Session 30

IT Security: Threats, Vulnerabilities and Countermeasures

Phillip Loranger, DoED CISO
Robert Ingwalson, FSA CISO

START HERE
GO FURTHER
FEDERAL STUDENT AID

New Cyber Security World

- New threats
- New tools and services to protect
- New organization to manage
- Better results under worse conditions
  - cyber crime impact
  - Better audit results

START HERE
GO FURTHER
FEDERAL STUDENT AID

Introduction to Cyber Crime

- Cyber crime and terrorism has escalated during recent years
- It is well-organized
- It is advanced technically
- It is well-financed
- It has adopted a new view
  - The old view: quick entry and exit
  - The new view: hidden long term presence
  - The best attack is undetected, and undetectable

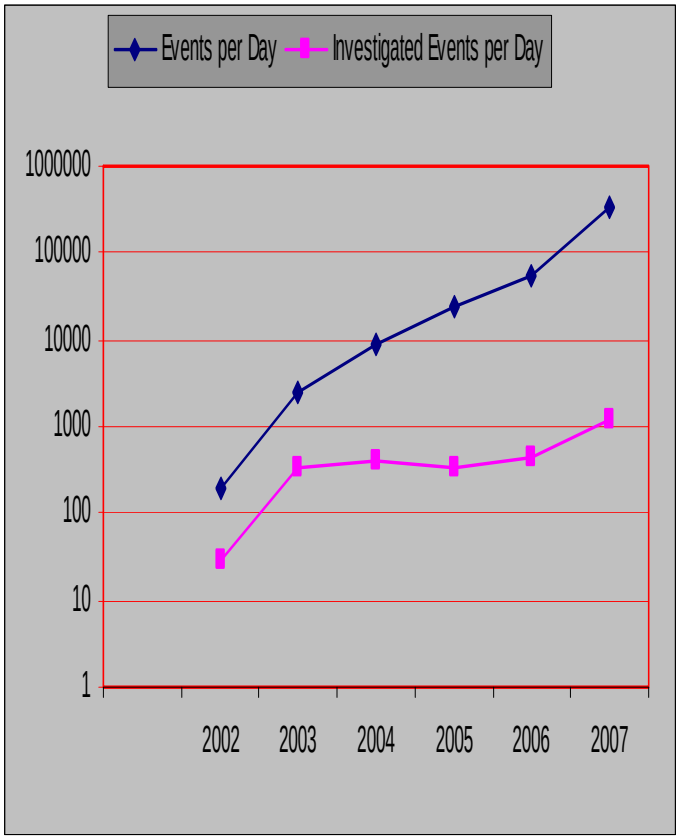
Why the Increase In Cyber Intelligence

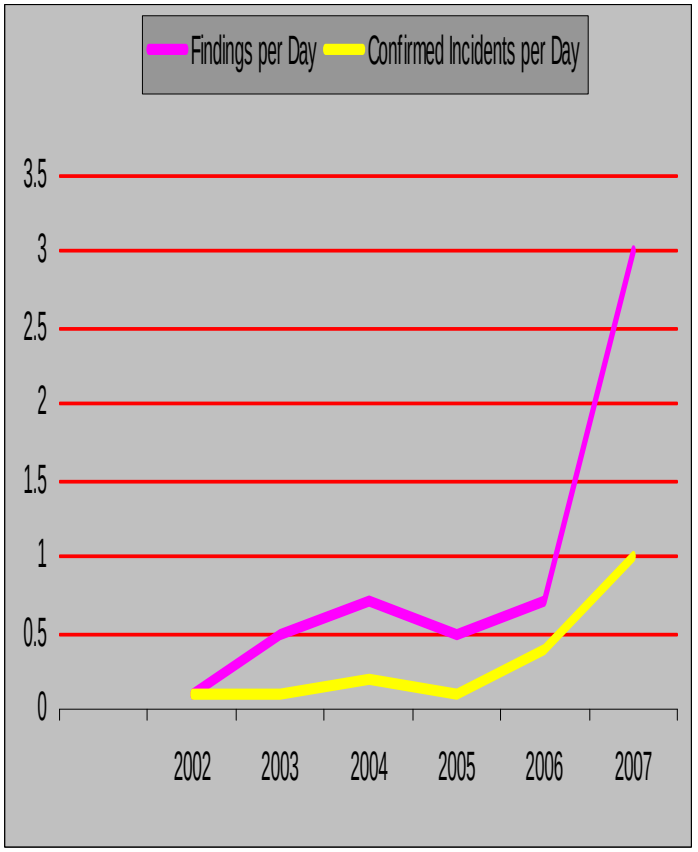
- Recent open source network compromises disclosure, becoming more common, used as a nation enabler
- Easier to steal digits, than to integrate a spy
- Larger ROI in stealing R&D, vice actually doing it. (Past events have shown that .EDU has been used as a gateway to .GOV)

