The CAG – An Earthquake in Security Compliance and How Security Is Measured

ALAN PALLER
DIRECTOR OF RESEARCH
SANS INSTITUTE
APALLER@SANS.ORG

An Earthquake In Security Compliance

- The unpleasant wake up call for senior executives across government and industry
- What caused the failures?
- Out of the ashes, the CNCI and a new way forward
- 2009 Consensus Audit Guidelines (CAG)
- How this applies to application development
- The 25 most dangerous programming errors
- 2009 Dawn of a new era of measureable security

TOP NEWS December 7, 2008, 10:19PM EST

U.S. Is Losing Global Cyberwar, Commission Says

Center for Cybersecurity Operations is proposed to protect military, government, and corporate electronics from criminals and other nations

By Keith Epstein

The U.S. faces a cybersecurity threat of such magnitude that the next President should move quickly to create a Center for Cybersecurity Operations and appoint a special White House advisor to oversee it. Those are among the recommendations in a 44-page report by the U.S. Commission on Cybersecurity, a version of which will be

BW EXCLUSIVES

Super Bowl Advertisers Hope for the Best

Daschle, Too, Has a Tax Problem

Business Ex

FEATURED

Wireless We

Social Media users

Biofuels 69 n

Entrepreneu

Enterprise 2.

How top management learned of the security failures (all actual events)

- FBI visits and reports that the Chinese have taken all documents from their legal department.
- CIO and security officer ask for a meeting to report that two divisions are offline because of the Conficker worm. The division directors are screaming.
- Auditors report that the websites at their agencies or companies have been penetrated and are infecting their visitors (citizens and customers) with keystroke loggers – causing their bank accounts to be emptied. Question of liability arises immediately.

Evidence helping management isolate the key cause of failure (again all real)

- No one in the security or operations group is able to explain how it happened – even after weeks of review. Security and ops blame each other and both blame "careless users."
- Security officers claim that their security assessors said they had met compliance standards (FISMA or ISO 27001, for example) – and then say "no system is completely safe unless you unplug it."
- On deeper analysis, there were known defenses against the attacks – but they were not implemented (because they were not "required in the compliance standards.")

Three questions from CEOs

1. What do we have to do?
2. How much is enough?
3. Whom can I trust to answer those two questions?

Enter the Comprehensive National Cyber Initiative (CNCI)

- $30 billion to try to stop these attacks and mitigate their damage.
- The key CNCI theme: “offense must inform defense.”
- The cause of the failures are finally located: compliance standards that did not prioritize the controls or provide measures of effectiveness.
- Inescapable conclusion: Congress asked the wrong people to write the rules. The compliance standards writers had little experience with offense – they simply didn’t know what needed to be done first or how to test whether it was effective.

