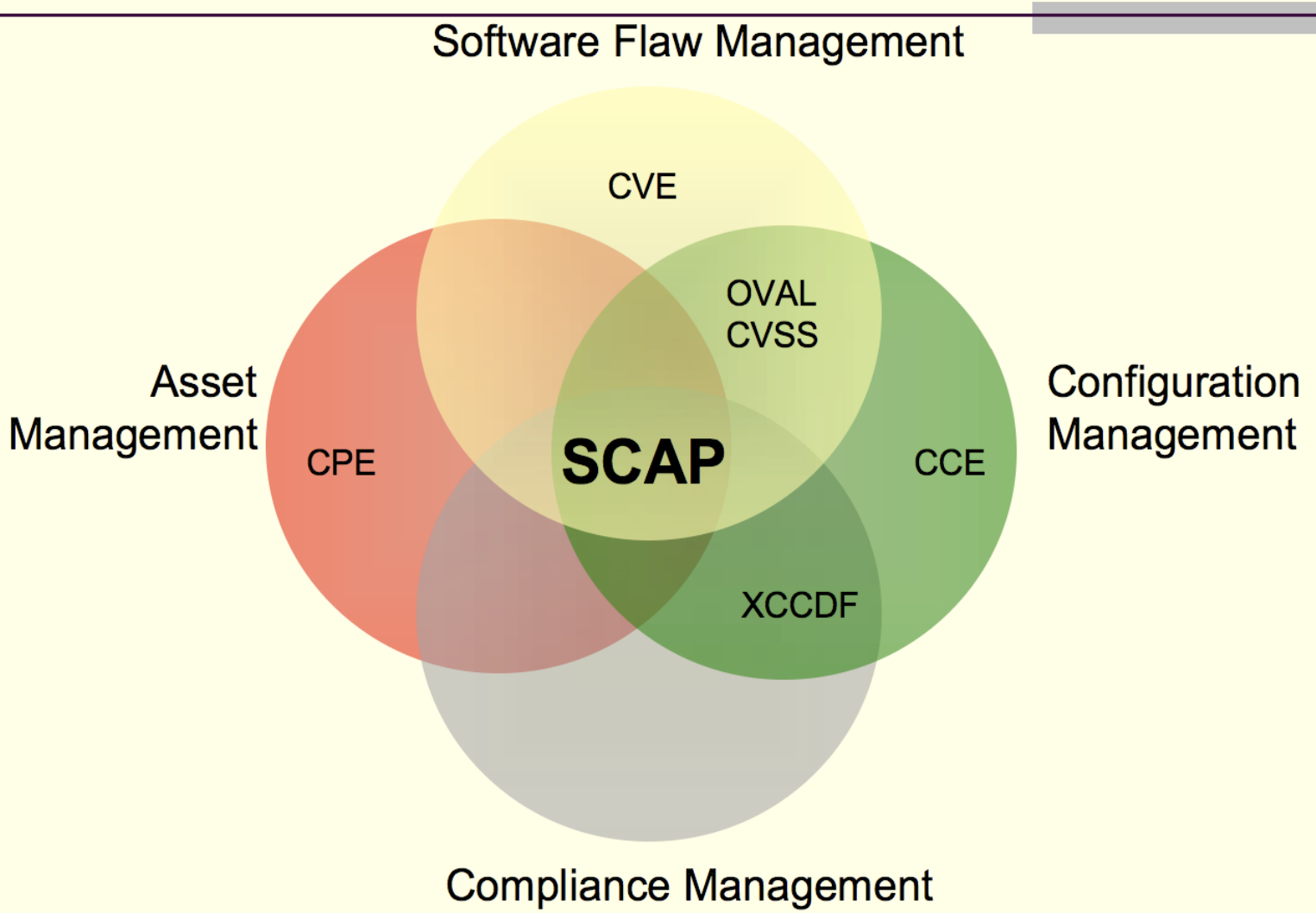
Finding the Atoms:
CVE, CCE, CPE

Matthew N. Wojcik

26 September 2007

MITRE

SCAP Interoperability



IA Content vs IA Tools

- IA Content
  - Knowledge about vulnerabilities, threats, misconfigurations, best practices, etc
  - DISA STIGS, NIST Benchmarks, IAVA, US-CERT alerts
- IA Tools
  - Vulnerability scanners, IDS, Patch management systems, AV products, configuration management systems

Benefits of Decoupling IA Content from IA Tools

- Consistency, transparency, and concreteness in the specification and measurement of IA requirements
- Consistency in the communication of IA information between tool categories (e.g. vuln assessment to patch management, asset inventory to vuln assessment)
- Organizational subcomponents can make autonomous tool investments and still achieve global integrated reporting

Benefits of Decoupling IA Content from IA Tools (2)

- Policy writers have concrete foundations for expressing requirements for technical controls
- IA tool vendors can import (vs create) government supplied IA content
- Software vendors and government agencies have improved technical collaboration on secure configuration guidance for vendor products

How To Decouple IA Content from IA Tools

- Identify the basic entities that IA Content needs to reference
  - Vulnerabilities, configuration settings, etc
- Provide a machine-readable language for making assertions about the basic IA entities (XCCDF/OVAL)
- Express IA requirements as documents in the XCCDF/OVAL language

The Pieces

- Enumerations (CVE, CCE, CPE)
  - Catalog the fundamental entities in IA business
    - Software packages, vulnerabilities, misconfigurations
- Languages (XCCDF, OVAL)
  - Support the creation of machine-readable assertions about those entities
- Content (STIGS, Benchmarks, Checklists)
  - Packages of assertions supporting a specific application
    - Vuln assessment, config guidance, asset inventory
- Tools
  - Interpret IA content in context of enterprise network

Enumerated Entities

- **Vulnerabilities**
  - **CVE-2007-1751**
  - Microsoft Internet Explorer 5.01, 6, and 7 allows remote attackers to execute arbitrary code by causing Internet Explorer to access an uninitialized or deleted object, related to prototype variables and table cells, aka "Uninitialized Memory Corruption Vulnerability."
- **Configuration Settings**
  - **CCE-299**
  - **Definition:** The "restrict guest access to application log" policy should be set correctly.
  - **Technical Mechanism:**

    (1)HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\RestrictGuestAccess

    (2) defined by Group Policy
  - **Parameters:** enabled/disabled
- **Software Packages**
  - **CPE:/o:microsoft:windows-nt:xp::pro**

Languages

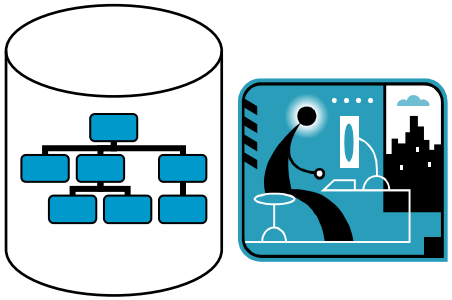
- OVAL
  - XML language framework for assertions about software configuration state
- XCCDF
  - XML language framework for packaging and documenting checklist requirements and results

Enumerations - What are they?

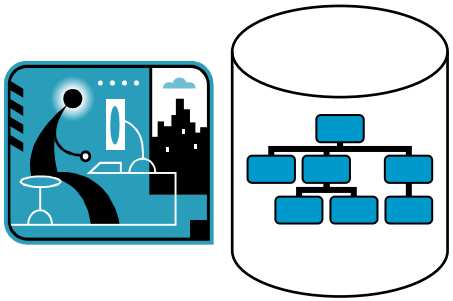
- Common identifiers for "atoms" of information
  - Standardized way to refer to “what we care about”
- Similar to
  - VINs
  - ISBNs
  - Scientific Names

Enumerations in Real Life - ISBN

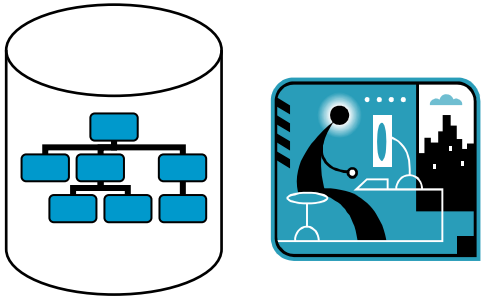
Publishers
- Viking
- Springer Verlag



Booksellers
- Amazon
- Barnes & Nobles



Libraries
- Library of Congress
- Middletown Elementary



ISBN 0553213113

Customers

Reviewers
- New York Times
- Oprah?

Benefits of the SCAP Enumerations

- Enables faster, more accurate correlation
  - Standardized identifiers used in:
    - Databases
    - Tools
    - Guidance
- Facilitates information exchange
  - Requirements – what do we need to check for?
  - Reporting – what did we find?
  - Information flows:
    - Across the configuration management lifecycle
    - Through different communities of interest
- Allows increased automation
  - Diverse tools can share input and output

The Pieces (redux)

- Enumerations (CVE, CCE, CPE)
  - Catalog the fundamental entities in IA business
    - Software packages, vulnerabilities, misconfigurations
- Languages (XCCDF, OVAL)
  - Support the creation of machine-readable assertions about those entities
- Content (STIGS, Benchmarks, Checklists)
  - Packages of assertions supporting a specific application
    - Vuln assessment, config guidance, asset inventory
- Tools
  - Interpret IA content in context of enterprise network

Enumerated Entities (redux)

- **Vulnerabilities**
  - **CVE-2007-1751**
  - Microsoft Internet Explorer 5.01, 6, and 7 allows remote attackers to execute arbitrary code by causing Internet Explorer to access an uninitialized or deleted object, related to prototype variables and table cells, aka "Uninitialized Memory Corruption Vulnerability."

