ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1528.2
(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Vulnerability/state
exchange

Common platform enumeration name matching

Recommendation ITU-T X.1528.2

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	**X.1520–X.1539**
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1528.2

Common platform enumeration name matching

Summary

Recommendation ITU-T X.1528.2 defines the specification for common platform enumeration (CPE) name matching. The CPE name matching specification is part of a stack of CPE specifications that support a variety of use cases relating to IT product description and naming. The CPE name matching specification provides a method for conducting a one-to-one comparison of a source CPE name to a target CPE name. In addition to defining the specification, this Recommendation also defines and explains the requirements that IT products must meet to claim compliance. This is achieved by listing the relevant clauses of the NIST Interagency Report 7696 Common Platform Enumeration: Name Matching Specification version 2.3 and showing whether they are normative or informative.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1528.2	2012-09-07	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Common platform enumeration (CPE) is a structured method of describing and identifying classes of applications, operating systems, and hardware devices present in an enterprise's computing assets. CPE can be used as a source of information for enforcing and verifying IT management policies relating to these assets, such as vulnerability, configuration, and remediation policies. IT management tools can collect information about installed products, identify products using their CPE names, and use this structured information to help make fully or partially automated decisions regarding the assets.

CPE name matching is one of several modular CPE specifications that work together in layers to perform various functions. CPE name matching defines a method for conducting a one-to-one comparison of a source CPE name to a target CPE name. By logically comparing CPE names as sets of values, CPE name matching methods can determine if common set relations hold. For example, CPE name matching can determine if the source and target names are equal, if one of the names is a subset of the other, or if the names are disjoint.

One example of the value of CPE name matching is in determining if a particular product is installed on a system. Suppose that an organization is identifying which of its systems have any variation of the fictitious product, XYZ Visualizer Enterprise Suite 4 installed. This could be represented with the following well-formed CPE name (WFN) [CPE23-N:5.1]:

```
wfn:[part="a",vendor="xyz",product="visualizer_enterprise_suite",
version="4\.*",update=ANY,edition=ANY,language=ANY]
```

An asset management tool could collect information on the software installed on a system and compare its XYZ Visualizer Enterprise Suite installation characteristics to the WFN above. Suppose that the WFN for the fictitious product for a particular installed instance of XYZ Visualizer Enterprise Suite was reported as:

```
wfn:[part="a",vendor="xyz",product="visualizer_enterprise_suite",
version="4\.2\.3",update=NA,edition=NA,language="en\-us"]
```

Using these two example WFNs, CPE name matching methods perform a pairwise comparison of attribute values in the first (source) WFN to those in the second (target) WFN, yielding a list of the set relations between each pair of attributes (e.g. equal, superset). This list of comparison results is then assessed, leading to a determination that the first WFN represents a superset of the second WFN. This can be interpreted to mean that the system being examined does indeed have a variation of the fictitious product, XYZ Visualizer Enterprise Suite installed.

Although this may seem like a trivial example, CPE name matching is a powerful and flexible way of performing product comparisons in a standardized, automated manner. CPE name matching is also used by other CPE specifications to conduct more complex tasks, such as searching for product names in CPE dictionaries and performing complex comparisons of sets of product versions. For example, determining if a system is running a particular operating system version, running two particular applications, and not running a third particular application.

Recommendation ITU-T X.1528.2

Common platform enumeration name matching

1   Scope

This Recommendation defines the specification for CPE name matching. It also defines and explains the requirements that producers of CPE name matching implementations, such as software and services, must meet to claim conformance with this Recommendation.

As this Recommendation defines these specifications by listing the relevant clauses of the NIST Interagency Report 7696 Common Platform Enumeration: Name Matching Specification version 2.3 and showing whether they are normative or informative, all other versions are out of the scope of this Recommendation as are all CPE specifications other than CPE name matching.

2   References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[NISTIR 7696]   NIST Interagency Report 7696, *Common Platform Enumeration: Name Matching Specification Version 2.3, August 2011*.

3   Definitions

3.1   Terms defined elsewhere

None.

3.2   Terms defined in this Recommendation

None.

4   Abbreviations and acronyms

CPE   Common Platform Enumeration

NIST   National Institute of Standards and Technology

NISTIR   NIST Interagency Report

WFN   Well-formed CPE Name

5 Conventions

The following terms are considered equivalent:

• In ITU use of the word 'shall' and 'must' and their negatives are considered equivalent.

• In ITU use of the word 'shall' is equivalent to the NISTIR use of the word 'MUST'.

• In ITU use of the phrase 'shall not' is equivalent to the NISTIR use of the term 'MUST NOT'.

NOTE – In the NISTIR use of the words 'shall' and 'must' (in lower case) are used for informative text.

6 Name matching specification

This clause defines the specification for common platform enumeration (CPE) name matching. It provides direct references to NIST Interagency Report 7696 Common Platform Enumeration: Name Matching Specification version 2.3 through alignment of the clauses with the section numbers such that clause 6.x aligns with [NISTIR 7696] section x with matching titles.

6.1 Introduction

[b-NISTIR 7696] section 1 is informative.

6.2 Definitions and abbreviations

[b-NISTIR 7696] section 2 is informative.

6.3 Relationship to existing specifications and standards

[b-NISTIR 7696] section 3 is informative.

6.4 Conformance

[b-NISTIR 7696] section 4 is informative.

6.5 Name matching overview

[NISTIR 7696] section 5 is normative.

6.5.1 CPE name constructs

[NISTIR 7696] section 5.1 is normative.

6.5.2 Technical constraints

[NISTIR 7696] section 5.2 is normative.

6.6 Set relations

[NISTIR 7696] section 6 is normative.

6.6.1 Attribute comparison relations

[NISTIR 7696] section 6.1 is normative.

6.6.2 Name comparison relations

[NISTIR 7696] section 6.2 is normative.

6.6.3 Wild card attribute comparison

[NISTIR 7696] section 6.3 is normative.

6.7 CPE name matching pseudocode

[NISTIR 7696] section 7 is normative.

6.7.1 Overview of CPE name matching pseudocode

[NISTIR 7696] section 7.1 is normative.

6.7.2 CPE name matching pseudocode: core functions

[NISTIR 7696] section 7.2 is normative.

6.7.3 CPE name matching pseudocode: support functions

[NISTIR 7696] section 7.3 is normative.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems