auditing. With this new approach, government agencies can apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure while making more efficient use of available resources.

Protecting Generating Networks with Unidirectional Security Gateways

Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Most electric-sector security practitioners are aware of unidirectional gateway technology and its advantages over firewalls in one circumstance or another, but many are still unclear as to what a unidirectionally-protected "big picture" network looks like. In this article, we describe the network architecture deployed routinely to protect power plant control networks. A simplified version of the network is illustrated below.

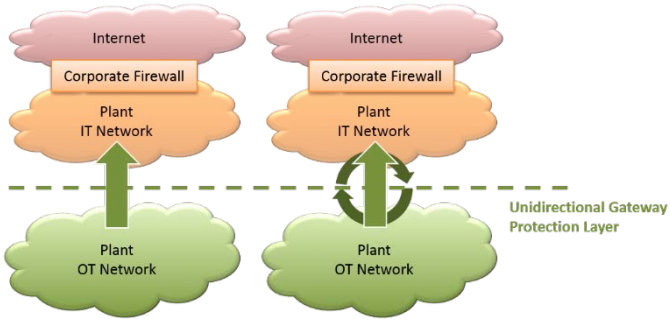


The design strategy behind this architecture is simple - replace at least one layer of firewalls in the layered, defense-in-depth network with unidirectional gateways, thus protecting our most important control system components from network attacks originating on less-trusted networks, such as corporate networks and the Internet.

Safe IT/OT Integration

The vast majority of power plants choose the IT/OT firewall layer as the layer to replace with unidirectional protections. Cross-zone communications at this layer serve many functions. In the discussions below, each IT/OT integration function is considered independently. In practice, many or all of these functions are combined into a single set of unidirectional gateway equipment. Let's look at each of the functions in turn.

Primary IT/OT Interface: The primary IT/OT interface is used to monitor real-time operations continuously for purposes such as predictive maintenance, operations optimization and widespread awareness of key performance indicators. The majority of unidirectionally-protected power plants deploy unidirectional gateway technology



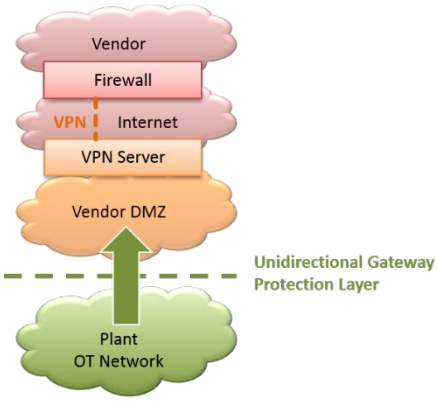
Safe IT/OT Integration

at this interface, but newer installations also use flip technology at this interface, and it is a flip that is illustrated in high-level diagram above. For readers unfamiliar with gateways or the flip:

- A unidirectional gateway is hardware that is physically able to transmit information in only one direction, coupled with software that makes copies of industrial servers, most often process historian databases, or various types of OPC servers. Users and applications on the corporate network needing access to real-time data can query the replicas for that data.
- A flip is a kind of unidirectional gateway whose orientation can reverse on a schedule. A flip can physically send information in only one direction at a time, and makes copies of industrial servers just like the gateways do.

At unidirectionally-protected sites, security updates are communicated to plant networks on removable media - most commonly write-once CD's. At flip sites, the flip is configured to pull such updates automatically, on a schedule.

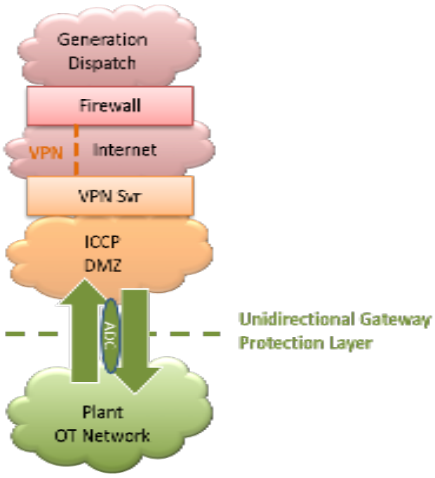
Vendor Monitoring: The majority of coal, gas and hydro plants have remote connections to their turbine vendors for vendor monitoring and diagnostics, and many have similar connections to other vendors as well. These vendors monitor physical equipment or control-system components continuously, and adjust system parameters from time to time. Unidirectionally-protected plants meet the monitoring need with server replication; the vendors monitor the replica servers. Most unidirectionally-protected plants meet the "occasional adjustment" need with remote screen view technology. Remote screen view makes a real-time feed of screen images available to vendor support personnel, while site personnel operate control system equipment. The vendors generally advise plant personnel over the phone throughout these adjustments.



Vendor Monitoring and Diagnostics

Generation Dispatch Center: Most power plants need to report power production and other parameters to a generation dispatch center continuously. Some plants have such schedules pre-set far into the future; such plants can deploy unidirectional gateways to replicate ICCP servers to permit continuous monitoring by dispatch centers. The majority of plants not only report thein status continuously to a dispatch center, but receive second-by-second updates of power production setpoints from that center as well.

