Common Configuration Enumeration (CCE)

David Mann

Joseph A. Sain

9 July 2012

MITRE

Agenda

- Overview
- CCE Content
- Outreach
- Progress
- CCE Infrastructure
- Four Hard Problems

CCE Overview

- CCE provides unique identifiers to security-related system configuration issues
- Facilitates correlation of configuration data across multiple information sources and tools.
- Consistent identifiers address the following 5 use cases:
  - Guide Document Authoring and System Design
  - Configuration Management Life Cycle
  - Configuration Audit Tool Configuration
  - Audit Tool Result Integration
  - Regulatory Compliance

Outreach

- Cisco IOS
  - CCE team is working with Cisco to develop CCE submission candidates for IOS Release Trains
- Center for Internet Security
  - Engaged in discussions with CIS in the development of a tool that produces CCE output from CIS Benchmarks
- DISA
  - Working with DISA in the development of CCE submissions that reference the DISA STIGs

Progress

- Three new platform groups released
  - Polycom HDX, Microsoft Exchange 2007, Microsoft Exchange 2010
- New platform groups nearing completion
  - Apache (Linux), Tomcat
- Updates to most other platform groups in progress
- Participating in NSA-led Creating SCAP Content team
  - Chartered with assigning CCEs to DISA STIGs
  - Several new platform groups to result from this effort, including Apache (Windows), SQL Server, JBoss
  - Microsoft SCM Windows 7 CCE content complete, awaiting publicly available reference source
- Revision to CCE Content Decisions document nearing completion

CCE Infrastructure

- Developing a corporate application that will:
  - Ingest CCE candidate spreadsheets
  - Load them into a MySQL database
  - Enable CCE Analysts to edit multiple CCEs
  - Using SOLR for Faceted searching across all platform groups
  - Output CCE Platform Groups in Excel and XML for publication
- Benefits:
  - Greatly reduce CCE content processing time
  - Enable more frequent CCE Releases
  - Facilitate consistency within and across platform groups
  - Streamline the publication process
- Expected to be released to production September 2012

Four Hard Problems for Discussion

- Publicly Available Reference Documents
  - No reference, no ID
- Proprietary IDs
  - Economics and Provisioning
  - Lessons Learned
- Platform Groups vs. Code Base Realities
  - Linux:
    - Kernel, Distro, 3rd Party supported code
  - Cisco Release Trains
    - "A vehicle for delivering Cisco software to a specific set of platforms and features"
      - Mainline train – Most stable release
      - Enterprise Train
      - Service Provider Train
      - Technology Train – New features and bug fixes
- CCE Content Decisions/Counting Issues

Publicly Available Reference Documents

- CCE has maintained that at least one publicly available reference document is required in order for a CCE to be valid
  - Essential for Audit Software Vendor Validation
- Online reference documents may not be permanently available
  - Sponsors have pulled their security guides
  - Microsoft Security Compliance Manager 2.5 Install package does not include their configuration baselines as downloadable documents (as in SCM 1.0)
- MITRE will continue to require that at the time of publication of the CCE submission, the reference document is publicly available
  - MITRE cannot guarantee subsequent availability of source documents

Proprietary IDs

- MITRE recommends all configuration information providers use and publish their own, proprietary IDs for configuration issues
- CVE Lessons Learned:
  1. Vulnerability info providers think in terms of "vulnerabilities"
     - Primary source vendors think in terms of their codebase, features, tech support articles or security guide sections
  2. Vulnerability info providers use proprietary IDs
     - Avoids CVE being the bottle neck and level of abstraction wars
     - Makes their information specifically referenceable
     - Configuration info providers don't provide IDs and content can't be referenced accurately
  3. CVE IDs are used as correlators, not primary keys
     - CCE IDs often have the unrealistic expectation of being universal ID for all things for all parties

