October 2013 / Issue 25

# The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

## this issue



## NIST Framework Update

In February this year, President Obama gave an executive order to improve critical infrastructure cyber security, calling on NIST to establish a "cyber security framework" to reduce cyber risk to critical infrastructure within approximately one year of the order.

U.S. critical infrastructure, which covers around 16 different industry types, includes power, chemical, oil, gas, and water industries.

In response, NIST has developed a new framework that encompasses the "best of the best" national and international standards. These new NIST standards are based on a review of over 320 guidelines, directives, best practices, models, specifications, policies, and regulations. It is important to understand that the framework does not replace, but rather complements, an organization's existing cyber security program. The organization can use its current processes and leverage the framework to identify opportunities to improve their cyber security risk management process. Alternatively, an organization without an existing cyber security program can use the framework as a reference to establish one.

| Function | Category | Subcategory | Informative Reference(s) |
|---|---|---|---|
| IDENTIFY | | | |
| PROTECT | | | |
| DETECT | | | |
| RESPOND | | | |
| RECOVER | | | |

Such tools act as a reference, industries that are less regulated and have a need for a corporate mandate or industry standard can identify risks and threats, determine what areas are critical and need to be protected, detect malware and viruses or threats that could shut them down, form an incident response plan, and develop a recovery plan. The importance of this framework is it provides a first step based on solid cyber security best practices to help develop cyber security compliance programs.

**October 2013**
**Cyber Attack Statistics**
**- Hackmageddon.com**

Attack Motivations
- 55% Hacktivism
- 44% Cyber Crime
- 10% Cyber Espionage

Top 3 Attack Targets
- 33% Government
- 21% Industry
- 6% Law Enforcement

Top 5 Attack Techniques
- 21% Defacement
- 20% Account Hijacking
- 19% Unknown
- 15% SQL
- 9% DDoS

# Industry News

## US researchers find 25 security vulnerabilities in SCADA systems

*From www.computerweekly.com, 10/18/13*

U.S. researchers have identified 25 zero-day vulnerabilities in industrial control SCADA software from 20 suppliers that are used to control critical infrastructure systems. Attackers could exploit some of these vulnerabilities to gain control of electrical power and water systems, according to Wired.com. Nine of these potential exploits have so far been reported to the suppliers concerned and the U.S. Department of Homeland Security. The vulnerabilities were found in devices that are used for serial and network communications between servers and substations. Electrical engineer Chris Sistrunk and consultant Adam Crain said these products have been overlooked as hacking risks because the security of power systems is focused on IP communication. Serial communication has not been considered as an important or viable attack vector, but the researchers say breaching a power system through serial communication devices can be easier than attacking through the IP network because it does not require bypassing layers of firewalls.

## Gas lines, power companies targeted by cyber attacks

*From www.theepochtimes.com, 10/16/13*

One of the cyber doomsday scenarios often painted by security advocates is an attack on the U.S. energy grid. Mechanized farms would be frozen, communication and innovation gone, and the U.S. economy brought to a standstill. A coordinated cyber attack using existing technology could bring the country to its knees. After surveying more than 100 energy companies in May, Representatives Edward Markey and Henry Waxman said more than a dozen of the companies reported "daily," "constant," or "frequent" attempts of people trying to hack their networks. One utility reported it faced close to 10,000 attacks each month. During his 2013 State of the Union Address, President Barack Obama warned of the growing threats in cyberspace, saying "Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems."

## Power plant plight: U.S. utilities' soft underbelly for hackers

*From www.rt.com,10/18/13*

New research revealed this month shows that many of the nation's vital infrastructure systems are more vulnerable to cyber attacks than previously expected. In fact, researchers Chris Sistrunk and Adam Crain have discovered 25 different security system weaknesses that could potentially permit hackers to sabotage or crash servers that control water systems and electric substations. Throughout the course of their research, Sistrunk and Crain discovered that the products of more than 20 vendors had significant security vulnerabilities. Hackers could, for example, crash a power station's master server by guiding it into an infinite loop, or cause power outages by remotely injecting their own make-shift code into a server. "Every substation is controlled by the master, which is controlled by the operator," Sistrunk told Wired, which broke the story. "If you have control of the master, you have control of the whole system, and you can turn on and off power at will."

