SUMMARY ON THE ACTIVITIES OF THE NARUC COMMITTEE ON CRITICAL INFRASTRUCTURE

NAWC Annual Conference
Tucson, AZ

October 12, 2010

DISCLAIMER

- The opinions expressed in this presentation are mine, and mine alone, and are not those of the Commission, any Commissioner (other than myself) or any member of the staff of the Commission. Further, nothing in this presentation should be attributed to any case or matter before the Commission, to any member of the staff of the Commission, other Commissioner or the Commission.

ABOUT THE CI COMMITTEE

- Established on a temporary basis after the September 11, 2001 terrorist attacks
- Now a permanent NARUC committee

ABOUT THE CI COMMITTEE

- Purpose: To provide State regulators with a forum to analyze solutions to utility infrastructure security and delivery concerns
- As demonstrated on Sept. 11 and later during subsequent hurricanes, particularly Hurricane Katrina, protection of the nation's water, energy and telecommunications infrastructure is critical to the national security interests of the United States

ABOUT THE CI COMMITTEE

- The CI Committee, together with its Staff Subcommittee, gives State regulators opportunities to share best practices and collaborate amongst themselves and their federal counterparts together with private sector partners

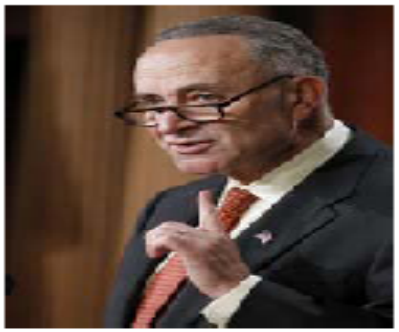
WHY WORRY ABOUT CI?

THE REPUBLIC

Report: NRC needs more tools to try to keep terrorists from getting jobs at nuclear plants

MICHAEL GORMLEY Associated Press Writer
First Posted: October 04, 2010 - 6:45 am
Last Updated: October 04, 2010 - 3:26 pm

Photos:



FILE - In this Aug. 5, 2010 file photo, Sen. Charles Schumer, D-N.Y., talks about immigration and border security during a news conference on Capitol Hill in Washington. A federal audit set to be released Monday, Oct. 4, 2010, calls for the Nuclear Regulatory Commission to improve nuclear power plant security against infiltration by potential terrorists. An outline of the findings was provided to The Associated Press by Schumer, who had called for the audit by the NRC's inspector general in March after a suspected al-Qaida member, Sharif Mobley, was found to have worked in a New Jersey nuclear power plant for six years. (AP Photo/Alex Brandon, File)

ALBANY, N.Y. — The Nuclear Regulatory Commission should be given better access to criminal databases and foreign travel history to try to keep terrorists from getting jobs inside the nation's nuclear power plants, federal auditors said in a report Monday.

The commission's inspector general, at the behest of Sen. Charles Schumer, began the review after a suspected al-Qaida member, Sharif Mobley, was found to have worked in a New Jersey nuclear power plant for six years.

"The terrorists look for our weak pressure points and it's certainly possible they may say, 'Maybe we can send someone to infiltrate a nuclear power plant,'" Schumer, of New York, told The Associated Press in an interview. "It's not that these power plants are rife with terrorists ... but all you need is one."

Mobley's arrest showed that the nation needs better security to protect nuclear plants from terrorist infiltration, and the NRC "truly stepped up to the plate and provided concrete, actionable recommendations that can be put in place immediately," Schumer said.

Schumer discussed the audit and security issues during a series of news

The Washington Post

U.S. power plants at risk of attack by computer worm like Stuxnet

8

By Ellen Nakashima
Washington Post Foreign Service
Friday, October 1, 2010; 2:49 PM

A sophisticated worm designed to infiltrate industrial control systems could be used as a blueprint to sabotage machines that are critical to U.S. power plants, electrical grids and other infrastructure, experts are warning.

The discovery of Stuxnet, which some analysts have called the "malware of the century" because of its ability to damage or possibly destroy sensitive control systems, has served as a wake-up call to industry officials. Even though the worm has not yet been found in control systems in the United States, it could be only a matter of time before similar threats show up here.

"Quite honestly you've got a blueprint now," said Michael J. Assante, former chief security officer at the North American Electric Reliability Corporation, an industry body that sets standards to ensure the electricity supply. "A copycat may decide to emulate it, maybe to cause a pressure valve to open or close at the wrong time. You could cause damage, and the damage could be catastrophic."

Joe Weiss, an industrial control system security specialist and managing partner at Applied Control Solutions in Cupertino, Calif., said "the really scary part" about Stuxnet is its ability to determine what "physical process it wants to blow up." Said Weiss: "What this is, is essentially a cyber weapon."

Researchers still do not know who created Stuxnet, or why.

The antivirus security firm Symantec analyzed the worm this summer and, by taking control of servers it had been connected to, determined that the malware had infected about 45,000 computers around t he world. Most of those infected - about 30,000 - were in Iran. Those computers were not the targets, but the finding suggested that the target was nearby.

Speculation has focused on Iran's nuclear enrichment facilities, and this week Iranian officials said they suspect a foreign organization or nation designed the worm.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-10-272-01—PRIMARY STUXNET INDICATORS

September 29, 2010

OVERVIEW

ICS-CERT has been actively investigating and reporting on the Stuxnet vulnerability. To date, ICS-CERT has released ICSA-10-201-01-Malware Targeting Siemens Control Software[a] (including Updates B & C) and ICSA-10-238-01-Stuxnet Mitigations[b] (including Update B).

