CPE™

cpe.mitre.org

Common Platform Enumeration (CPE)

Overview of Release 2.3

Brant A. Cheikes
bcheikes@mitre.org

MITRE

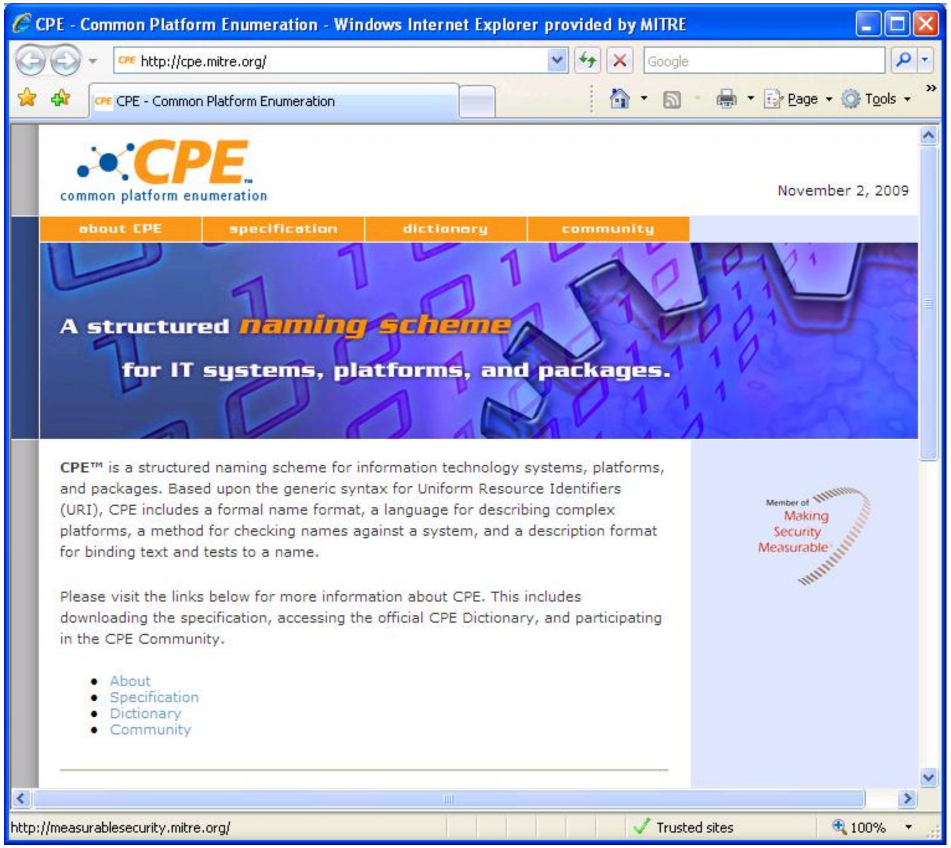
Session Objectives

- High-level tutorial on CPE
- Focus on latest release: CPE 2.3
- Describe the problem that CPE solves
- Provide examples of CPE names, CPE applicability language statements
- Illustrate the name matching procedure
- Discuss key challenges and next steps

What is CPE?

cpe.mitre.org

- CPE is:
  - A MITRE-led open standard
  - A structured naming scheme for IT products
  - Enabling technology for security automation
- CPE encompasses:
  - Two prescribed name formats
  - An authoritative dictionary of vetted, approved names
  - Algorithms for comparing names
  - A language for describing complex platforms

