Cyber Threats and Vulnerabilities

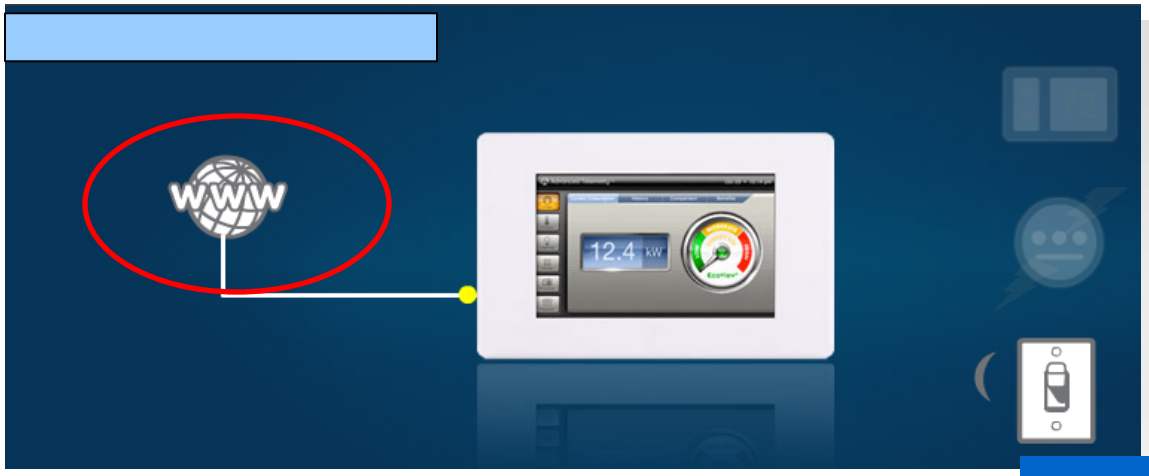
- Attacks on EMCS
- Attack Vectors
- Attack Demonstration

"For every attack reported there's a hundred attacks unreported." Eric Byres

John H. Saunders, Ph.D.
Professor & Director, Center for Cyber Security, National Defense University

The views expressed herein are personal and do not reflect the official policy or position of the National Defense University, The Department of Defense, or the U.S. Government.

How Did Max Do That?



Remote Access Via the Wo
Wide Web

Login	Password
johnson	control
honeywell	webs
Med (Siemens)	med

GovEnergy
www.govenergy.gov

See e.g. http://www.cyxla.com/passwords/passwords.html

Attack: Ghost Exodus

Case 3:09-cr-00210-B Document 11 Filed 07/22/2009 Page 5 of 5

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
JUL 22 2009
CLERK, U.S. DISTRICT COURT
By _____ Deputy

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA

v.

JESSE WILLIAM MCGRAW (1)

3-09 CR-210-B

INDICTMENT

18 U.S.C. § 1030(a)(5)(A) and § 1030(c)(4)(B)(i)(II)
Transmitting a Malicious Code

18 U.S.C. 1030(a)(5)(A) and § 1030(c)(4)(B)(i)(II) and (IV)
Transmitting a Malicious Code

2 Counts

A true bill rendered:

DALLAS FOREPERSON

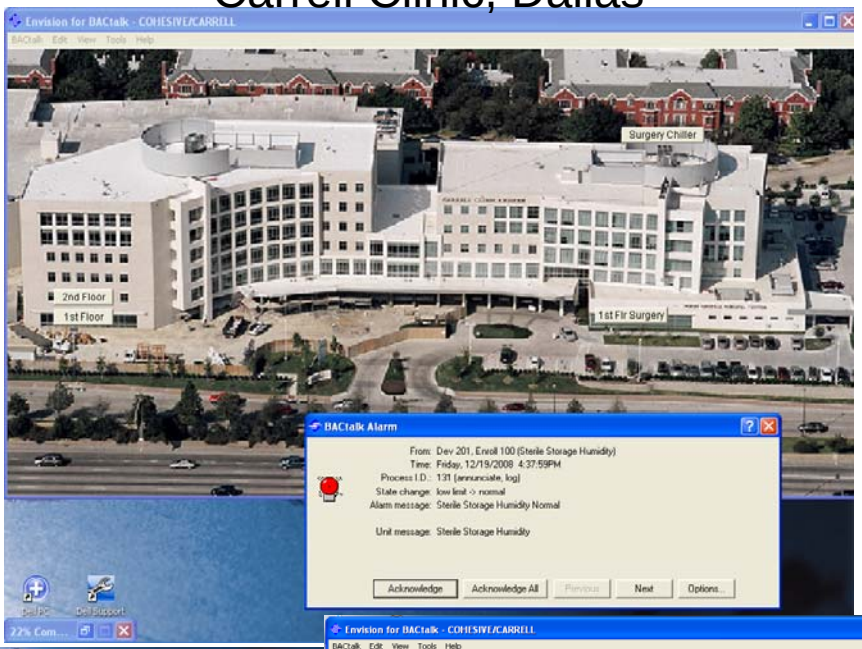
Filed in open court this _____day of _____, A.D. 2009.

