



• August 15-18, 2010 • Dallas, Texas •  
• Dallas Convention Center •

## Session 8

# Cyber Security Solutions to the Installation-wide Energy Management and Industrial Control Systems

**Mike Aimone**

**[Aimonem@Battelle.org](mailto:Aimonem@Battelle.org)**

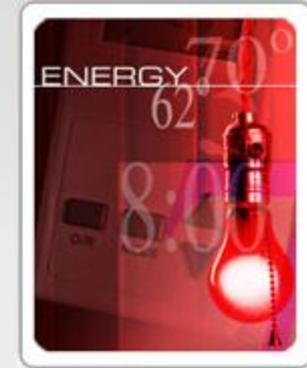
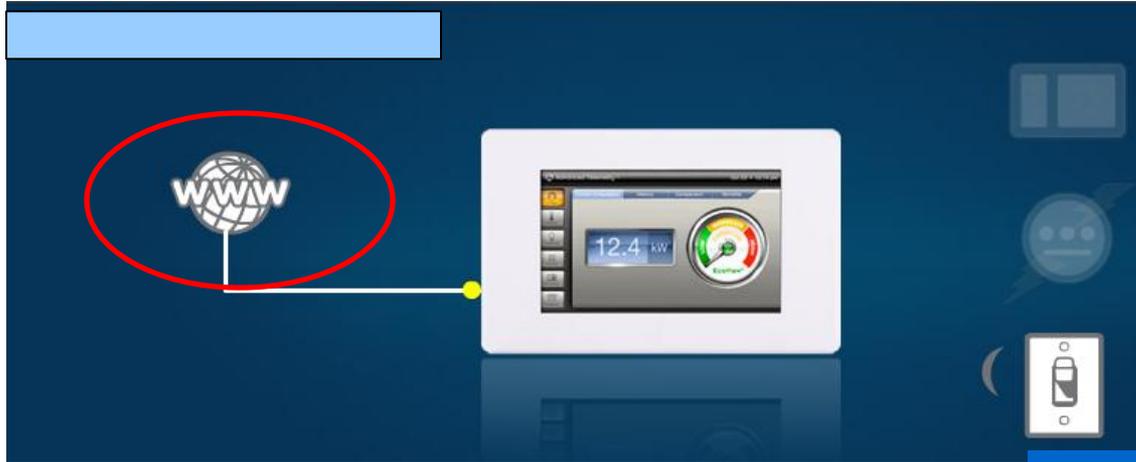


# Opening Comments

# Cyber Security & Industrial Control Systems

- **Computerized and Networked DOD Industrial Control Systems Require A Level Security Consistent with Information Assurance Guidelines**
  - **Processes, Tools and Techniques Are Different than solutions provided to the IT Network**
- **Presenters**
  - **Cyber Threats & Vulnerabilities – Dr John Saunders, NDU**
  - **Defense in Depth: The Federal Standards – Dr Ron Ross, NTIS**
  - **DoD Information Assurance for Industrial Control Systems– Ms Stacey Tyley, OSD/I&E**
  - **Industry Approaches and Resources for Securing SCADA/ICS – Mr Andy Bochman, IBM/Rational Di vision**

# How Did Max Do That?



ENERGY MANAGEMENT SYSTEMS



Login	Password
johnson	control
honeywell	webs
Med (Siemens)	med

<http://www.cyxla.com/passwords/passwords.html>



# Attack: Pacific Energy

7  
8 UNITED STATES DISTRICT COURT  
9 FOR THE CENTRAL DISTRICT OF CALIFORNIA  
10 February 2009 Grand Jury

11 UNITED STATES OF AMERICA, ) CR No. 09-  
12 )  
13 Plaintiff, ) I N D I C T M E N T  
14 v. ) [18 U.S.C. § 1030(a)(5)(A)(i),  
15 MARIO AZAR, ) (B)(i): Unauthorized  
16 Defendant. ) Impairment Of A Protected  
17 ) Computer]



