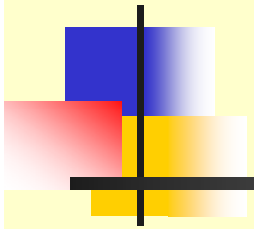


Cyber Security Update

Denise Heagerty
CERN Computer Security Officer

HEPiX Meeting, CERN, 5-9 May 2008

Acknowledgements

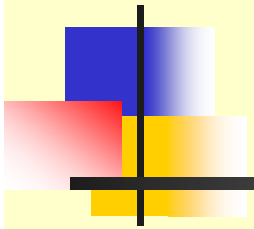
- **Thanks to the following people for their contributions and suggestions for this presentation:**
  - Lionel Cons, CERN
  - Bob Cowles, SLAC
  - Sebastien Dellabella
  - Jan Iven, CERN
  - David Jackson, STFC
  - Stefan Lueders, CERN
  - Djilali Mamouzi
  - David Myers, CERN
  - Romain Wartel, CERN

Overview

These slides cover a selection of security highlights during the past few months for:

- **Web Security**
- **Windows Security**
- **Linux Security**
- **Mac security**
- **Controls Security**
- **Miscellaneous**

This presentation complements information in 'Operational security for a Grid environment' by Romain Wartel



Web Security Update

Web (in)security update

- **IFRAME injection attacks continue**
  - Inserts IFRAME HTML tags into web pages
  - Loads malware from another site into this IFRAME
  - Relies on finding vulnerable web servers
    - Unfortunately they are not difficult to find!
  - Targets vulnerabilities in Web browsers and plug-ins
    - E.g. vulnerabilities in media players are common
- **Insufficient file protections are targets**
  - Including AFS file space – check if your ACLs are too open!
  - Used for hosting inappropriate content (malware, SPAM, ...)
  - Automated tools post to open forums, blogs, wikis, guestbooks, etc...
    - http://pandalabs.pandasecurity.com/archive/XRumer.aspx

Any insecure web site is likely to be attacked

Hackers jack thousands of sites, including U.N. domains

It's a repeat of earlier attacks that relies on an SQL injection, says Websense

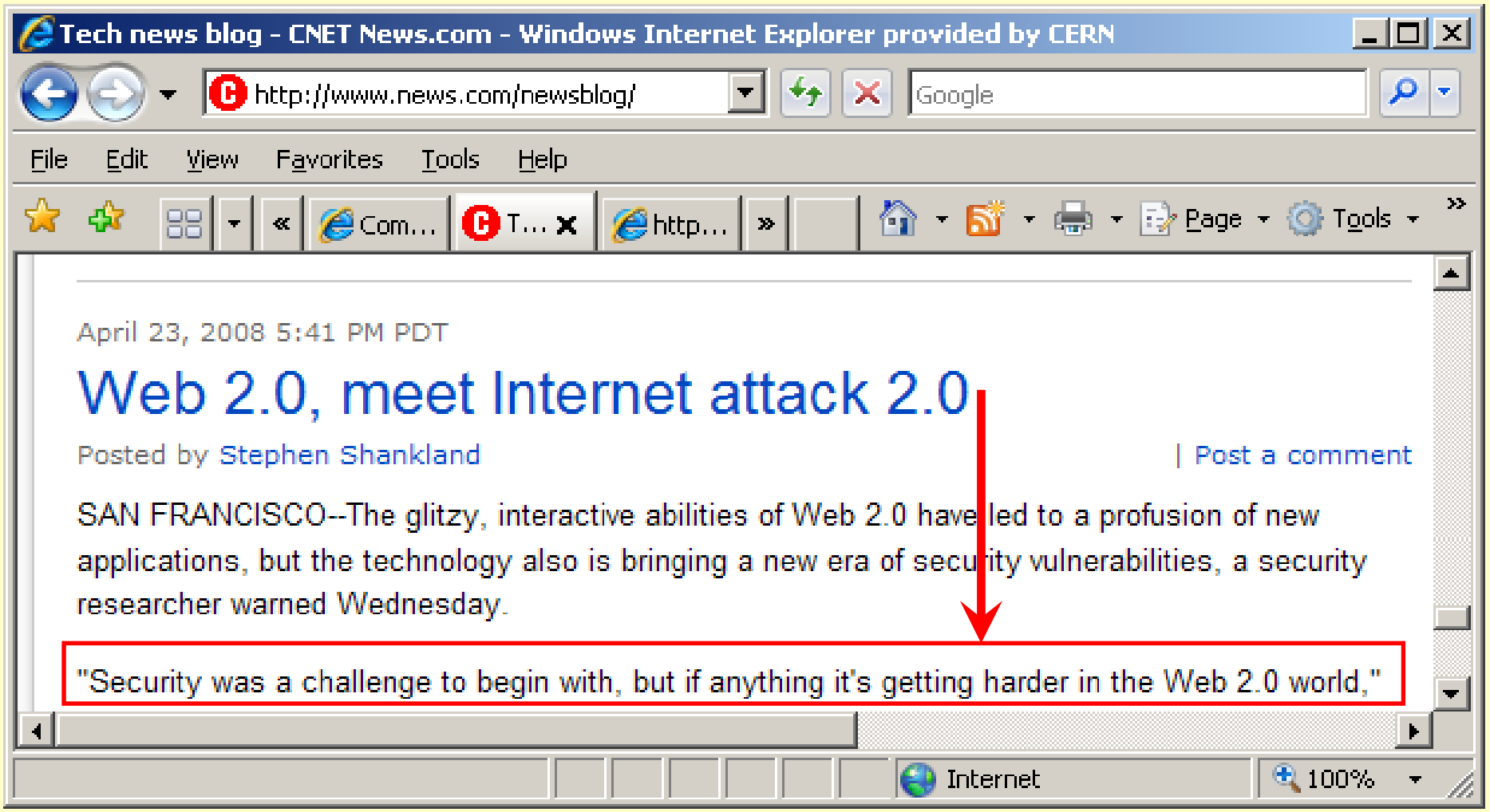
By Gregg Keizer Comments 4 Recommended 48 Share