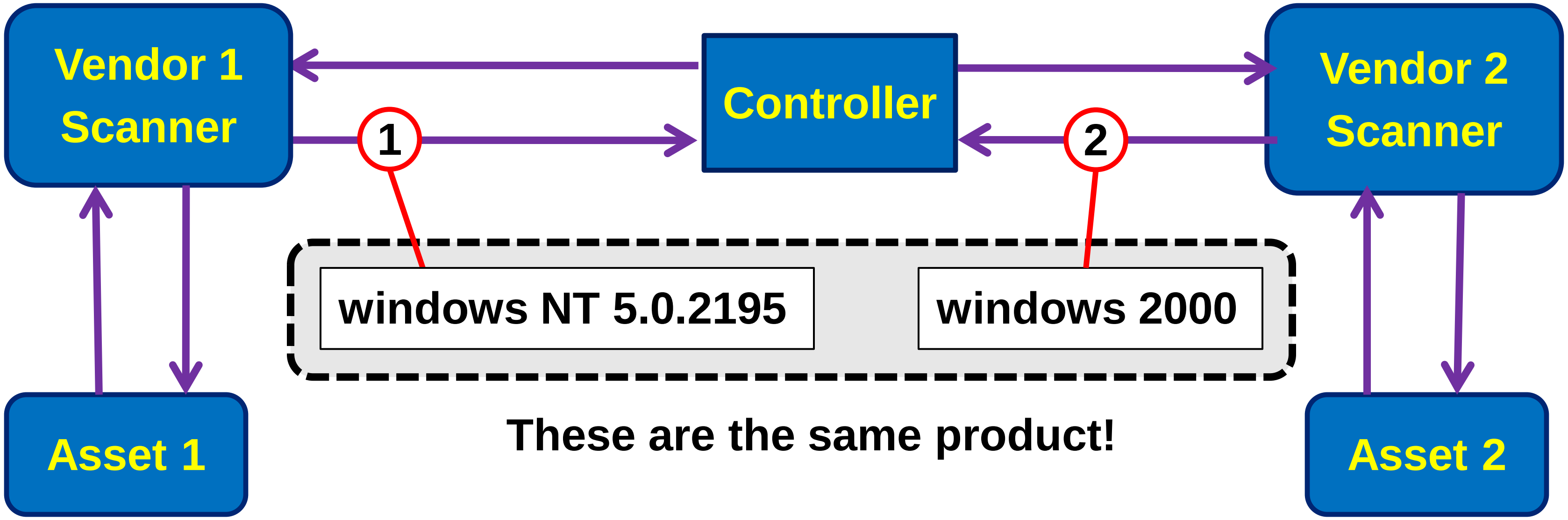

CPE - Common Platform Enumeration - Windows Internet Explorer provided by MITRE
http://cpe.mitre.org/
Google
CPE - Common Platform Enumeration
Page
Tools
CPE
common platform enumeration
November 2, 2009
about CPE
specification
dictionary
community
A structured naming scheme
for IT systems, platforms, and packages.
Member of Making Security Measurable
http://measurablesecurity.mitre.org/
Trusted sites
100%

CPE™ is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

Please visit the links below for more information about CPE. This includes downloading the specification, accessing the official CPE Dictionary, and participating in the CPE Community.

- About
- Specification
- Dictionary
- Community

What Problem Does CPE Solve?



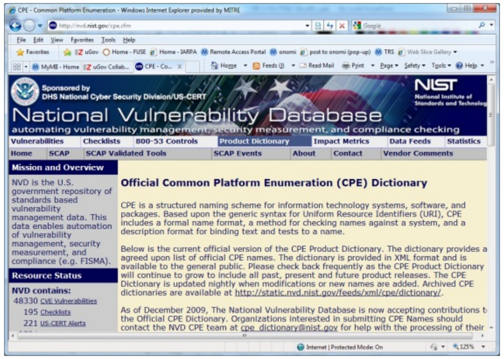
These are the same product!

Interoperable IT Product Names

How Does CPE Solve the Problem?

cpe.mitre.org

NIST NVD



CPE - Common Platform Enumeration - Windows Internet Explorer provided by MITRE

http://nvd.nist.gov/cpe.cfm

Sponsored by DHS National Cyber Security Division/US-CERT

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53 Controls | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

48330 CVE Vulnerabilities
195 Checklists
221 US-CERT Alerts

Official Common Platform Enumeration (CPE) Dictionary

CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Below is the current official version of the CPE Product Dictionary. The dictionary provides a agreed upon list of official CPE names. The dictionary is provided in XML format and is available to the general public. Please check back frequently as the CPE Product Dictionary will continue to grow to include all past, present and future product releases. The CPE Dictionary is updated nightly when modifications or new names are added. Archived CPE dictionaries are available at http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/.