# 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>

**Search In Site**

En 16001 Energy management systems

Search Extended search

**Latest Search Results**

- En 16001 Energy management systems Full Download
- En 16001 Energy management systems [Trusted Download]
- En 16001 Energy management systems Fast Download
- En 16001 Energy management systems Torrent

More Results of En 16001 Energy management systems

En 16001 Energy management systems search full download.En 16001 Energy management systems search trusted download.En 16001 Energy management systems search fast download.En 16001 Energy management systems search torrent.En 16001 Energy management systems search full download.En 16001 Energy management systems search trusted download.En 16001 Energy management systems search fast download.En 16001 Energy management systems search torrent.

Site Info:

**Top Contributors:**

1	tronghoa	7960
2	wines	3894
3	hiencong	146
4	kep	46



**1-Wire HVAC monitoring system**

posted Jul 29th 2009 1:52pm by Steve Watkins  
 filed under: home entertainment hacks, home hacks

**Practical Attacks against the MSP430 BSL\***

[Work in Progress]

Travis Goodspeed  
 1933 Black Oak Street  
 Jefferson City, TN, USA  
 travis@radiantmachines.com

**ABSTRACT**  
 This paper presents a side-channel timing attack against the MSP430 serial bootstrap loader (BSL), extending a theoretical attack with the details required for a practical implementation. Also investigated is the use of voltage glitching to attack a disabled BSL.

**1. SUMMARY**  
 The Texas Instruments MSP430 low-power microcontroller is used in many medical, industrial, and consumer devices. It may be programmed by JTAG or a serial bootstrap loader (BSL) which resides in masked ROM.

Recent versions of the BSL may be disabled by setting a value in flash memory. When enabled the BSL is protected

Figure 1: BSL Entry Sequence (Chips w/ Shared JTAG Pins)

**WINCRACK.COM**

Download crack or serial for Energy Lens - Energy Management Software 1.6

**DO NOT GO TO THIS SITE**



### 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 used transparently and controlled effectively.

**PROFenergy: Energy costs under control**  
An important key to reducing the energy costs: Shutting down production during non-productive periods as well as acquiring measured energy data in a granular fashion. With this as objective, PROFIBUS & PROFINET International offers the solution.

**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



### '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 drive is all it takes to install the Trojan. Siemens has advised users to avoid the use of a USB stick on all computers running WinCC software.

The Trojan has been designated as STUXNET and propagates using USB drives infected with malformed shortcut (.lnk) files. It is activated when the user inserts the USB drive and views the contents with Windows Explorer. The application that displays the file contents is specifically aimed at WinCC it could be installed on any Windows system that accepts .lnk files. It appears to rely on an exploit of a vulnerability in Windows .lnk file handling.

Without valid Microsoft controls that require drivers to be digitally signed, the code contains the digital signature of Realtek Semiconductor Corp.



Trojan target: WinCC

# 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**

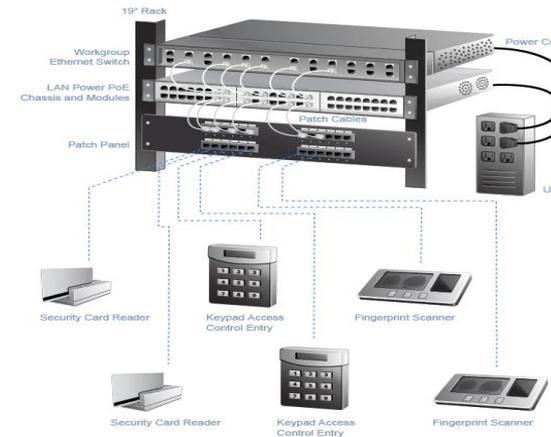
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

