Automated Security Measurement/ FISMA Technical Control Automation

Stephen Quinn & Peter Mell

Computer Security Division

NIST

I’m from the Federal Government…

and I’m (almost) here to help you!!

Gifts to Community

- COTS Tool Vendors –
  - Provision of an enhanced IT security data repository
    - No cost and license free
    - CVE/OVAL/XCCDF/CVSS
    - Cover both patches and configuration issues
  - Elimination of duplication of effort
  - Cost reduction through standardization
- Federal Agencies
  - Automation of technical control compliance (FISMA)
  - Ability of agencies to specify how systems are to be secured

Current Problems

Conceptual Analogy

Current Problems

Conceptual Analogy Continued (2)

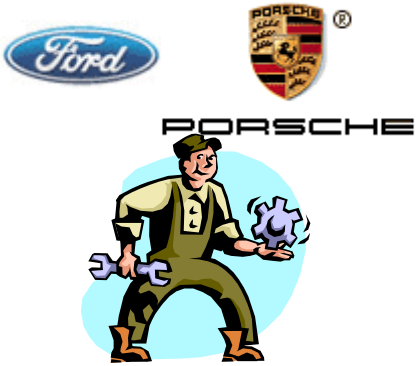
Outsource

In-House

Current Problems

Conceptual Analogy Continued (3)

Outsource



In-House

a.) Troubleshoot/Analyze

- Conduct Testing
- Is there a problem?
- Cause of error condition?
- Is this check reporting correctly?

b.) Document/Report Findings

c.) Recommendations

d.) Remediate

Current Problems

Conceptual Analogy Continued (5)

Standardize & Automate

a.) Troubleshoot/Analyze

- Is there a problem?
- Cause of error condition?
- Is this check reporting correctly?

More DATA

Outsource

In-House

a.) Troubleshoot/Analyze

- Conduct Testing
- Is there a problem?
- Cause of error condition?
- Is this check reporting correctly?

b.) Document/Report Findings

c.) Recommendations

d.) Remediate

Current Problems

Conceptual Analogy Continued (6)

Before

After

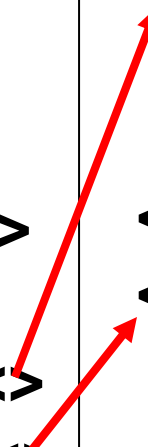
XML Made Simple

XCCDF - eXtensible Car Care Description Format

```
<Car>
  <Description>
    <Year> 1997 </Year>
    <Make> Ford </Make>
    <Model> Contour </Model>
  <Maintenance>
    <Check1> Gas Cap = On <>
    <Check2>Oil Level = Full <>
  </Maintenance>
 </Description>
</Car>
```

OVAL – Open Vehicle Assessment Language

```
<Checks>
  <Check1>
    <Location> Side of Car <>
    <Procedure> Turn <>
  </Check1>
  <Check2>
    <Location> Hood <>
    </Procedure> … <>
  </Check2>
</Checks>
```



FISMA Compliance

Starting Point

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-37

System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18

Security Control Documentation

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-26 / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

Common FISMA Statements

- While FISMA compliance is **Important**, it can be **Complex** and **Laborious**.
- “Can parts of FISMA compliance be streamlined and automated”?
- “My organization spends more money on compliance than remediation”.

Fundamental FISMA Questions

What are the NIST Technical Security Controls?

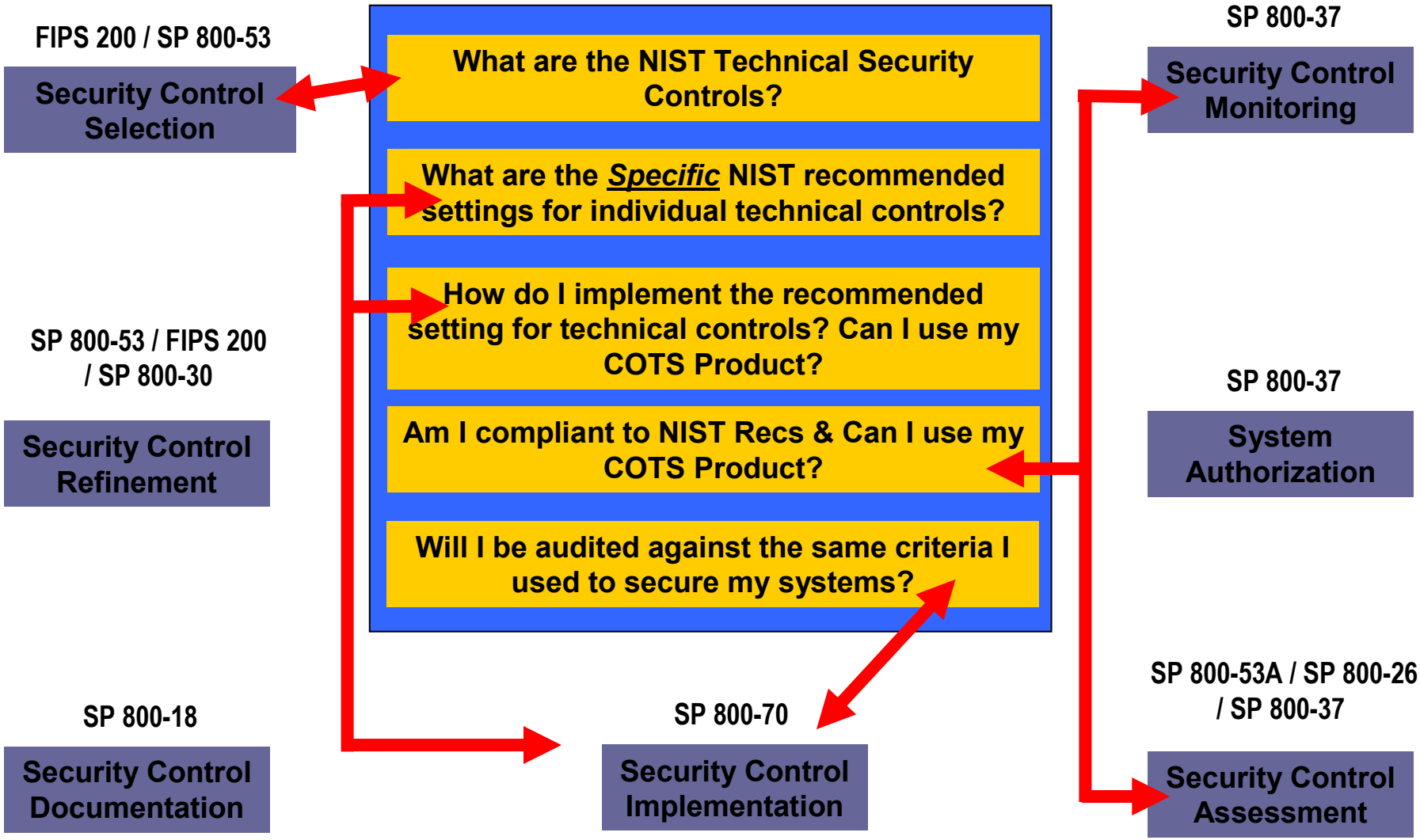
What are the *Specific* NIST recommended settings for individual technical controls?