April 23, 2008 (Computerworld) Large numbers of legitimate Web sites, including government sites in the U.K. and some operated by the United Nations, have been hacked and are serving up malware, a security researcher said today as massive JavaScript attacks last detected in March resume.

"They're using the same techniques as last month, of an SQL injection of some sort," said Dan Hubbard, vice president of security research at Websense Inc., referring to large-scale attacks that have plagued the Internet since January.

Web developers need to check their code !

Javascript with Ajax is an easy target for attack:

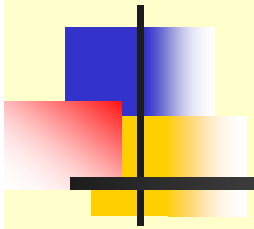


Malware Distribution Networks

- **Report by Google on drive-by-download attacks:**
  - http://research.google.com/archive/provos-2008a.pdf
  - avoiding the dark corners of the Internet does not limit exposure to malware
  - state-of-the-art anti-virus engines are lacking in their ability to protect against drive-by downloads
  - users may be lured into the malware distribution networks by content served through online Ads
    - e.g. http://www.theregister.co.uk/2008/04/28/yahoo_serves_rogue_ads/
  - 1.3% of the incoming search queries to Google's search engine return at least one link to a malicious site

Web security advice

- **Require secure coding practices**
  - Especially (but not only) for custom built web applications
  - http://cern.ch/security/webapps/
- **Educate users that web surfing has risks**
  - Advertising, photos and videos *can* and *do* regularly contain malware
  - Be cautious of links in IM, Blogs and Online forums (e.g. social networking). Attackers have matured beyond using SPAM
  - *Rich* content and plug-ins increase chances of attacks
  - Even reputable sites can serve 3rd party content, e.g. advertising
- **Consider blockers for JavaScript and advertising**
  - e.g. NoScript and AdBlock for Firefox
  - Disadvantages are that frequent updates are required and users need to understand what is being blocked and why



Windows Security Update

Windows Security Update

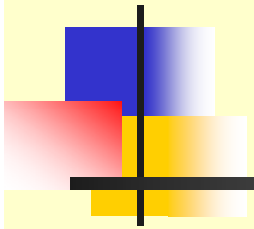
- **Windows computers remain a key target for attackers**
  - Trojan Web links in SPAM Email, Instant Messaging and Online Forums
  - Trojans targeting vulnerable applications:
    e.g. Adobe PDF, Word, Quicktime, VLC, Mplayer, Winamp
  - Applications are often an easier target than the OS – keep them secure
  - Users are the weakest link and vulnerabilities are a fact of life

