Common Platform Enumeration (CPE)

Overview of Release 2.3

MITRE

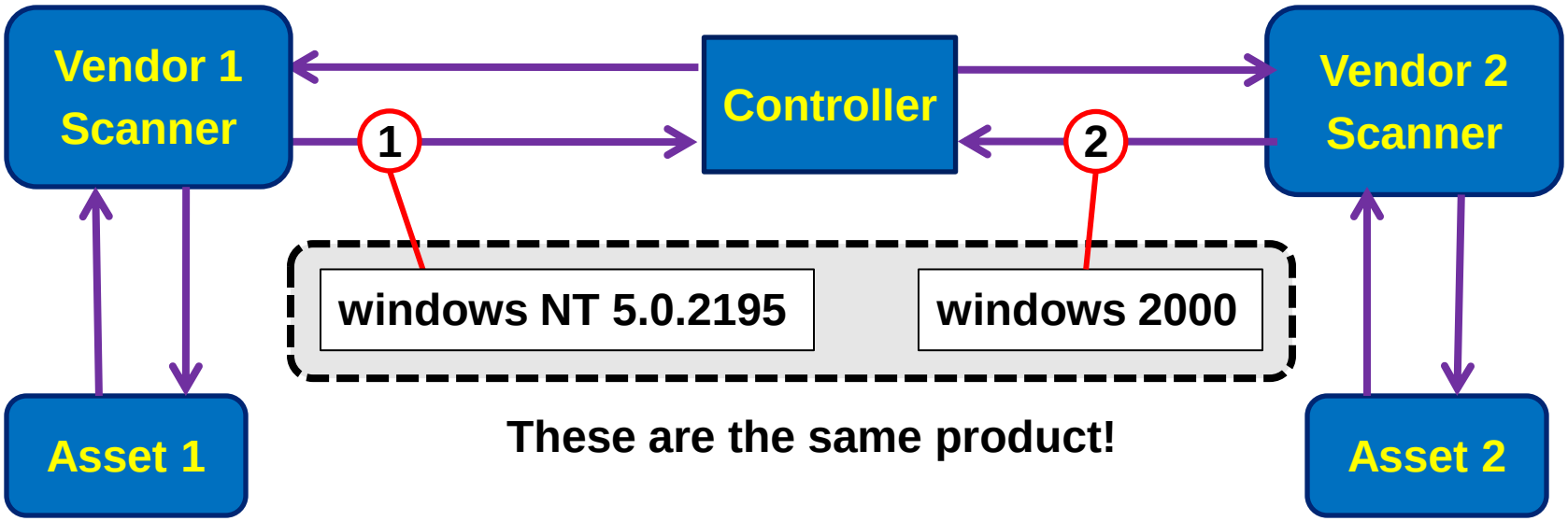
Session Objectives

- "Elevator speech" introduction to CPE
- Orientation to CPE v2.3 draft standard suite
  - Naming
  - Matching
- Q&A
- A peek ahead

What is CPE?

- **CPE is:**
  - **A MITRE-led open standard**
  - **A structured naming scheme for IT products**
  - **Enabling technology for security automation**
- **CPE encompasses:**
  - **A prescribed name format**
  - **A language for describing complex platforms**
  - **A methodology for assigning canonical names**
  - **An algorithm for comparing names**