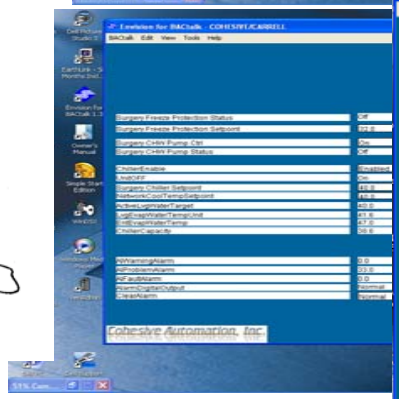
Clerk

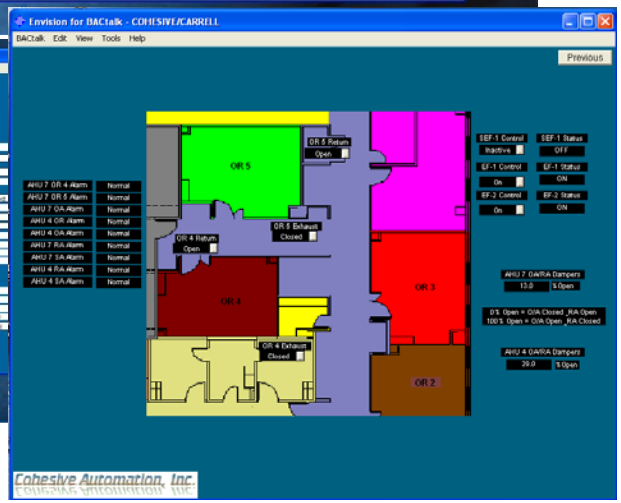
JESSE WILLIAM MCGRAW - In Custody (Seagoville)

UNITED STATES ~~DISTRICT~~/MAGISTRATE JUDGE 7/22/09
Criminal Complaint 3:09-MJ-207
Magistrate Case No. 3:09-207-MJ