Why the Increase In Cyber Intelligence

- Economic motivation
- Globalization empowerment
- Continuous national interest into US directions and intentions
- If you can't out shoot them out spend them. (costly to recover form breaches)

Incident Trends



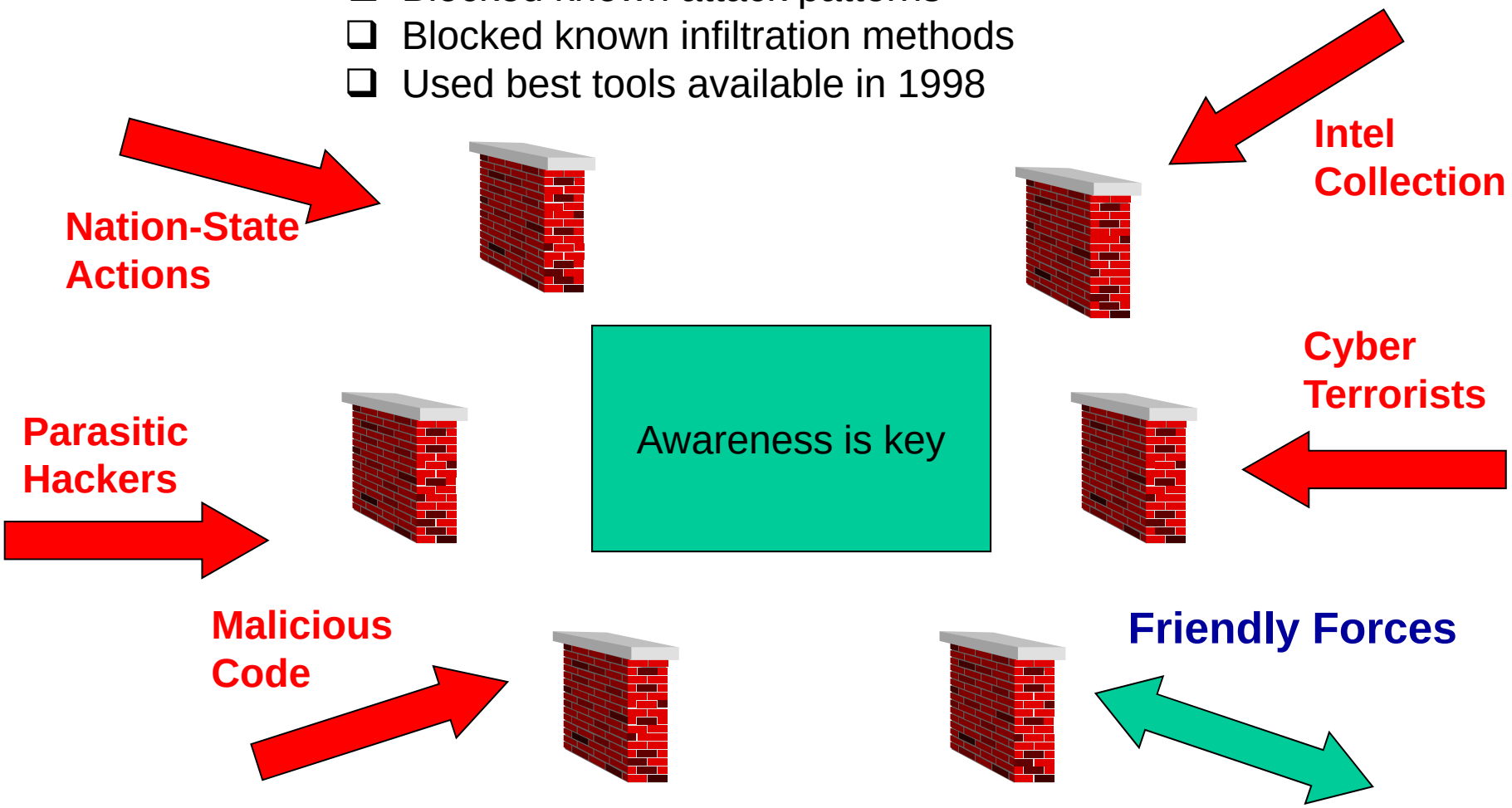


Typical Civil Agency Cyber Levels of Interest / Activities

START HERE
GO FURTHER
FEDERAL STUDENT AID

Previous Defense Strategy

- Blocked known attack patterns
- Blocked known infiltration methods
- Used best tools available in 1998