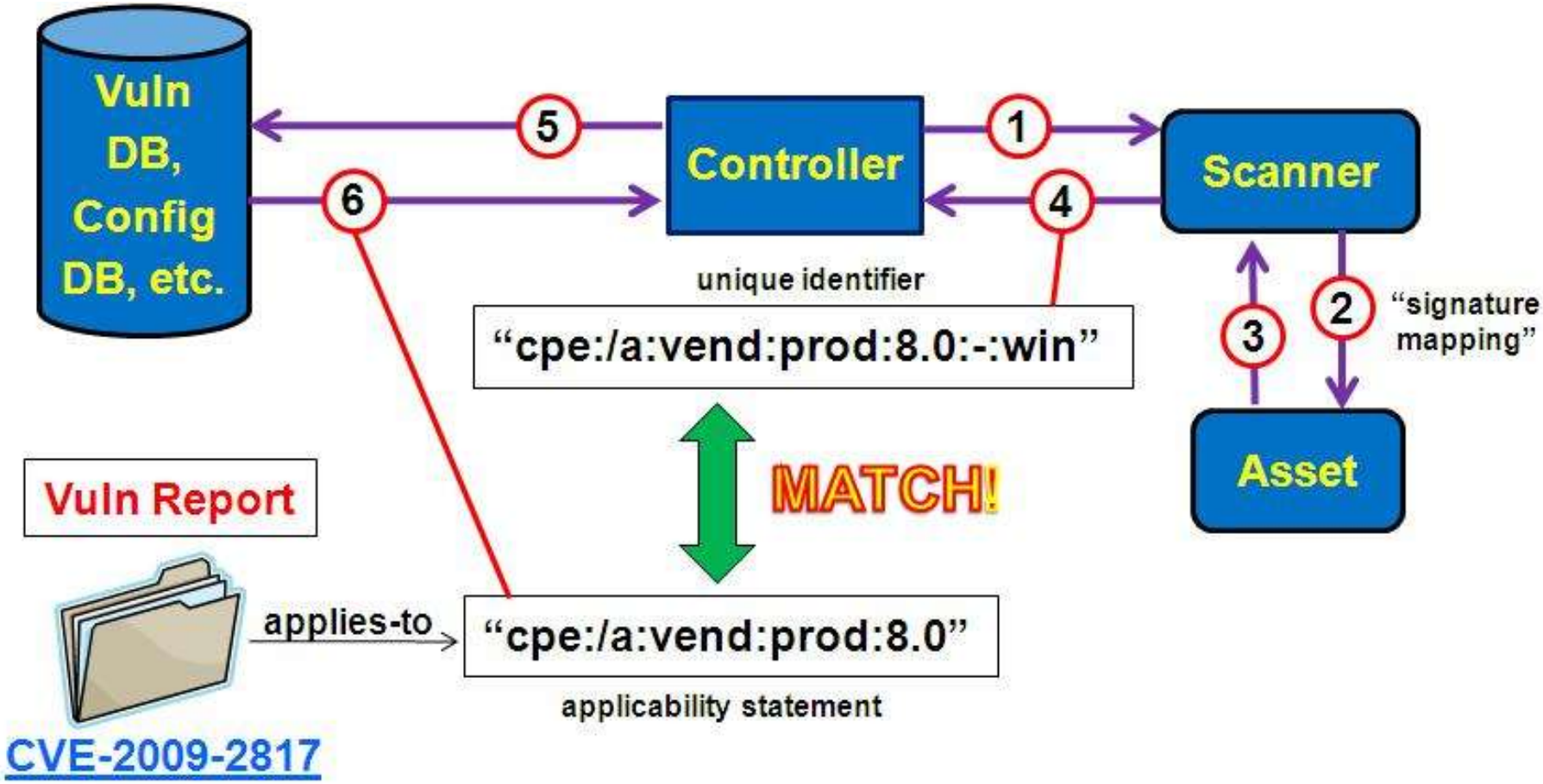
What Problem Does CPE Solve?



Interoperable IT Product Names

CPE Concept of Operations

cpe.mitre.org



Technical Use Case Analysis

- **Study performed in November 2008**
  - **To better understand the technical use cases**
  - **Interviewed members of the CPE Community**
  - **See: http://cpe.mitre.org/about/use_cases.html**

- **Four technical use cases were identified:**
  - **Software Inventory**
  - **Network-Based Discovery**
  - **Forensic Analysis/System Architecture**
  - **IT Management**

- **Software Inventory identified as a "must have"**

State of the Standard

- **Current CPE version is 2.2**
  - **Specification published in March 2009**
    - **See: http://cpe.mitre.org/specification**
  - **Part of SCAP 1.0, 1.1**

- **Draft version 2.3 released for public comment 26 Aug 2010**
  - **Implemented as three NIST Interagency Reports**
    - **Draft NIST IR 7695—Naming**
    - **Draft NIST IR 7696—Matching**
    - **Draft NIST IR 7697—Dictionary**
  - **See: http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-XXXX (replace "XXXX" with the IR number)**
  - **Public comment period closed 15 Sep 2010**
  - **Final drafts expected by end of 2010, for inclusion in SCAP 1.2**