How do I implement the recommended setting for technical controls? Can I use my COTS Product?

Am I compliant to NIST Recs & Can I use my COTS Product?

Will I be audited against the same criteria I used to secure my systems?

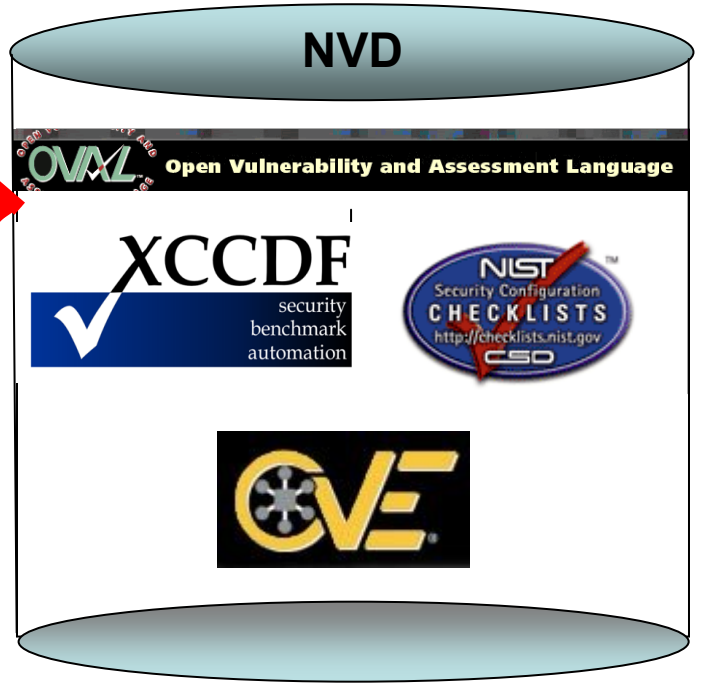
FISMA Documents



Automation of FISMA Technical Controls

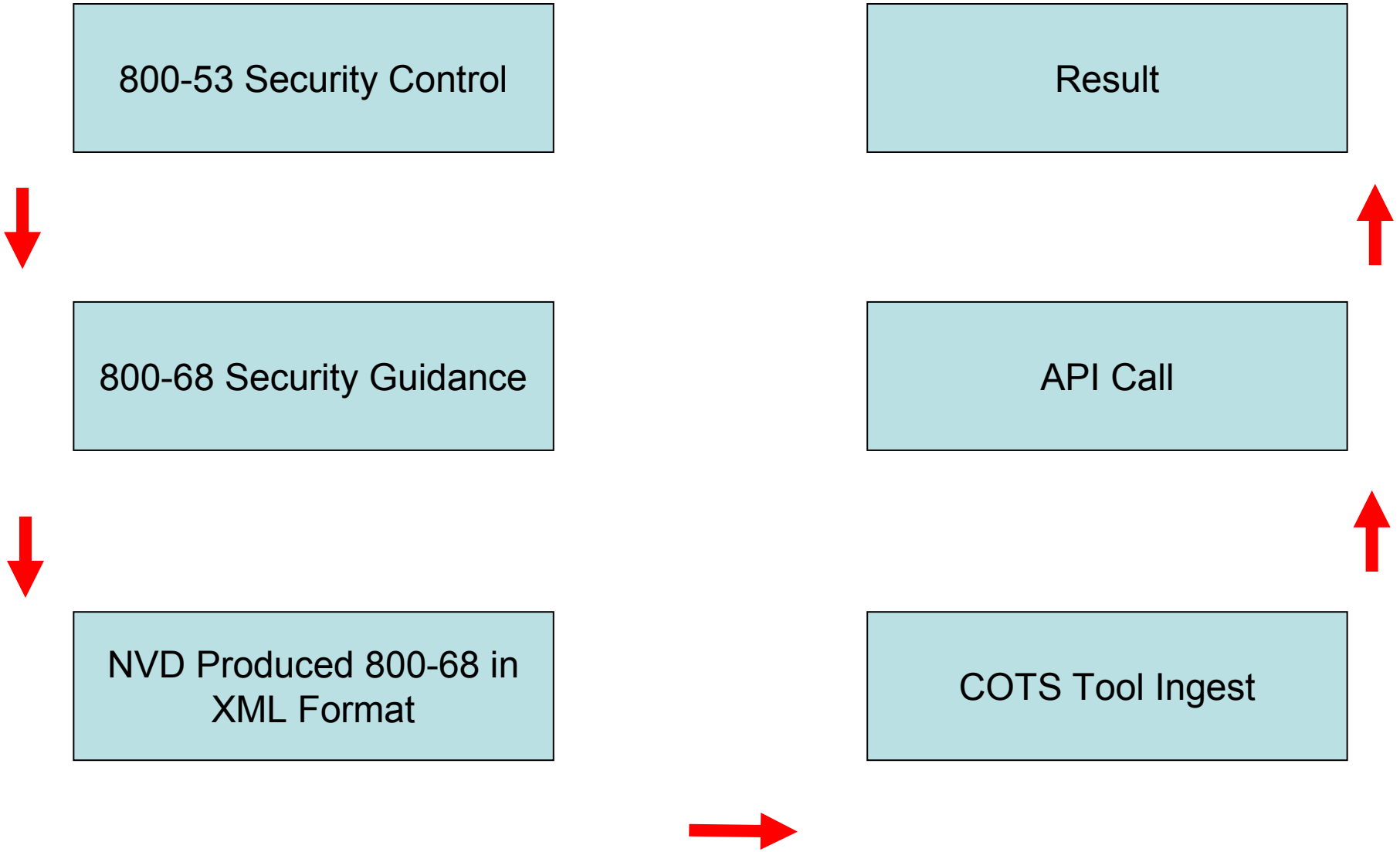
COTS Tools

- What are the NIST Technical Security Controls?
- What are the ***Specific*** NIST recommended settings for individual technical controls?
- How do I implement the recommended setting for technical controls? Can I use my COTS Product?
- Am I compliant to NIST Recs & Can I use my COTS Product?
- Will I be audited against the same criteria I used to secure my systems?