START HERE GO FURTHER FEDERAL STUDENT AID

Government Response: A New Cyber Initiative

- Security measures are essential and urgent in the face of stronger criminals and nations
- The P **Government Response: A New Cyber Initiative** resident issued directives, on January 8, 2008, that we strengthen our defenses
  - National Security Directive 54 and Homeland Security Directive 23
  - Collectively, the cyber initiative is to secure the government's computer systems against attacks by foreign adversaries and other intruders
- OMB has mandated all agencies will have a Trusted Internet Connection (TIC)
- A national multi-part defense against cyber crime
- Department of Education is part of the defense
- First combination of separate federal security areas
  - National defense and intelligence
  - Sensitive civilian information
- Two major goals in this cyber initiative:
  - One: stop critical vulnerabilities now in each agency
  - Two: extend protection from global predators by cross-agency cooperation

Threat Summary

- Exfiltration of US sensitive data from local networks and systems committed by hostile countries and organizations increasing
- FBI Report to Congress: Terrorist cell used stolen PII/ SI to conduct much of their business
- Increased cases of a critical nature against critical networks identified by the US CERT
- In FY 2009, events detected will continue to rise
- Stronger awareness and countermeasures will be required to protect against future threats

Security Vulnerabilities

Know your vulnerabilities

- OWASP

  (http://www.owasp.org)
- National Vulnerability Database

  (http://nvd.nist.gov)
- SANS Top 20

  (www.sans.org/top20)
- Others

OWASP Top 10 Security Vulnerabilities

- **1 - Cross Site Scripting (XSS)** XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
- **2 - Injection Flaws** Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
- **3 - Malicious File Execution** Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
- **4 - Insecure Direct Object Reference** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
- **5 - Cross Site Request Forgery (CSRF)** A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
- **6 - Information Leakage and Improper Error Handling** Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
- **7 - Broken Authentication and Session Management** Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
- **8 - Insecure Cryptographic Storage** Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
- **9 - Insecure Communications** Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
- **10 - Failure to Restrict URL Access** Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

OWASP Top 1: Cross Site Scripting

– What is Cross Site Scripting?

- In it's simplest form, it's a process that can occur anywhere a web application uses input from a malicious user to generate output without validating or encoding the input.
- During a Cross Site Scripting attack, a malicious source sends a script that is executed by the end user's browser. It allows attackers to embed code from one webpage into another webpage by changing its HTML code.
- It's been used to deface web sites, conduct phishing attacks, or it can take over a user's browser and force them to execute commands they're unaware of.
- Cross Site Scripting attacks usually come in the form of JavaScript however, any active content poses a potential danger.

– Prevention

- Validate the users input against what is expected
- Encode user supplied output
- After you believe you've done the right things during code development, inspect your code with a scan.

OWASP Top 2: Injection Flaws (SQL Injection)

– What is SQL Injection

- SQL injection is the actual injection of SQL commands into web applications through user input fields.
- When an application uses internal SQL commands and you also have user input capabilities (like a login screen), SQL commands can be injected that can create, read, update, or delete any data available to the application.

– Prevention

- You can put tight constraints on user inputs. But the best method of preventing SQL injection is to avoid the use of dynamically generated SQL in your code. Instead use stored or canned procedures.
- And then again, run a scan to make sure your application is not vulnerable to SQL injections.

OWASP Top 3: Malicious File Execution

– What is Malicious File Execution

- When Developers program applications to use input files provided by the user and the bad guy is the one entering the file, a malicious file is executed unknowingly, thus we have malicious file execution.
- Malicious file execution attacks can occur anytime the application accepts filenames or files from a users.
- When these files are executed, they can be used to do just about anything from stealing data to taking over the entire system.

– Prevention

- Strongly validate user input using "accept known good" as a strategy, or isolate incoming files and check them legitimacy before executing them.
- Disable certain PHP commands: I suggest that you visit the OWASP website to see what commands to disable.

OWASP Vulnerabilities: A Common Thread

From looking at OWASP vulnerabilities it appears that there is a common theme. Applications with Dynamic code or user inputs have the most vulnerabilities – and that seems to be the current trend in application development.