Brief History of CPE 2.3

- First proposed during CPE session at ITSAC 2009
  - "Goal: Enhance near-term usability while working on a comprehensive solution"
- Requirements collected during February 2010 "Developer Day" CPE workshop
- CPE Core Team formed in March 2010
  - MITRE, NIST, DOD, Cisco, McAfee, nCircle
- CPE v2.3 developed on short timeline (March thru July)
  - Fundamental changes to the "architecture" of CPE
  - Minimal changes to the functionality of CPE

Significant Changes in v2.3

- General:
  - CPE defined as a "specification stack"
  - Multiple specifications, formatted as NIST IRs
- Naming:
  - Introduces the "Well-Formed Name" (WFN) abstraction
  - Adds several new name attributes
  - Defines two "bindings"
    - URI (v2.2-style) and Formatted String bindings
  - Specifies procedures for binding and unbinding
- Matching:
  - Attribute-level and name-level matching defined separately
  - Comparison of attribute-value pairs is unordered
  - Support provided for single- and multi-character wildcards

Adopt CPE 2.3 if…

- You want to exchange additional platform information
  - Four new attributes: sw_edition, target_sw, target_hw, other
- You want to be free of URI formatting rules
  - Formatted string binding is simpler
- You want to be able to match within attribute values
  - Single- and multi-character wildcards supported
- You want more flexible ways to compare names

CPE 2.3 Specification Stack

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

Naming (1 of 5): The Well-Formed Name (WFN)

cpe.mitre.org

NOTATION

```
wfn:[part="a",vendor="microsoft",
     product="internet_explorer",
     version="8\.0\.6001",
     update="beta",edition=NA]
```

- A WFN is:
  - an abstraction, not intended for machine interchange
  - an unordered list of attribute-value pairs
- Eleven (11) allowed attributes are specified
- Attribute values are:
  - Logical values (ANY or NA), or
  - Character strings obeying certain requirements

Naming (2 of 5): The Well-Formed Name (WFN)