As of December 2009, The National Vulnerability Database is now accepting contributions t the Official CPE Dictionary. Organizations interested in submitting CPE Names should contact the NVD CPE team at cpe_dictionary@nist.gov for help with the processing of their

Proposed new names

CPE Community

CPE Dictionary

Approved names

Published names

35K+ CPE Names

Oct 2011

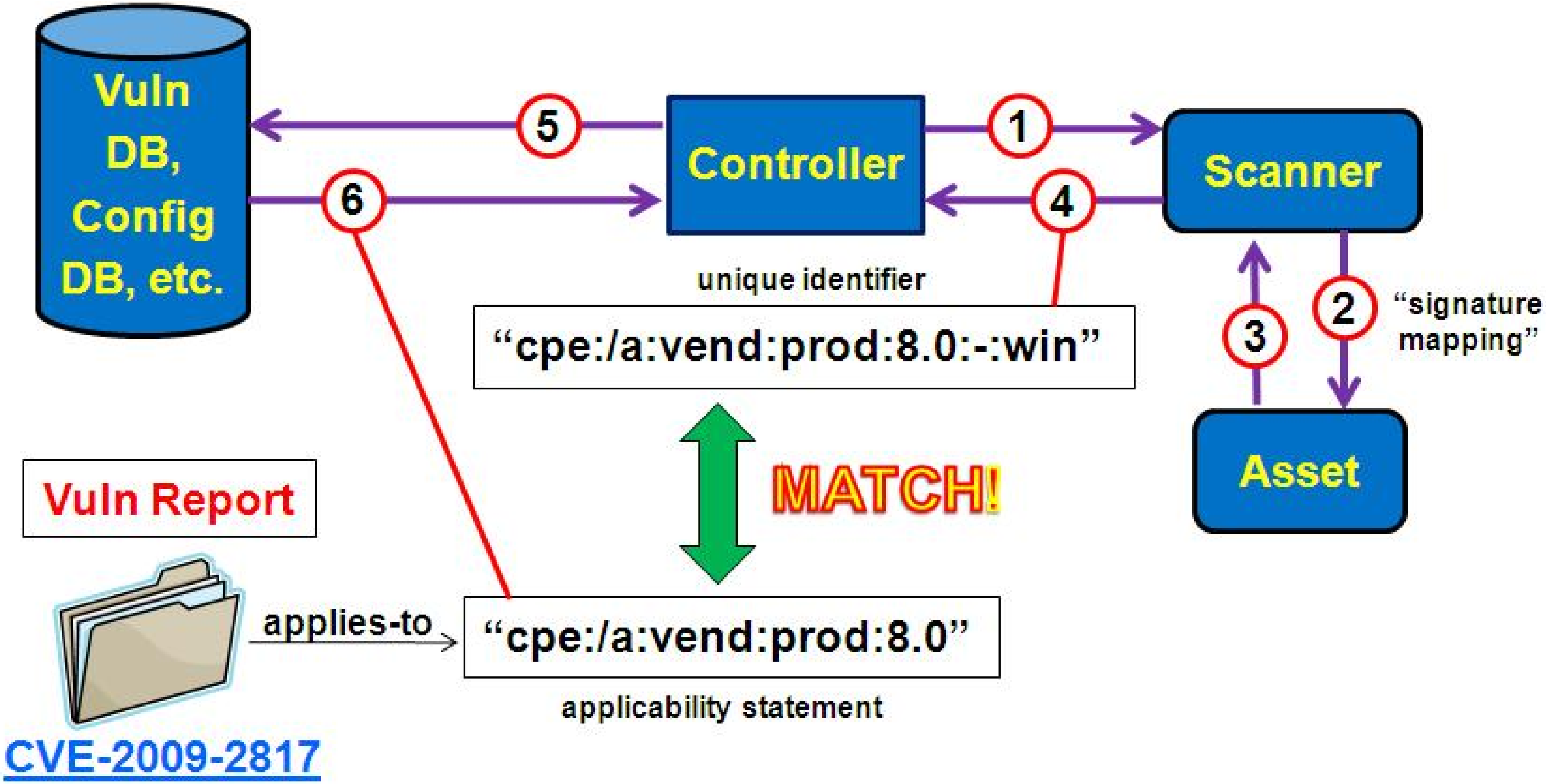
Adoption Drives Success

CPE Adopters

Products

CPE Use Case Example

