“Whoever finds it, names it”
• English = “apple”
• French = “pomme”
• Spanish = “manzana”
• Russian = “яблоко”
• Japanese = “リンゴ”
• German = “apfel”
Difficult to Integrate Information
Common Identifier Needed

Standardization of terms will allow for seamless communication.
What do we mean by standardization?

- Community Consensus
- Open Content
- Common Identifier (cross-reference)
- Common Understanding (known format)
Enumerations Defined

• a naming scheme
  – specific entities identified using a common term
• defined set of things
  – seen to be members of the same category
• used by multiple groups
  – communicate with each other
  – coordinate activities
• just enumerate the entities
  – trying to do more leads to many problems related to different use cases

By keeping things simple, we can accomplish a lot.
Benefits of Enumerations

• Enable faster, more accurate correlation
  – Standardized identifiers used in:
    • Databases
    • Tools
    • Guidance

• Facilitate information exchange
  – Requirements – what do we need to check for?
  – Reporting – what did we find?
  – Roll-up – how do standard elements map to local needs?
  – Information more easily flows:
    • Across the configuration management lifecycle
    • Through different communities of interest

• Allow increased automation
  – Diverse tools can share input and output
IA Data Without Enumerations

• data correlation is:
  – Mostly manual
  – Key word driven
  – Costly
  – Error prone
  – Pair-wise between data sets
  – Unscalable

• result:
  – Data is locked in proprietary repositories
common identifiers:

- Community agree upon “tags”
- Easily added to legacy repositories & tools

KEY: common identification enables correlation!

- Faster
- More accurate
- Less expensive
• CVE - Vulnerabilities
  – CVE-2006-4838
    Description: Multiple cross-site scripting (XSS) vulnerabilities in DCP-Portal SE 6.0 allow remote attackers to inject arbitrary web script or HTML via the (1) root_url and (2) dcp_version parameters in (a) admin/inc/footer.inc.php, and the root_url, (3) page_top_name, (4) page_name, and (5) page_options parameters in (b) admin/inc/header.inc.php

• CCE - Configuration Settings
  – CCE-2116-2
    Description: The "restrict guest access to application log" policy should be set correctly.
    Parameters: enabled/disabled

• CPE - Platforms
  – cpe:/o:microsoft:windows_xp:::pro
    Title: Microsoft Windows XP Professional
Common Platform Enumeration (CPE™)

• 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
<table>
<thead>
<tr>
<th>Sponsor</th>
<th>NSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Type</td>
<td>Open Working Group</td>
</tr>
<tr>
<td>Maturity</td>
<td>- Concepts mature, content in development</td>
</tr>
<tr>
<td></td>
<td>- Version 2.1 released Jan 31, 2008</td>
</tr>
<tr>
<td>Adoption</td>
<td>- Early stages</td>
</tr>
<tr>
<td></td>
<td>- Used by NVD, FDCC</td>
</tr>
<tr>
<td></td>
<td>- 7 SCAP Validated products</td>
</tr>
</tbody>
</table>
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

```
```
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_xp::sp2```

would be a subset of

```cpe:/o:microsoft:windows_xp```
• Collection of known CPE Names
  – help users determine which names exists
  – help those creating new names
  – enough information to identify the platform
    • others can build more elaborate repositories based off dictionary

• Hosted by NIST at:
  http://nvd.nist.gov/cpe.cfm
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
• Dictionary of standardized descriptions for vulnerabilities and exposures
  – Over 31,000 entries
• Publicly accessible for review or download from the Internet

**ID:** CVE-2007-1751  
**Description:** 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."

**Reference:** BUGTRAQ : 20070612 ZDI-07-038 - Microsoft Internet Explorer
  - Prototype Dereference Code Execution Vulnerability

**Reference:** MS : MS07-033
# CVE Status

<table>
<thead>
<tr>
<th>Sponsor</th>
<th>DHS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Type</td>
<td>Editorial Board</td>
</tr>
<tr>
<td></td>
<td>- Membership by invitation / nomination</td>
</tr>
<tr>
<td>Maturity</td>
<td>Mature</td>
</tr>
<tr>
<td>Adoption</td>
<td>Widespread</td>
</tr>
<tr>
<td></td>
<td>- Over 280 products in 27 countries</td>
</tr>
<tr>
<td></td>
<td>- Over 80 officially compatible</td>
</tr>
</tbody>
</table>
Leveraging CVE compatibility
CVE List

• List of all known CVE identifiers
  – 32,261 (as of sept 10, 2008)
  – hosted at http://cve.mitre.org
  – xml feed

• NVD at NIST provide full search capabilities
  – additional metadata
The Center of Many Activities

- ISS X-Force, Security Focus, NIST ICAT, More to come...
- CERIAS, Ernst & Young
- Academic, Articles, and Conf. Presentation
- SANS, CERIAS
- ISS, CERT/CC,BindView, Others
- Private Databases
- Public Databases
- Advisories
- 51 Articles ~5 Languages
- Press
- common Problems
- SANS
- Top Twenty List
- Other
- ID S, Assessment, Comparison
- Tools & Services
- Incident reporting, Translations, “Comprehensive” info source
- © 2008 The MITRE Corporation. All rights reserved
Assigns standardized identifiers to configuration issues, allowing comparability and correlation

**ID:** CCE-3121-1

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

**Technical:**
(1)HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\RestrictGuestAccess

**Mechanisms:**
(2) defined by Group Policy

**Parameter:** enabled/disabled
<table>
<thead>
<tr>
<th>Sponsor</th>
<th>NSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Type</td>
<td>Open Working Group</td>
</tr>
</tbody>
</table>
| Maturity       | - Concepts mature, content in development  
|                | - Version 5 released Mar 5, 2008 |
| Adoption        | - Early stages  
|                 | - Microsoft security (Office 2007, Server 2008)  
|                 | - Primary identifier for FDCC  
|                 | - 7 SCAP Validated products |
The use of CCE-IDs as tags provide a bridge between natural language, prose-based configuration guidance documents and machine-readable or executable capabilities such as configuration audit tools.

- last digit is a check digit
- assigned on per platform basis
Descriptions

• a humanly understandable description of the configuration issue

• describes the configuration control
  – but does not assert a recommendation
Technical Mechanisms

• the technical setting that is being identified
  – for any given configuration issue there may be one or more ways to implement the desired result

• specific mechanisms
  – registry keys
  – group policy paths
  – api calls
Parameters

• parameters that would need to be specified in order to implement a CCE on a system
  – describes the possible values or the conceptual range of values

• the human readable notation
  – “enabled” instead of “1”
Enumerations - Creation

- content teams ensure uniqueness
- leverage vendor and community knowledge
- regular updates to official lists
- feedback channel to report issues
When dealing with information from multiple sources, use of consistent identifiers can

– improve data correlation
– enable interoperability
– foster automation
– and ease the gathering of metrics for use in situation awareness, IT security audits, and regulatory compliance.