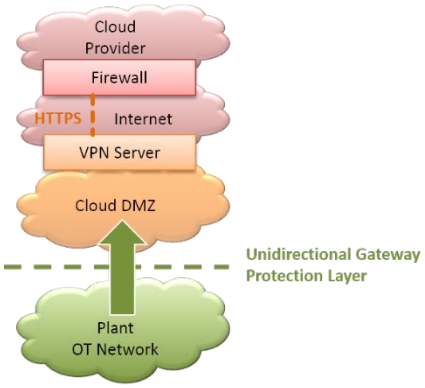
Some such plants lease serial lines to exchange ICCP information with dispatch centers, but a more secure solution is a pair of "inbound/outbound" unidirectional gateways replicating ICCP servers. Inbound/outbound gateways are two independent unidirectional gateway deployments, each replicating an ICCP server in one direction. The inbound gateway polls the dispatch center's ICCP server and emulates that server to plant systems. The outbound gateway polls the plant ICCP server and emulates that server to the dispatch center EMS. These two channels



Control Center Communications

are generally deployed on different sub-networks and are unable to communicate with each other, though both are able to communicate with control center and plant ICCP servers.

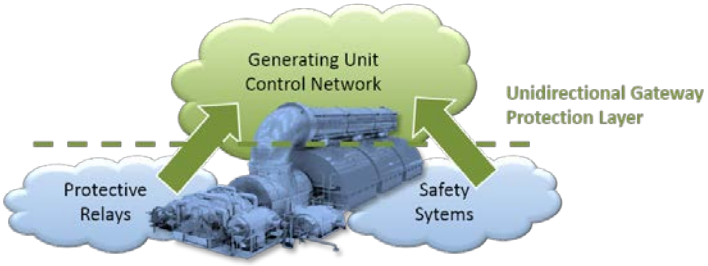
Cloud Providers: Communications with cloud services is similar to communications through the primary IT/OT interface, and is called out separately in the diagram because of the high degree of interest in this emerging field for power plants. Communications with cloud service providers may be via unidirectional gateways, or if occasional updates from cloud applications are necessary, may be via the flip as well.



Cloud Services

Safety and Protection Systems

In some cases, owners and operators decide they wish to continue to use firewalls at the IT/OT interface, but still need safety instrumented systems and protective relays protected unidirectionally. Such plants always deploy unidirectional gateway technology at the interface between control networks and the safety & protection networks. Unidirectional gateways poll safety and protection devices and emulate those devices to control systems. This design provides for continuous monitoring of the status of safety systems and equipment protection systems without any risk of a network attack pivoting through intermediate systems and networks in order to reconfigure, reprogram, disable or otherwise compromise safety systems and protective relays.



Protecting Safety and Protection Networks

Benefits of Unidirectional Protections

The primary driver for deploying a unidirectionally-protected network is improved security and cyber-threat risk reduction. The biggest cyber threat to power plants is not random, accidental side-effects of infections by high-volume malware, but targeted attacks. When an individual or group deliberately targets a site, they design their attack to bring about as much damage as possible, at a time as inopportune as possible for the targeted site. By far the biggest attack vector for these modern, targeted attacks is interactive remote-control attacks, across the Internet, pivoting through intermediate networks, connections and systems and breaching intermediate firewalls. Unidirectional gateway and related technologies defeat these interactive remote control attacks, as well as more conventional network virus, worm and insider attacks.

A secondary driver in North America, France, Israel and other jurisdictions with cyber security regulations in place, is reduced compliance costs. The NERC CIP V5 and proposed V6 standards for example, have 37 additional, costly “external routable connectivity” rules that large medium-impact power plants must follow when they use firewalls, rules that do not apply to plants protected exclusively by unidirectional gateway technology.

An additional driver for unidirectional gateway deployments is operating cost reductions. Power plant IT/OT firewalls tend to be complex: many streams of data, applications and users are typically configured to reach through the firewall to request data from plant systems. Maintenance of these complex firewall configurations is costly, because of the risk that any error in configuration might relax firewall protections unacceptably. Monitoring of firewall logs and communications through firewalls is even more costly, but such monitoring is essential, because of the very real risk that some attack will breach the firewall.

In contrast, unidirectional gateway technology and related technologies are generally deployed to replicate a number of servers in whole or in part, and these configurations rarely change. Furthermore, even if unidirectional configurations change over time, unidirectional gateway technologies do not forward messages, and the physical, unidirectional, remote-control-defeating nature of the gateways makes them intrinsically safer than firewalls. As a result, gateway deployments do not warrant the same degree of continuous, costly scrutiny that is mandatory for firewalls.

Looking Forward

Control system security standards all over the world are being updated to reflect the strength of unidirectional protections. Industrial control system owners and operators in all industries are considering and deploying unidirectional gateways to dramatically improve the security posture of their industrial control system networks.