So if you're building applications of that nature, make sure you test them carefully.

SANS Top 20 Security Vulnerabilities

The Top 20 Most Critical Internet Security Vulnerabilities (Updated) - The Experts Consensus

Top Vulnerabilities in Windows Systems

- W1. Windows Services
- W2. Internet Explorer
- W3. Windows Libraries
- W4. Microsoft Office and Outlook Express
- W5. Windows Configuration Weaknesses

Top Vulnerabilities in Cross-Platform Applications

- C1. Backup Software
- C2. Anti-virus Software
- C3. PHP-based Applications
- C4. Database Software
- C5. File Sharing Applications
- C6. DNS Software
- C7. Media Players
- C8. Instant Messaging Applications
- C9. Mozilla and Firefox Browsers
- C10. Other Cross-platform Applications

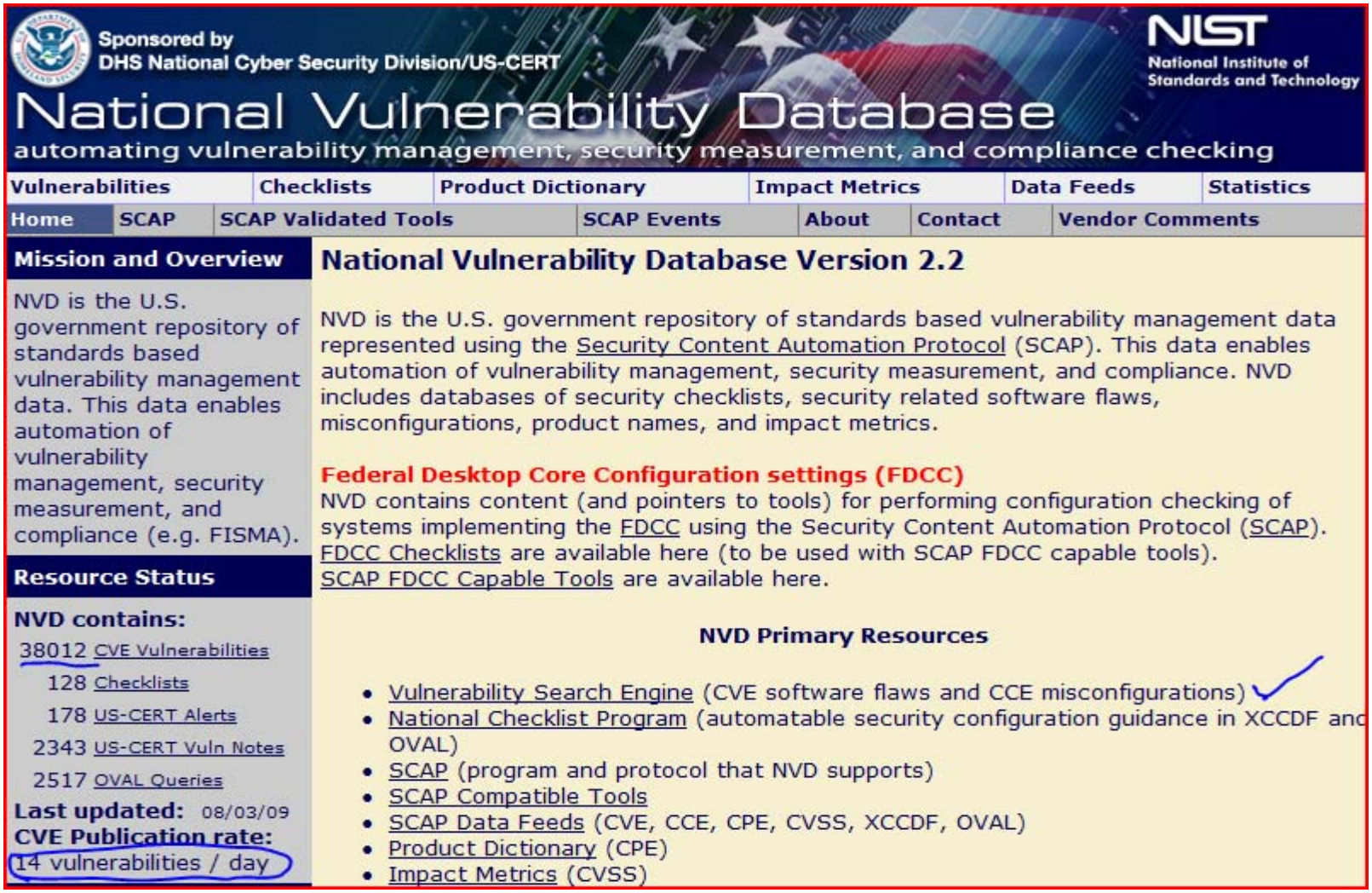
Top Vulnerabilities in UNIX Systems

- U1. UNIX Configuration Weaknesses
- U2. Mac OS X

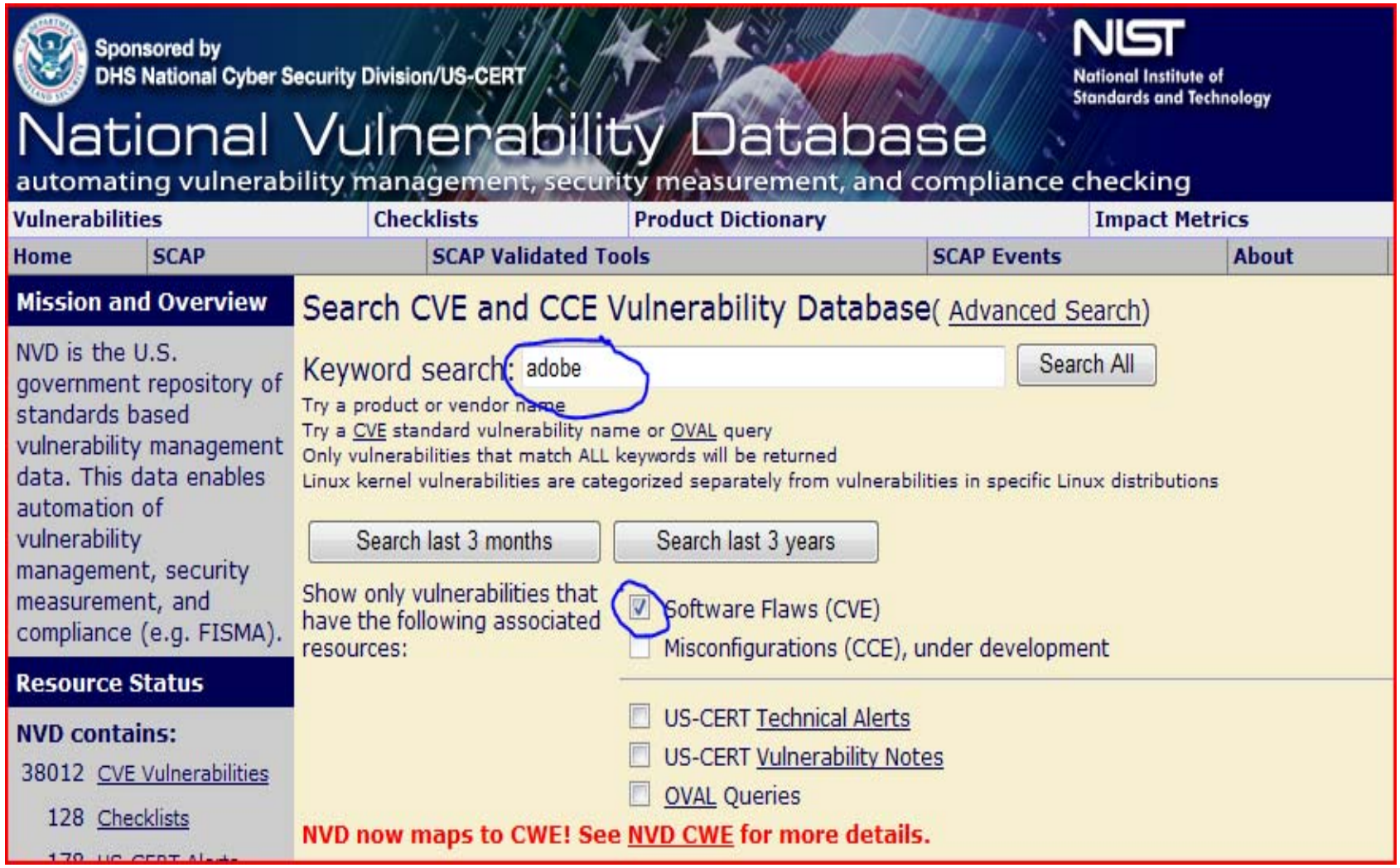
Top Vulnerabilities in Networking Products

- N1. Cisco IOS and non-IOS Products
- N2. Juniper, CheckPoint and Symantec Products
- N3. Cisco Devices Configuration Weaknesses