Stuxnet uses four zero-day exploits (two of which have been patched[b]) and takes advantage of a vulnerability also exploited by Conficker, which has been documented in Microsoft Security Bulletin MS-08-067.[c] The known methods of propagation include infected USB devices, network shares, STEP 7 Project files, WinCC database files, and the print spooler vulnerability addressed by MS-10-061.[d] The malware can be updated through a command and control infrastructure as well as peer-to-peer communication using the Remote Procedure Call (RPC) protocol.

The malware also interacts with Siemens SIMATIC WinCC or SIMATIC STEP 7 software. Exact software versions and configurations that may be affected are still being analyzed jointly by ICS-CERT and Siemens. We have listed the following indicators for use in detecting this malware.

PRIMARY MALWARE INDICATORS

INDICATOR LIST OVERVIEW

The following indicator list was developed by ICS-CERT and will be useful in detecting malicious files in systems infected with Stuxnet. Tests were performed on two systems. One system was a new installation of Windows XP SP3 that was subsequently infected with Stuxnet. The other machine was the same Windows configuration but also included Siemens WinCC and STEP 7 software installations. Based on these tests, ICS-CERT has determined that these indicators fall into two groups. Some indicators appear on systems whether or not they have Siemens WinCC/STEP 7 installed, and the others only appear on systems with WinCC/STEP 7 installed.

a. ICS-CERT Advisory, http://www.us-cert.gov/control_systems/pdf/ICSA-10-201-01C - USB Malware Targeting Siemens Control Software - Update C.pdf, website last accessed September 28, 2010.
b. ICS-CERT Advisory, http://www.us-cert.gov/control_systems/pdf/ICSA-10-238-01B - Stuxnet Mitigation.pdf, website last accessed September 28, 2010.
c. Microsoft Security Bulletin, http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx, website last accessed September 28, 2010.
d. Microsoft Security Bulletin, http://www.microsoft.com/technet/security/bulletin/ms10-061.mspx, website last accessed September 28, 2010.

RECENT ACTIVITIES

- 2010—The committee hosted twice-monthly conference calls on various topics
  - Cybersecurity
  - Ice storm responses
  - Recent conference call on the J100 RAMCAP standard for risk and resilience management of water and wastewater systems

RECENT ACTIVITIES

- Cybersecurity
  - *InformationWeek,* Feb. 5, 2010--annual spending on smart grid cybersecurity will more than triple from $1.2 billion last year to $3.7 billion in 2015.
  - *Montreal Gazette,* Sept. 10, 2010--Cyber security a growing concern in energy sector

RECENT ACTIVITIES

- Ice Storm Responses
  - Energy and Water Dependency Issues

RECENT ACTIVITIES

- J100 RAMCAP
  - There are three key upgrades in the RAMCAP® methodology that differentiate it from earlier methodologies that may have been applied in the water sector:
    - RAMCAP provides guidance for calculating the Probability of Attack in a more granular fashion in that it is not assumed to be 100% or 1.
    - RAMCAP provides guidance for calculating the probability of a specific natural hazard occurring at a given utility (i.e., earthquake, tornado, and hurricane).
    - RAMCAP provides guidance for calculating asset and utility resilience.

RECENT ACTIVITIES

- Semi-annual meetings of the Committee
  - Winter Committee Meetings (2010)—Presentations
    - ARRA State and Local Energy Assurance Planning and Implementation—presentation by U.S. Department Of Energy (DOE)
    - Protective Security Advisor Program—presentation by the Department of Homeland Security (DHS)
    - Promoting Community-Based Water Resiliency—presentation by U.S. Environmental Protection Agency (EPA)

RECENT ACTIVITIES

- Worked with the National Association of State Energy Officials to issue a national guide for writing and implementing energy assurance plans by the States
- Contributed to the update of the National Infrastructure Plan in 2010
- Participated as members of the national government coordinating councils for the energy sector, water sector, and communications sector

RECENT ACTIVITIES

- Hosted two trainings, one at NARUC's Southeastern US regional meetings in Point Clear, Alabama, with over 80 attendees, and another training at the NARUC Summer Committee meetings in Sacramento, California
- These trainings, funded by DHS, provided Commissioners with the basic terms and concepts of critical infrastructure protection and how they apply to regulators and the regulation of utility services for water, telecommunications, energy and transportation, as well as other independent sectors

RECENT ACTIVITIES

- July 2010—Members of the Committee and staff subcommittee were key participants in a national preparedness exercise called "Secure Grid 2010" hosted by DOD, DOE and DHS in Colorado Springs, Colorado
- Exercise focused on cybersecurity for the electric sector and on interdependencies with other sectors, including the water sector

RECENT ACTIVITIES

- CI Committee worked with NARUC Grants & Research Department to organize and host tabletop exercises for five states: Ohio, Pennsylvania, Maine, Michigan and Texas
- Michigan and Texas scenarios were focused on electric, gas and telecommunications infrastructure
- Maine scenario explored the impact of major flooding on the Kennebeck River, with critical impacts to water systems
- Ohio and Pennsylvania scenarios explored the disabling of drinking water systems due to severe and extended power outages in the Lake Erie region.

RECENT ACTIVITIES

- NARUC continues to implement two grants from DOE and Homeland Security and build partnerships with the Federal government, the private sector, and between states to improve the protection of essential utility assets.

FUTURE ACTIVITIES

- CI Committee Strategic Planning Session later this month to develop long range strategy and direction for the Committee
- NARUC Annual Conference in Atlanta, Georgia, November 14-17, 2010
- Continued twice-monthly conference calls for the remainder of 2010 to discuss timely issues relating to CI

QUESTIONS?

Terry Jarrett

Commissioner

Missouri Public Service Commission

terry.jarrett@psc.mo.gov

www.psc.mo.gov