- **Configuration Settings**
  - **CCE-299**
  - **Definition:** The "restrict guest access to application log" policy should be set correctly.
  - **Technical Mechanism:**

    (1)HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\RestrictGuestAccess

    (2) defined by Group Policy
  - **Parameters:** enabled/disabled

- **Software Packages**
  - **cpe:/o:microsoft:windows-nt:xp::pro**

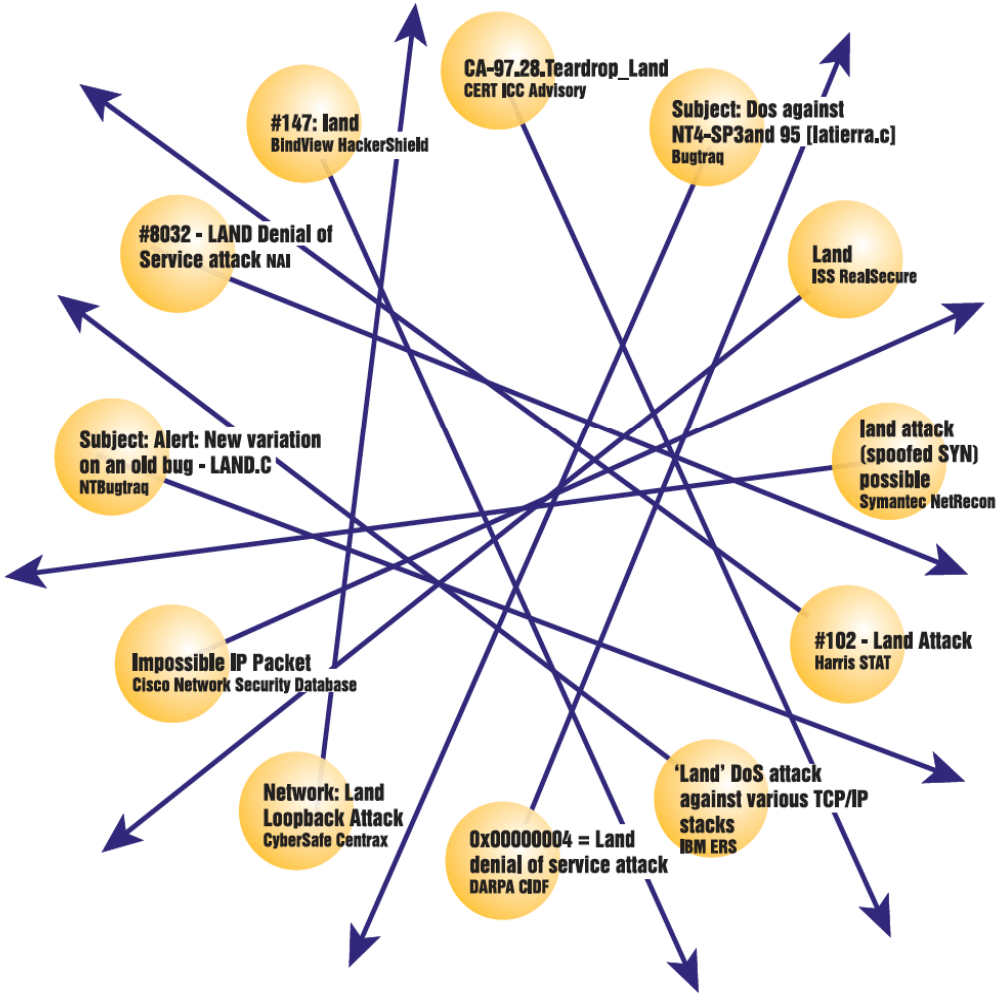
QUESTIONS

Common Vulnerabilities and Exposures

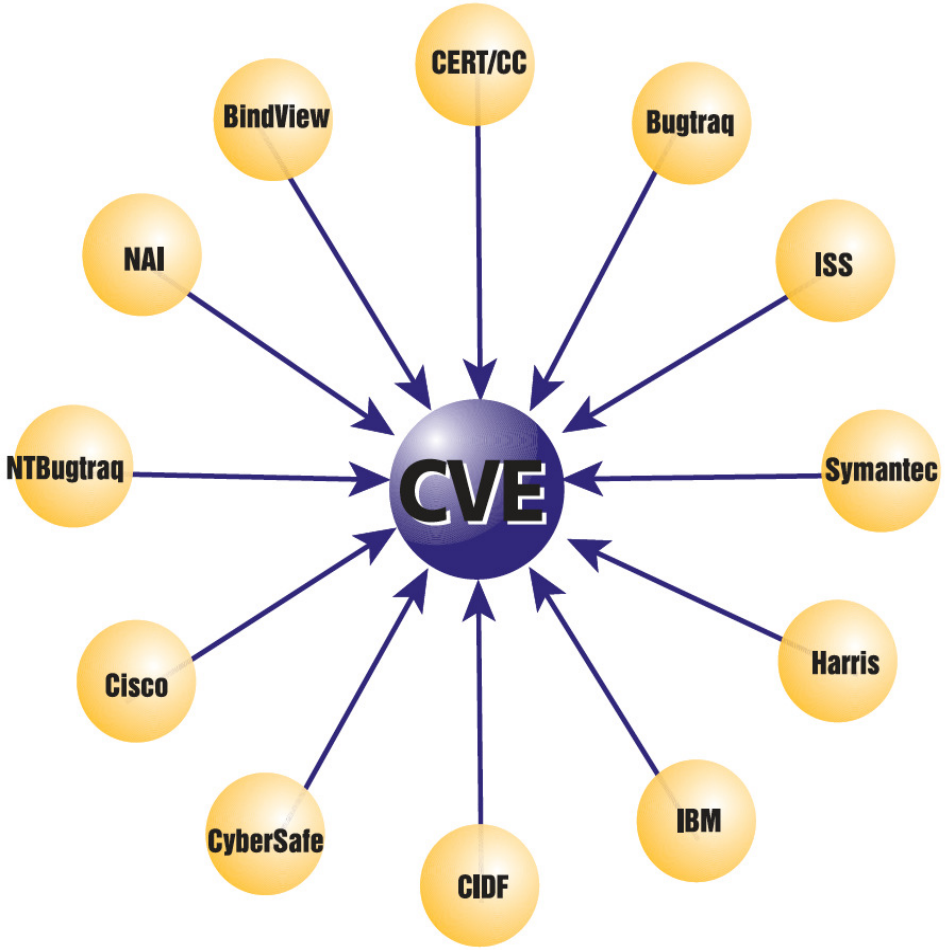
MITRE

CVE Is…
A Single ID for Each Vulnerability

Without CVE



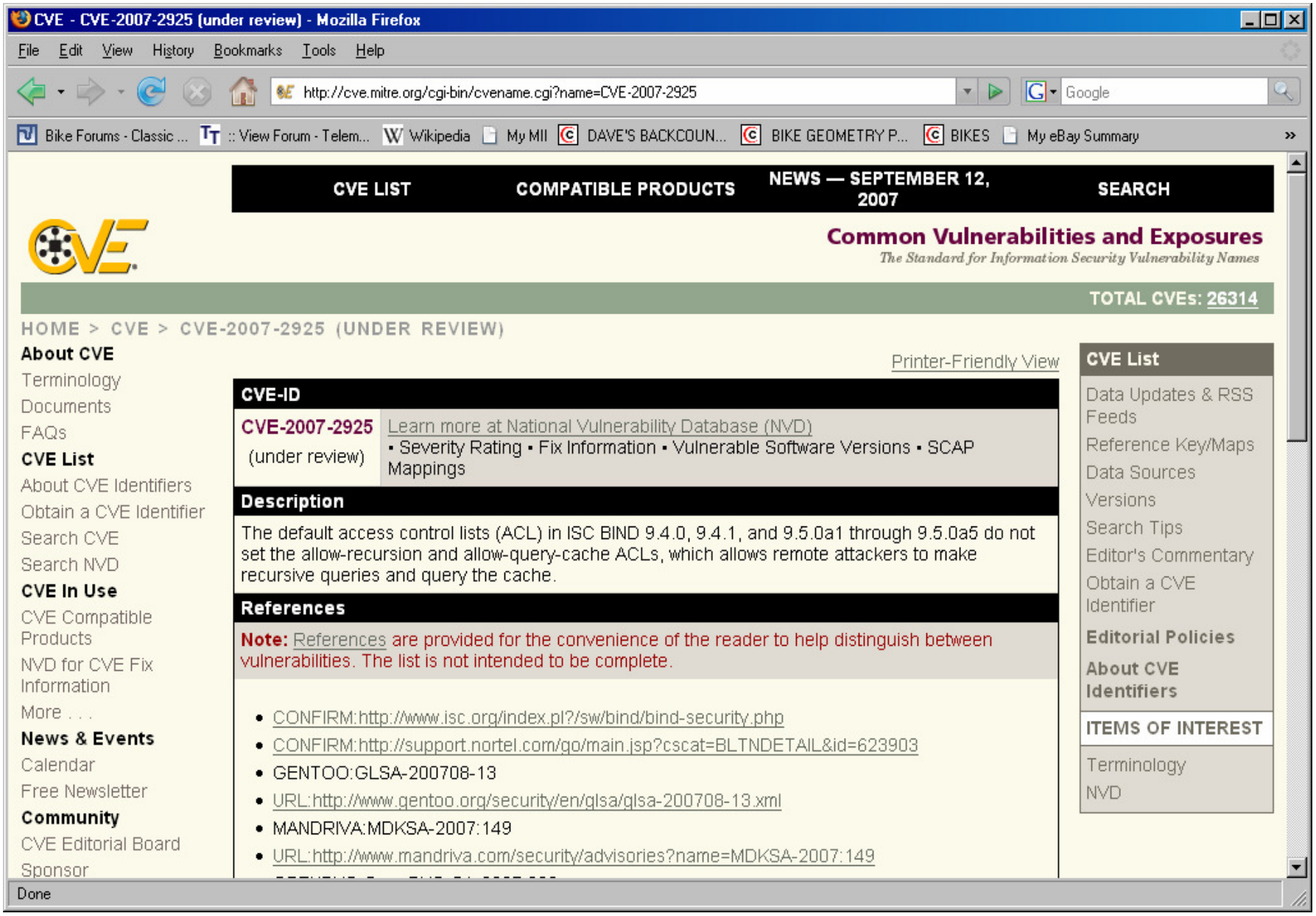
With CVE



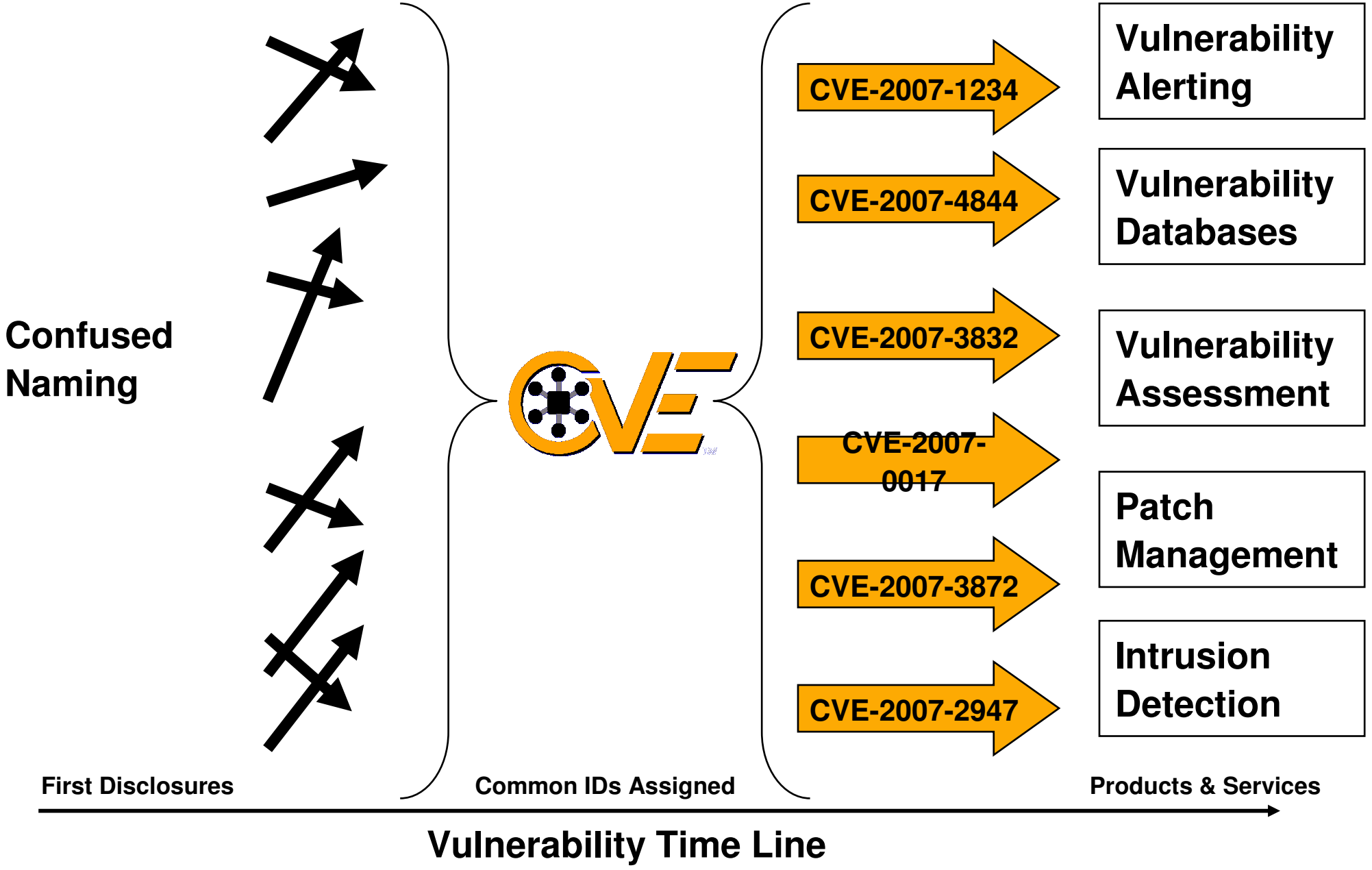
CVE-1999-0016 Land IP denial of service.

MITRE

CVE Is…
An Individual Definition



CVE Is…
A Common Identification Process



MITRE

CVE Is…
Industry Adoption & Compatibility Program

- CVE ids used in over 300 products and services …
  - … from over 20 different countries
  - Vulnerability Databases, Security Advisories and Archives, Vulnerability Notification Services, Vulnerability Assessment and Remediation Tools, Vulnerability Assessment Services, Intrusion Detection Tools, Incident Management, Data/Event Correlation Tools, Educational Materials, Patch Management

- CVE Compatibility Program
  - Over 100 products and services
  - MITRE evaluations

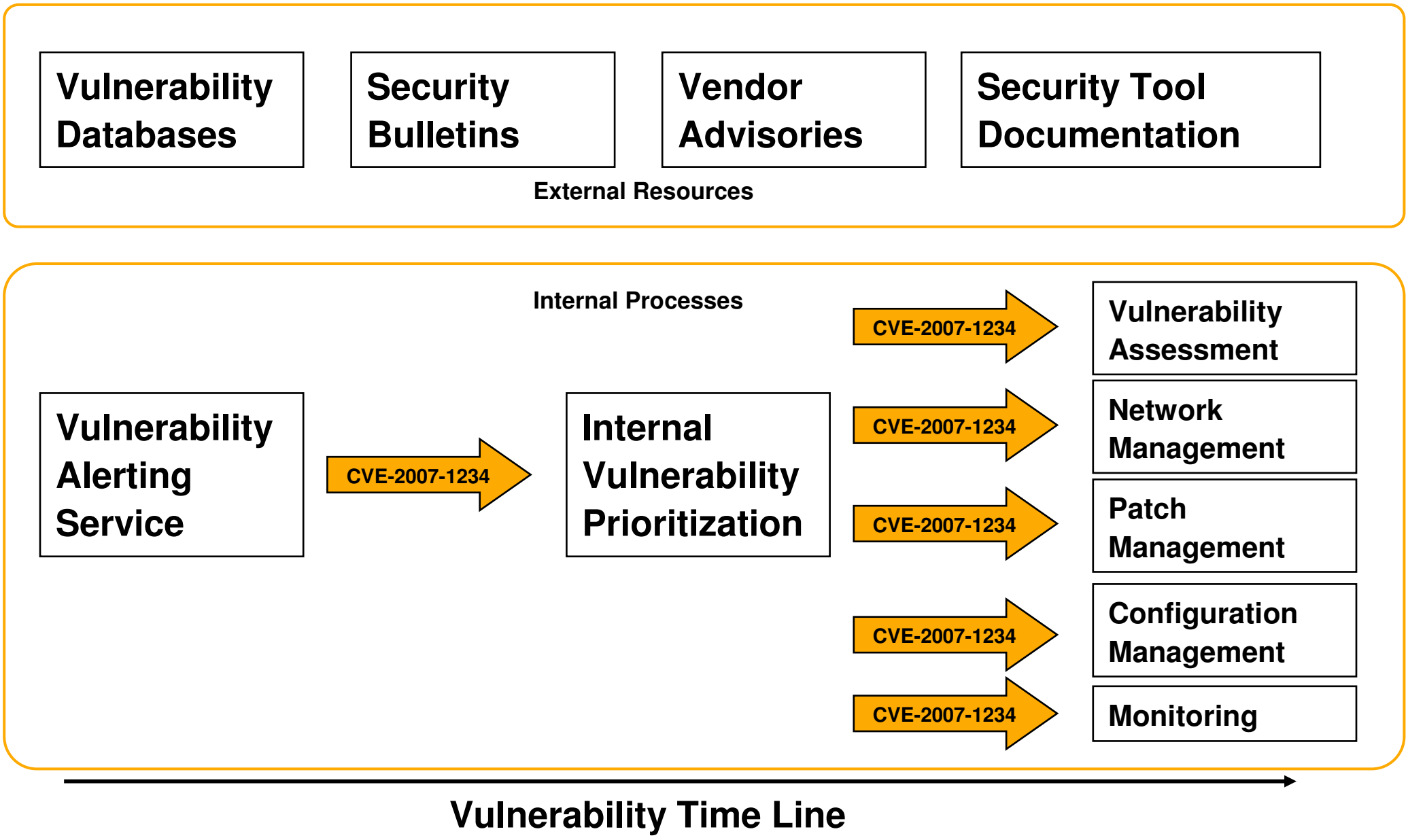
- Compatibility Ensures
  - Data presented with CVE ids
  - Can find data with CVE ids
  - Use of CVEs is complete and accurate

CVE Is …
Industry Collaboration – Editorial Board

CVE Is…
A Well Established Program

- Founded in 1999
  - Over 25,000 vulnerabilities identified
- Led by the MITRE Corporation
  - Federally Funded Research and Development Center (FFRDC)
  - Chartered to work in public interest
  - Prohibited from competing with industry
- Sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security
- More information at cve.mitre.org

CVE in the Enterprise
CVE Based Vulnerability Management



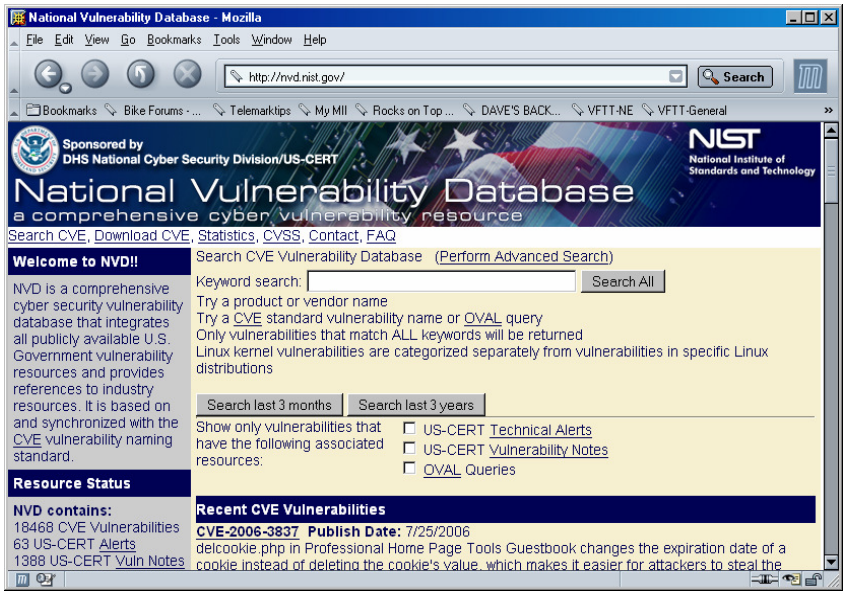
CVE in the Enterprise
Benefits of a CVE-Enabled VM Process

