Supporting Network Devices

April 28th, 2008

MITRE

Goals

From AlterPoint:

"There exists a strong market need to automate the checking of network vulnerabilities. Strong customer demand for automated network security and compliance solutions are clear evidence of this need."

- add support for new network devices
  - currently just IOS and CatOS
- make easy to add new component schemas in the future
  - abstract out common tests

Roadblocks

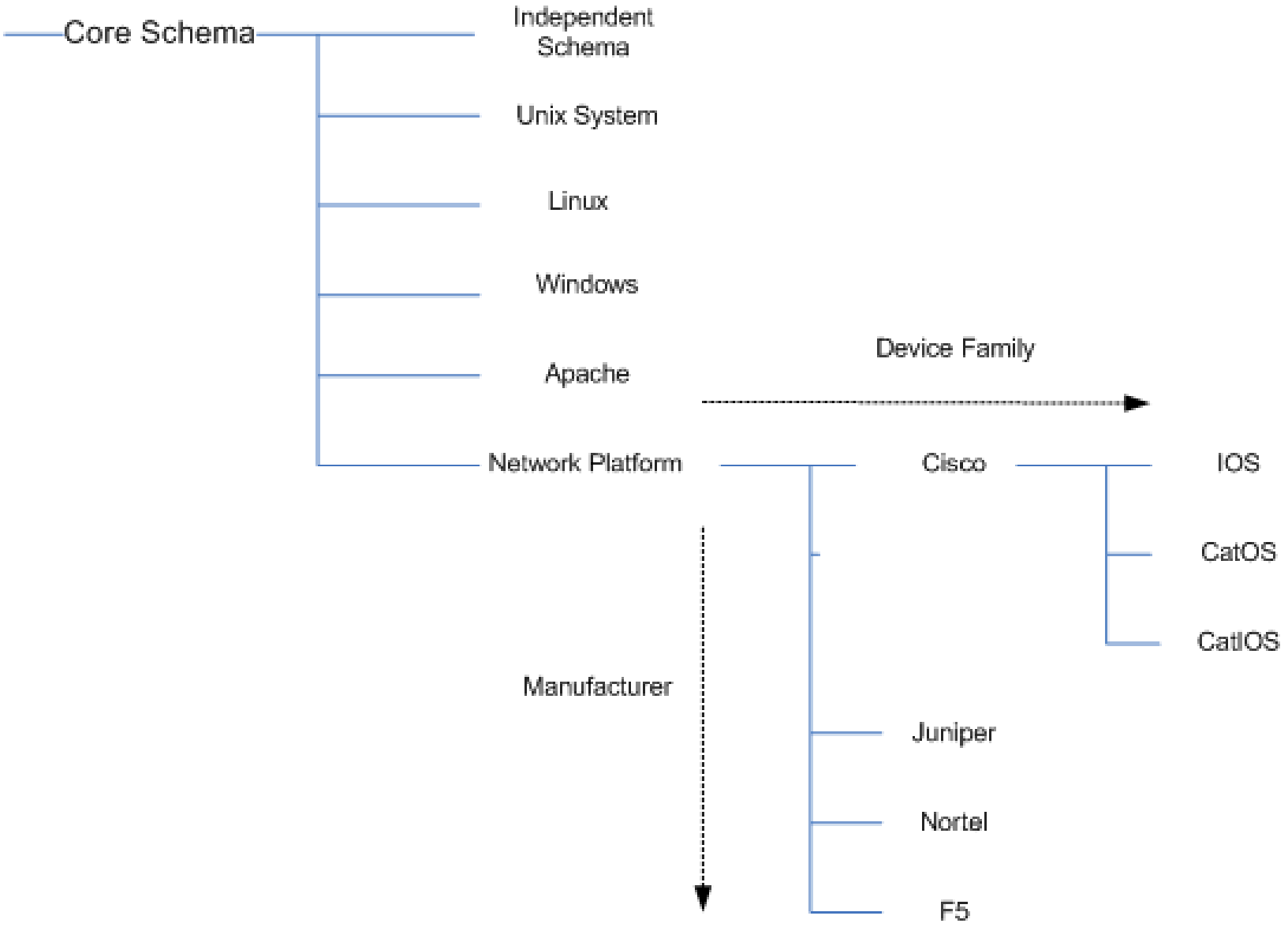
- difference in <system_info>
- flexible model is needed
  - support tests outside original scope
    - for example a generic config file test
  - new hardware types
- devices will become more componentized
  - collapse multiple hardware modules within a single chassis

MITRE

System Info

- unclear what 'architecture' would mean in the network device world
  - limited to exactly one item and thus is not suitable for describing devices with bladed architectures containing multiple cards or daughter cards.

- each device component includes
  - model number
  - optional type (chassis, card, daughter card.)


Core Schema
Independent Schema
Unix System
Linux
Windows
Apache
Network Platform
Device Family
Cisco
IOS
CatOS
CatIOS
Manufacturer
Juniper
Nortel
F5

Network Device Component Schema

In the same way that the "UNIX System" schema abstracts general characteristics of different Unix platforms, it is possible to define a general "Network Device" schema that abstracts cross-vendor network device characteristics.

- device_type_test
  - vendor
  - class (router, switch, firewall, etc)
  - component

- config_file_test

MITRE

Additional Component Schemas

- as needed component schema are added at to deal with specific devices
  - a network platform may introduce a new type of configuration type, which requires device specific parsing to accommodate testing

Versions

- OS Version is one of the most difficult things to test.
  - different approaches for each device
- A sub-schema better handles specialized testing for OS versioning
  - remove the ios_version type from DatatypeEnumeration

Other Changes

- add alpha_version type to the DatatypeEnumeration
  - just like the "version" type

"version" supports comparison of a dotted-integer hierarchical version number (like 10.3.2)

"alpha_version“ would support the same dotted hierarchy approach, but would be based on string compares of the components, so that versions such as "4.2r8.1“ could be compared without specialized tests.

MITRE