cpe.mitre.org

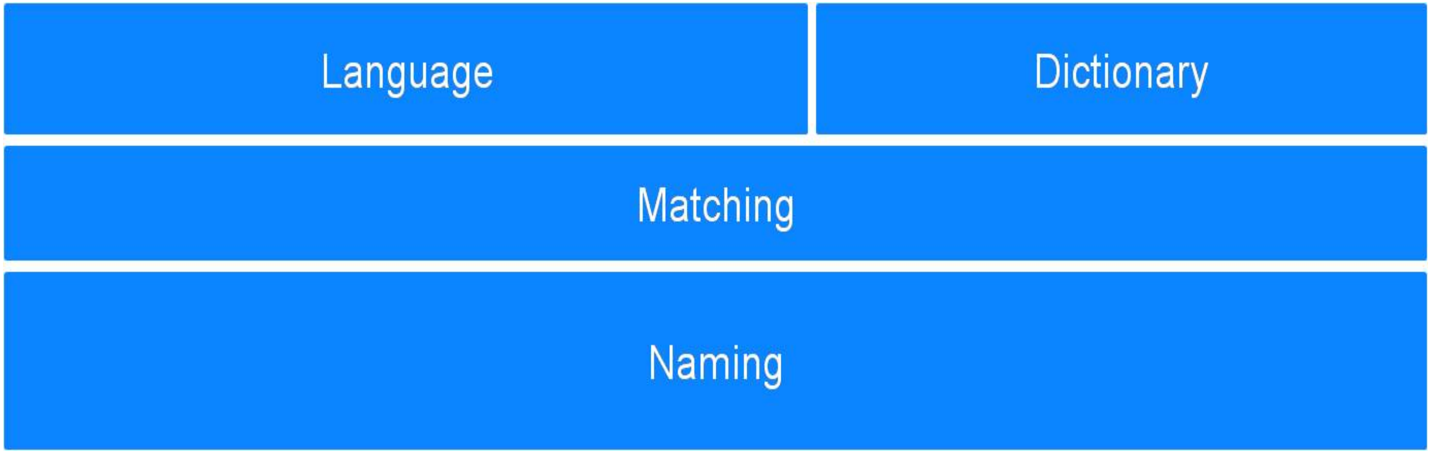


State of the Standard

cpe.mitre.org

- CPE is in a transition period
- CPE 2.3 is the current version
  - Specified by four NIST Interagency Reports (August 2011)
    - NIST IR 7695—Naming
    - NIST IR 7696—Matching
    - NIST IR 7697—Dictionary
    - NIST IR 7698—Applicability Language
  - Required in SCAP 1.2
- CPE 2.2 continues to be supported
  - Specification published in March 2009
  - Required in SCAP 1.0, 1.1