cpe.mitre.org

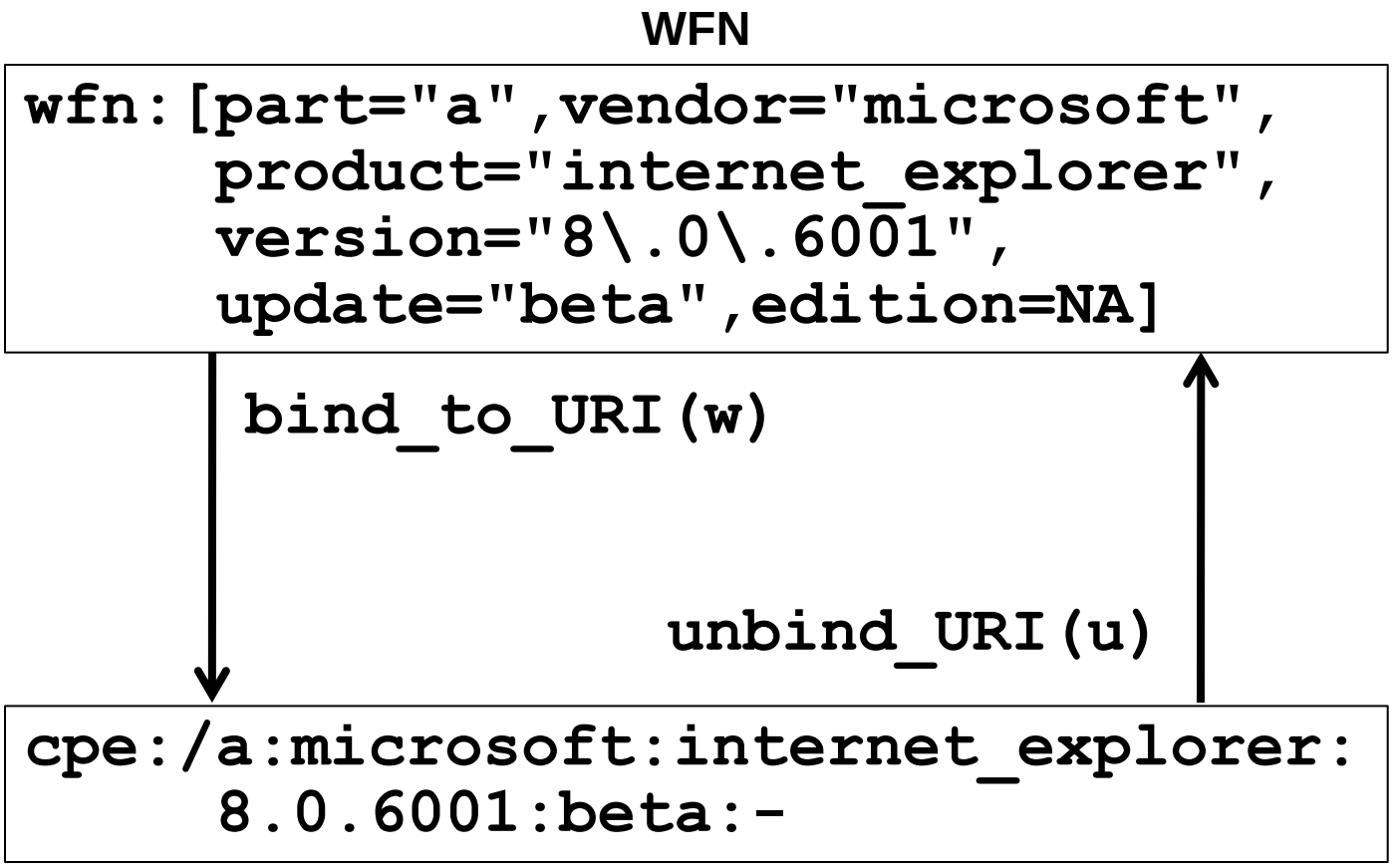
NOTATION

```
wfn:[part="a",vendor="microsoft",
     product="internet_explorer",
     version="8\.0\.6001",
     update="beta",edition=NA]
```

IMPORTANT NOTE!!