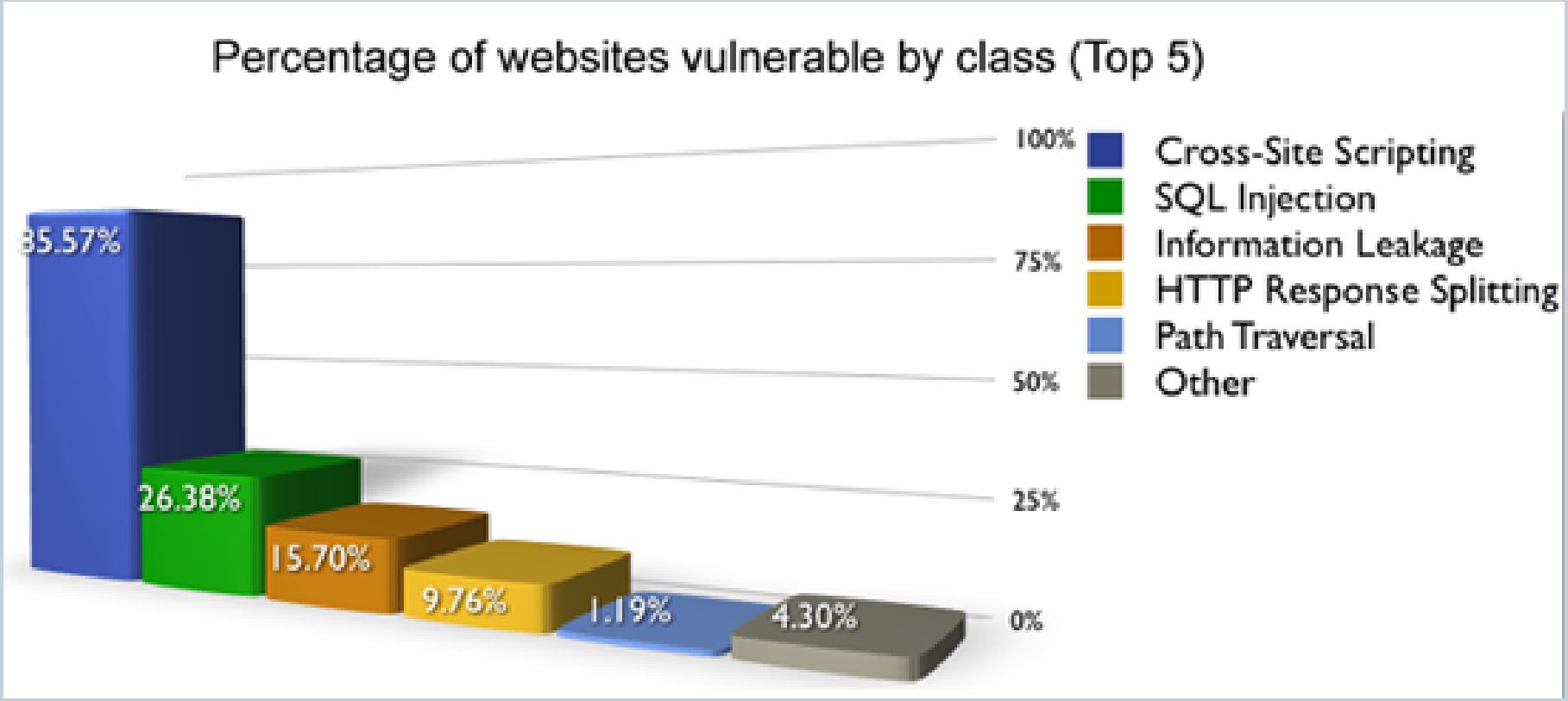
Learning from the error: new language in FISMA2008

- *"Establish security control testing protocols that ensure that the information infrastructure of the agency, including contractor information systems operating on behalf of the agency, are effectively protected against known vulnerabilities, attacks, and exploitations."*
- *"Establish a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms."*

An example: secure coding & design of applications

Web Applications: How Vulnerable?

2006 Vulnerability Statistics (31,373 sites)



** http://www.webappsec.org/projects/statistics/

Places you visit
January: 87,000 web sites infected and infecting visitors who trusted them.

Mass hack infects tens of thousands of sites

Then they serve visitors multiple exploits, including October RealPlayer attack

Gregg Keizer Today's Top Stories ▸ or Other Networking and Internet Stories ▸

Comments (8) Recommendations: 141 — Recommend this article

January 07, 2008 (Computerworld) -- Tens of thousands of Web sites have been compromised by an automated SQL injection attack, and although some have been cleaned, others continue to serve visitors a malicious script that tries to hijack their PCs using multiple exploits, security experts said this weekend.

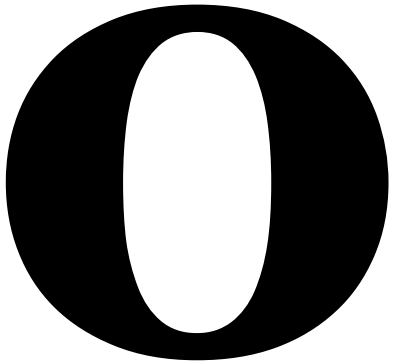
Roger Thompson, the chief research officer at Grisoft SRO, pointed out that the hacked sites could be found via a simple Google search for the domain that hosted the malicious JavaScript. On Saturday, said Thompson, the number of sites that had fallen victim to the attack numbered more than 70,000. "This was a pretty good mass hack," said Thompson, in a **post** to his blog. "It wasn't just that they got into a server farm, as the victims were quite diverse, with presumably the only common point being whatever vulnerability they all shared."