CPE 2.3 Specification Stack



Language

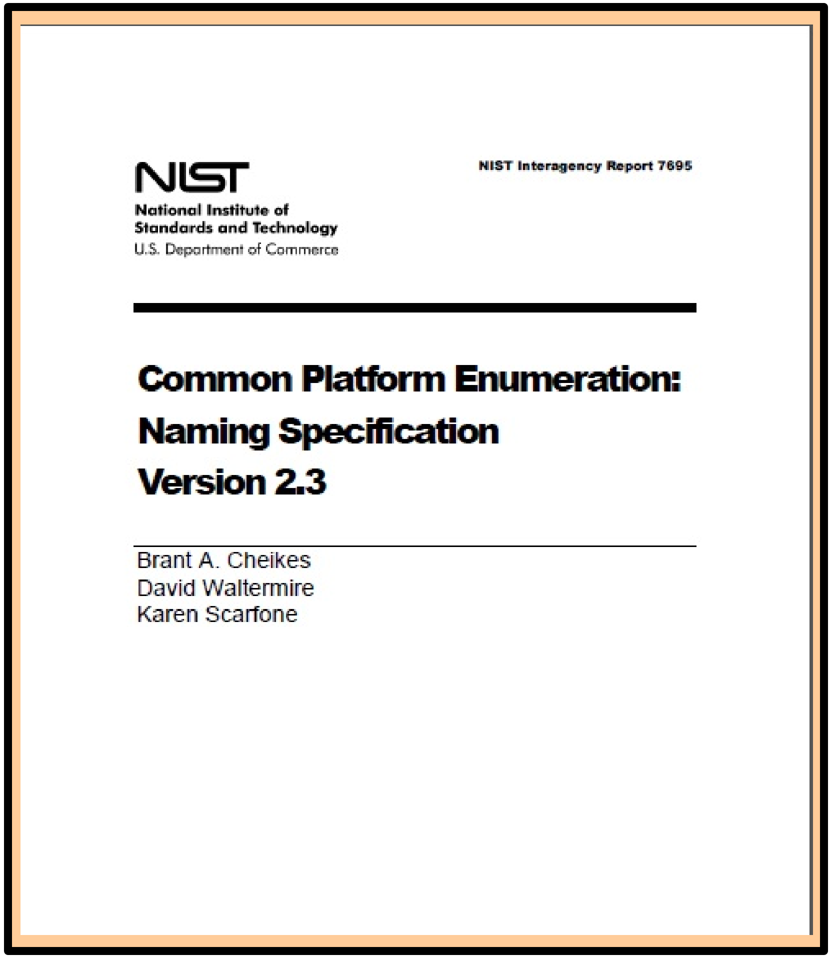
Dictionary

Matching

Naming

- Modular
- Easier to maintain
- Easier to extend
- More flexible w/r/t specifying conformance requirements

Naming Specification Overview



NIST Interagency Report 7695

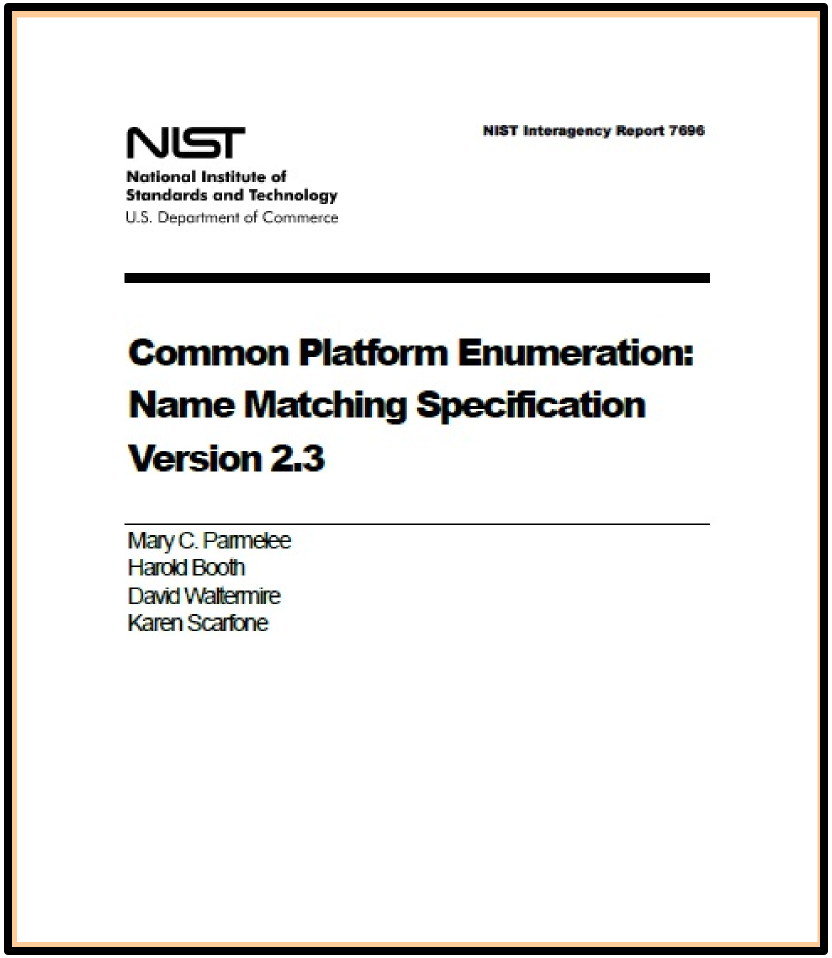
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Common Platform Enumeration:
Naming Specification
Version 2.3