Automated Compliance

The Connected Path



Automated Compliance

800-53 Security Control

AC-7 Unsuccessful Login Attempts

800-68 Security Guidance

AC-7: Account Lockout Duration

AC-7: Account Lockout Threshold

NVD Produced 800-68 in XML Format

```
- <registry_test id="wrt-9999" comment="Account Lockout
Duration Set to 5" check="at least 5">
- <object>
  <hive>HKEY_LOCAL_MACHINE</hive>
  <key>Software\Microsoft\Windows</key>
 <name>AccountLockoutDuration</name>
 </object>
- <data operation="AND">
 <value operator="greater than">5*</value>
```

COTS Tool Ingest

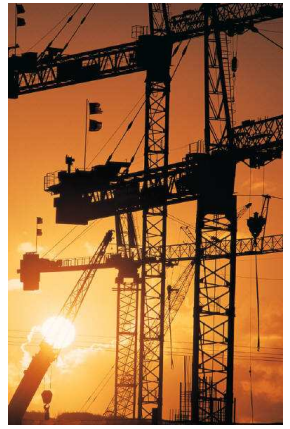
Result

```
RegQueryValue (lpHKey, path, value, sKey, Value, Op);
If (Op == '>" )
if ((sKey < Value )
return (1); else
return (0);
```

API Call

```
lpHKey = "HKEY_LOCAL_MACHINE"
Path = "Software\Microsoft\Windows\"
Value = "5"
sKey = "AccountLockoutDuration"
Op = ">"
```

Wrapping together existing initiatives



- Mitre - Common Vulnerability Enumeration (CVE)
- Mitre - Open Vulnerability Assessment Language (OVAL)
- NSA - eXtensible Configuration Checklist Description Format (XCCDF)
- FIRST – Common Vulnerability Scoring System (CVSS)
- NIST - National Vulnerability Database
- NIST - NIST Checklist Program

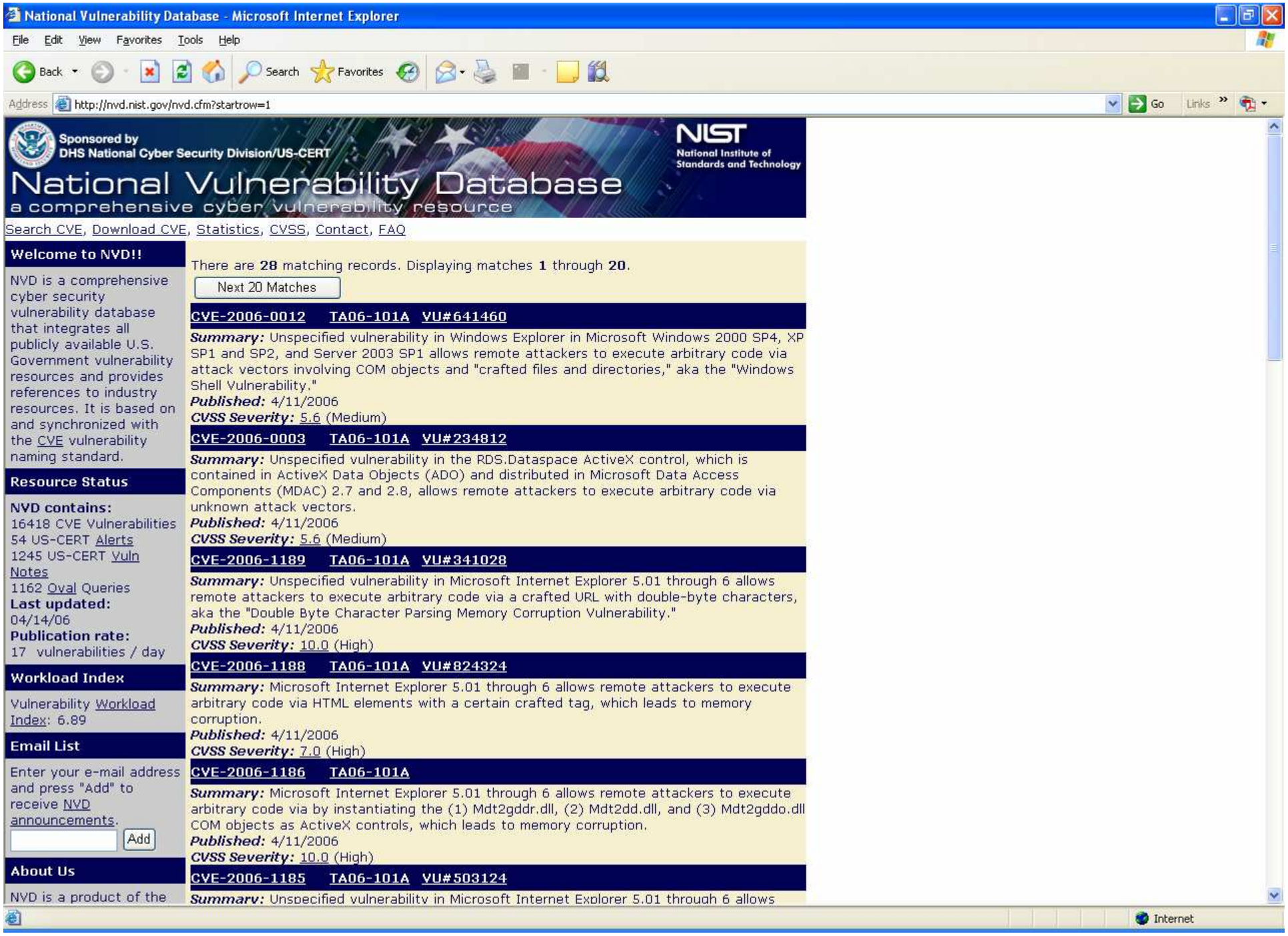
Existing NIST Products

- National Vulnerability Database
  - 2.2 million hits per month
  - 20 new vulnerabilities per day
  - Integrated standards: 244 products, 20 vendors, 8 vendors 24 products
- Checklist Program
  - 91 separate guidance documents
  - Covers 140 IT products