- **Srizbi Trojan: SPAM relay using rootkit technology**
  - A more advanced form of the Storm botnet
  - Difficult to detect until it becomes a SPAMbot
  - http://www.news.com/8301-10789_3-9933683-57.html?tag=bl

Advice on securing Windows computers

Centrally managing computers can help:

- **Ensure patching for applications as well as the operating system**
- **Ensure anti-virus runs correctly and pattern files kept updated**
- **Configure secure defaults, especially for web browsers**
- **Only use privileges for actions that require them**
- **90% of compromised Windows computers at CERN in 2007 were privately managed**
  - e.g. laptops owned privately or by outside institutes
  - => Centrally managed computers were more secure



Linux Security Update

Slides contributed by
Jan Iven, CERN

Linux Security (1)

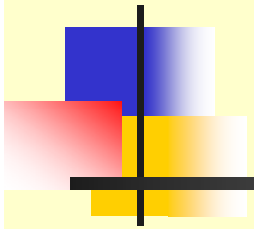
- **Linux x86_64 *insta*-root (CVE-2007-4573)**
  - (at least) 1 machine compromised at CERN
    - via a compromised user account
  - Delay between (public) announce and public exploit: 2 days (and 2 more for updates to appear)
  - Vendor assessments:
    - SECUNIA: “less critical”
    - Red Hat: “important”...

Linux Security (2)

- **Vendor assessments (ex: RHEL4)**
  - Marc Cox, Red Hat did some analysis: http://www.redhatmagazine.com/2008/02/26/risk-report-three-years-of-red-hat-enterprise-linux-4/
  - CERN analysis since Oct 2007 (ad-hoc):
    - 93 security errata for RHEL4+extras
    - 25 “critical”: 12 Mozilla&friends, 4 Java, 2 flash-plugin, acroread, ...
    - 27 “Important”: kernel, PDF, ...
  - But nobody (seems?) to be exploiting Firefox et.al. on Linux?
  - **Lessons**:
    - User-assisted (browser|mail) things get overrated by industry
      - Who would use a browser as root? Oh, wait...
    - Traditional “local root exploits” get underrated by industry

Linux Security (3)

- **Linux security tools – stagnation?**
  - Red Hat has added lots of nifty things in 2005/6 – 1 minor addition in 2007...
    - Are they used/useful? (SELinux → “off” is standing recommendation by Google... 90k hits)
    - Red Hat: could downgrade 1 advisory in 2004 (double-free caught by glibc) only
  - chkrootkit/rkhunter – no update = no new Linux rootkits?
  - StJude/Zeppoo: RIP.



Mac Security Update

Safari zero-day exploit nets $10,000 prize

- **Apple fell first in CanSecWest "*pwn-2-own*" contest**
- **Vista fell next**
- **with a few hours of tweaking exploit will also work on OS X and Linux**
  - *according to the contest winner*

The Register » Security »

Safari zero-day exploit nets $10,000 prize

Pwn'd in 12 hours

By Dan Goodin in Vancouver → More by this author

Published Friday 20th April 2007 23:38 GMT

Nail down your security priorities. Ask the experts and your peers at The Register Security Debate, April 17, 2008

A New York-based security researcher spent less than 12 hours to identify and exploit a zero-day vulnerability in Apple's Safari browser that allowed him to remotely gain full user rights to the hacked machine. The feat came during the second and final day of the CanSecWest "pwn-2-own" contest in which participants are able to walk away with a fully-patched MacBook Pro if they are first able to hack it.

First Rogue Cleaning Tool for Mac

Macsweeper:

- always finds something to fix (a trick to make you buy it)
- similar to *Cleanator* for Windows

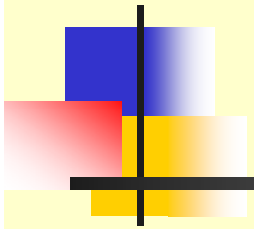
QuickTime Security Update

Technical Cyber Security Alert TA08-094A

- Original release date: April 3, 2008 - Source: US-CERT
- **Apple Mac OS X** running versions of QuickTime prior to 7.4.5
- **Microsoft Windows** running versions of QuickTime prior to 7.4.5

- **Overview**
  - Apple QuickTime contains multiple vulnerabilities as described in the Apple Knowledgebase article HT1241. Exploitation of these vulnerabilities could allow a remote attacker to execute arbitrary code or cause a denial-of-service condition

- **Special alert for Windows: non-US language versions**
  - SWITCH-CERT have reported that auto-updates of Quicktime fail on non-US language versions of Windows - s/w re-installation required



Controls Security Update

Slides contributed by

Stefan Lueders, CERN

Heart Device is vulnerable to attack

Potentially fatal !

