Facility Control Systems Vulnerabilities, Alert / Advisories Overview

Luis Ayala, **Senior Technical Expert - Facilities & Construction**
Defense Intelligence Agency

David Retland, **Acquisition, Technology and Facilities**
Office of the Director of National Intelligence

Unrestricted Cyber-Warfare

David Retland, ODNI

Luis Ayala, DIA

24 March 2015

Industrial Control Systems Risk

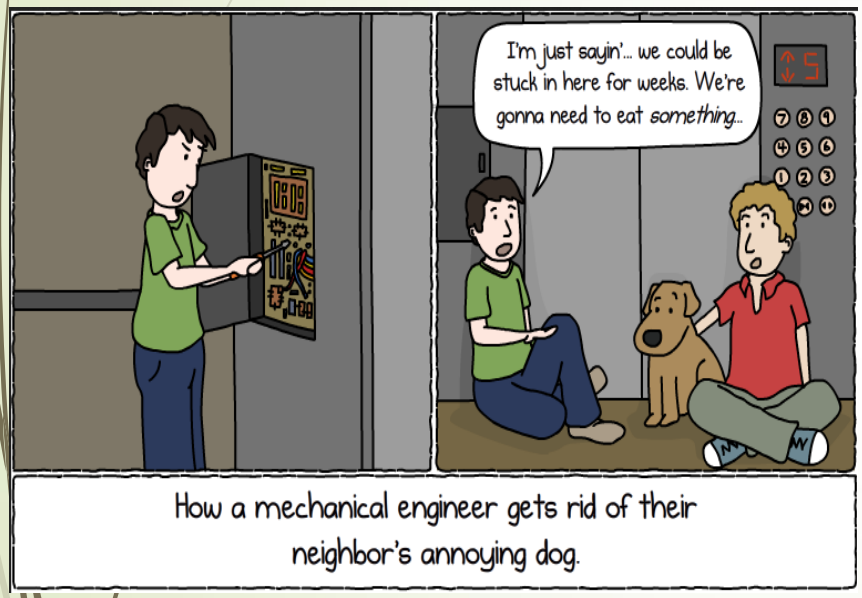
- Director of National Intelligence Warning
  - Cyber attacks pose a CRITICAL national and economic security concern (January 2012 testimony before Congress)
- Secretary of Defense Warning
  - A Cyber attack on our nation's critical infrastructure could cause a major disruption

Recent Incidents

- 2014: Cyber incident at a wastewater treatment plant
- 2013: Target breach
- 2010: Stuxnet
- 2009: Security guard at Dallas-area hospital loaded a malicious program onto the system that controlled the HVAC for two floors
- 2006: Los Angels city employees hacked into computers that controlled the city's traffic lights

Hacking: Evolution…

Then



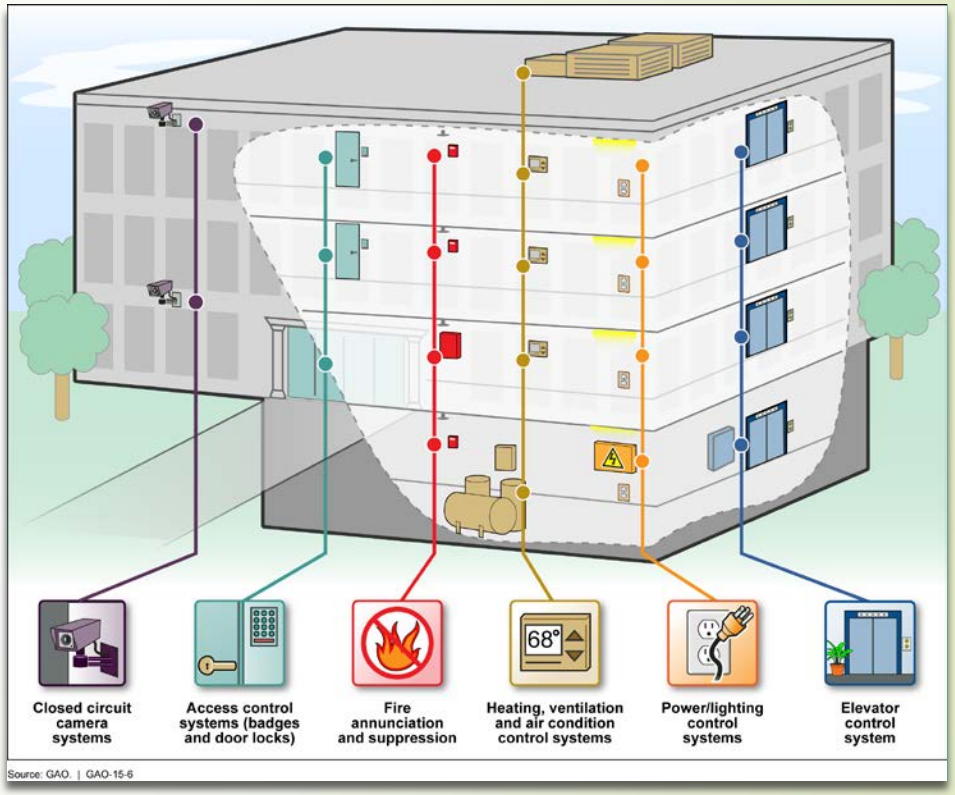
Hacking into a building's control system required someone on the inside with specific knowledge of the system