Symantec Corp. cited reports by other researchers -- including one identified only as "websmithrob" -- that fingered a SQL vulnerability as the common thread. "The sites [were] hacked by hacking robot by means of a SQL injection attack, which executes an iterative SQL loop [that] finds every normal table in the database by looking in the sysobjects table and then appends

MORE RELATED CONTENT
- FAQ: Why is enterprise search harder than Google Web search?
- Old exploit keeps on tickin' for hackers
- Office, Windows Server chief Jeff Raikes to retire from Microsoft

TODAY'S TOP STORIES
- Macworld forecast: Thin, light notebook 'sure bet'
- Microsoft changes mind, goes public with Vista SP1

How many of the critical application security controls does NIST 800-53 specify?



A central theme of the CNCI (Comprehensive National Cyber Initiative)

"DEFENSE MUST BE INFORMED BY THE OFFENSE"

Who understands offense?

- NSA Red Teams
- NSA Blue Teams
- DoD Cyber Crime Center (DC3)
- US-CERT (plus 3 agencies that were hit hard)
- Top Commercial Pen Testers
- GAO
- Top Commercial Forensics Teams
- JTF-GNO
- AFOSI
- Army Research Laboratory
- DoE National Laboratories
- FBI and NIC-JTF

Would they be willing to combine their knowledge of attacks and offense to define the most important defensive investments CIOs must make?

Yes, under the direction of John Gilligan?

1. **CIO OF US DEPARTMENT OF ENERGY**
2. **CIO OF US AIR FORCE**
3. **CO-CHAIR OF THE FEDERAL CIO COUNCIL SECURITY COMMITTEE**
4. **KEY MEMBER OF THE COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY**
5. **PRES. OBAMA'S TRANSITION TEAM LEAD FOR IT AND INFORMATION SECURITY FOR BOTH DOD AND THE INTELLIGENCE COMMUNITY**

Consensus Audit Guidelines (CAG)

- The twenty key controls
  1. 15 subject to automation
  2. 5 that are important but cannot be easily automated

Consensus Audit Guidelines (CAG)

Steps to broad implementation

1. Agree on the controls that would stop or quickly recover from the known attacks
2. Provide real-world examples of those attacks
3. Agree how to automate and measure effectiveness
4. Public review period (Feb 3-24) and revision
5. Pilot program in two agencies and tuning
6. Gain CIO and IG agreement to adopt the CAG as the official controls and measures for .gov and contractors
7. Encourage commercial organizations to use the CAG as a new minimum standard of due care.
8. Keep controls current through multi-agency governance

#3
Secure Software Configuration

ACTUAL SECURITY IMPROVEMENTS?
57 DAYS TO 72 HOURS FOR PATCHING

COST?

HUNDREDS OF MILLIONS IN DOCUMENTED SAVINGS

USER SATISFACTION?

SUBSTANTIAL REDUCTION IN HELP DESK CALLS – MUCH HAPPIER USERS.

#7
Application Security

HOW WOULD YOU MEASURE THE EFFECTIVENESS OF APPLICATION SECURITY?

- DO TOOLS MEASURE THE RIGHT THINGS??
- DO PROGRAMMERS KNOW HOW TO WRITE SECURE CODE?

The “top 25” security flaws

“A new minimum standard of due care”

BBC Low graphics | Help Search Explore the BBC

NEWS Watch ONE-MINUTE WORLD NEWS

News Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment
Also in the news

Video and Audio

Have Your Say
In Pictures

Page last updated at 11:09 GMT, Tuesday, 13 January 2009

E-mail this to a friend Printable version

Dangerous coding errors revealed

The US National Security Agency has helped put together a list of the world's most dangerous coding mistakes.

The 25 entry list contains errors that can lead to security holes or vulnerable areas that can be targeted by cyber criminals.

Experts say many of these errors are not well understood by programmers.

Experts say many of these errors are not well known

Accor
led to

It is th
agreement on the worst things that can creep into software as it is being written.

New York State published procurement language at www.sans.org/appseccontract incorporating the top 25

SEE ALSO
Alarm raised on teenag

2009 : The dawn of a new era based on minimum standards of due care

- Agreement on what controls must be done first
- Automated measurement of effectiveness of the controls
- Shared development of solutions
- Joint procurement of all control an tools to enlarge the market and bring down their costs
- Interoperability standards developed to enable switching out old tools and switching in new tools without outages
- Constant update based on new attacks