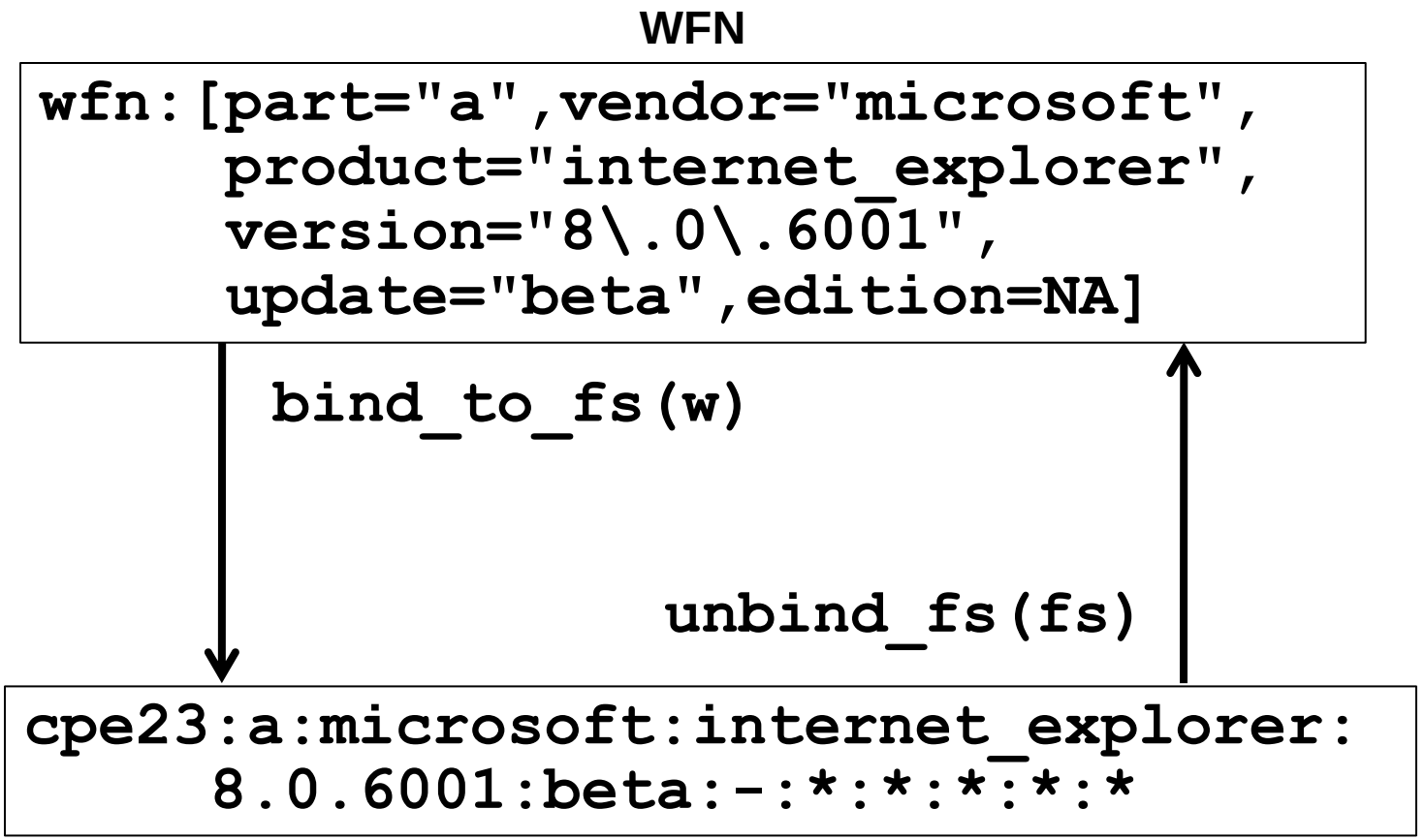
WFNs by themselves do not solve the interoperable-name problem!