- Coordinate your people and processes
  - Speak the same language across groups with CVE
- Inform your people
  - Better access to external vulnerability related information with CVE
- Equip your people
  - Utilize CVE Compatible products and services
- CVE enables…
  - … fast & accurate correlation of vulnerability information across different data sets and tools
  - … fast & accurate coordination of people and processes

CVE in the Enterprise
Compatible Products

- More information on Compatible Products at http://cve.mitre.org/inuse/index.html

- HIGHLIGHTED PRODUCT
  NIST's National Vulnerability Database (NVD)
  - Available on-line at http://nvd.nist.gov/nvd.cfm
  - Robust search capability for CVE data set
  - Cross-links to US-CERT Alerts and Vuln Notes
  - Cross-links to OVAL definitions
  - CVSS scores
  - Fix and patch information
  - Sponsored by DHS



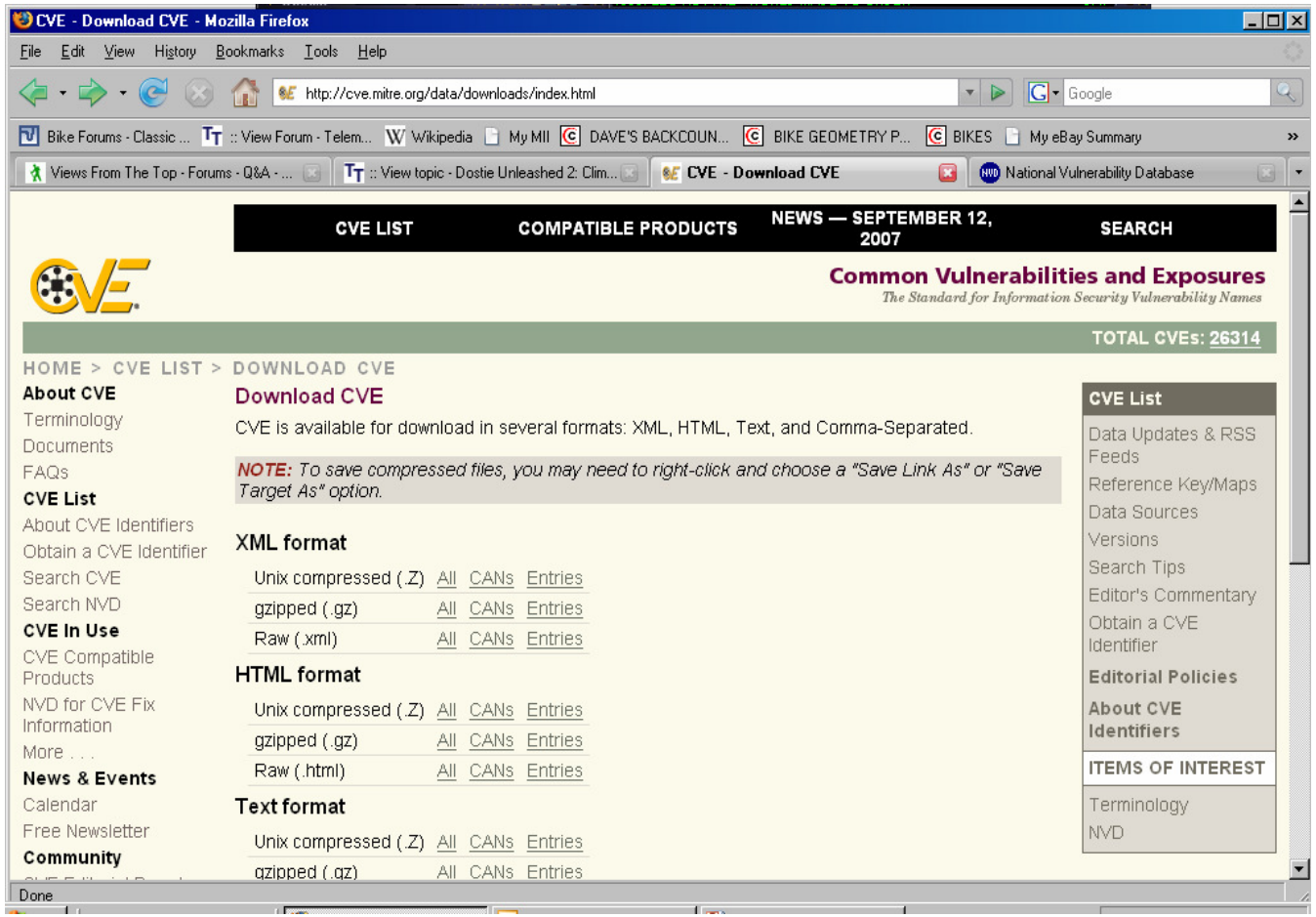
MITRE

CVE in Products & Services
Benefits of CVE Use & Compatibility

- Provides immediate, real process-level value to end customers
- Incorporation of mature standard provides higher perception of trust and maturity to products
- High value first step towards SCAP
  - Relatively low cost (text and hyper-links)

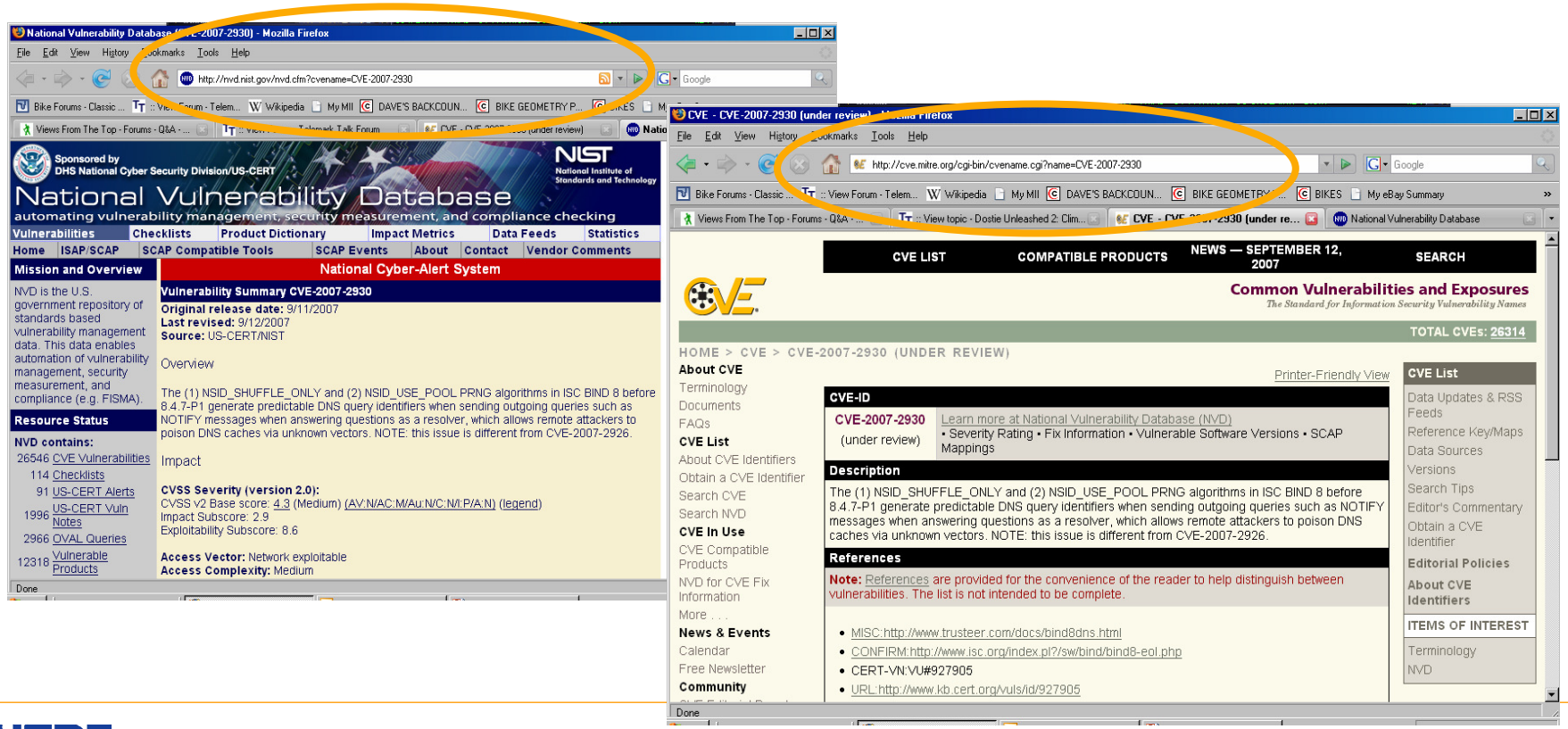
CVE in Products & Services
Steps Toward CVE Use & Compatibility

- **Get official CVE dataset from MITRE**
  - **Available for download at http://cve.mitre.org/cve/cve.html**
  - **Formats: XML, HTML, Text, CSV**