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

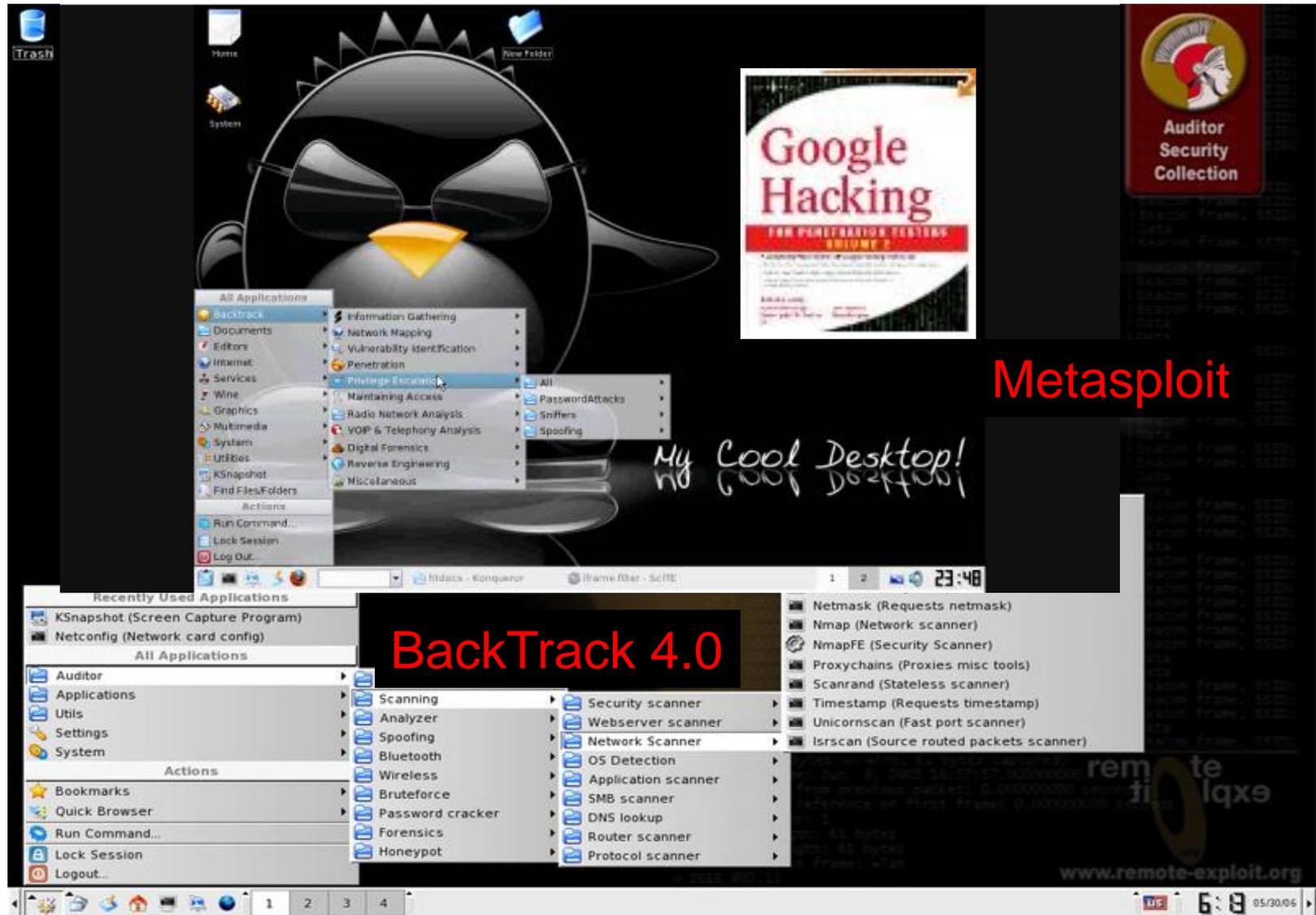
August 4, 2010

### 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.



# Attack Tools: The Hacker Desktop



Metasploit

BackTrack 4.0