Now

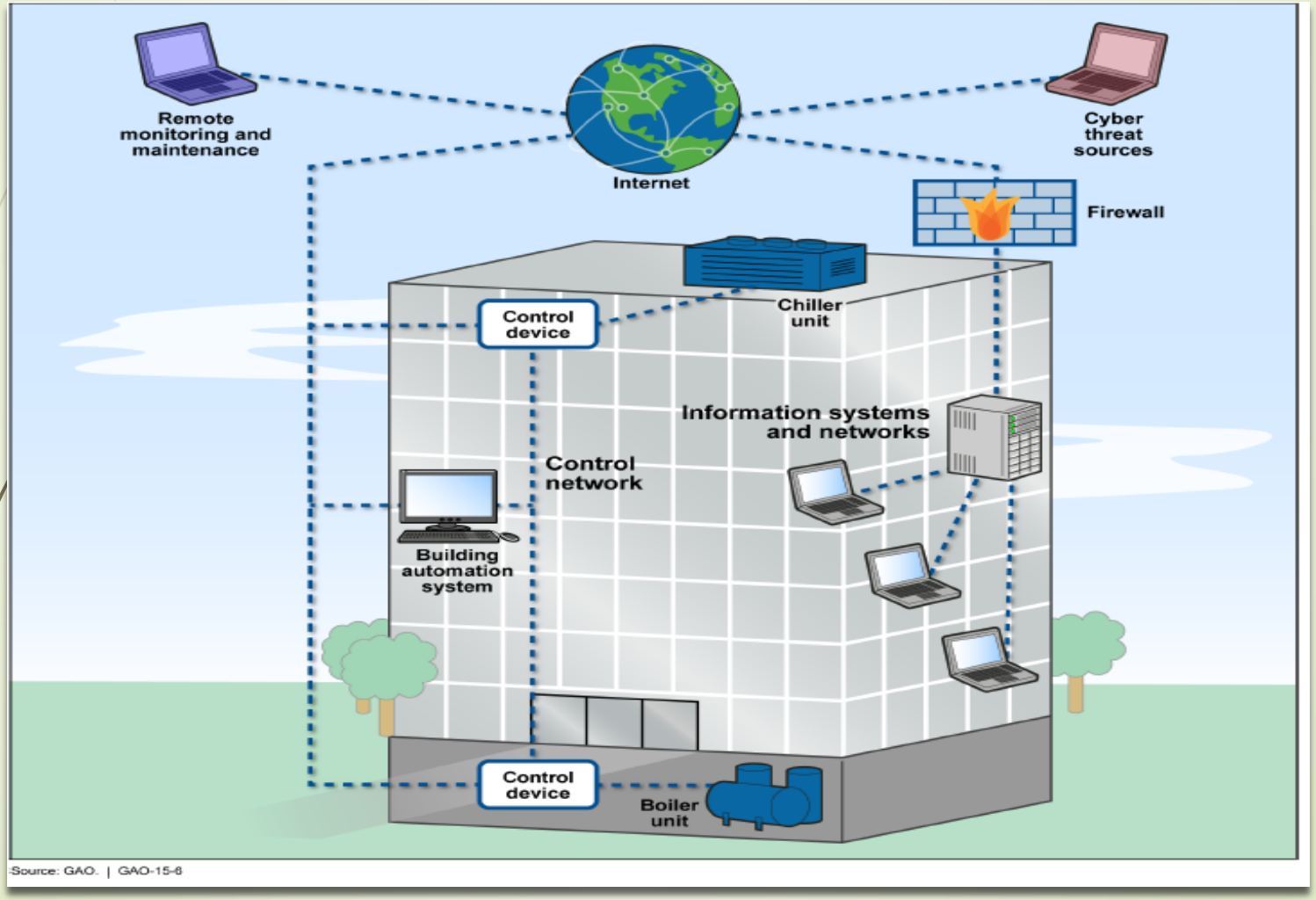
Hacking into a building's control system can be achieved on the outside using a remote device as simple as a laptop (facemask is optional)