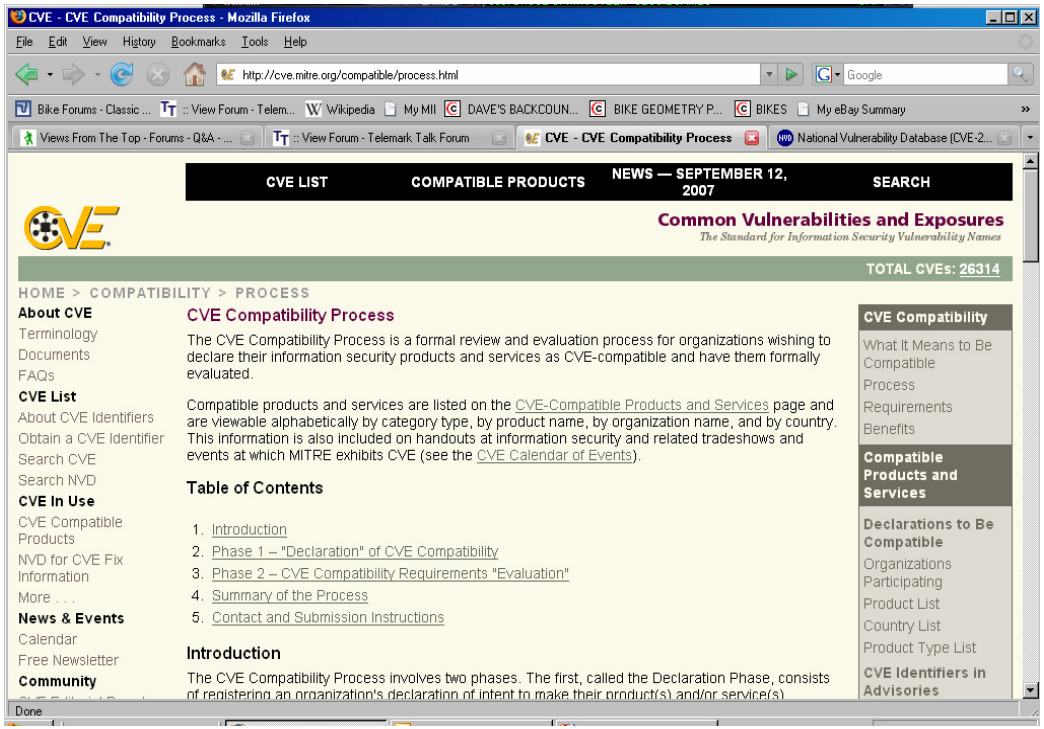
CVE in Products & Services
Steps Toward CVE Use & Compatibility

- **Map your proprietary data to CVE**
  - **Requires human analysis**
- **Add CVE ids to proprietary data**
  - **Can be added as simple tags in text fields**
  - **CVE and NVD web sites provide stable hyper-link structures**



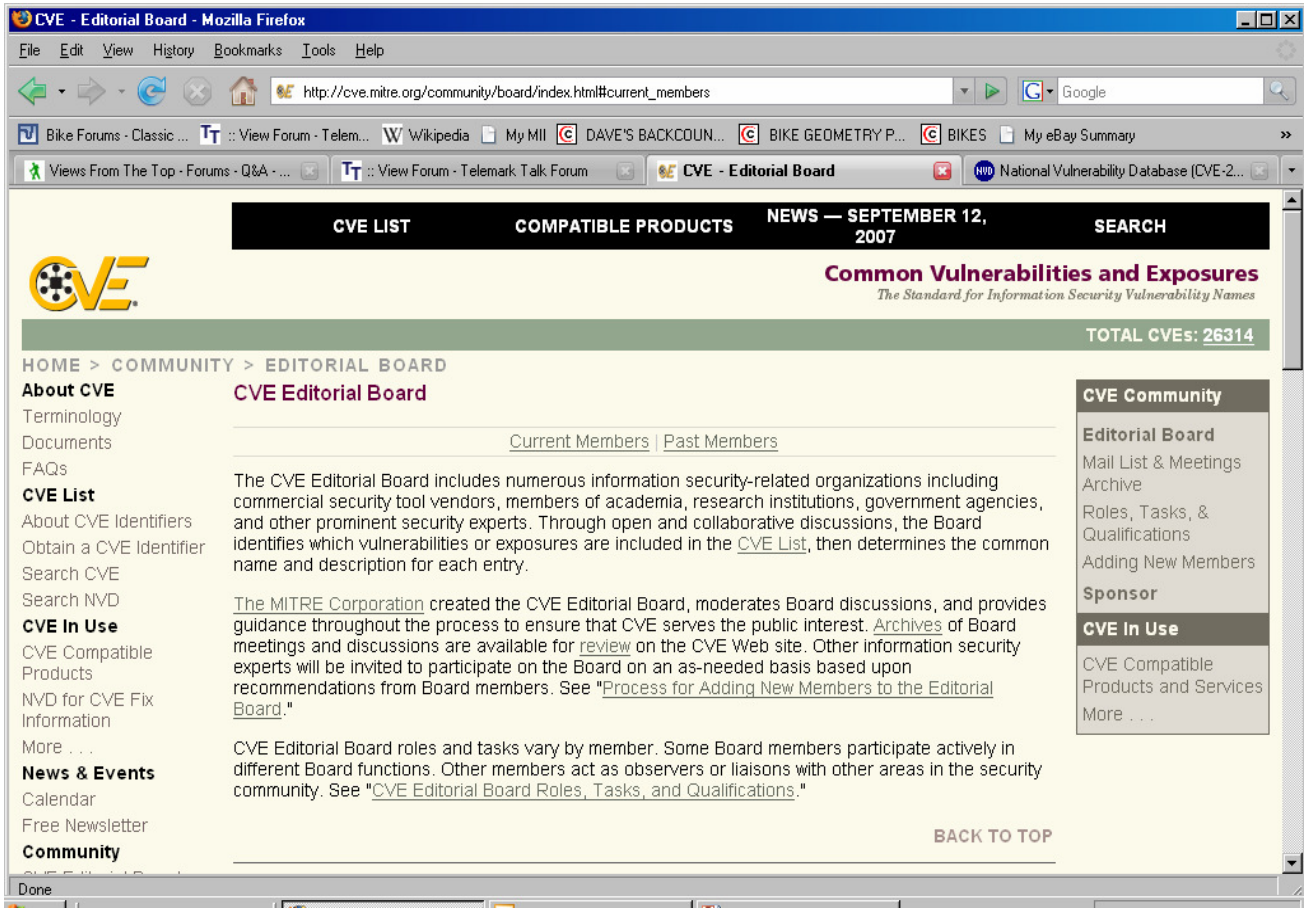
CVE in Products & Services
Steps Toward CVE Use & Compatibility

- **Provide CVE lookup capability**
  - **Allows users to find CVE related information in your product**
- **File for CVE Compatibility**
  - **More info at: http://cve.mitre.org/compatible/process.html**
  - **Contact information: cve@mitre.org**



CVE in Products & Services
Steps Toward CVE Use & Compatibility

- **Participate in CVE Editorial Board**
  - **Open Meeting on Friday, September 21 at 11:00 am at NIST**
  - **More info at: http://cve.mitre.org/community/board/index.html**



Summary

- CVE Is…
  - … Common identifiers for vulnerabilities
  - … Used in over 300 vulnerability products and services
- CVE in the Enterprise
  - Incorporate CVE in internal processes
  - Enable fast & accurate correlation of vulnerability information
  - Enable fast & accurate coordination of people and processes
- CVE in Products & Services
  - Low barrier to entry
  - High value to end customers
  - Tangible first step towards SCAP

QUESTIONS

Common Configuration Enumeration

MITRE

Starting Points

- **Motivating Questions:**
  1. What is a CCE?
  2. What are the problems that motivate the creation of CCEs?
  3. How will CCE help to solve the problems?

- **Motivating configuration statements:**
  - The required permissions for the directory %SystemRoot%\System32\Setup should be assigned
  - Never add user passwords to the users.conf file through a text editor
  - The "account lockout threshold" setting should be configured correctly
  - Use strong passwords
  - The startup type of the Remote Shell service should be set correctly

What Is CCE? – Basic Concept (1/6)

- Definition 1 – CCE assigns common identifiers (tags) to single configuration statements to allow for fast, accurate correlation across different repositories such as:
  - Security guides
  - Benchmarks (XCCDF/OVAL)
  - Vendor guidance documents and documentation
  - Configuration Assessment tools (and manual audit reports)
  - Configuration Management tools
  - Consolidated Reporting systems

- EXAMPLE
  - CCE-658
  - Definition: The "account lockout threshold" setting should be configured correctly
  - Parameters: number of attempts

What Is CCE? – Practical Meaning (2/6)

- **Definition 2 – If a configuration issue can be verified by an assessment tool or applied by configuration management system, it should be assigned a CCE id**

- **Should Get CCEs:**
  - **The required permissions for the directory %SystemRoot%\System32\Setup should be assigned**
  - **The "account lockout threshold" setting should be configured correctly**
  - **The startup type of the Remote Shell service should be set correctly**
- **Should NOT Get CCEs:**
  - **Never add user passwords to the users.conf file through a text editor**
  - **Use strong passwords**

What Is CCE? – Guidance Resource (3/6)

- Definition 3 – CCE is a forum of industry experts (CCE Working Group) and lessons learned (Content Decisions) that can be leveraged by configuration guidance authors to allow content to be written in manner that facilitates better technical implementation

- Example: Use strong passwords
  - The "minimum password age" setting should meet minimum requirements. (CCE-324)
  - The "minimum password length" setting should meet minimum requirements. (CCE-100)
  - The "password must meet complexity requirements" setting should be configured correctly. (CCE-633)
  - The "enforce password history" setting should meet minimum requirements. (CCE-60)
  - The "store password using reversible encryption for all users in the domain" setting should be configured correctly. (CCE-479)

What Is CCE? – Entries Defined (4/6)

CCE-299

Definition: The "restrict guest access to application log" policy should be set correctly.