National Vulnerability Database

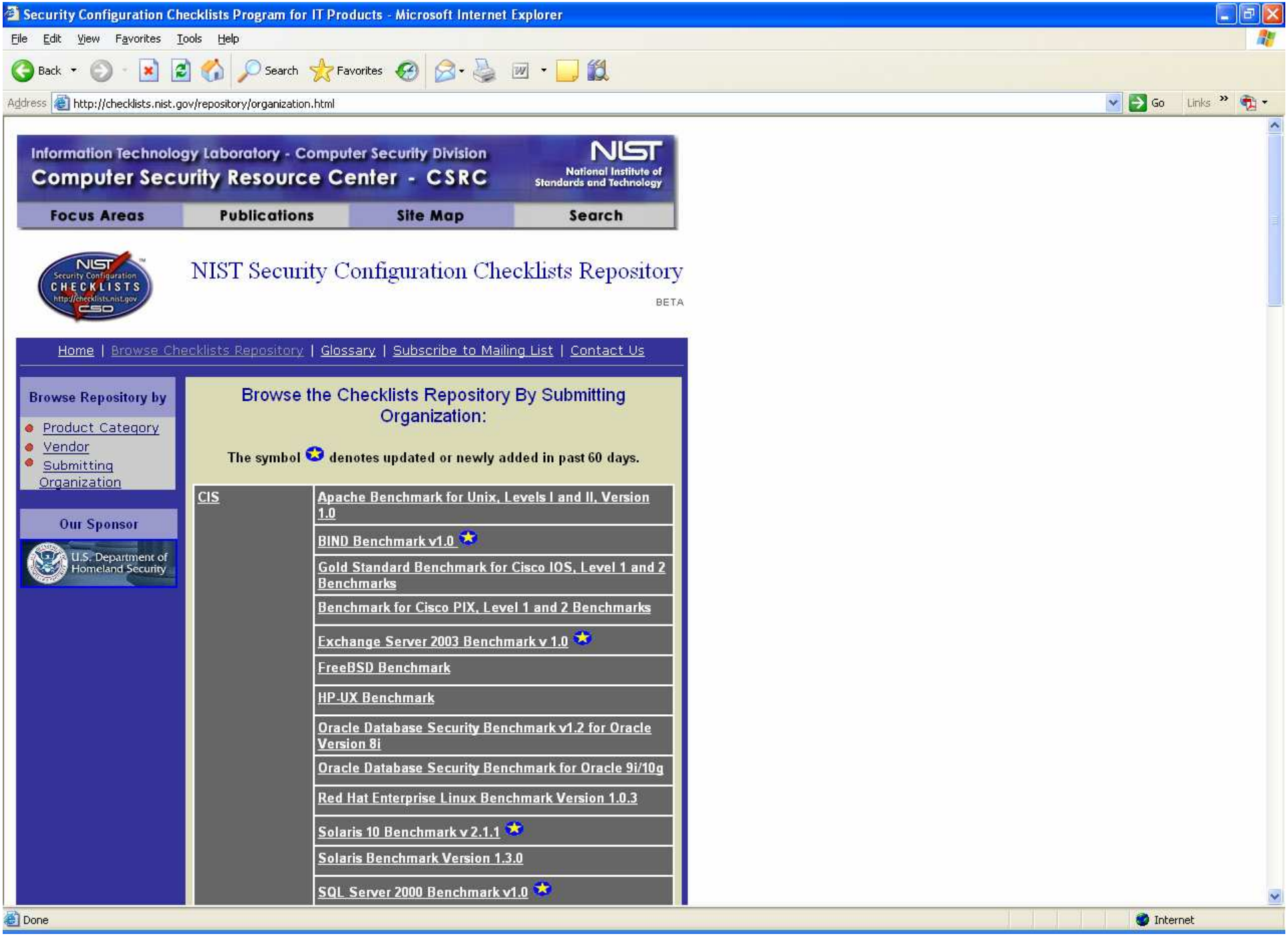
- NVD is a comprehensive cyber security vulnerability database that:
  - Integrates all publicly available U.S. Government vulnerability resources
  - Provides references to industry resources.
  - It is based on and synchronized with the CVE vulnerability naming standard.
  - XML feed for all CVEs
  - http://nvd.nist.gov