## Cyber security attacks spike industry and governmental concern

*From www.controldesign.com, 10/21/13*

The demand for cyber security products and services continues to grow, and is predicted to have an even more promising future, according the "Industrial Cyber Security Global Market Research Study," from ARC Advisory Group. An increase in security concerns surrounding facilities along with more government influences are responsible for the growing demand. Greater supply of product consolidations, expanded services and a shift from emerging to mature market players is also influencing demand. The study suggests anyone involved in protecting critical company assets be aware and understand new developments in the cyber security marketplace because there are a variety of continual technological and organizational decisions to be made that can have devastating consequences if mistakes are made. Examples such as Stuxnet and Shamoon cyber attacks have increased industry and governmental concern on the security of their critical infrastructure. Companies are learning that even the most secure systems are vulnerable to cyber attacks. Industrial organizations are some of the largest victims of cyber crime and cyber warfare.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2013 / Issue 25

# Cyber News

## Adobe hacked: source code, customer data stolen

*From www.darkreading.com, 10/3/13*

Earlier this month, Adobe revealed it had suffered massive "sophisticated attacks" on its network that resulted in the theft of sensitive information including payment card information on 2.9 million customers, as well as of source code for multiple Adobe software products, including Adobe Acrobat, ColdFusion, ColdFusion Builder, and other Adobe software. Brad Arkin, chief security officer of Adobe, said in a blog post that the attacks may be related. "Very recently, Adobe's security team discovered sophisticated attacks on our network, involving the illegal access of customer information as well as source code for numerous Adobe products. We believe these attacks may be related," Arkin said.

## Dick Cheney altered implanted heart device to prevent terrorist hack attacks

*From arstechnica.com, 10/19/13*

Former Vice President Dick Cheney was so concerned that terrorists might hack the medical device implanted near his heart in order to deliver a fatal shock that he disabled a function that allowed the defibrillator to be administered wirelessly, the Associated Press reported. The revelation, made in an interview to be aired on CBS's *60 Minutes* program, echoes concerns that researchers have raised for years about the vulnerability of implanted medical devices, which are equipped with computerized functions and wireless capabilities that allow the devices to be administered without requiring additional surgery. In June, the US Industrial Control Systems Cyber Emergency Response Team warned that an array of medical devices contain backdoors that make them vulnerable to potentially life-threatening hacks. An episode of the Showtime series *Homeland* portrayed a similar assassination scenario. "I found it credible," Cheney said on the 60 Minutes segment concerning the *Homeland* plot line. "I know from the experience we had, and the necessity for adjusting my own device, that it was an accurate portrayal of what was possible."

## Suspect behind "Blackhole" malware toolkit believed arrested in Russia

*From arstechnica.com, 10/9/13*

The man believed to be responsible for distributing the notorious Blackhole malware toolkit has been arrested in Russia, a source told Reuters. The source, a former Russian police detective in contact with Russia's federal government, said that the man went by "Paunch" in hacking circles. No other information was given, but a spokesman for Europol in the Hague told Reuters that the police agency "had been informed that a high-level suspected cyber-criminal" had been arrested in Russia. Blackhole is a widely known exploit toolkit that makes "drive-by" attacks easier for hackers to execute. It allows criminals to inject malware onto PCs that either visit exploit sites or are redirected to exploit sites from compromised websites. As one of the primary names behind Blackhole, Paunch kept the toolkit current as new weaknesses in commonly used programs were discovered: in 2012 Paunch released Blackhole 2.0, and recent custom versions of the toolkit incorporated ways to exploit vulnerabilities in Adobe Reader and Java's browser plugin.

## China no longer top source of cyber attacks

*From www.computerweekly.com, 10/21/13*

Indonesia has overtaken China as the top source of cyber attacks, according to the latest study of internet traffic from content delivery firm Akamai. According to the firm's *State of the internet* report, Indonesia's share of observed attack traffic in the second quarter of 2013 increased to 38%, pushing China into second place with a 33% share. The report said ports 80 and 443 were the most commonly targeted ports, accounting for 41% of observed attacks combined. Port 445, the perennial top target, fell from first place for the first time since the first quarter of 2008, dropping to 15% of observed attacks. Distributed denial of service (DDoS) attacks also increased in the second quarter, up by 54% compared with the first three months of the year.

# Consultant's Corner

## Cyber Security and the Test Bed

The best way to find out how any system will react to changes is to try the changes. However, the problem with this is that trying untested changes on a process system could have devastating effects not only on production and operations but also on safety and future security of the system and the plant or plants that depend on these systems.