Technical References (1 or more):

(1) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\RestrictGuestAccess
(2) defined by Group Policy

Parameters (1 or more): (1) enabled/disabled

- **Standardized Identifier - Similar to existing CVE and CME**
- **Definition - Describes the configuration control…**
  - **… but does not assert a recommendation**
- **Technical References - Describes mechanisms used to achieve the intended affect**
- **Parameter – Describes conceptual range of values**

What Is CCE? – Parameters (5/6)

- GOAL: Comparable configuration settings get same CCE
- Example: Different parameter values
  - Comparable statements:
    - DISA Gold Disk Tool for W2K:
      Account logon lockout threshold = 3
    - CIS Level 1 Benchmark for W2K:
      Account logon lockout threshold = 50
  - Unifying CCE:
    - CCE-123: The maximum number of failed login attempts should meet minimum requirements
    - Parameter: Maximum number of attempts

What Is CCE? – Technical References (6/6)

- GOAL: Comparable configuration settings get same CCE

- Example: Different technical references
  - Comparable statements:
    - Windows 2000 Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD
    - Windows XP Local Security Policy: Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL
    - Windows VISTA Group Policy Object Editor: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL
  - Unifying CCE:
    - CCE-133: The "Disable CTRL+ALT+Delete Requirement for Logon" policy should be set correctly.
    - Parameter: Enabled or disabled

Problem & Solution (1/2): Add Clarity to Guidance

- PROBLEM – Traditional configuration guidance documents lack sufficient detail to facilitate consistent technical interpretation and implementation
- SOLUTION – Inclusion of CCEs in guidance documents can:
  - Augment prose with “atomized” configuration specifics
  - Prompt guide authors to add configuration specifics necessary for consistent technical implementations
  - Provide lightweight “structure” to document configuration specifics
- PROSE: Use strong passwords
- SUPPORTING CCEs
  - The "minimum password age" setting should meet minimum requirements. (CCE-324)
  - The "minimum password length" setting should meet minimum requirements. (CCE-100)
  - The "password must meet complexity requirements" setting should be configured correctly. (CCE-633)

Problem & Solution (2/2): Fast, Accurate Correlation

- PROBLEM – There is a growing need to correlate configuration data across multiple sources…
  - Configuration Guides (e.g. NSA, STIGs)
  - Vendor Documentation (e.g. MS TechNet)
  - System Audit Tools (e.g. DISA Gold Disk, eEye)
  - Configuration Management Tools (e.g. Citadel, Tivoli)
  - Consolidated Reporting Tools (e.g. DISA VMS)

- …But it is impossible to quickly and accurately correlate configuration issues

- SOLUTION – Tag configuration atoms with CCE IDs
  - Easily added in reference fields
  - Common identification enables correlation

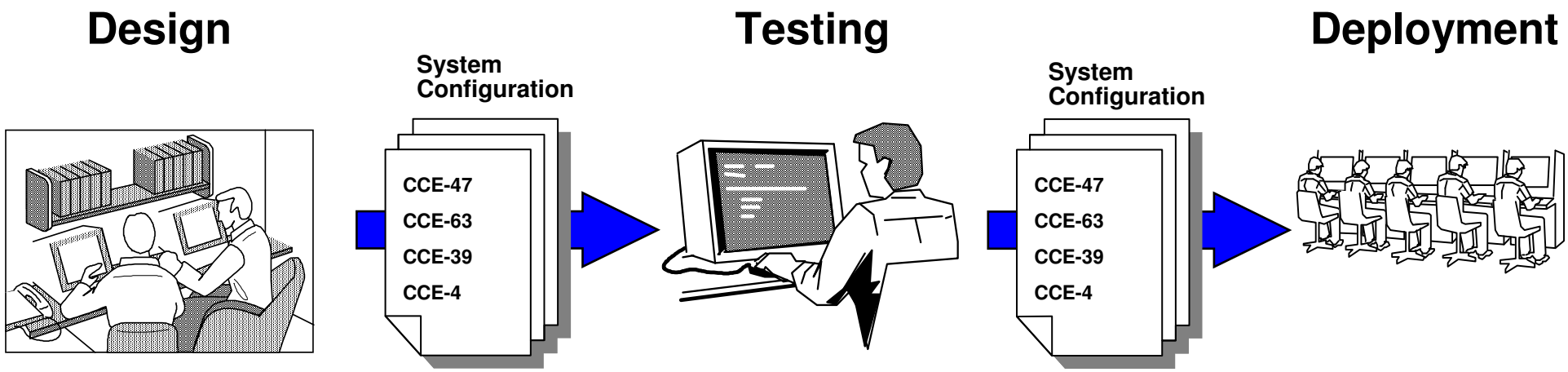
Use Case – System Design (1/5)

- SCENARIO – System designer working to merge configuration guidance with local operational constraints. She needs to find more information about a configuration issue and its ramifications. She will look for this information in sources such as:
  - Vendors technical support resources
  - Other 3rd party configuration guides
  - Peer groups and discussion forums

- DISCUSSION EXAMPLES:
  - Use strong passwords
  - The "minimum password age" setting should meet minimum requirements. (CCE-324)

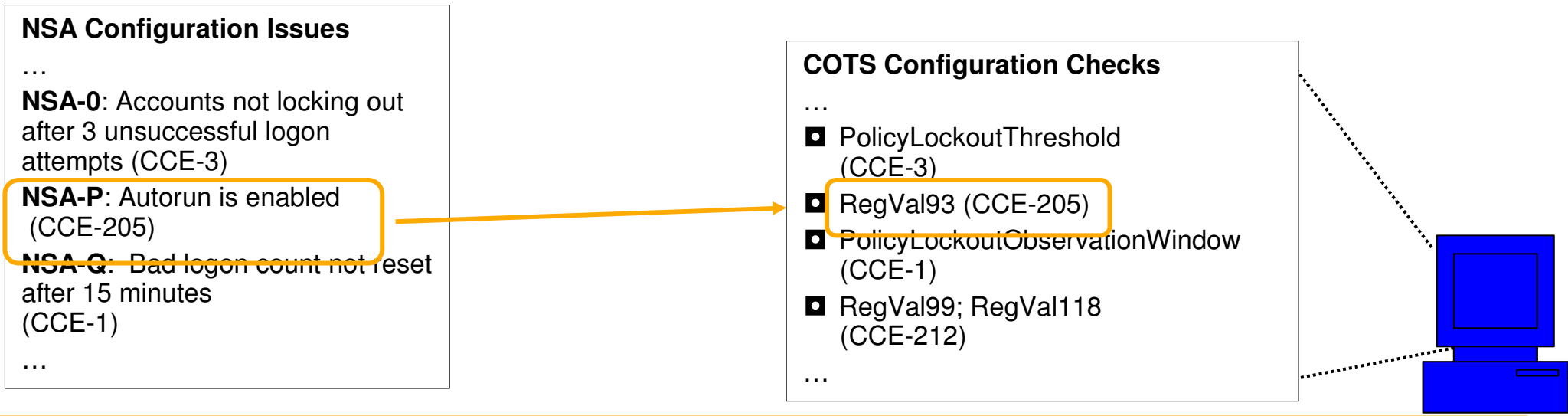
Use Case – Configuration Management (2/5)

- **SCENARIO – An organization has different groups responsible for system design, testing and deployment. These groups need to be able to communicate quickly and accurately about different configuration controls. Portions of these processes are becoming automated.**
- **DISCUSSION EXAMPLES:**
  - **Use strong passwords**
  - **The "minimum password age" setting should meet minimum requirements. (CCE-324)**



Use Case – System Audit (3/5)

- **SCENARIO – An auditor is creating an audit plan for a system based on the security guide. He must interpret prose based statements and convert them into specific technical findings statements. When available, he must identify checks in available products that will test systems for auditable configuration settings.**
- **DISCUSSION EXAMPLE:**
  - **Windows CD Autorun**

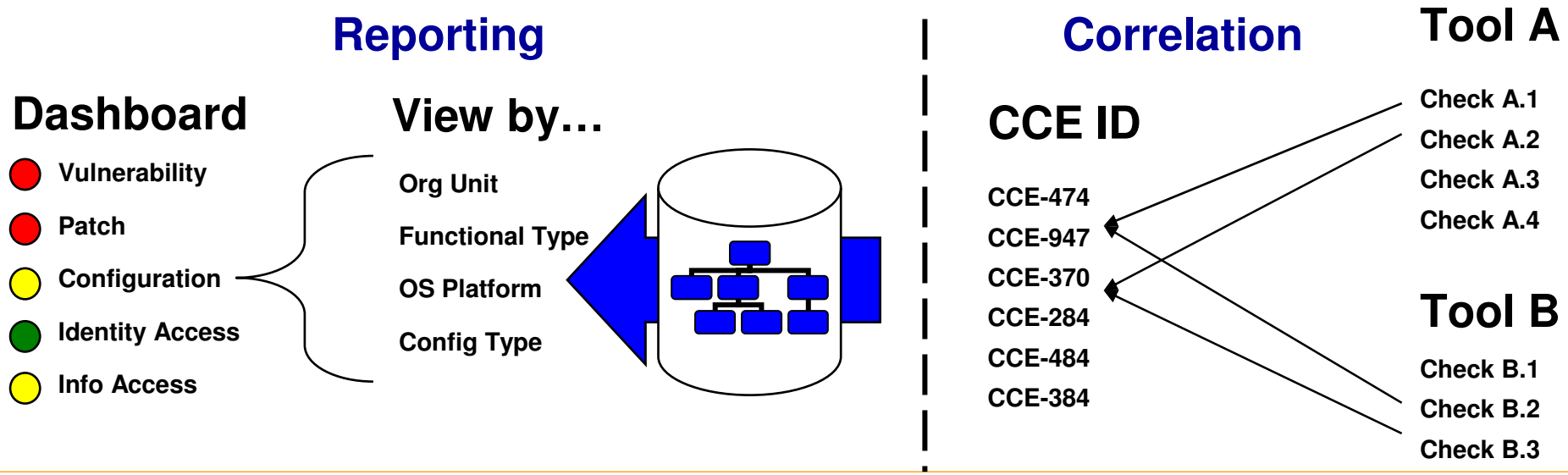


MITRE

Use Case – Consolidated Reporting (4/5)

- **SCENARIO – A manager is responsible for consolidating system audit reports on the same platform or application based on data from multiple sources including:**
  - **Manual system audits**
  - **Commercial Assessment Products (numerous)**

  However, the configuration findings are all identified with proprietary names. Correlating the data is expensive and error prone.