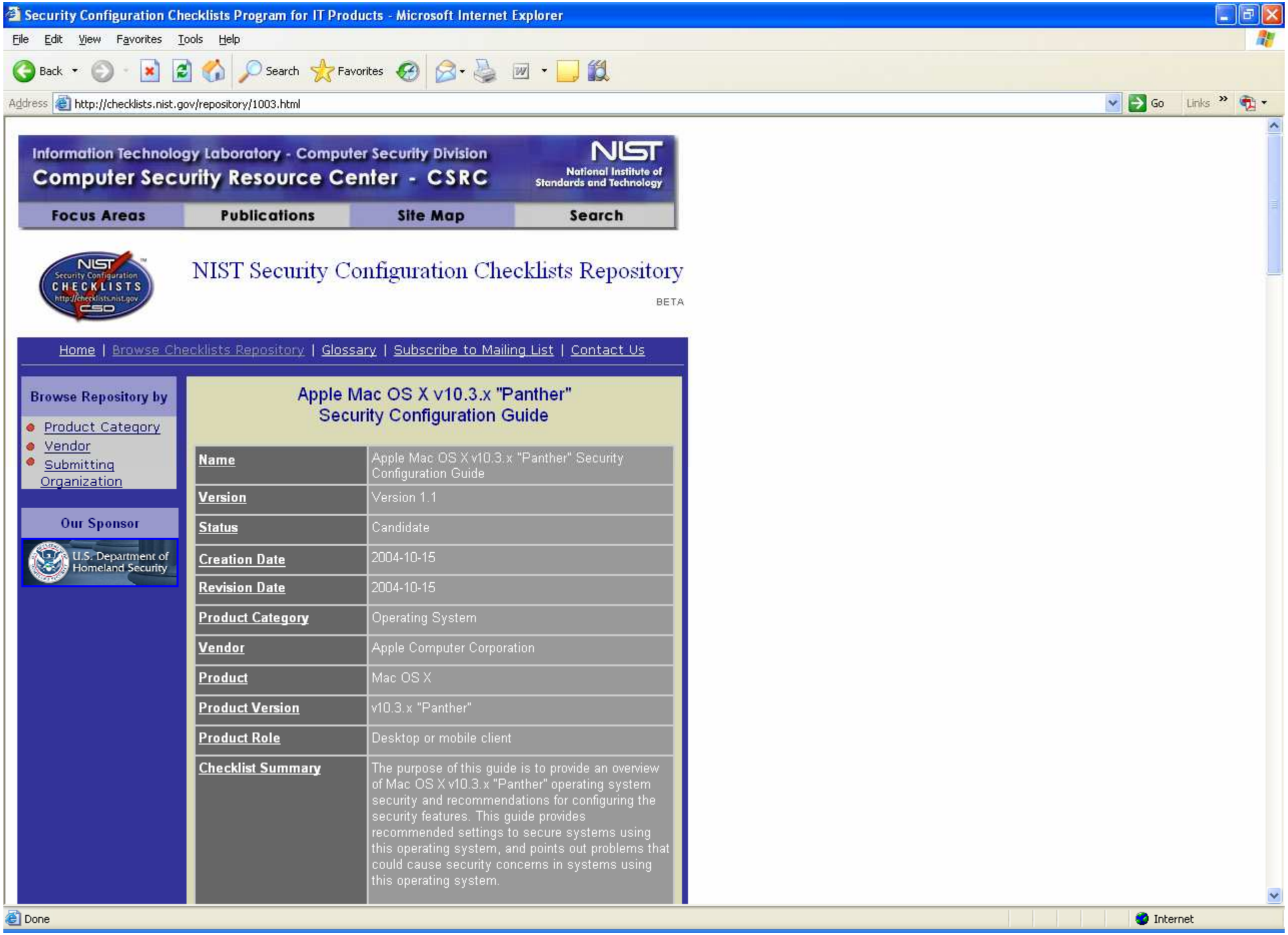

National Vulnerability Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://nvd.nist.gov/
Go Links
Sponsored by DHS National Cyber Security Division/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
a comprehensive cyber vulnerability resource
Search CVE, Download CVE, Statistics, CVSS, Contact, FAQ
Welcome to NVD!!
NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the CVE vulnerability naming standard.
Resource Status
NVD contains:
16418 CVE Vulnerabilities
54 US-CERT Alerts
1245 US-CERT Vuln Notes
1162 Oval Queries
Last updated:
04/14/06
Publication rate:
17 vulnerabilities / day
Workload Index
Vulnerability Workload Index: 6.89
Email List
Enter your e-mail address and press "Add" to receive NVD announcements.
Add
About Us
NVD is a product of the
Search CVE Vulnerability Database (Perform Advanced Search)
Keyword search:
Search All
Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions
Search last 3 months
Search last 3 years
Show only vulnerabilities that have the following associated resources:
US-CERT Technical Alerts
US-CERT Vulnerability Notes
OVAL Queries
Recent CVE Vulnerabilities
CVE-2006-1790 Publish Date: 4/14/2006
A regression fix in Mozilla Firefox 1.0.7 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the InstallTrigger.install method, which leads to memory corruption.
CVE-2006-1738 Publish Date: 4/14/2006
Unspecified vulnerability in Mozilla Firefox and Thunderbird 1.x before 1.5 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0 allows remote attackers to cause a denial of service (crash) by changing the (1) -moz-grid and (2) -moz-grid-group display styles.
CVE-2006-1737 Publish Date: 4/14/2006
Integer overflow in Mozilla Firefox and Thunderbird 1.x before 1.5 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary bytecode via JavaScript with a large regular expression.
CVE-2006-1742 (Firefox, Thunderbird, Mozilla suite, SeaMonkey)
Publish Date: 4/14/2006 CVSS Severity: 2.3 (Low)
The JavaScript engine in Mozilla Firefox and Thunderbird 1.x before 1.5 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0 does not properly handle temporary variables that are not garbage collected, which might allow remote attackers to trigger operations on freed memory and cause memory corruption.
CVE-2006-1741 (Firefox, Thunderbird, Mozilla suite, SeaMonkey)
Done
Internet


National Vulnerability Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://nvd.nist.gov/nvd.cfm?startrow=1
Go Links
Sponsored by DHS National Cyber Security Division/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
a comprehensive cyber vulnerability resource
Search CVE, Download CVE, Statistics, CVSS, Contact, FAQ
Welcome to NVD!!
NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the CVE vulnerability naming standard.
Resource Status
NVD contains:
16418 CVE Vulnerabilities
54 US-CERT Alerts
1245 US-CERT Vuln Notes
1162 Oval Queries
Last updated:
04/14/06
Publication rate:
17 vulnerabilities / day
Workload Index
Vulnerability Workload Index: 6.89
Email List
Enter your e-mail address and press "Add" to receive NVD announcements.
Add
About Us
NVD is a product of the
There are 28 matching records. Displaying matches 1 through 20.
Next 20 Matches
CVE-2006-0012 TA06-101A VU#641460
Summary: Unspecified vulnerability in Windows Explorer in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via attack vectors involving COM objects and "crafted files and directories," aka the "Windows Shell Vulnerability."
Published: 4/11/2006
CVSS Severity: 5.6 (Medium)
CVE-2006-0003 TA06-101A VU#234812
Summary: Unspecified vulnerability in the RDS.Dataspace ActiveX control, which is contained in ActiveX Data Objects (ADO) and distributed in Microsoft Data Access Components (MDAC) 2.7 and 2.8, allows remote attackers to execute arbitrary code via unknown attack vectors.
Published: 4/11/2006
CVSS Severity: 5.6 (Medium)
CVE-2006-1189 TA06-101A VU#341028
Summary: Unspecified vulnerability in Microsoft Internet Explorer 5.01 through 6 allows remote attackers to execute arbitrary code via a crafted URL with double-byte characters, aka the "Double Byte Character Parsing Memory Corruption Vulnerability."
Published: 4/11/2006
CVSS Severity: 10.0 (High)
CVE-2006-1188 TA06-101A VU#824324
Summary: Microsoft Internet Explorer 5.01 through 6 allows remote attackers to execute arbitrary code via HTML elements with a certain crafted tag, which leads to memory corruption.
Published: 4/11/2006
CVSS Severity: 7.0 (High)
CVE-2006-1186 TA06-101A
Summary: Microsoft Internet Explorer 5.01 through 6 allows remote attackers to execute arbitrary code via by instantiating the (1) Mdt2gddr.dll, (2) Mdt2dd.dll, and (3) Mdt2gddo.dll COM objects as ActiveX controls, which leads to memory corruption.
Published: 4/11/2006
CVSS Severity: 10.0 (High)
CVE-2006-1185 TA06-101A VU#503124
Summary: Unspecified vulnerability in Microsoft Internet Explorer 5.01 through 6 allows
Internet

NIST Checklist Program

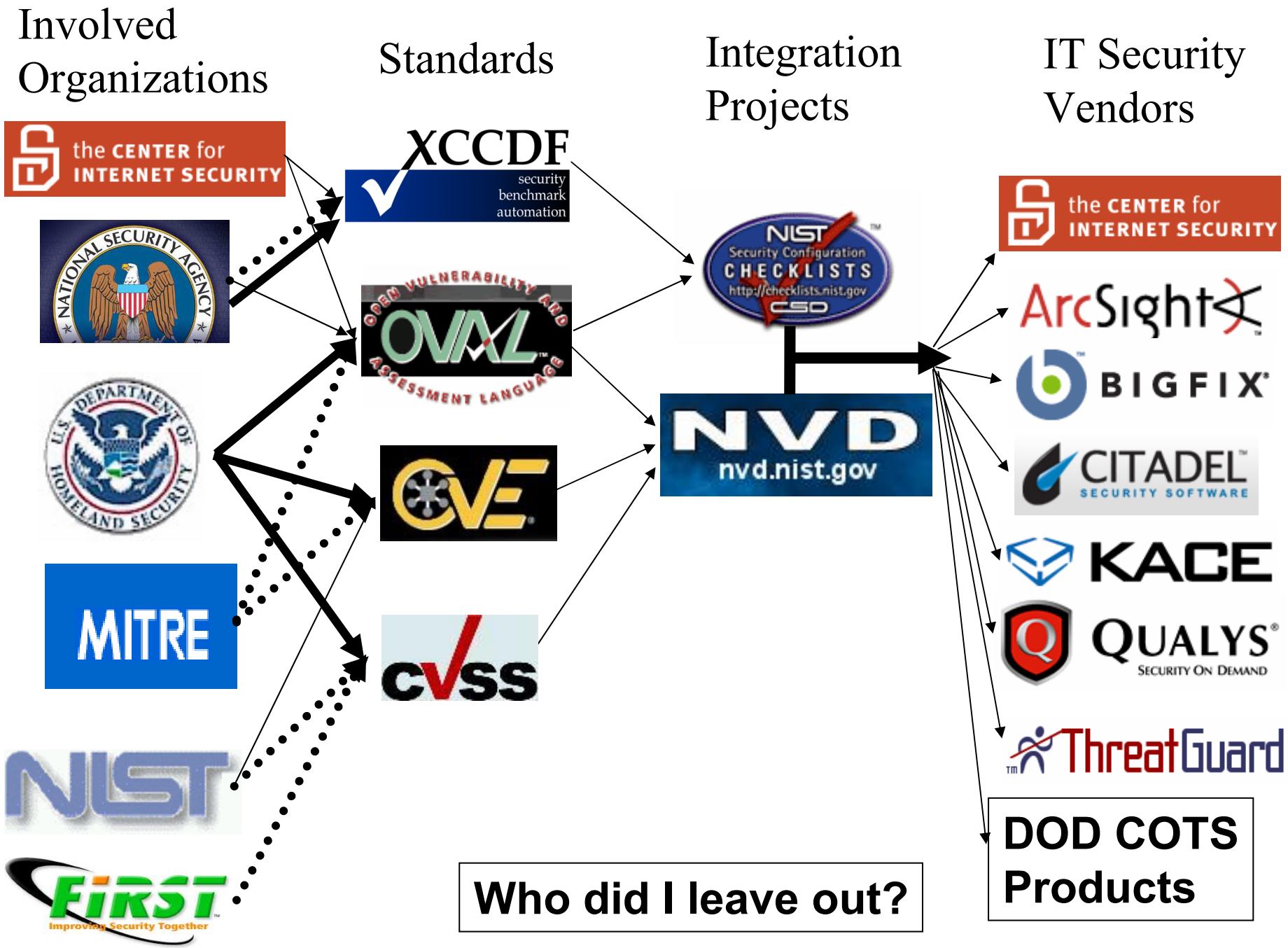
- Encourage Vendor Development and Maintenance of Security Guidance.
- Currently Hosts 95 separate guidance documents for over 143 IT products.
  - In English Prose and automation-enabling formats (i.e. .inf files, scripts, etc.)
- Need to provide configuration data in standard, consumable format.
- http://checklists.nist.gov