Brant A. Cheikes
David Waltermire
Karen Scarfone

- NIST IR 7695 specifies the basic concepts and syntax of CPE names
- Defines the Well-Formed Name (WFN) and two allowed bindings
  - URI binding
  - Formatted string binding
- Specifies mechanical procedures for translating between binding forms

Matching Specification Overview



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Interagency Report 7696

Common Platform Enumeration: Name Matching Specification Version 2.3

Mary C. Parmelee
Harold Booth
David Waltermire
Karen Scarfone

- **NIST IR 7696 specifies the procedures for comparing two Well-Formed Names and determining the relationship between them**
  - **EQUAL**
  - **SUBSET**
  - **SUPERSET**
  - **DISJOINT**

Dictionary Specification Overview

NIST Interagency Report 7697

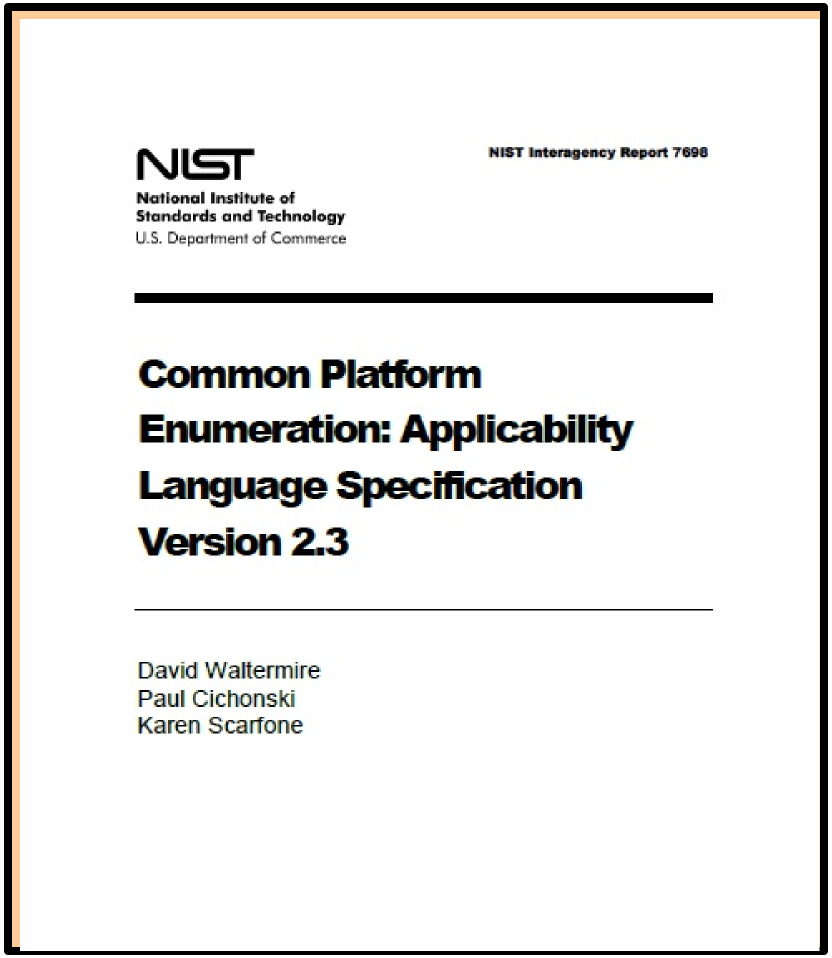
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Common Platform Enumeration: Dictionary Specification Version 2.3