MITRE

Use Case – Compliance / C&A (5/5)

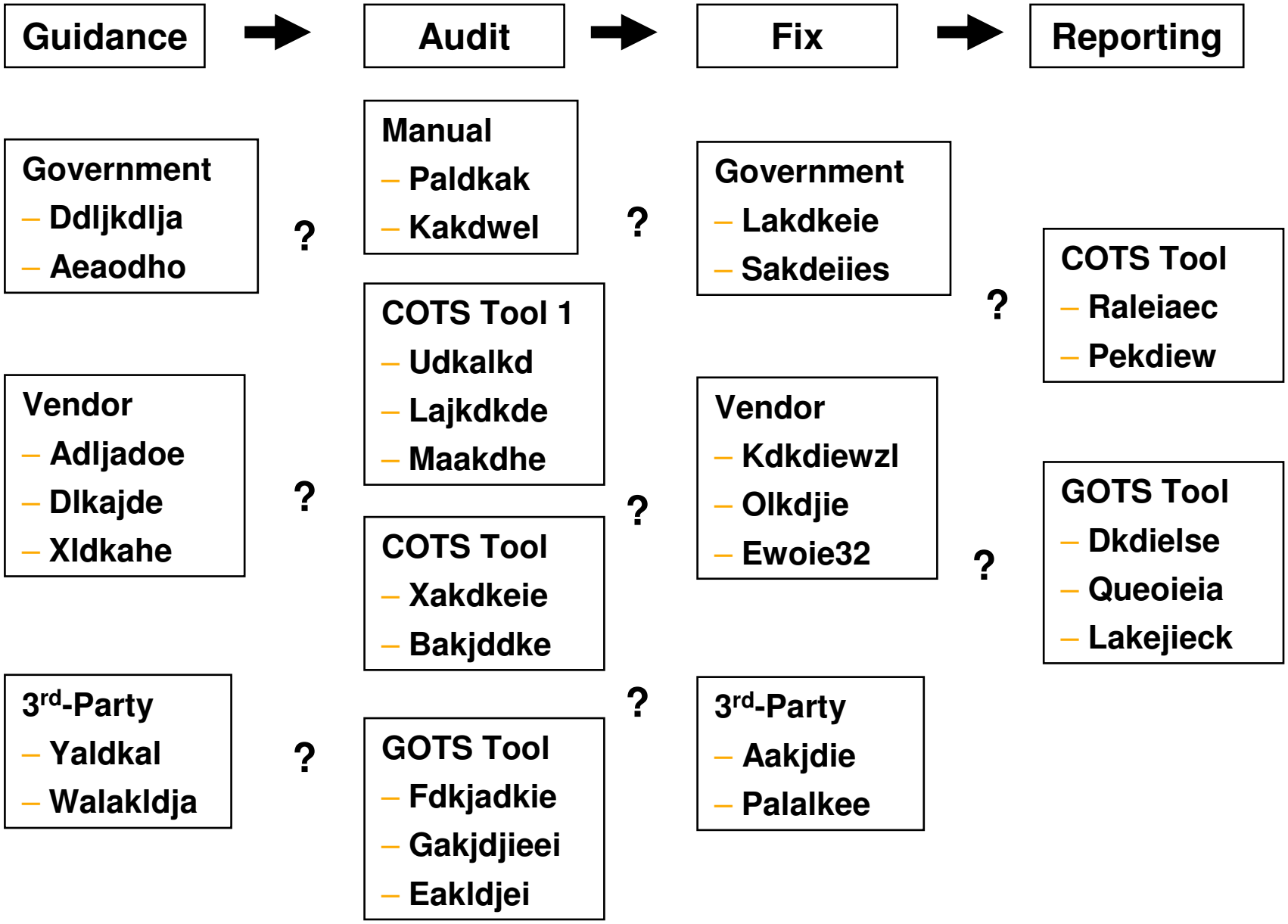
- **SCENARIO: A CISO or system owner must demonstrate that she has implemented appropriate configuration controls to meet regulatory or certification requirements. The relationships between requirements and controls may be many to many. Because there is no standardized way to reference controls, the auditor or certifier has difficulty understanding the system owner's control decisions and how they support the requirements.**

CCE provides common language

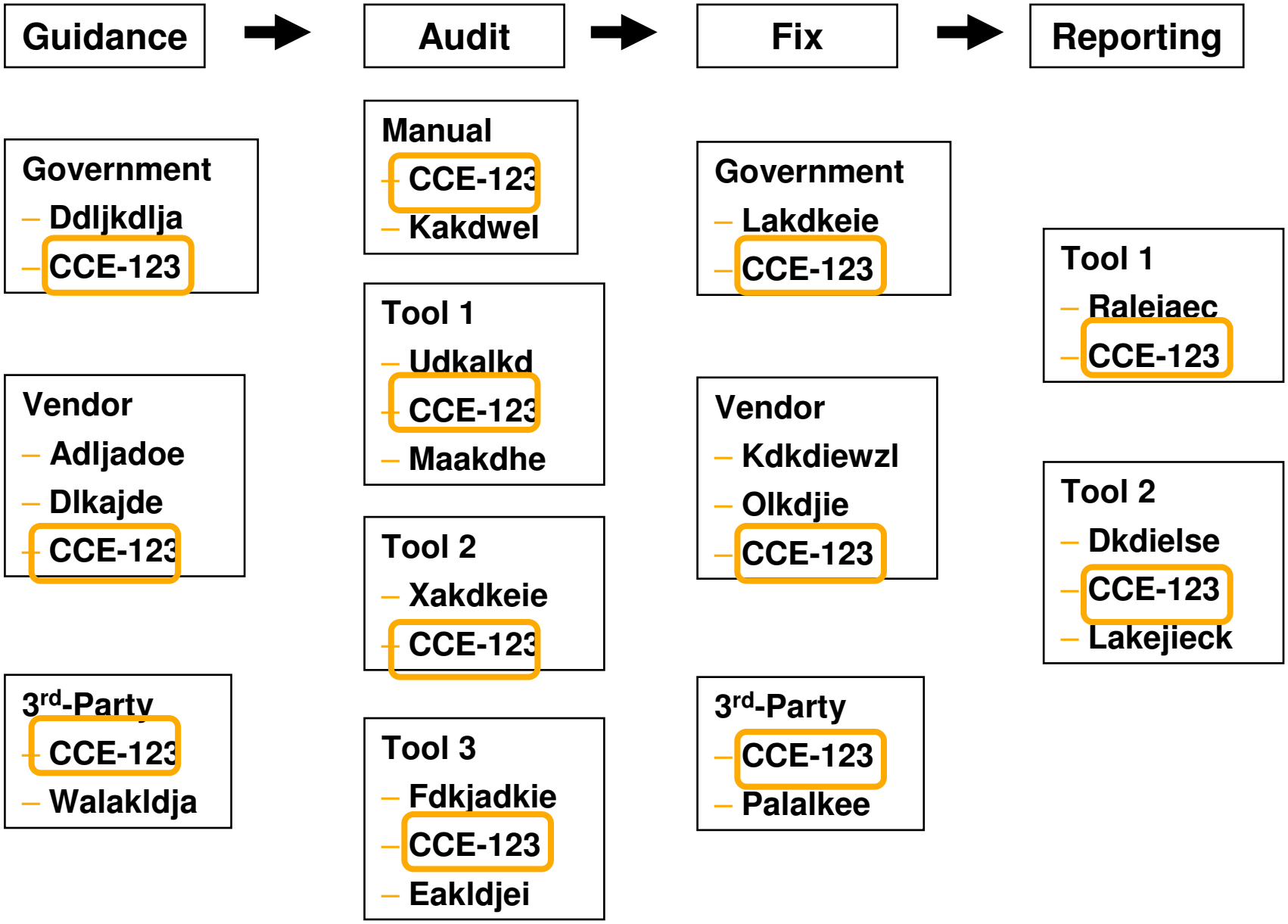
sp 800-53 Requirements	MAPPING	Configuration Controls
Security Requirement No. 1	1 TO 1	CCE-435
Security Requirement No. 2	1 TO MANY	CCE-246, CCE-993
Security Requirement No. 3 Security Requirement No. 4	MANY TO 1	CCE-169
Security Requirement No. 5 Security Requirement No. 6	MANY TO MANY	CCE-243, CCE-135, CCE-187

TABLE 2: SAMPLE REQUIREMENTS TRACEABILITY MATRIX

The Guidance Life-cycle Without CCE (1/2)



The Guidance Life-cycle With CCE (2/2)