Naming (3 of 5): Binding WFN to URI



CPE v2.2-style URI binding

Naming (4 of 5): Binding WFN to Formatted String



Naming (5 of 5): Allowed Attributes

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

Carried over from CPE 2.2

- sw_edition
- target_sw
- target_hw
- other

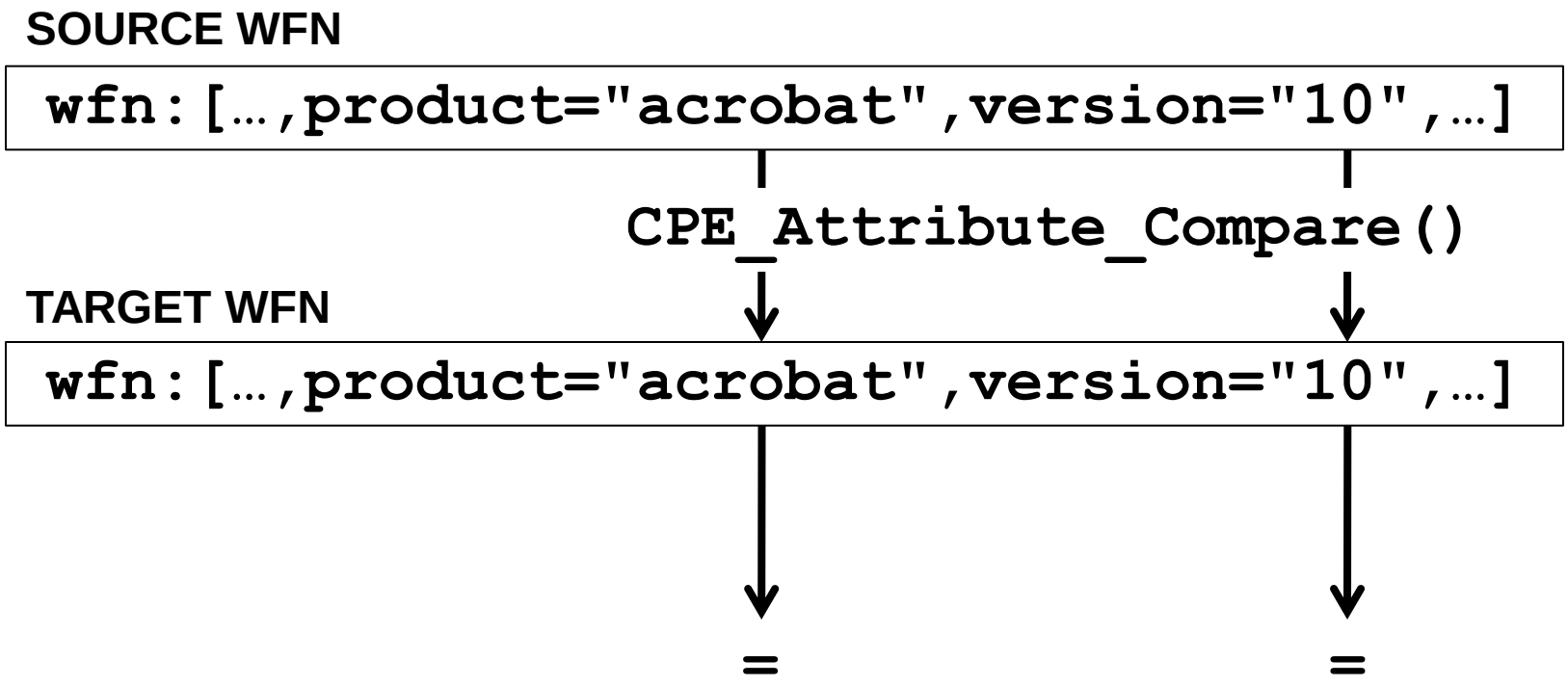
New in CPE 2.3

Matching (1 of 5): Overview

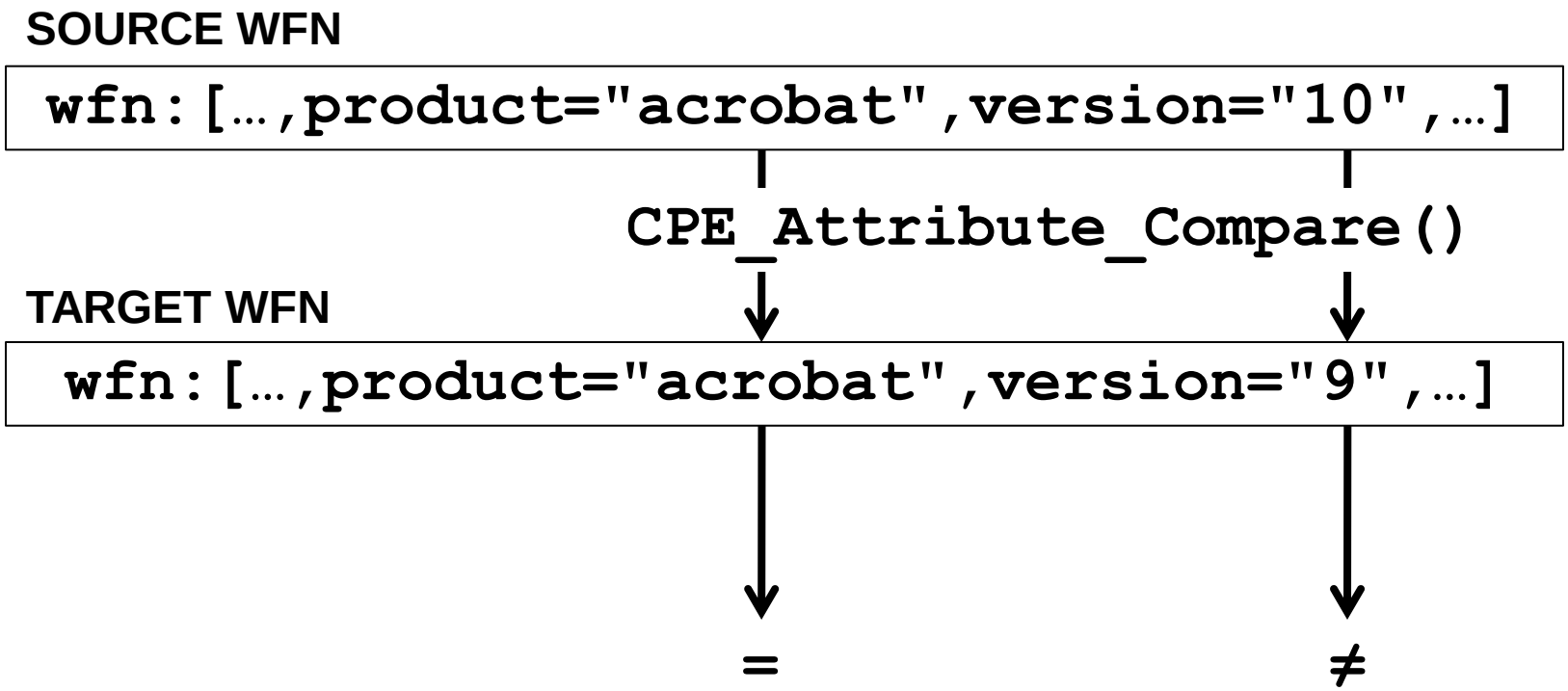
- All matching algorithms specified in terms of WFNs
  - So matching is agnostic to binding