Paul Cichonski
David Waltermire
Karen Scarfone

- NIST IR 7697 specifies the Dictionary data model, requirements for Dictionary creation and maintenance, and basic concepts for Dictionary operation

Language Specification Overview



NIST

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Interagency Report 7698

Common Platform Enumeration: Applicability Language Specification Version 2.3

David Waltermire
Paul Cichonski
Karen Scarfone

- NIST IR 7698 specifies a language for creating and using “applicability language statements”
- Enables the definition of a “platform” as a structure of ANDs, ORs and NOTs of CPE names

CPE 2.3 Significant Changes (1/2)

- **Naming:**
  - Adds four new name attributes
  - Defines the Well-Formed Name and two allowed "bindings"
    - URI (v2.2-style) and Formatted String
  - Specifies procedures for binding and unbinding
  - Lays foundation for limited use of wildcards for name matching

- **Matching:**
  - Defines attribute- and name-level matching separately
  - Allows unordered comparison of attribute-value pairs
    - Eliminates version 2.2 “prefix property”
  - Enables limited matching with single- and multi-character wildcards

CPE 2.3 Significant Changes (2/2)

cpe.mitre.org

- Dictionary:
  - Extends the data model to allow both URI and formatted string name bindings
  - Defines name acceptability criteria, including name completeness and uniqueness
  - Defines dictionary entry provenance and the deprecation process
  - Defines required dictionary management documents
  - Opens the door to “extended CPE dictionaries”

- Applicability Language:
  - Adds support for formatted string binding
  - Adds the cpe:check-fact-ref element which allows calls to external checking systems such as OVAL

CPE 2.3 Name Attributes

cpe.mitre.org

- part
- vendor
- product
- version
- update
- edition
- language

Carried over from CPE 2.2

- sw_edition
- target_sw
- target_hw
- other

New in CPE 2.3

CPE 2.3 Name Examples

- (Application) Microsoft Office 2007 Professional Service Pack 2
  - URI: cpe:/a:microsoft:office:2007:sp2:professional
  - FS: cpe:2.3:a:microsoft:office:2007:sp2:-:*:professional:*:*:*

- (Operating System) Microsoft Windows 7 64-bit Service Pack 1
  - URI: cpe:/o:microsoft:windows_7:-:sp1:x64
  - FS: cpe:2.3:o:microsoft:windows_7:-:sp1:-:*:*:*:x64:*

- (Hardware) 3Com Router 3012
  - URI: cpe:/h:3com:3c13612
  - FS: cpe:2.3:h:3com:3c13612:-:*:*:*:*:*:*:*

CPE 2.3 Applicability Language Example

```
<cpe:platform id="789">
  <cpe:title>
    Microsoft Windows XP with Internet Explorer 7.x or 8.x
  </cpe:title>
  <cpe:logical-test operator="AND" negate="FALSE">
    <cpe:fact-ref
       name="cpe:2.3:o:microsoft:windows_xp:*:*:*:*:*:*:*:*"/>
    <cpe:logical-test operator="OR" negate="FALSE">
      <cpe:fact-ref
         name="cpe:2.3:a:microsoft:internet_explorer:7.*:*:*:*:*:*:*:*"/>
      <cpe:fact-ref
         name="cpe:2.3:a:microsoft:internet_explorer:8.*:*:*:*:*:*:*:*"/>
    </cpe:logical-test>
  </cpe:logical-test>
</cpe:platform>
```

CPE 2.3 Name Matching: Overview

cpe.mitre.org

- All matching algorithms specified in terms of WFNs
  - So matching is agnostic to binding

- Specified functions:
  - `Compare_WFNs(source, target)`
    - Pairwise compares source attribute values to target attribute values
    - Returns a table of results
  - `CPE_x(source, target)`
    - x one of EQUAL, DISJOINT, SUBSET, SUPERSET
    - Compares a source WFN to a target WFN and returns TRUE if the set-theoretic relation holds between source and target