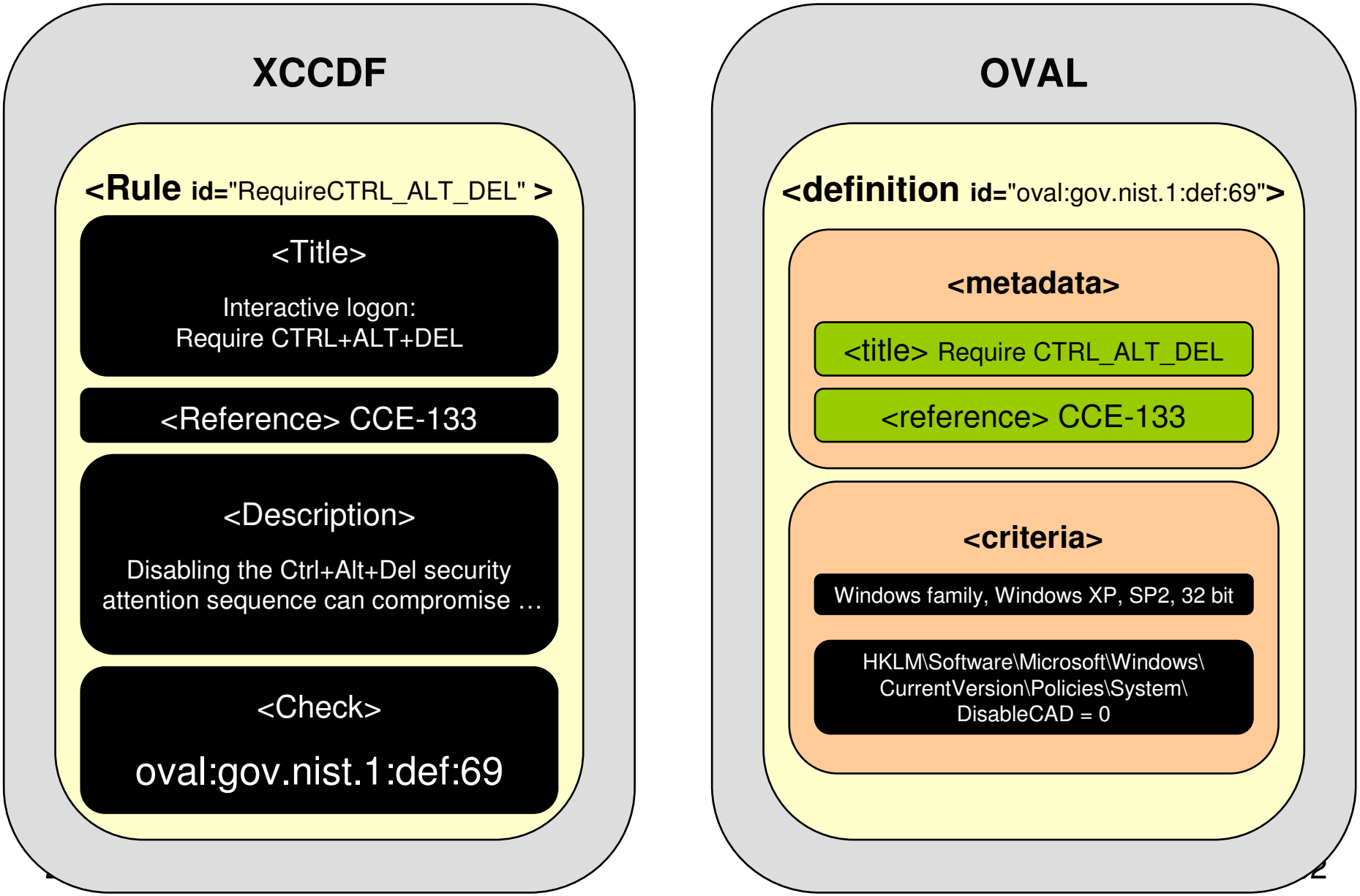
CCE Status – (1/2)

- CCE Working Group
  - ArcSight, Big Fix, Configuresoft, CERIAS-Purdue, Center for Internet Security, Citadel, DISA, eEye, Modulo Security (Brazil), nCircle, NIST, NSA, TriSixty, Microsoft, PatchLink, Secure Elements, Sun, Symantec, ThreatGuard, University of Nebraska-Omaha
  - MITRE Contact: cce@mitre.org
- Windows CCE List v4.0
  - Over 900 issues for: W2K, XP & Win 2003, VISTA, IE7, Office
  - Cross references for: Center for Internet Security Benchmarks, DISA Stigs & GoldDisk, NSA Security Guides, NIST S-CAP, Microsoft Security Guides
  - Download at: http://cce.mitre.org

CCE Status – Future Directions (2/2)

- Unix/Linux
  - Level of Abstraction
  - Agreement on core issues
- Synonyms and related issues
  - Minimum password length
  - There exists accounts with null passwords
- Higher level configuration statements
  - Needed for roll-up
- Scalable CCE creation and modification
  - Create CCEs at guidance authoring
  - Wikipedia or Web 2.0 model?

XCCDF-OVAL Connection



QUESTIONS

Common Platform Enumeration

MITRE

CPE Use Cases

- Common Names
  - different tools sharing information
- Matching
  - different levels of abstraction

Overview

- CPE Name
  - identifies a platform type
    - does not ID a system
  - ideally associated with an OVAL Inventory Definition
- CPE Language
  - used to combine CPE Names to identify complex platform types
- CPE Dictionary
  - collection of known CPE Names

Status

- 2.0 official release
  - Friday September 14th
  - specification and dictionary available
  - dictionary based on NVD product dictionary
  - http://cpe.mitre.org/

CPE Name Format

- repeatable format
  - 2 people in different rooms will come up with the same name

- name is built by using known information
  - 7 (optional) components

cpe:/ part : vendor : product : version : update : edition : language

Part

cpe:/ **part** : vendor : product : version : update : edition : language

h = hardware part

o = operating system part

a = application part

Vendor

cpe:/ part : **vendor** : product : version : update : edition : language

- **organization-specific label of DNS name**
  - **should already be unique**

Organization Full Name	DNS Domain	CPE component
Cisco Systems, Inc.	**cisco.com**	**cisco**
The Mozilla Foundation	**mozilla.org**	**mozilla**
University of Oxford	**oxford.ac.uk**	**oxford**

Examples

cpe:/a:zonelabs:zonealarm_internet_security_suite:7.0

cpe:/o:redhat:enterprise_linux:3

cpe:/o:microsoft:windows-nt:xp:sp2:pro

cpe:/a:adobe

cpe:/a:jon_smith:tool_name:1.2.3

Prefix Property

- set of platforms identified by a long name should be a subset of the set of platforms identified by a shorter initial portion of that same name
  - called the “prefix property”
  - allows matching to take place

For example:

cpe:/o:microsoft:windows-nt:xp:sp2

would be a subset of

cpe:/o:microsoft:windows-nt:xp

OVAL's Use of CPE

- inventory definitions
  - reference metadata
- <affected> element
  - identify platforms that definition targets
  - not in version 5.3
    - added <affected_cpe_list> to xsd:any
- would like to make this part of criteria
  - current split leads to confusion

XCCDF's Use of CPE

- profile, group, rule
  - identify target platforms
- Example
  - a guide might have one rule apply for Windows XP systems and another rule apply for Windows Vista systems

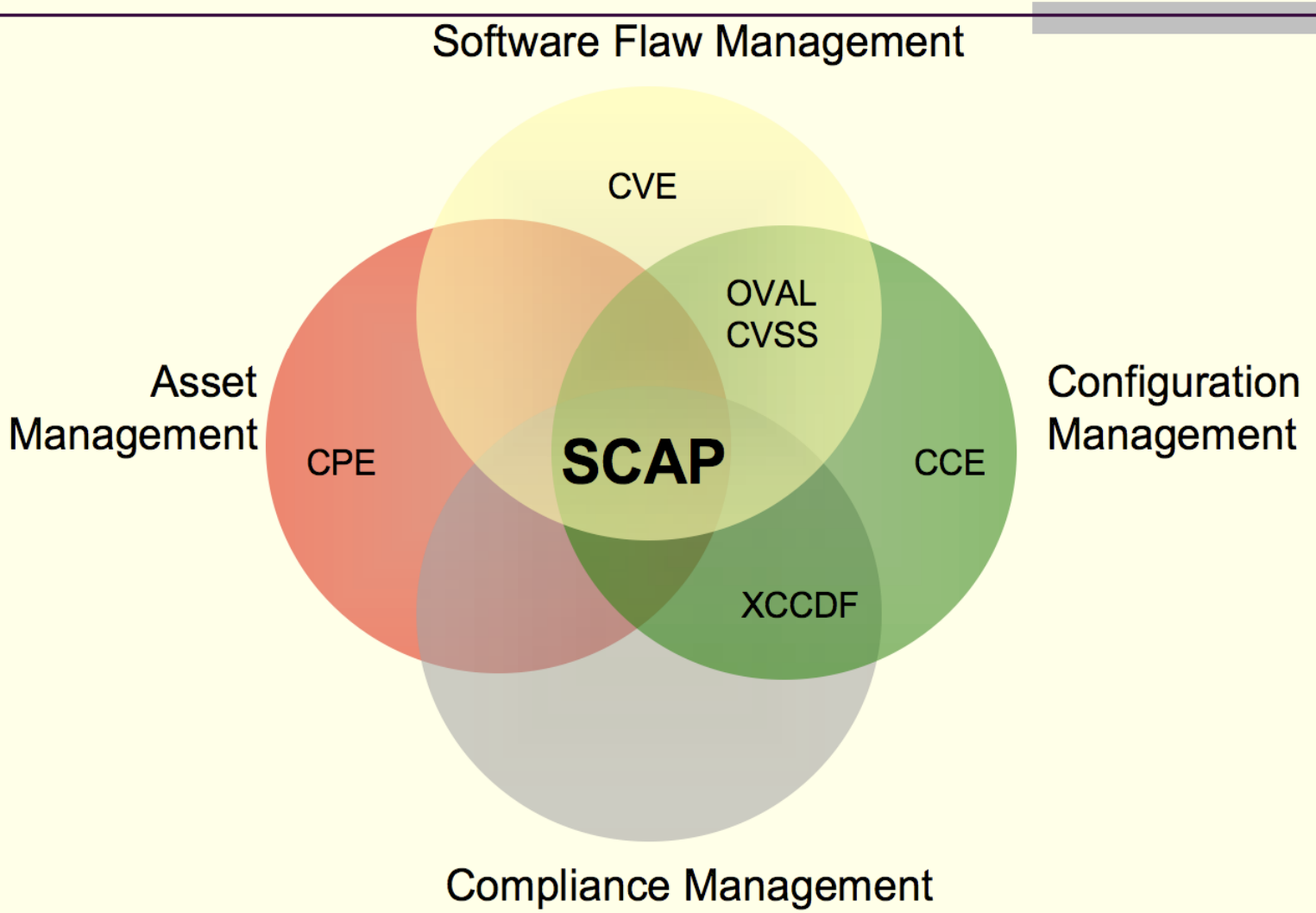
Challenges

- Dictionary Support
  - contributions from vendors
  - quality
- Boundaries of CPE
  - What problems are we trying to solve and what problems are we NOT trying to solve?

CPE Resources

- Web site: http://cpe.mitre.org
- Mailing list: cpe-discussion-list
  - Open forum for developing the specification
  - registration form
    - http://cpe.mitre.org/registration.html

SCAP Interoperability



QUESTIONS