Carrell Clinic, Dallas







GovEnergy
www.govenergy.gov

Attack: Pacific Energy

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2009 Grand Jury

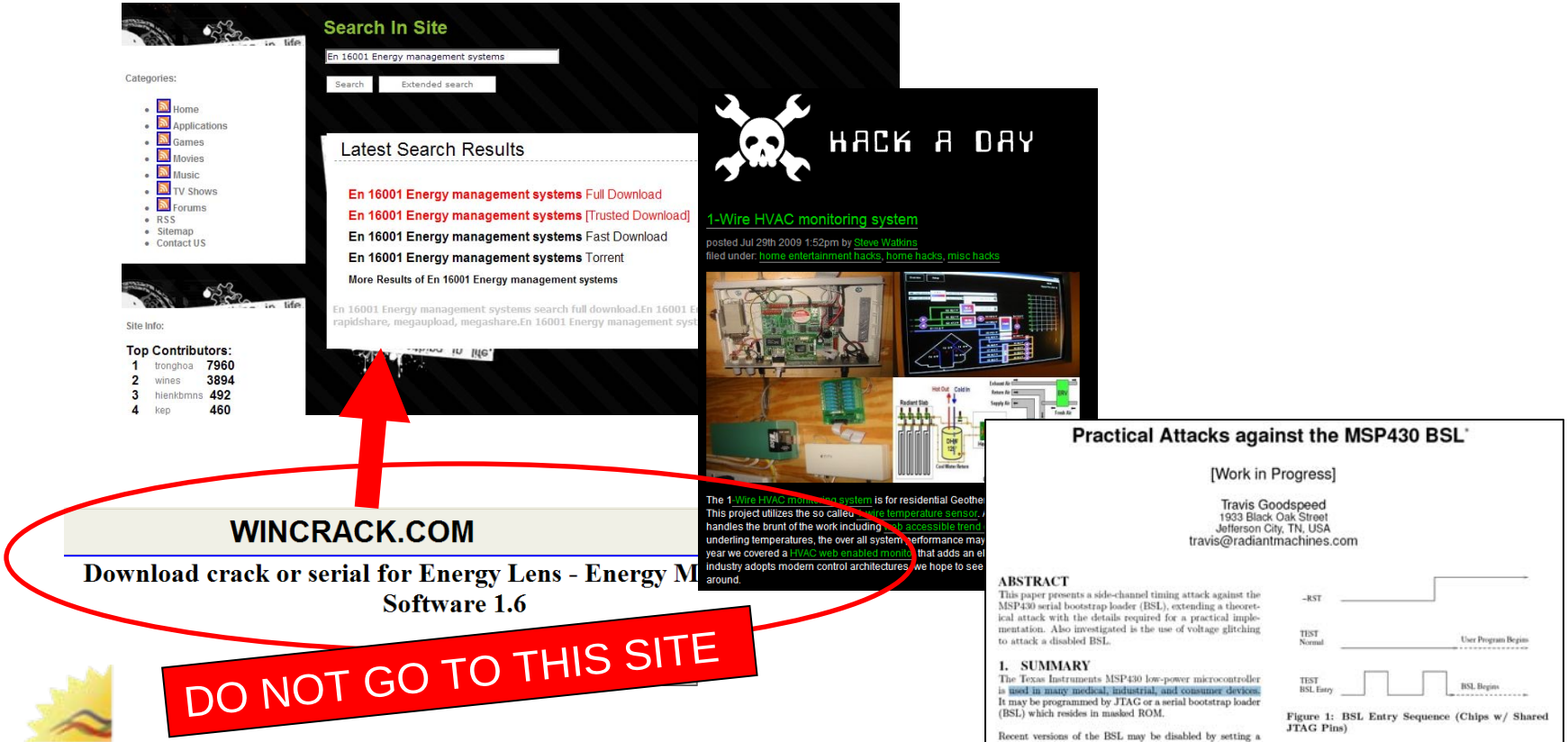
UNITED STATES OF AMERICA, Plaintiff, v. MARIO AZAR, Defendant.	)))))))))	CR No. 09- I N D I C T M E N T [18 U.S.C. § 1030(a)(5)(A)(i), (B)(i): Unauthorized Impairment Of A Protected Computer]

PACIFIC ENERGY

GovEnergy
www.govenergy.gov

Attack: GEXA Energy

- On Feb. 5, 2008, GEXA Energy terminated Kim's employment as a database administrator and permanently revoked his access to all GEXA Energy facilities, computer networks, and information technology systems, the report says. Approximately three months later, Kim remotely accessed the GEXA Energy computer network and GEXA Energy Management System (GEMS) database.
  http://www.darkreading.com/insiderthreat/security/cybercrime/showArticle.jhtml?articleID=221900552



GovEnergy
www.govenergy.gov

Attack Tools: The Hacker Desktop

http://vimeo.com/2295785

Attack Vector: Vulnerability Exploitation

Recent Vulnerability Announcements 2010

Aug 5. CVE 2965 thru 2968. Severity 7.8

- The FTP daemon in **Wind River VxWorks** does not close the TCP connection after a number of failed login attempts, which makes it easier for remote attackers to obtain access via a brute-force attack.
- The loginDefaultEncrypt algorithm in loginLib in Wind River VxWorks before 6.9 does not properly support a large set of distinct possible passwords, which makes it easier for remote attackers to obtain access via a (1) telnet, (2) rlogin, or (3) FTP session.
- The INCLUDE_SECURITY functionality in Wind River VxWorks 6.x, 5.x, and earlier uses the LOGIN_USER_NAME and LOGIN_USER_PASSWORD (aka LOGIN_PASSWORD) parameters to create hardcoded credentials, which makes it easier for remote attackers to obtain access via a (1) telnet, (2) rlogin, or (3) FTP session.
- The WDB target agent debug service in Wind River VxWorks 6.x, 5.x, and earlier, as used on the **Rockwell Automation 1756-ENBT series** A with firmware 3.2.6 and 3.6.1 and other products, allows remote attackers to read or modify arbitrary memory locations, perform function calls, or manage tasks via requests to UDP port 17185, a related issue to CVE-2005-3804.