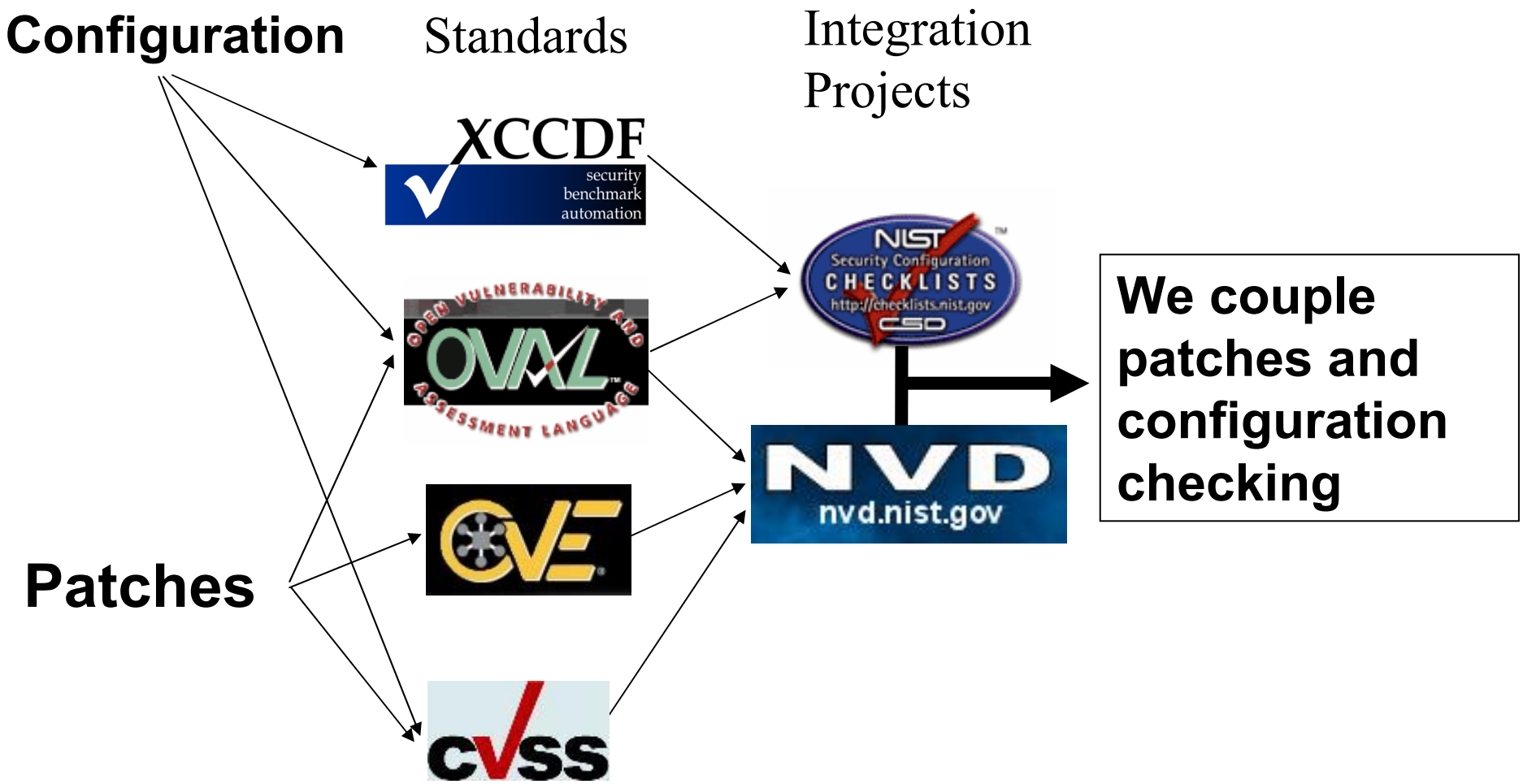

Security Configuration Checklists Program for IT Products - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://checklists.nist.gov/repository/organization.html
Go Links
Information Technology Laboratory - Computer Security Division
Computer Security Resource Center - CSRC
NIST National Institute of Standards and Technology
Focus Areas Publications Site Map Search
NIST Security Configuration Checklists Repository
BETA
Home | Browse Checklists Repository | Glossary | Subscribe to Mailing List | Contact Us
Browse Repository by
Product Category
Vendor
Submitting Organization
Our Sponsor
U.S. Department of Homeland Security
Browse the Checklists Repository By Submitting Organization:
The symbol denotes updated or newly added in past 60 days.
CIS
Apache Benchmark for Unix, Levels I and II, Version 1.0
BIND Benchmark v1.0
Gold Standard Benchmark for Cisco IOS, Level 1 and 2 Benchmarks
Benchmark for Cisco PIX, Level 1 and 2 Benchmarks
Exchange Server 2003 Benchmark v 1.0
FreeBSD Benchmark
HP-UX Benchmark
Oracle Database Security Benchmark v1.2 for Oracle Version 8i
Oracle Database Security Benchmark for Oracle 9i/10g
Red Hat Enterprise Linux Benchmark Version 1.0.3
Solaris 10 Benchmark v 2.1.1
Solaris Benchmark Version 1.3.0
SQL Server 2000 Benchmark v1.0
Done
Internet


Security Configuration Checklists Program for IT Products - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://checklists.nist.gov/repository/1003.html
Go Links
Information Technology Laboratory - Computer Security Division
Computer Security Resource Center - CSRC
NIST National Institute of Standards and Technology
Focus Areas Publications Site Map Search
NIST Security Configuration Checklists Repository
BETA
Home | Browse Checklists Repository | Glossary | Subscribe to Mailing List | Contact Us
Browse Repository by
Product Category
Vendor
Submitting Organization
Our Sponsor
U.S. Department of Homeland Security
Apple Mac OS X v10.3.x "Panther" Security Configuration Guide
Name | Apple Mac OS X v10.3.x "Panther" Security Configuration Guide
Version | Version 1.1
Status | Candidate
Creation Date | 2004-10-15
Revision Date | 2004-10-15
Product Category | Operating System
Vendor | Apple Computer Corporation
Product | Mac OS X
Product Version | v10.3.x "Panther"
Product Role | Desktop or mobile client
Checklist Summary | The purpose of this guide is to provide an overview of Mac OS X v10.3.x "Panther" operating system security and recommendations for configuring the security features. This guide provides recommended settings to secure systems using this operating system, and points out problems that could cause security concerns in systems using this operating system.
Done
Internet

eXtensible Configuration Checklist Description Format

- Designed to support:
  - Information Interchange
  - Document Generation
  - Organizational and Situational Tailoring
  - Automated Compliance Testing
  - Compliance Scoring
- Published as NIST IR 7275
- Foster more widespread application of good security practices