Platform groups vs. Code Base Realities

- CCE content provisioning has increasingly involved primary source vendors who don't think like the configuration audit community
  - See issues in terms of code base branches, features, tech support efforts, 3rd party package integration
- Microsoft Security Content Manager is a hybrid between local security policy management and AD GPOs
  - Features come and go release to release
  - No way to reference them
- Red Hat Enterprise Linux is a collection of open source packages that are maintained outside of their control
  - Reuse of existing CCEs would make their lives easier
  - What then defines a RHEL Release?
  - Kernel, Distro, 3rd party supported code
- Cisco IOS release trains are dependent on hardware and deployment type
  - Major versions branch off into many sub-versions

MITRE

Counting Issue (1) – Default Objects

- **EXAMPLE: The following statements are appropriate CCE statements. Each of these statements should receive their own CCE.**
  - **The startup type of the Fax service should be configured correctly**
    - **Parameter 1: Start-up type (disabled, manual, automatic)**
  - **The startup type of the Alerter service should be configured correctly**
    - **Parameter 1: Start-up type (disabled, manual, automatic)**
  - **The startup type of the Clipbook service should be configured correctly**
    - **Parameter 1: Start-up type (disabled, manual, automatic)**
- **ISSUE: Should default objects be handled as parameters?**

CCE Content Decision (1)

- CD.H1 Individual Default Objects (Split)
- RULE: In those cases when the same configuration control can be associated with multiple default objects, a CCE id is assigned for the control as it applies to each individual default object. In such cases, the name for both the control and the individual default object should be identified in the CCE description.
- DISCUSSION: Default objects often have particular security relevance and are addressed individually. To facilitate this, CCE issues an id to each object.
- An object is considered default if it is an instance of an object that is created by the system with no user input.

Counting Issue (2) – Default sets

- **EXAMPLES:**
  - **CCE-14300-8 - Password hashes are shadowed or not shadowed for all accounts in /etc/passwd as appropriate.**

- **ISSUE: What is the relationship between grouping mechanisms (e.g. directories and user groups) and individual objects within that grouping mechanism (e.g. files and users)?**

CCE Content Decision (2)

- CD.H2 Default Sets of System Objects (Split)
- RULE: Some systems provide default grouping mechanisms for objects. The Administrators group of users on Windows systems is one such example.
- In those cases where the same configuration control can be associated with all system objects within a default system defined set, then separate CCE ids are assigned for each default set and the identity of the default set (which creates the context for each control) is included in the description of the CCE.
- The following template for the corresponding description may be used:
- The [control name] for all [system object type] in the [default group] should be configured correctly.

Counting Issue (3) – The “all” qualifier

- **EXAMPLE: The following statements receive the same CCE id:**
  - **The minimum password length for all users should be 8 characters.**
  - **The minimum password length for all users should be 12 characters.**
- **The description for the associated CCE id should be:**
  - **The minimum password length for all users should be configured correctly.**
- **ISSUE: Will we assign CCEs for configuration control statements based on the use of the “all” qualifier?**

CCE Content Decision (3)

- CD.H3 “All” System Objects (Include)
- RULE: In those cases where the same configuration control can be associated with all system objects of the same kind, then single CCE id is assigned for the control and the qualifier “all” is included in the description of the CCE along with the name of the type of system object.
  - The following template for the corresponding description may be used:
  - The [control name] for all [system object types] should be configured correctly.
- DISCUSSION: It is important to note that two different statements that assert that the same control should be set to different values for all system objects of the same kind will receive the same CCE ids.