National Vulnerability Database

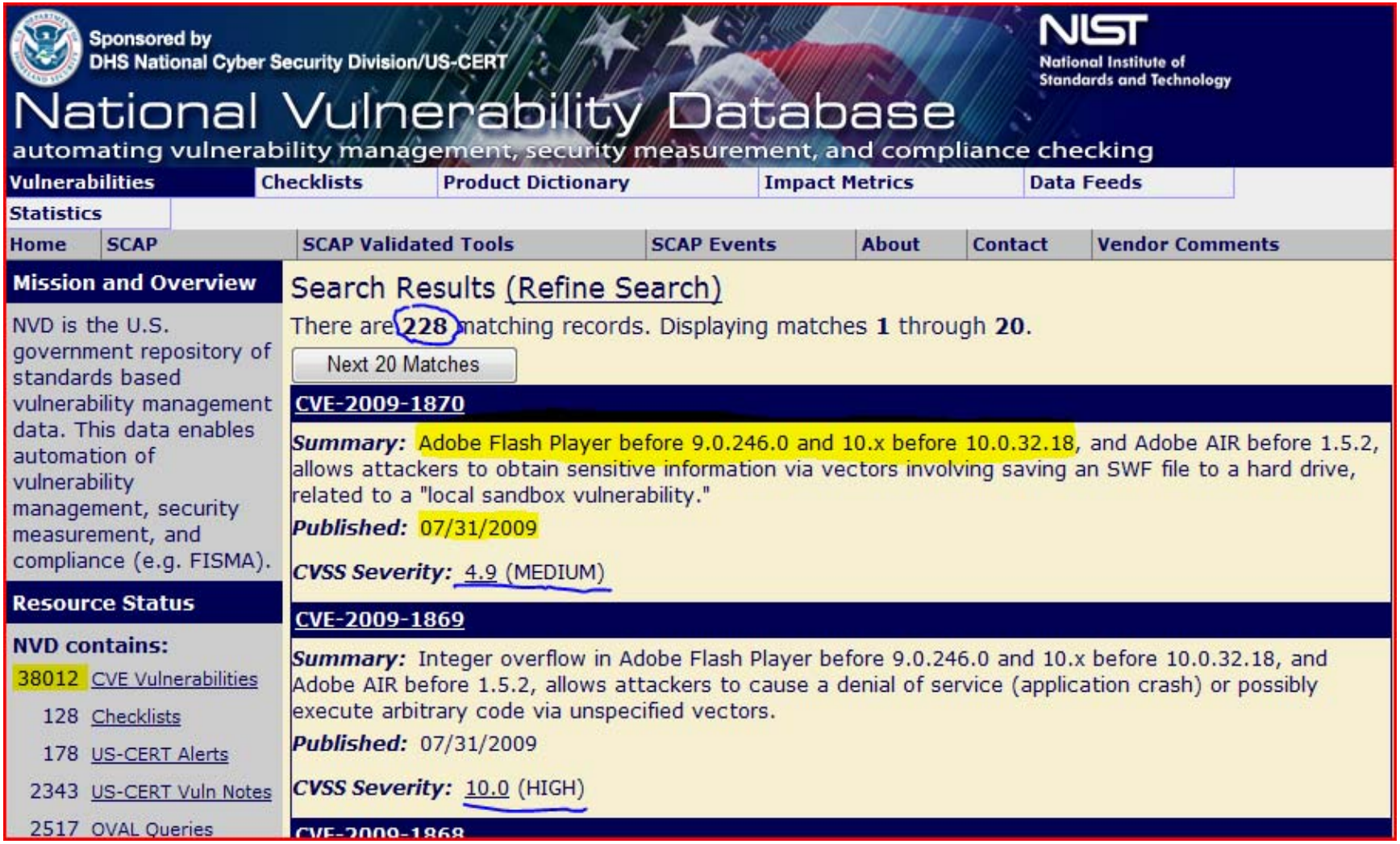


National Vulnerability Database



START HERE
GO FURTHER
FEDERAL STUDENT AID

National Vulnerability Database



Other Vulnerabilities

- Code Mistakes
- Untrained Users
- Insecure Configuration Settings

Code Mistakes

- Federal Student Aid has had Code Mistakes
  - Implement Prevention in Code
  - Thoroughly Test
  - Use Tools

Untrained Users

- Security ignorance compromises data
- Provide the training
- Rules of Behavior
- Annual refresher training

START HERE
GO FURTHER
FEDERAL STUDENT AID

Insecure Configuration Settings

- NIST, DISA, CIS vs. Business Needs
- Builds
- System Upgrades
- Vulnerability Scans

- Note: Federal Student Aid Secure Configuration Guides are based off the NIST checklist located at http://checklists.nist.gov

START HERE GO FURTHER FEDERAL STUDENT AID

Items of Special Interest

- Keyloggers & WSNPOEM
  - What are these threats and why are they of Special Interest to Federal Student Aid and learning institutions?
  - What can be done to mitigate these threats?