Involved Organizations
Standards
Integration Projects
IT Security Vendors
the CENTER for INTERNET SECURITY
NATIONAL SECURITY AGENCY
U.S. DEPARTMENT OF HOMELAND SECURITY
MITRE
NIST
FIRST
Improving Security Together
XCCDF
security benchmark automation
OVAL
OPEN VULNERABILITY AND ASSESSMENT LANGUAGE
CVE
CVSS
NIST Security Configuration CHECKLISTS
http://checklists.nist.gov
CSD
NVD
nvd.nist.gov
the CENTER for INTERNET SECURITY
ArcSight
BIGFIX
CITADEL
SECURITY SOFTWARE
KACE
QUALYS
SECURITY ON DEMAND
ThreatGuard
DOD COTS Products
Who did I leave out?


Configuration
Standards
Integration
Projects
XCCDF
security
benchmark
automation
OVAL
OPEN VULNERABILITY AND ASSESSMENT LANGUAGE
CVE
CVSS
Patches
NIST
Security Configuration
CHECKLISTS
http://checklists.nist.gov
CSD
NVD
nvd.nist.gov
We couple patches and configuration checking

Security Measurement

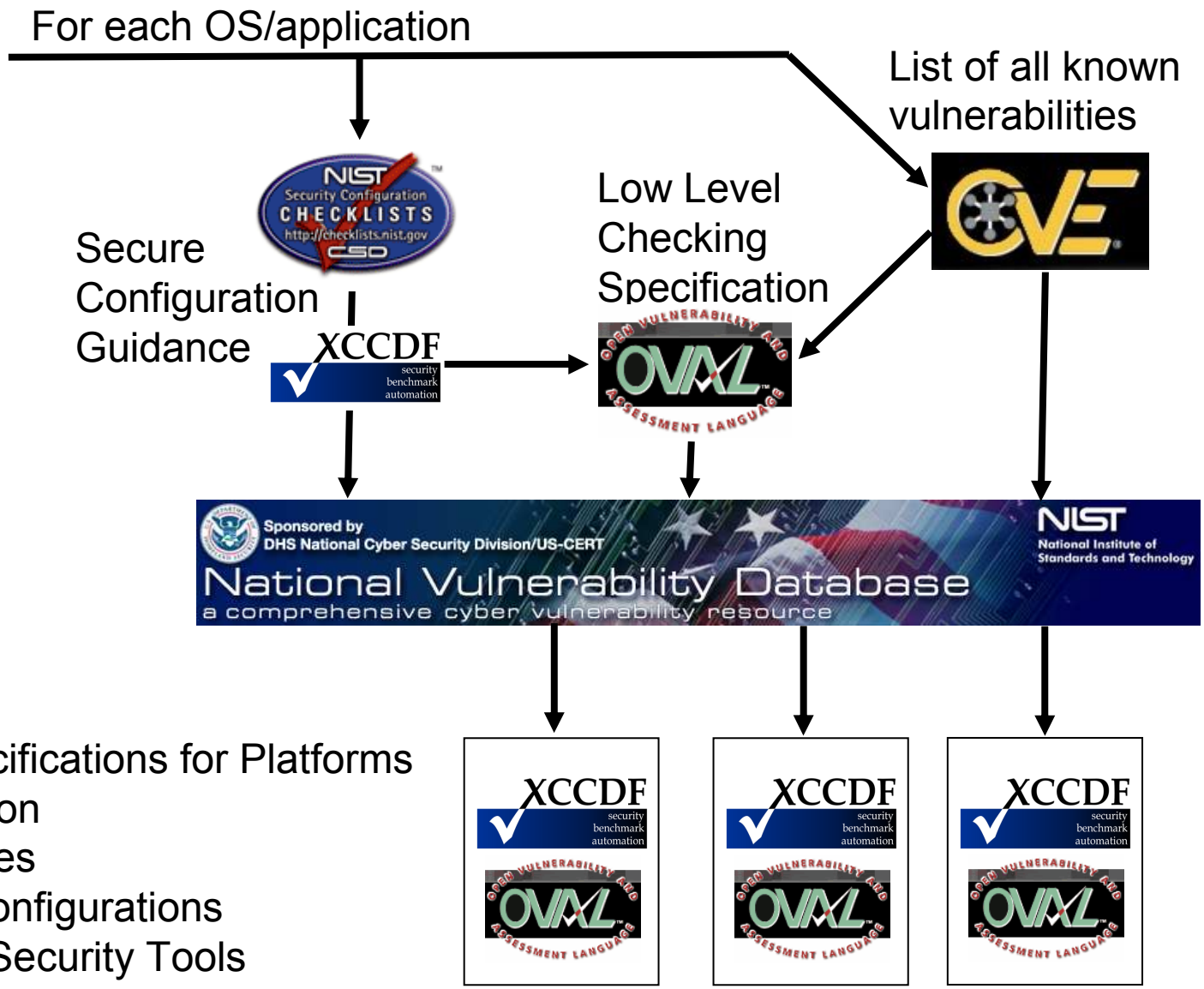
- How secure is my computer?
  - Measure security of the configuration
    - Measure conformance to recommended application and OS security settings
    - Measure the presence of security software (firewalls, antivirus…)
  - Measure presence of vulnerabilities (needed patches)
- How well have I implemented the FISMA requirements (NIST SP800-53 technical controls)?
  - Measure deviation from requirements
  - Measure risk to the agency

Setting Ground Truth/Defining Security

FISMA/FIPS 200

800-53

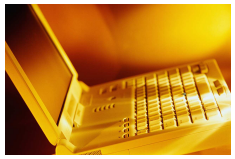
Required technical security controls

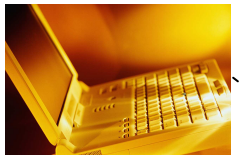


Security Specifications for Platforms And Application

- Vulnerabilities
- Required Configurations
- Necessary Security Tools

Automated Security Measurement System





Automated Measurement System

Vulnerability Checking Tools

XCCDF security benchmark automation

OVAL Open Vulnerability and Assessment Language

Definition of What it means to Be Secure

FISMA Security Requirements

Organizational Impact Rating

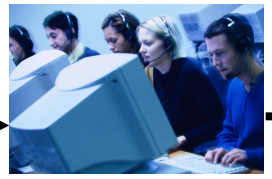
FIPS 199

Deviation from Requirements

CVSS

Impact Scoring System

Impact to the System



CVSS

Impact to the Agency

U.S. Department of Homeland Security

Our Gifts Today

- NIST Windows XP Configuration Guide (SP 800-68)
- http://csrc.nist.gov/itsec/download_WinXP.html
- Policy statement represented in XCCDF
- Configuration checks represented in OVAL
- Currently ALPHA version (NOT YET TESTED)
- Covers: registry settings, file permission checks, password policies, account lockout policies, audit policies
- Download at: http://checklists.nist.gov/NIST-800-68-WinXPPro-XML-Alpha-rev1.zip
- Content will be updated periodically; however, format will remain constant at least until the NIST Workshop in September 2006.