Aug 5 CVE 2862, 2201-2212 (Jun30) Severity 9.3

- Adobe Acrobat arbitrary code execution or denial of service simply thru execution of carefully crafted PDF files

July 22 *CVE* 2772 Severity 6.9

- Microsoft vulnerability payload(see CVE 2568 severity 9.3) targets **Siemens Simatic WinCC and PCS 7** SCADA system uses a hard-coded password, which allows local users to access a back-end database and gain privileges, as demonstrated in the wild in July 2010 by the Stuxnet worm,

See: http://nvd.nist.gov/home.cfm

Energy Management with SIMATIC

With SIMATIC, the integrated automation system from Siemens, companies optimize the decisive levers for increasing their productivity and competitiveness: time, costs and quality.

The issue of saving energy costs plays a crucial role here. Thanks to its unique portfolio, SIMATIC enables system-wide efficient use of energy. Energy resources can be transparently and controlled effectively.

PROFIenergy: Energy costs under control

An important key to reducing the energy costs: Shutting down productive periods as well as acquiring measured energy data in granular fashion.

With this as objective, PROFIBUS & PROFINET International [illegible]

'Stuxnet' Trojan Targets Siemens WinCC

20 July 2010

Siemens is alerting its users in the USA that a malware program (Trojan) is targeting the Simatic WinCC and PCS 7. The Trojan is spread by USB memory sticks and takes advantage of Microsoft security vulnerabilities. First noticed on 14 July, the malware affects all Windows computers from XP on up.

Apparently, a simple viewing the contents of the USB [illegible] the Trojan. Siemens has [illegible]voiding the use of a USB stick on all [illegible] WinCC software.

[illegible]de has been designated [illegible] and propagates using USB drives [illegible]ed with malformed shortcut (*.lnk*) [illegible]ed when the user inserts the USB [illegible]d views the contents with Windows [illegible] application that displays the file [illegible]cifically aimed at WinCC it could be [illegible]ny Windows system that accepts [illegible]a. It appears to rely on an [illegible]erability in Windows .lnk file handling.

[illegible]n Microsoft controls that require drivers to be digitally signed, the code contains the digital signature of Realtek Semiconductor Corp.

Trojan target: WinCC

MS CVE 2568

- XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7
- via .LNK & .PIF; Shares, WebDAV

"For every attack reported there's a hundred attacks unreported." Eric Byres

Other EMCS Sample Attack Vectors

- **Email w Adobe Attachment**
  - Gather Personal / organizational email addresses
  - Send faked Pay/benefits notice w Adobe Attachment
  - Buffer overflow installs trojan/keystroke logger
  - Monitor access from workstation to EMCS
  - Capture URL, login & password
- **Local Connect**
  - Disconnect Device RJ-45 cable
  - Plug into PC or plug into empty socket on switch
  - Use Zenmap to run scan on common non-routable address space
  - Execute Wireshark on identified space to effect packet capture

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT Advisory-10-216-01: Adobe Reader/Acrobat Critical Vulnerability

August 4, 2010

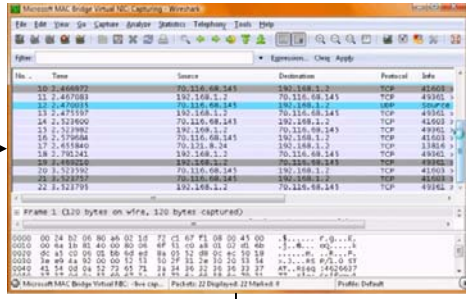
OVERVIEW

US-CERT has confirmed with Adobe that a newly disclosed, critical vulnerability exists in Adobe Reader. By convincing a user to open a specially crafted file that exploits this vulnerability, an attacker could execute arbitrary code on a user's system.

GovEnergy
www.govenergy.gov

Sample Attack Vector & Demo: Wireless Network ID & Inject

- Identify Wireless Access Point
- If open, connect. If not, crack with e.g *Airmon/crack*, then connect.
- Set wireless card on promiscuous mode.
- Capture packets with *Wireshark* (may need to do ARP Cache poisoning to foil network switch)
- Analyze captured data to Identify device addresses, protocols
- Use *Netcat* to inject denial of service packet



nc 7.1.1.105 502 –w 1 <c:\coil8-off.hex

GovEnergy
www.govenergy.gov