Item of Special Interest: Keyloggers

- What's a Keylogger and how does it exploit a Web Application?
  - Downloaded unknowingly
  - Resident on Personal Computers
  - Captures User Activity
  - Usually part of a malicious Network or BOTNET
  - Education notified of compromises by US-CERT

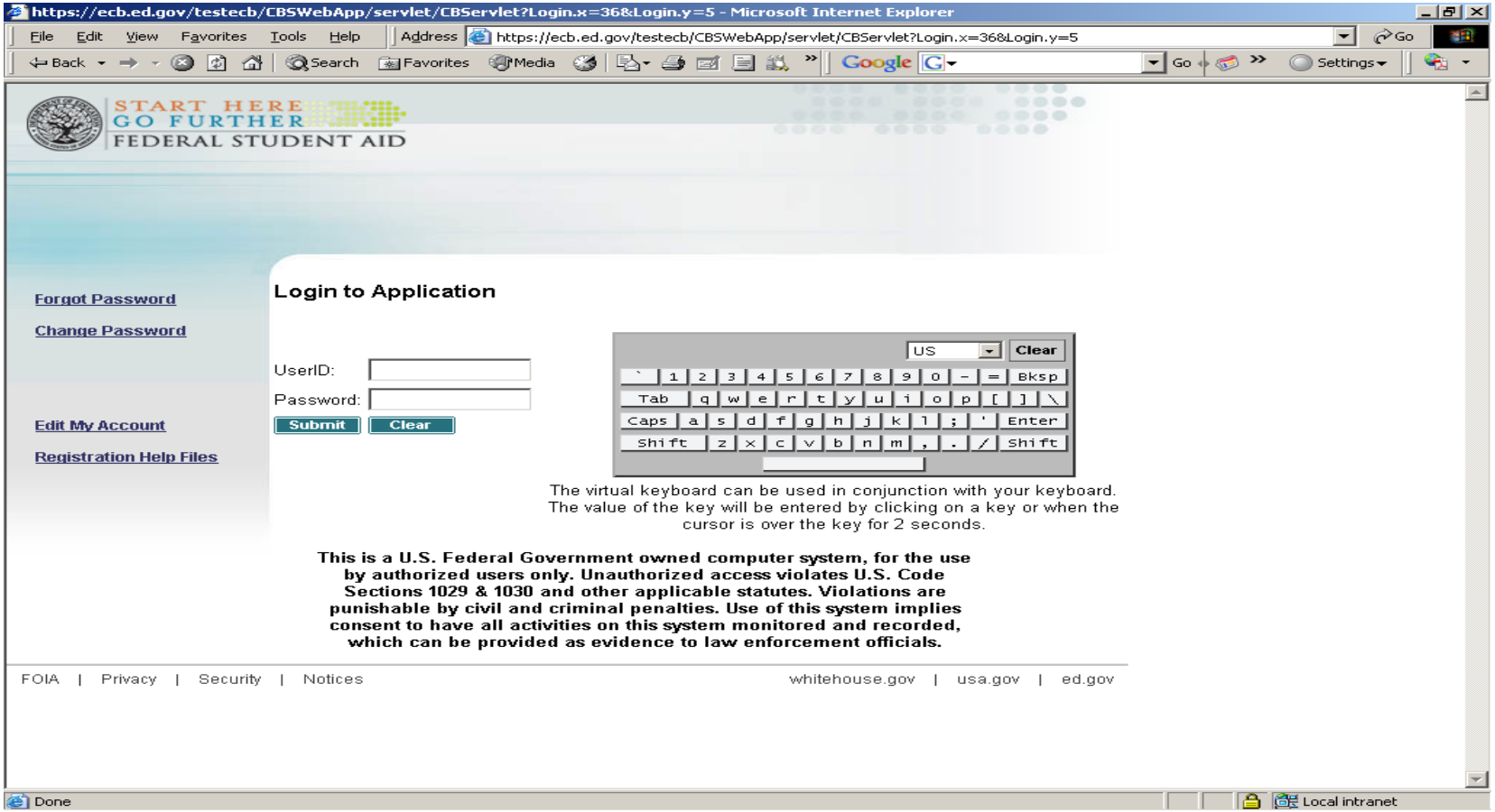
START HERE GO FURTHER FEDERAL STUDENT AID