NIST 800-68 in Context of 800-53

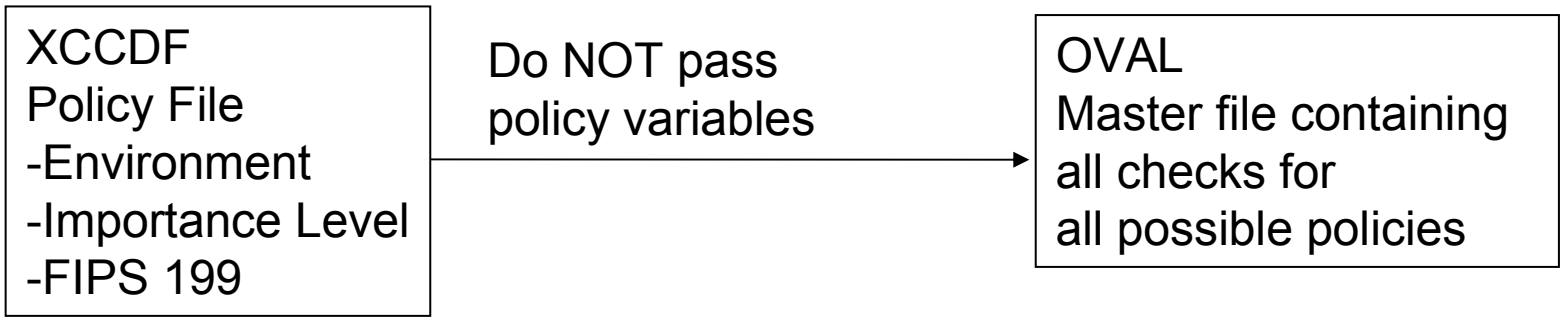
- 800-53, Appendix D specifies security control applicability according to High, Moderate, and Low impact rating of an IT System.
- 800-68 provides specific configuration information according to environment (Standalone, Enterprise, SSLF, and Legacy)
- The NIST XML specifies the applicable 800-68 security settings according to the 800-53 guidelines.

EXAMPLE:

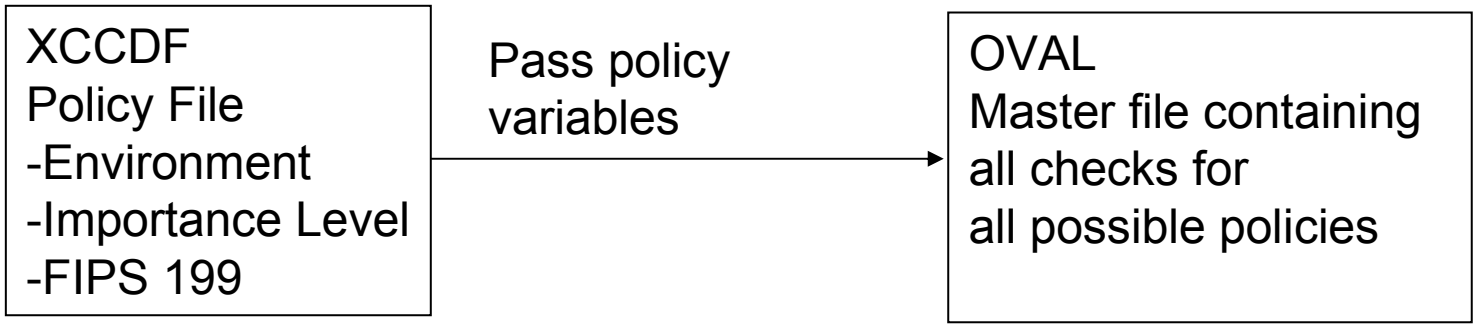
- AC-12 (session termination) is applicable for IT systems with either moderate or high impact rating, but not for system rated at a low.
- The XCCDF profile for High and Moderate systems enables the group for AC-12 rule execution, but disables the group for low system.
- The XCCDF rules ‘refer’ to the appropriate OVAL definitions in the companion OVAL file (named: WindowsXP-SP800-68.xml)

OVAL and XCCDF Implementation

Implementation with XCCDF (stand alone OVAL)

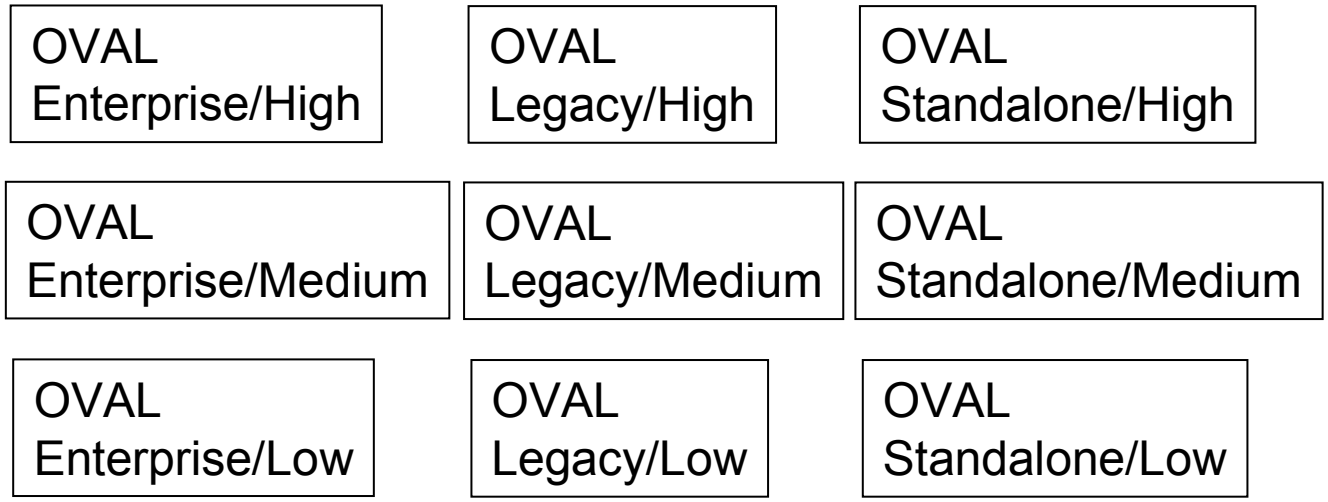


Implementation with XCCDF (dependant OVAL)



OVAL and XCCDF Implementation

Implementation without XCCDF



OVAL files work by themselves

Each OVAL file checks with respect to a particular policy

Questions?

Stephen Quinn (NIST Checklist Program)
Peter Mell (National Vulnerability Database)
Computer Security Division
NIST, Information Technology Laboratory
stquinn@nist.gov, mell@nist.gov