Counting Issue (4) – User Defined Groups

- **EXAMPLE (ALLOWED): The following statements receive the same CCE id:**
  - **The minimum password length for all users in the Accounting user group should be 8 characters.**
  - **The minimum password length for all users in the Human Resources user group should be 12 characters.**

- **EXAMPLE (DISALLOWED): The following statement would not be assigned a CCE:**
  - **The startup type of nonessential services should be correct**

- **ISSUE: Under what conditions will CCEs be issued for user defined groups?**

CCE Content Decision (4)

- CD.H4 User-Defined Sets of System Objects (Merge)
- RULE: Some systems provide users with the ability to create grouping mechanisms for objects. For example, on Windows systems, administrators can create new user groups. In those cases where the same configuration control can be associated with all system objects within a user-defined set, then a single CCE ids is assigned for the control and the first parameter to be associated with the CCE is a target parameter to specify the name of the user-defined set.
- The following template for the corresponding description may be used:
  - The [control name] for all [system object types] in a specified [name of grouping mechanism type] should be configured correctly.
- DISCUSSION: It is important to note that two different statements that assert that the same control should be set to different values for all system objects in different user-defined sets will receive the same CCE id. Also, this content decision only applies to user-defined sets in those cases where the set can be fully defined using a system supporting grouping mechanism.

Counting Issue (5) – User Defined Objects

- **EXAMPLE (DISALLOWED):**
  - **Autoplay on all Drive Types should be properly configured for the specified objects.**
    - **Parameter 1: TARGET: (machine, user)**
    - **Parameter 2: Status (enabled, disabled)**
- **EXAMPLE (ALLOWED): The following statements would be assigned separate CCEs:**
  - **The 'Turn off Autoplay' machine setting should be configured correctly.**
    - **Parameter 1: Status (All drives, CD-ROM drives, Disabled)**
  - **The 'Turn off Autoplay' setting for a specified user should be configured correctly.**
    - **Parameter 1: TARGET: user**
    - **Parameter 2: Status (All drives, CD-ROM drives, Disabled)**
- **ISSUE: How should CCEs be assigned for user defined objects?**

CCE Content Decision (5)

- CD.H5 Single User-Defined System Objects (Merge)
- RULE: In those cases where the same configuration control can be associated with multiple user-defined system objects, then a single CCE id is assigned for the control and the first parameter to be associated with the CCE is a target parameter to specify the name of a given user-defined objectt.
- The following template for the corresponding description may be used:
  - The [control name] for a specified [system object types] should be configured correctly.
- DISCUSSION: It is important to note that two different statements that assert that the same control should be set for two user-defined system objects will receive the same CCE id.

Counting Issue (6) – Compliance Checks

- **EXAMPLE: The following statements receive their own CCE ids:**
  - **The "minimum password length" policy should meet minimum requirements.**
  - **There exists at least 1 account on the system whose password does not comply with the minimum password length policy.**

- **ISSUE: A setting the controls the creation of new objects is different from the state of objects already in existence.**

CCE Content Decision (6)

- **CD.H6 Configuration Setting / Compliance Check (Split)**
- **RULE: A global configuration setting and the existence of items that violate that configuration setting receive separate CCE ids. That is, the following 2 types of statements will each be given their own, separate CCE ids:**
  - **Apply a configuration setting to ensure that all newly created instances of type X have the characteristic Y.**
  - **The system has at least 1 instance of type X that fails to have the characteristic Y.**

Counting Issue (7) – Platform Groups

- **EXAMPLE: Red Hat Enterprise Linux**
  - **Total RHEL 5 CCEs: 431**
  - **Apache CCEs: 10**
  - **Avahi CCEs: 11**
  - **DHCP CCEs: 14**
  - **Dovecot CCEs: 9**
  - **Gnome CCEs: 7**
  - **OpenLDAD CCEs: 16**
  - **OpenSSH CCEs: 13**
  - **Squid-cache CCEs: 24**
  - **Kernel CCEs: ????**

- **ISSUE: When do you create a new platform group?**
  - **When do you combine platform groups?**

CCE Content Decision (7)