Keylogger Mitigations

- Train users
- Implement effective Anti-Spyware, Anti-Virus
- Keep patches and versions current
- Firewall
- Automatic form filler programs
- Cut and paste
- One-time passwords
- Smartcards
- Virtual keyboards

Virtual Keyboard

A virtual keyboard is provided on Federal Student Aid's Enterprise Security login page and does not require end users to acquire additional software.



START HERE GO FURTHER FEDERAL STUDENT AID

Virtual Keyboard

- *Some of the features of Federal Student Aid's Virtual Keyboard Include:*
  - Highly effective in evading true "Key Logging"
  - Widely used by many financial institutions
  - Low cost technology to deploy (even for 50 million users)
  - Does not require any new hardware or software on client machines
  - Can work in conjunction with the existing keyboard
  - Keys can be entered by mouse click or by leaving mouse on the key for 2 seconds
  - Virtual keyboard randomly shifts on the screen

Item of Special Interest: WSNPOEM

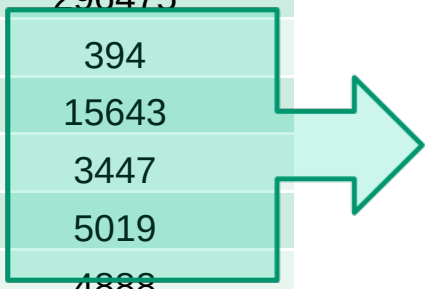
- WSNPOEM
  - What is it?
    - Variant of the Banker/InfoStealer/Bancos/Zbot family (identified as PWS-Banker.gen.bw by McAfee, as Infostealer.Banker.C by Symantec, as Trojan-Spy.Win32.Bancos.aam by Kaspersky and as Mal/Zbot-A by Sophos).
  - How does it exploit a Web Application?
    - WinInet interception
    - In-process key-logging
  - How do we know about it and what's the impact?
  - What can be done?

Item of Special Interest WSNPOEM

- How do we know about it:
  - Since 2004 we have been receiving periodic files from US-CERT
  - Now provided weekly
  - Government wide concern
- Impact:
  - > 22,000 unique compromised SSNs
  - > 300 unique compromised userids and passwords
  - Analysis from the raw logs has identified wsnpoem as the number one threat

Item of Special Interest: WSNPOEM

Malware	Occurances
wsnpoem_v2	296475
wsnpoem_v3	394
wsnpoem_v6	15643
wsnpoem_v4	3447
wsnpoem	5019
haxdoor	4888
nethelper	4025
win32agent	3412
fireming	3063
silentbanker_v2	1583
passsickle	264
manda	259
nowhere	217
win32agent_v4	39
urlzone	6



- The wsnpoem malware & variants make up **95%** of the incidents captured in the US-CERT files

Item of Special Interest: WSNPOEM

- What can be done at the application side?
  - Require two factor authentication
    - Virtual Keyboards, URL encoding, header encryption, shared keys, security questions, and images are all vulnerable to this type of attack
  - Training and awareness for client side prevention
    - Train those that are accessible
    - Broadcast messages or post warnings on websites
- What can be done at the client side?
  - Use two factor authentication
  - Keep patches and versions current
  - Run reputable security software scans (in safe mode)

Item of Special Interest: FSA Actions

- Revoke User Access
- Notify User / School
- Review Logs
- Assist User / School Clean Computer

START HERE
GO FURTHER
FEDERAL STUDENT AID

How Much Security is Enough?

- We implement security based on Cost vs. Risk
  - Threat * Vulnerability = Risk
  - Cost of Implementing Controls – Cost of not Implementing Controls = Cost

START HERE GO FURTHER FEDERAL STUDENT AID

Questions?

START HERE
GO FURTHER
FEDERAL STUDENT AID

Contact Information

We appreciate your feedback and comments. We can be reached at:

Phillip Loranger

- Phone: (202) 245-6507
- Email: Phillip.Loranger@ed.gov

Robert Ingwalson

- Phone: (202) 377-3563
- Email: Robert.Ingwalson@ed.gov

START HERE GO FURTHER FEDERAL STUDENT AID