HOME PAGE | MY TIMES | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times

Business

WORLD | REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

MEDIA & ADVERTISING | WORLD BUSINESS | SMALL BUSINESS | YOUR MONEY | DEALBOOK | MARKETS | RESEAR

A Heart Device Is Found Vulnerable to Hacker Attacks

By BARNABY J. FEDER
Published: March 12, 2008

SIGN IN TO E-MAIL OR SAVE THIS
PRINT
REPRINTS
SHARE

ROCK 'N ROLL WILL NEVER DIE

To the long list of objects vulnerable to attack by computer hackers, add the human heart.

The threat seems largely theoretical. But a team of computer security researchers plans to report Wednesday that it had been able to gain wireless access to a combination heart defibrillator and pacemaker.

They were able to reprogram it to shut down and to deliver jolts of electricity that would potentially be fatal — if the device had been in a person. In this case, the researcher were hacking into a device in a laboratory.

The researchers said they had also been able to glean personal patient data by eavesdropping on signals from the tiny wireless radio that Medtronic, the device's maker, had embedded in the implant as a way to let doctors monitor and adjust it without surgery.

The report, to published at www.secure-medicine.org, makes clear that the hundreds of

Boeing's new 787: vulnerable?

Boeing's new 787:

The network providing Internet access for passengers is connected to the plane's control, navigation and communication systems

WIRED

HOME | SUBSCRIBE » | SECTIONS » | BLOGS » | READ MAGAZINE

POLITICS : SECURITY

FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack

By Kim Zetter 01.04.08 | 7:30 PM

The Boeing 787 Dreamliner aircraft makes its public debut July 8, 2007, amidst employees and special guests outside the Boeing assembly plant in Everett, Washington.
Photo: Robert Sorbo / Corbis

Boeing's new 787 Dreamliner passenger jet may have a serious security vulnerability in its onboard computer networks that could allow passengers to access the plane's control systems, according to the U.S. Federal Aviation Administration.

The computer network in the Dreamliner's passenger compartment, designed to give passengers in-flight internet access, is connected to the plane's control, navigation and communication systems, an FAA report reveals.

Stronger regulations to secure the Electric Grid

The U.S. DHS and the U.S. FERC are now regulating the cyber-security for control systems in the electricity sector. The standards CIP-002 to CIP-009 are mandatory.

“The Federal Energy Regulatory Commission (FERC) today approved eight new mandatory critical infrastructure protection (CIP) reliability standards to protect the US’s bulk power system against potential disruptions from cyber security breaches (2008/02/01)”

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

About the Committee | Press Center | Issues Area | Legislation | Hearings

Hearings & Markups

»Home »Hearings & Markups

“The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid.”

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
Wednesday, October 17, 2007

2:00 p.m. in 311 Cannon House Office Building

Subcommittee on Emerging Threats, Cybersecurity
and Science and Technology

Hearing

“The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid.”

WITNESSES

PANEL I

Mr. Greg Wilshusen
Director
Information Security Issues
Government Accountability Office

Mr. Greg Garcia
Assistant Secretary
Office of Cyber Security and Telecommunication
Department of Homeland Security

Mr. Tim Roxey
Technical Assistant to the President CGG/Security
Deputy to the Chair, NSCC & PCIS
Constellation Generation Group

PANEL II

Mr. Joe Weiss
Managing Director
Applied Control Solutions

Chairman

Rep. Bennie G. Thompson (D-MS)

Search our Site
search go

Email Sign Up
Sign up to receive the latest news from the Democrats of the U.S. House Homeland Securit Committee.
email
sign up

Security Standards for Automation

Industrial Control Systems

The ISA has started the ISA Security Compliance Institute

- to be a driving force to enhance control system cybersecurity

- to establish a set of well engineered specifications and processes for the testing and certification of critical control system products