Production can be disrupted by changes that have immediate effects on the system such as viruses that, for example, run CPU usages up too high, delete files, or erase data. Operations can be disrupted by the same actions. Safety will be compromised by any issues in the control system that affects either the system or the reactive ability of the operators. And finally, the future security of the cyber system may be compromised by any undetected software that opens connections to an outside host or sends out any system info that may be used to gain access to the system.

Testing any changes to control, process, or SCADA systems on a fully configured test bed will reveal most threats to these systems before these threats can infect a process system. The trick is to fully configure the test bed as well as fully analyze the results of any tests conducted.

Analysis must include any pertinent information from the host, including scans for changes in ports and services, scans for installed applications, and logs from anti-virus and anti-spyware programs.

The most often missed information that can be gained from a test bed is "does this change try to contact the outside world?" If a newly installed application tries to "call home" to open an outgoing connection that can be used to remote in by a bad actor, sometimes the only way to find out this information is to analyze the logs of a configured external firewall. These logs will show any test bed host attempts to open an outgoing connection. Analysis of these logs may be the only way to catch a zero-day threat that would not show up in anti-virus logs on the host in question.

The bottom line is that the only way to protect a control system is to test any and every change to be made to a control system and to test the change on a fully configured test bed first; then, fully analyze the results of the test bed test data.

This month's contributor to Consultant's Corner is
James Bassett
Consultant, Critical Infrastructure & Security Practice, Invensys
james.bassett@invensys.com

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2013 / Issue 25

# Consultant's Corner

### Tim Johnson, CISSP —CISP Principal Consultant

"Centralized Anti-Virus DAT repository deployments enable quick and reliable Anti-Virus updates for Stand Alone Control Systems."

### Doug Clifton, CISSP — Dir. CISP

"It's significantly less expensive to purchase Managed Security Services than to hire new staff with Security Experience."

### Steve Batson, CISSP — CISP Principal Consultant

"Implementing common security controls across disparate systems can greatly reduce the cost of security and maintenance."

### Michael Martinez — CISP Principal Consultant

"Being regulatory compliant does not ensure being secure. Cyber Security is a ongoing life cycle."

### Tom Jackson — CISP Principal Consultant

"According to Kaspersky Labs, applications like Adobe are primary targets for hackers to deliver viruses. Implementing patch management and update services is an effective fix."

Meet the CISP team and learn more about Cyber Security at http://www.real-time-answers.com/cyber-security/

**Cyber Security for the Nuclear Industry »**
Focusing on 10 CFR 73.54 and NEI 08-09 Reg. guide 5.71, learn more about cyber security in the nuclear industry.

**Cyber Security for Power Generation »**
As more and more electric power plants begin their NERC CIP compliance plan, many are left trying to understand where to start. See which areas require special attention.

**Cyber Security Compliance »**
Cyber compliant does not necessarily mean cyber secure. Identify the keys common to both.

**Cyber Security Threats »**
Cyber attacks are increasing. A continuous state of preparedness is required.

**Cyber Security Life Cycle »**
Cyber security cannot be maintained from a one-time initiative. Learn about a methodology designed to keep your site cyber secure well into the future.

**Cyber Security Consulting Advantage »**
Security and compliance take a tremendous amount of effort. Help is available to get secure and compliant … and stay that way.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2013 / Issue 25

# Invensys Critical Infrastructure and Security Practice (CISP)

Invensys CISP has capability in establishing, implementing and maintaining industry best practices to meet the demands for government regulations (NERC-CIP, NEI 08-09, CFATS), industry requirements and company compliance requirements. Attributes of Invensys CISP Critical Infrastructure Consulting include:

## Hardware Independence

CISP can work with any type of control system or type of technology a customer prefers for the security environment.

## Regulation Knowledge

CISP has a number of subject matter experts who understand a whole host of regulatory requirements as well as active participation in a number of industry and government groups.

## Technical Knowledge

The same CISP personnel who have regulatory knowledge are also well versed in the latest security policies, procedures, and technologies for intrusion detection and prevention, firewalls, DCS, and network architecture.

## Join us on Blogger

## Industry Knowledge

CISP has a number of resources that understand the demands of Controls Networks and the requirements for continued uptime.

## Proven Methodology

CISP follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the life cycle approach are Assessments, Development, Implement and Management.

invensys™

For additional information, please visit us at
**http://iom.invensys.com/CyberSecurity**

5601 Granite Pkwy. Suite 1000 Plano, TX 75024 ▪ P 214.295.6365 ▪ F 888.758.7675 ▪ **iom.invensys.com**