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

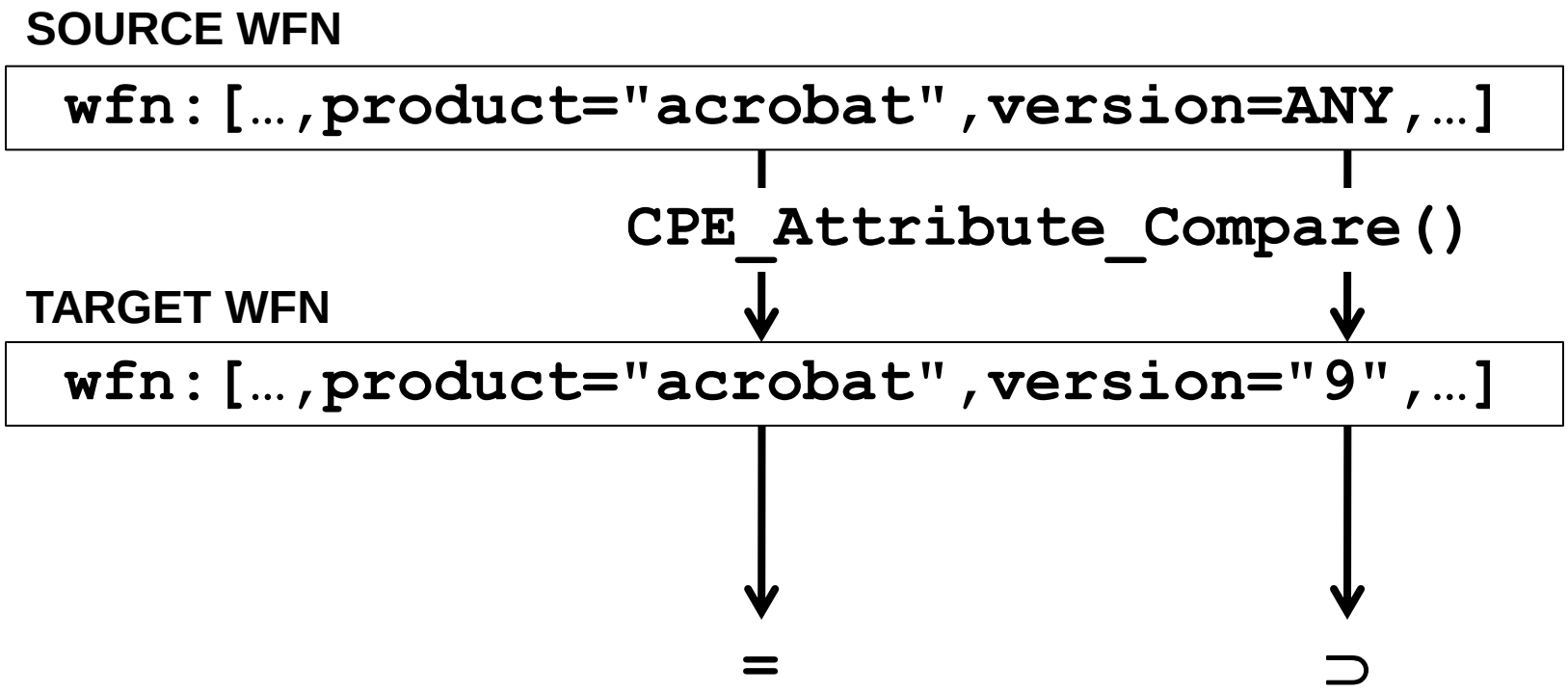
Matching (2 of 5): Example 1



Matching (3 of 5): Example 2



Matching (4 of 5): Example 3



Matching (5 of 5): CPE Name Matching Criteria

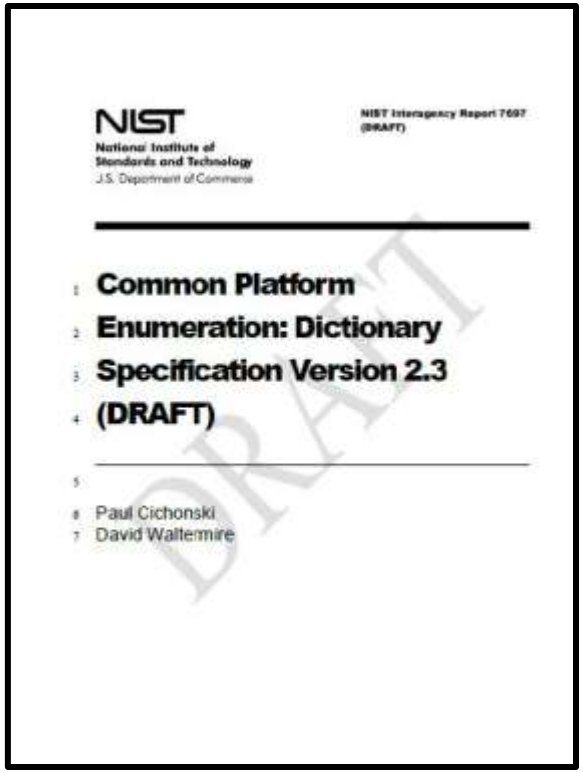
cpe.mitre.org

Name Match Number	If Attribute Outcome	Then Name Match Relation
1	If all attribute outcomes are DISJOINT (≠)	Then CPE name relation = DISJOINT (≠)
2	If all attribute outcomes are EQUAL(=)	Then CPE name relation = EQUAL (=)
3	If all attribute outcomes are SUBSET(⊂)	Then CPE name relation = SUBSET(⊂)
4	If all attribute outcomes are SUPERSET(⊃)	Then CPE name relation = SUPERSET (⊃)
5	If all attribute outcomes are INTERSECT (∩)	Then CPE name relation = INTERSECT (∩)

CPE Dictionary: Quick Summary

cpe.mitre.org

- Draft NIST IR 7697 defines the concept of a Common Platform Enumeration (CPE) Dictionary, the rules associated with CPE Dictionary creation and management, and the data model for representing a CPE Dictionary
  - Acceptance criteria
  - Deprecation process
  - Identifier lookup and dictionary searching
  - Management documents
  - Official and extended dictionaries
- NIST will continue to maintain the CPE Official Dictionary


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

NIST Interagency Report 7697 (DRAFT)

Common Platform Enumeration: Dictionary Specification Version 2.3 (DRAFT)

Paul Cichonski
David Waltermire

DRAFT

Anticipated FY11 Activities

- Finalize and publish the CPE 2.3 specification suite
- Get to work on CPE 3.0
  - Re-engage the CPE Community and Core Team
  - Two face-to-face "developer day" workshops
  - Two web conferences
- Develop a "vision" paper on CPE 3.0
- Develop a CPE 3.0 prototype/reference implementation

FY11 efforts to lay the foundation for CPE 3.0 specification in FY12

Q&A