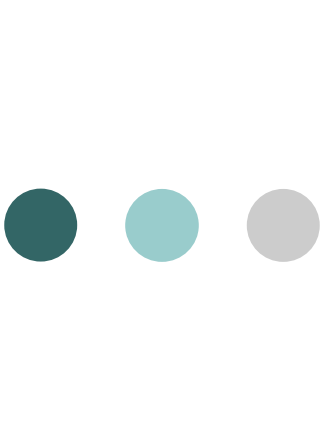


XCCDF-P

Andrew Buttner

July 12th, 2006

Overview

- NSA lead effort
- data model and XML representation for expressing qualifications and hierarchies of facts about platforms

Functional Requirements

- Able to distinguish between different kinds or families of platform facts
  - operating system version, installed services, hardware type, vendor, etc.
- Each fact must be able to be marked with a distinct, potentially unique identifier.

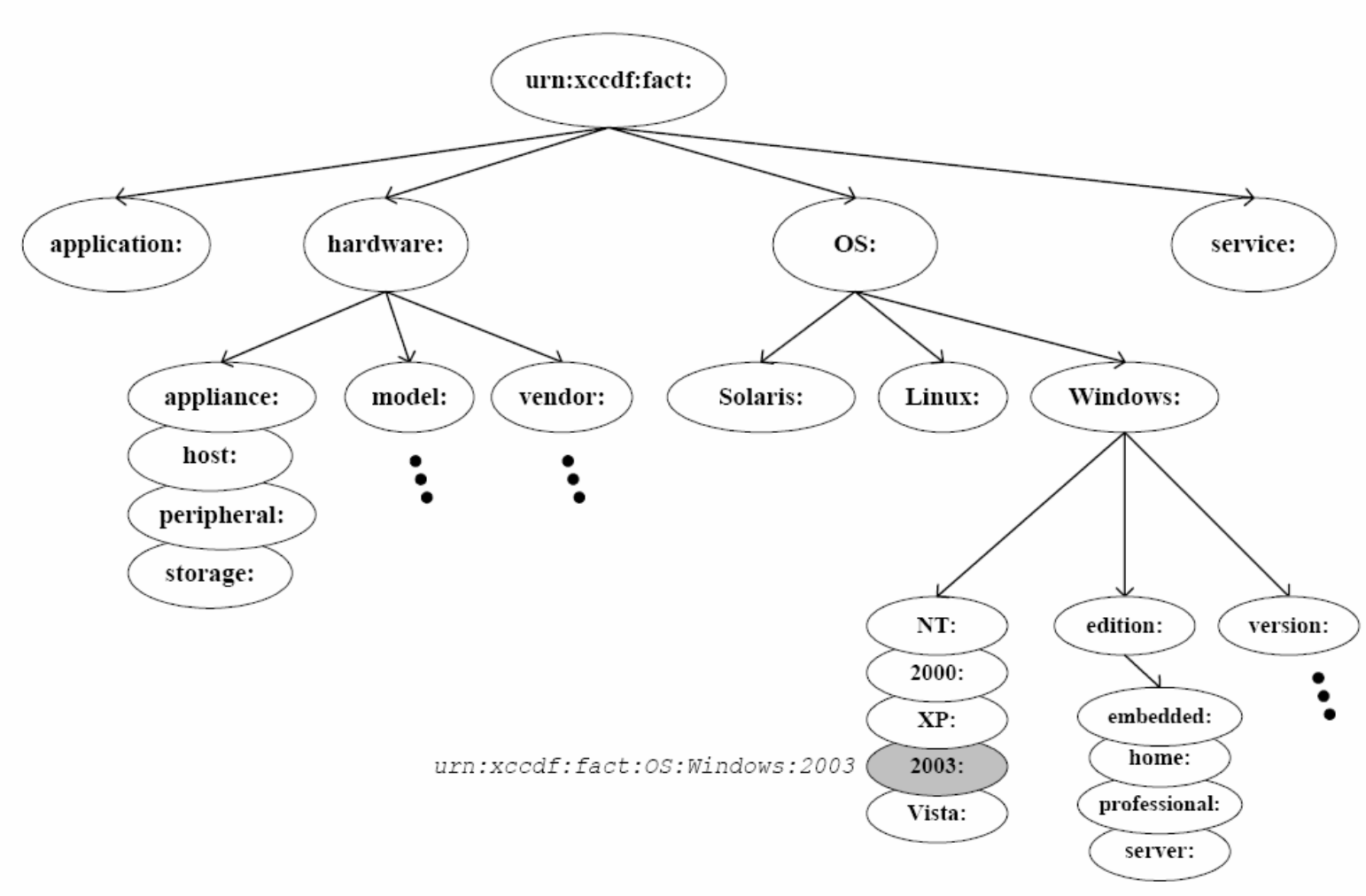
Functional Requirements (cont.)

- Able to express hierarchical relationships among facts.
  - For example, fact "Solaris" would be a child of fact "Unix" which would be a child of fact "OS".
- Able to express facts about several different aspects of a platform together
  - express the notion of "A Windows 2003 server with IIS 6.0 and MS-SQL Server".

Functional Requirements (cont.)

- Reduce or eliminate confusion or mis-identification based on string names
  - Are "Windows XP Professional" and "WinXP" the same OS platform?
  - Are "Java 5.0" and "J2RE 1.5.0" the same application platform?)
- Able to base the values of facts on external conditions at the time a target is actually being tested.

Hierarchical Naming Scheme



Hierarchical Naming Scheme (cont.)

- Falls apart when naming complex platforms
  - Windows 2003 server with IIS 6.0 and MS-SQL Server

Requirement For Naming

- Easy to read and to type
- Based on some kind of URI
- Able to express OS version and application versions
- Predictable and intuitive, easy to remember

Latest Idea

- Basic syntax: a URN with three parts:

urn:xccdf-p:/<HW-spec>/<OS-spec>/<app-spec 1>;<app-spec 2>;...

HW-spec ::= <supplier>:<model> [:<version>]
OS-spec ::= <supplier>:<family>:<version> [:<edition> [:<patchlevel>]]
app-spec ::= <supplier>:<prodname>:<version> [:<edition> [:<patchlevel>]

- any of the <field>s can be left blank.
- applications must appear in alphabetical order by supplier name, then product name.
- in all cases the supplier name is the base DNS domain for that organization.

Examples

- Windows XP Pro, SP2

urn:xccdf-p://microsoft.com:windows:xp:professional:sp2

- Red Hat Enterprise Linux 3 running Apache httpd 2.0.52 and MySQL 4.0

urn:xccdf-p://redhat.com:linux:enterprise:3/
apache.org:httpd::2.0.52;mysql.org:mysql::4.0

- Cisco 3725 router running IOS 12.4(T)8

urn:xccdp-p:/cisco.com:3725/cisco.com:ios:12.4(T)8

XML Representation

- How XCCDF-P is represented and passed around

```
<cdfp:Platform name="urn:xccdf-p://microsoft.com:windows:xp:professional:sp2">
    <cdfp:title xml:lang="en">Microsoft Windows XP Pro SP2</cdfp:title>
    <cdfp:check system="http://oval.mitre.org/XMLSchema/oval"
            href="win-platform-defs.xml" idref="OVAL-PLAT-WIN-XPSP2"/>
</cdfp:Platform>
```

Proposal

- a urn naming scheme
- an XML file of offical names
  - who hosts?
- ability to "predict" new names
  - in a way the ability to add to the XML file
- associated OVAL inventory definitions
  - who writes?