Vulnerabilities

- Closed circuit camera
- Access control
- Fire annunciation and suppression
- HVAC
- Power and lighting control
- Elevator control

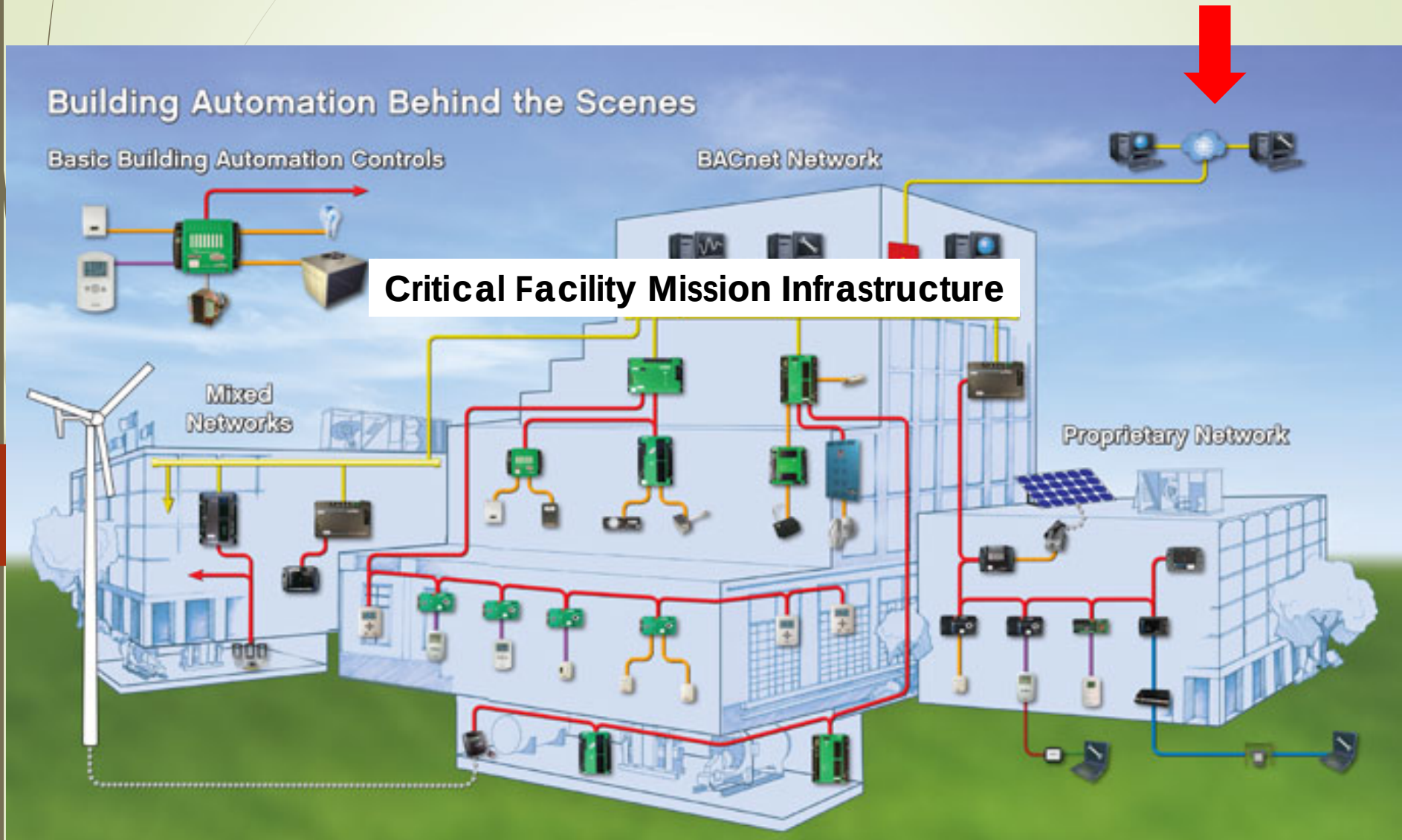


Connectivity via the Internet



Building Automation Systems (BAS)

Vulnerability is a "weakness in design or operation an adversary can exploit."
Department of Homeland Security



Cyber is a critical weapon

To an adversary, Cyberspace is merely another environment of opportunity . Unlike a ballistic missile, you can't trace trajectory back to source easily, or quickly (if at all).