- **BASIC REQUIREMENTS FOR CREATING PLATFORM GROUPS (BASIC PLATFORM GROUP CONTENT DECISION)**
  - **Ample evidence that the platform group has meaning and acceptance in a significant number of the CCE use cases.**
  - **Clear and definable producer of the platform.**
  - **The platform is well enough managed with respect to versions and variants that is it possible to create CCE platform groups for versions or sets of variants that are widely accepted as being "essentially the same".**
  - **There is at least one publicly available configuration guide that describes configuration controls for the platform group.**
  - **Large enough set of controls that can be associated with the new platform group to warrant the extra overhead costs and complexity of the new platform group.**
    - **The minimum number currently is in the 10-20 range.**
  - **High likelihood that the new platform group will be useful outside of the context of another (typically OS related) platform group.**

MITRE

Counting Issue (8) – Underlying Platforms

- Example 1: OS vs BIOS hardening
- Example 2: Apache vs Linux hardening
- Example 3: MS Office vs MS OS hardening

- ISSUE: How should CCEs be issued when a platform is (typically) deployed on top of another, underlying platform?

CCE Content Decision – draft (8)

- **UNDERLYING PLATFORM HARDENING (SPLIT)**
- **IN THOSE CASES WHERE:**
  - a) **the platform group is typically deployed on an identifiable underlying system (typically an OS)**
  - b) **there is an existing platform group for the associated underlying system (e.g. in the case of Internet Explorer, we can point to the Windows 7 platform group)**
  - c) **a secure deployment of the (application) platform requires hardening the underlying (OS) platform by enforcing particular configuration controls in the underlying (OS) platform itself**
  - d) **there is evidence the control will have relevance independent of the deployment of the application platform**
- **THEN CCEs are created for the underlying (OS) platform and placed in the platform group associated with the underlying (OS) platform and not in the platform group for the application.**

Counting Issue (9) – Technical Mechanisms

- **Example: CCE-2777-1**
  - **The "when maximum log size is reached" property should be set correctly for the System log.**
  - **Tech Mech (1) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\Retention**
  - **Tech Mech (2) defined by Group Policy**
- **Example 2: Apache configuration file locations on Windows vs on Linux.**

- **ISSUE 1: How do we assign CCEs when the control is the same but the underlying platforms are different?**
- **ISSUE 2: Is Active Directory a different platform?**

CCE Content Decision – draft (9)

- **SAME CONTROL/DIFFERENT TECHNICAL MECHANISMS (MERGE)**
- **IN THOSE CASES WHERE:**
  - **a) platform group is being defined for a platform that can be deployed on multiple underlying sub systems (e.g. same application on different OSes)**
  - **b) a configuration control exists that implements the same conceptual control with the same conceptual parameters on multiple underlying systems**
  - **c) the technical mechanisms for the control are different on multiple underlying systems**
- **THEN a single CCE is create, with care being taken to ensure that the description and parameters are defined in a manner than are meaningful on all underlying systems and different technical mechanisms are defined for each underlying system.**

Counting Issue (10) – Related Controls

- **Example 1:**
  - **CCE-3176-5**
  - **Domain Profile: Allow UPnP framework exception (SP2 only)**
- **Example 2:**
  - **Apache Web Server file permissions on Windows vs Linux**
- **ISSUE: What do we do when some controls apply to some variants of a platform group and not others?**
  - **Does this change when variants of a platform group are defined in terms of different underlying platforms (e.g. Apache on Windows vs Apache on Linux)?**

CCE Content Decision – draft (10)

- **RELATED CONTROLS (SPLIT)**
- **IN THOSE CASES WHERE:**
  - **a) a platform group contains controls for several variants of the platform group that are considered "essentially the same"**
  - **b) most configuration controls in the platform group are the same per the "Same control/different technical mechanism" CD (above, thus justifying having a single platform group)**
  - **c) there is one or more configuration controls that exist only in the context of one platform variant or another, particularly as evidenced by the inability to write CCE descriptions and parameters that will work on all variants**
- **THEN CCE entries will be created for each variant and placed in the larger platform group with no further descriptive information binding it to some variants and not others.**