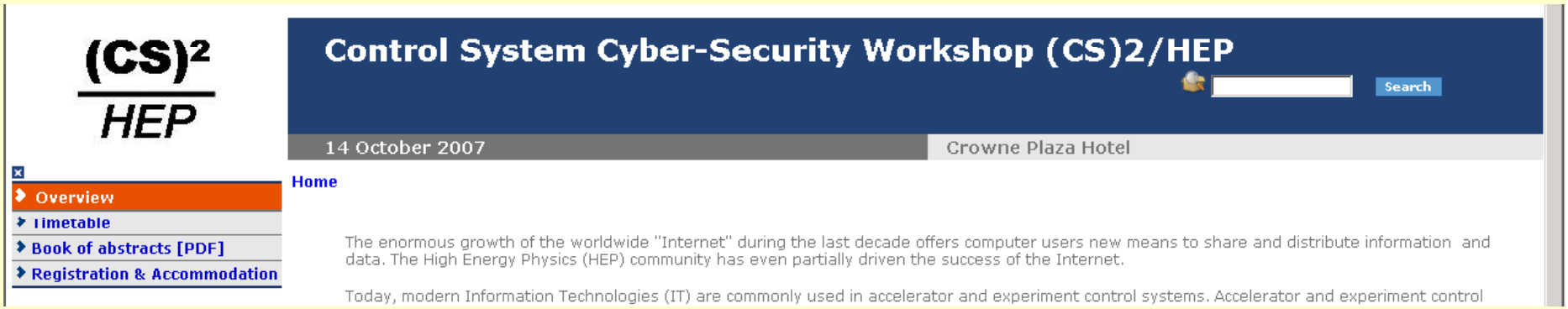
EuroSCSIE

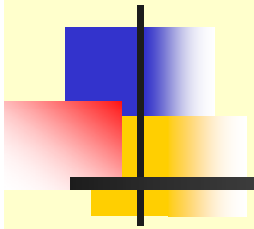
EuroSCSIE

- ***"European Information Exchange on SCADA and Control System Security"***
  - *"...of members from European based government, industry and research institutions depending upon and/or whose responsibility it is to improve the security of SCADA and Control Systems..."*
- **Users and governments from 10 European countries**
- **Chaired in 2007 by CERN (S. Lueders)**
  - 4 meetings were held

Control System Cyber Security in HEP

- **First workshop held during ICALEPCS2007**
  - Located in Knoxville, Tennessee, on 15 Oct 2007
- **Participants from several sites**
  - KEK, FNAL, SLAC, STFC, …
- **Useful discussion and information exchange**
- **Defence in depth is a common approach**
- **Summary paper and talk linked from**
  - http://indico.cern.ch/conferenceDisplay.py?confId=13367





Miscellaneous

Miscellaneous Updates

- Top security risks and trends compiled by SANS:
  - **http://www.sans.org/top20**
  - **http://www.sans.org/resources/10_security_trends.pdf**
- ecsirt incident classification scheme:
  - **http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6**
- Federated Model for Cyber Security (Argonne)
  - **www.anl.gov/it/federated**

ISSeG Project Web Site – Final Release

- **ISSeG: Integrated Site Security for Grids**
  - Site Security tools and advice targeted for Grid sites

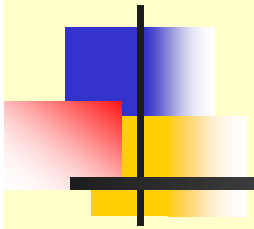
- **Final version of web site includes:**
  - Risk Analysis Tool
  - Security Recommendations
  - Security Training Material

- **For full information, visit:**

http://www.isseg.eu

Some conclusions…

- **The Internet world is not becoming a safer place**
- **Attacks are becoming more targeted**
  - Driven by money and criminal activity
  - e.g. compromised computers, accounts and data can be sold
  - Phishing targets passwords, personal data, credit card details, …
- **Secure coding practices are essential**
  - Custom built software, especially web apps, are a growing target
- **Privately managed computers / applications can increase risks**
  - Applications, plug-ins etc need to be patched (not just the OS)
  - Centralised management makes it easier to keep computers secure
- **Users need to be alert for malware**
  - Via links in IM, Blogs, Online forums (e.g. social networking), …
  - In photos, videos, advertising, documents, …
  - Relying solely on anti-virus software is not sufficient



Discussion