Unlike a Denial-of-Service attack or data theft, a cyber-attack on a BAS happens in real world, in real-time, when you don't expect it (or don't believe it).

Replacing 30-year old mechanical and electrical building equipment with modern equipment can make facilities more vulnerable to remote collection and disruption.

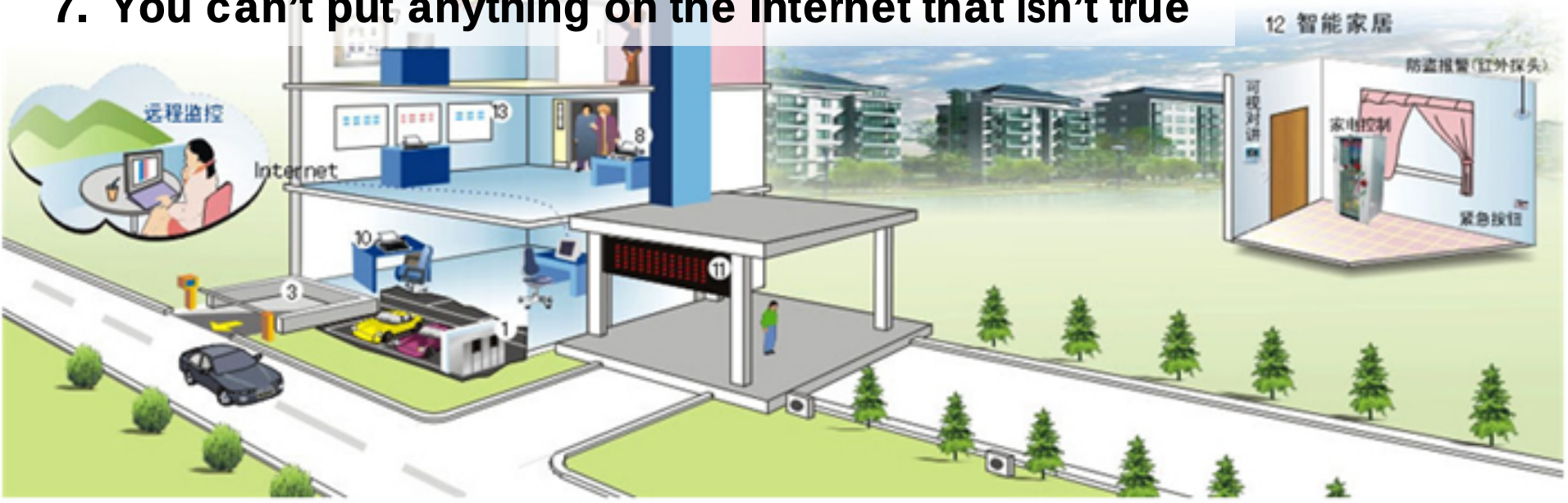
A hacker can do all this remotely to multiple sites simultaneously:

Monitor building occupancy
Change room temps
Set off alarms
Drain the cooling towers
Turn off the power
Monitor CCTV
Close all air vents
Turn off the lights
Contaminate water supply
Cut communications
Lock out maintenance staff
Change passwords
Turn off sewage pumps
Access corporate network thru BAS network to steal data
Unlock exterior doors, deactivate vehicle barriers, turn off security system

A hacker can even command a $2M backup generator to destroy itself. (2007 Aurora Project video courtesy of DHS and Idaho National Labs)

BAS Security Misconceptions:

1. My BAS is secure because it's not connected to the Internet (not true)
2. Security thru obscurity (fool's paradise)
3. My backup generators will come on if I lose power (this is the second attack)
4. Managed by same folks that manage desktop
5. IT staff and security staff are on top of this
6. Software updates and security patches are current
7. You can't put anything on the Internet that isn't true



National Science Foundation BAS

A hacker is just a Click away from sending everyone home.

Graphics - [41CS.CHILLER.PLANT (Read-Only)]

File Edit View Insert Dynamic Tools Window Help

SIEMENS Unit CHILLED WATER PLANT Location LOWER LEVEL 1 / ROOF

Note: Chiller Enable - Opens Valves, and Starts Pumps Sequentially

Advisory: Add Chiller / Drop Chiller

Tower Alarms: CT-1 Heat Trace NORMAL | CT-2 Heat Trace NORMAL | CT-1 Lo Level Alarm | CT-2 Lo Level Alarm | CT-1 Hi Level Alarm | CT-2 Hi Level Alarm

CHILLED WATER HEADER

CPF-1 49.11 DEG F SCHWS

SCHWP-4 Spd 0.00 PCT Fdbk 0.00 HZ Alarm

SCHWP-5 Spd 100.00 PCT Fdbk 60.00 HZ Alarm

SCHWP-6 Spd 0.00 PCT Fdbk 0.00 HZ Alarm

15.00 PSI 9.96 PSI SCHWR

EXP Tank Make Up Water ET-C1 62.26 PSI

AS-1 Filter 48.79 1DGF

Volume 1087.00 1GPM Energy 3262.00 KBPH 54.78 1DGF

FM-1 SEC CHW

Volume 1013.00 1GPM Energy 3686.00 KBPH

FM-2 PRIM CHW 54.97 DEG F

CHWP-1 CHWP-2 CHWP-3

47.65 1DGF 54.86 1DGF 47.72 DEG F 56.19 DEG F

Chemical Tank

Water Treatment Control Panel

CT1.START NONE ON CT2.START NONE ON

REQUIRED	CHWP's	1.00	CWP's	1.00	TOWERS	1.00
CHILLER 1	ENABLE	ON	STATUS	RUNNING	ALARM	NORMAL
CHILLER 2	ENABLE	OFF	STATUS	READY	ALARM	NORMAL

V-1 OPEN V-2 OPEN CH-1 75.50 DEG F

V-3 CLOSE V-4 CLOSE CH-2 75.50 DEG F

CW BYPASS NONE -0.00 PCT V-7

V-5 OPEN V-6 OPEN

CT-1 ENABLE NONE ON 186.86 DEG F Spd 63.27 PCT Fdbk 37.80 HZ Alarm

CT-2 ENABLE NONE OFF 282.92 DEG F Spd 63.27 PCT Fdbk 37.80 HZ Alarm

70.51 DEG F 70.88 DEG F

V-9 OPEN V-10 OPEN

70.00 DEG F 70.01 DEG F

70.71 DEG F CWP-1 CWP-2 CWP-3

LINKS:

MAIN MENU | CHILLER OPTIMIZATION | AIR HANDLER SYSTEMS | CHILLER MER / FIRE PUMP RM | OUTSIDE AIR | WetBulb 62.66 DEG F | Temperature 83.97 DEG F | Humidity 31.99 % RH

How Can Hackers Get Into My BAS?

Network (External) – Most BAS systems are accessible thru the Internet. A quick look at www.shodan.com identifies Industrial Control Systems by location, equipment manufacturer, network name, etc.

Network (Internal) – Many BAS can be accessed from the corporate network. A user that uses the same computer to access web sites can infect the BAS with malware.

Vendors – Some vendors install a modem in their hardware so they can "tweak" equipment remotely.