CPE 2.3 Name Matching: Attribute-Level Comparison

cpe.mitre.org

Source WFN

wfn:[part=“o”, vendor=“microsoft”, product=“windows_?”, version=ANY, update=ANY, edition=ANY, language=“en\-us”, software_edition=“home*”, target_sw=NA, target_hw=“x64”, other=NA]

Target WFN

wfn:[part=“o”, vendor=“microsoft”, product=“windows_7”, version=“6\.1”, update=“sp1”, edition=ANY, language=“en\-us”, software_edition=“home_basic”, target_sw=NA, target_hw=“x32”, other=ANY]

Compare_WFNs(source, target)

Attrib	Part	Vendor	Product	Version	Sw_ed	Tgt_sw	Tgt_hw	Other
Src	o	microsoft	windows_?	ANY	home*	NA	x64	NA
Tgt	o	microsoft	windows_7	6\.1	home_basic	NA	x32	ANY
Result	=	=	⊃	⊃	⊃	=	≠	⊂

CPE 2.3 Name Matching: Name Comparison Table

No.	If Attribute Relation Set =	Then Name Comparison Relation
1	If any attribute relation is DISJOINT (≠)	Then CPE name relation is DISJOINT(≠)
2	If all attribute relations are EQUAL (=)	Then CPE name relation is EQUAL (=)
3	If all attribute relations are SUBSET (⊂) or EQUAL (=)	Then CPE name relation is SUBSET(⊂)
4	If all attribute relations are SUPERSET (⊃) or EQUAL (=)	Then CPE name relation is SUPERSET (⊃)

CPE 2.3 Name Matching: Name-Level Results

CPE_DISJOINT=TRUE, CPE_EQUAL=FALSE

Attrib	Part	Vendor	Product	Version	Sw_ed	Tgt_sw	Tgt_hw	Other
Src	o	microsoft	windows_?	ANY	home*	NA	x64	NA
Tgt	o	microsoft	windows_7	6\.1	home_basic	NA	x32	ANY
Result	=	=	⊃	⊃	⊃	=	≠	⊂

CPE_SUPERSET=TRUE (equivalent to v2.2 CPE_NAME_MATCH)

Attrib	Part	Vendor	Product	Version	Sw_ed	Tgt_sw	Tgt_hw	Other
Src	o	microsoft	windows_?	ANY	home*	NA	x64	NA
Tgt	o	microsoft	windows_7	6\.1	home_basic	NA	x64	NA
Result	=	=	⊃	⊃	⊃	=	=	=

Open Issues and Challenges

- CPE does not solve the “signature mapping problem”
  - Left to vendors to determine which CPEs are installed on a given computing asset
  - A serious concern for asset inventory tool vendors
- CPE Dictionary maintenance is costly and error prone
  - A need-driven human-in-the-loop process driven by community submissions of candidate names
- Many community needs cannot be addressed without a major release which may break backwards compatibility
  - Representing relationships, e.g., part-of, next-version, …
  - Representing roles, e.g., server, client, domain-controller, …
  - Supporting needs of non-credentialed scanners

What’s Next?

cpe.mitre.org

- Support roll-out of CPE 2.3 Dictionary at NIST
  - Document all dictionary management procedures and naming guidelines
  - Convert all 2.2 URI names to 2.3 formatted strings
  - Build infrastructure to provide simultaneous support for CPE 2.2 and 2.3 dictionaries

- MITRE working with TagVault.org to explore use of “software identification tags” to link installed applications to their CPE names
  - See ISO/IEC 19770-2 for further information on software ID tagging

To Learn More

cpe.mitre.org

- CPE home page at MITRE:
  - http://cpe.mitre.org
- CPE home page at NIST:
  - http://nvd.nist.gov/cpe.cfm
- CPE 2.3 Specifications:
  - http://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf
  - http://csrc.nist.gov/publications/nistir/ir7696/NISTIR-7696-CPE-Matching.pdf
  - http://csrc.nist.gov/publications/nistir/ir7697/NISTIR-7697-CPE-Dictionary.pdf
  - http://csrc.nist.gov/publications/nistir/ir7698/NISTIR-7698-CPE-Language.pdf

Q&A