Thoughts on Content Decisions

- **“Counting CCEs is like cutting Jell-O. There is nothing in the Jell-O to guide the knife”**
  - **Adam Shostack (currently at Microsoft)**
- **“The striker [batter] may call for a low or high pitched ball. A "low ball" is ball that is a fair ball that is between the knees and the waist of the striker. A "high ball" is a ball that is a fair ball that is between the striker's waist and shoulders.**
  - **Baseball rules circa 1871**
  - **http://www.19cbaseball.com/rules-2.html**
- **“There is an error; but it is merely the accidental error of mistaking the abstract for the concrete. It is an example of what I will call the ‘Fallacy of Misplaced Concreteness.’”**
  - **A. N. Whitehead(1997) [1925]. *Science and the Modern World*.**

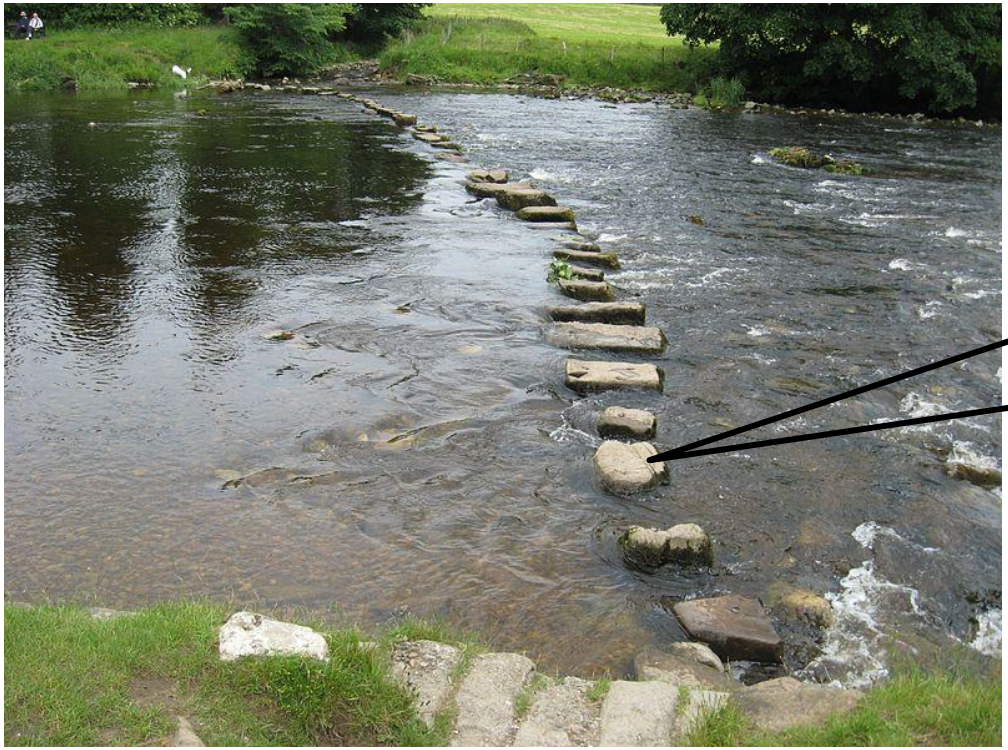
Thoughts on Content Decisions

- Three umpires walk into a bar…
  - "I call 'em as I see 'em."
  - "I call 'em as they is."
  - "They ain't nothin' till I call 'em."

- CCE Content Decisions
  - Are the CCE effort's attempt to define the "strike zone"
  - Are conceptual judgment calls, not concrete facts
  - Will continue to evolve with the configuration audit community
  - Consistency should not get in the way of moving the game along

CCE Counting: A Critical Step

Checklists, Configuration Management, Audit, Reporting …



Security Guides, Platform GUIs, System Commands…

MITRE