Insiders – An unsuspecting employee inserts a thumb drive into a USB and uploads malware unknowingly. A disgruntled employee puts in a "back door" after receiving a poor performance rating. A foreign spy installs a key logger on a computer to obtain Super-User Passwords or a Dropbox.

26 percent of SCADA cyber-attacks are attributable to 'insiders".

What Can I Do About It?

Step 1. Disconnect BAS from the Internet – Really disconnect, not hearsay. Many times the actual BAS does not look like the network diagram shows. Segment BAS into “zones” to prevent cross-contamination of malware.

Step 2. Implement aggressive Password Security Program – Change default passwords, delete former employee passwords immediately, change passwords frequently, lock out multiple attempts.

Step 3. Do not allow thumb drives or laptops to access BAS unless necessary.

Step 4. Disable unused Ports (there are thousands of back doors).

Step 5. Install Intrusion Detection Software.

Step 6. Install security appliance (hardware) at key points (such as Torfino).

Step 7. Inspect hardware regularly for rogue access points and key loggers.

Step 8. Monitor network performance and investigate anomalies.

Step 9. Audit historical network logs.

Step 10. Bring in an expert for penetration test and vulnerability assessment.

Cyber-Attack? .....Really?

info security
STRATEGY | INSIGHT | TECHNOLOGY

Latest
Yahoo! Releases On-Demand Passwords

News Topics Features Webinars White Papers Jobs Events & Conferences Directory

INFOSECURITY MAGAZINE HOME » NEWS » RUSSIAN HACKERS BEHIND FIRST SUCCESSFUL US SCADA SYSTEM ATTACK

21 NOV 2011 | NEWS

Russian hackers behind first successful US SCADA system attack

As reportedly previously SCADA – Supervisory Control and Data Acquisition – systems are often used for protecting critical national infrastructure platforms such as energy and telecommunications grids. The systems are usually based around an embedded and robust version of Windows, which makes them resilient against most malware.

The Reuters newswire suggests that the hackers gained access to the systems of a vendor of

Why Not Watch

Proof of Concept

The Reuters newswire suggests that the hackers gained access to the systems of a vendor of SCADA control systems and then used the knowledge gained – possibly tapping the use of default IDs and password – to attack and destroy the Illinois water pump system.

"The pump was apparently remotely activated and burnt out, though redundant systems meant no impact was felt by residents of the town",

Cyber-Attack? .....Really?

- Dutch hackers during the Gulf War

"At least one penetrated system directly supported U.S. military operations in Operation Desert Storm prior to the Gulf War. They copied or altered unclassified data and changed software to permit future access. The hackers were also looking for information about nuclear weapons. Their activities were first disclosed by Dutch television when camera crews filmed a hacker tapping into what was said to be U.S. military test information."

1992 -- Chevron -- Emergency system was sabotaged by disgruntled employee in over 22 states

1997 -- Worchester Airport -- External hacker shut down the air and ground traffic communication system for six hours

1998 -- Gazprom -- Foreign hackers seize control of the main EU gas pipelines using trojan horse attacks

2000 -- Queensland, Australia -- Disgruntled employee hacks into sewage system and releases over a million liters of raw sewage into the coastal waters

2002 -- Venezuela Port -- Hackers disable PLC components during a national unrest and general workers strike, disabled the country's main port

2003 -- U.S East Coast blackout -- A worm did not cause the blackout, yet the Blaster worm did significantly infect all systems that were related to the large scale power blackout

2003 -- Ohio Davis-Besse Nuclear Plant -- Plant safery monitoring system was shut down by the Slammer worm for over five hours

2003 -- Israel Electric Corporation -- Iran originating cyber attacks penetrate IEC, but fail to shut down the power grid using DoS attacks

2005 -- Daimler Chrysler -- 13 U.S manufacturing plants were shut down due to multiple internet worm infections (Zotob, RBot, IRCBot)

2005 -- International Energy Company -- Malware infected HMI system disabled the emergency stop of equipment under heavy weather conditions

2006 -- Middle East Sea Port -- Intrusion test gone wrong. ARP spoofing

“I am a peripheral visionary. I can see the future, but only way off to the side.”

- Steven Wright