~~CPE~~ SCAP Language

Current Problem

- Benchmarks must be manually selected for targets
  - A person must identify targets based on benchmark and profile applicability
  - Possible to miss targets that should be targeted
  - Problematic in large enterprises and with application oriented benchmarks
- Benchmarks and profiles are defined only in human-readable description strings
  - USGCB REHL5-*desktop*
  - Microsoft Windows 2003 *SSLF Domain Controller*
  - XP STIG – Profile *MAC-1_Sensitive*

Benchmark Requirements

- Define Benchmark, Group, Rule applicability
  - Precondition before further processing
  - XCCDF 1.1.4 and SCAP 1.1 allow this for the platform (CPE) tag
- Define Profile applicability
  - Identification
  - Auto-selection

SCAP Requirements

- Allow tools to make collections of benchmarks and auto-select benchmarks to run for each target type
  - E.g., Run all applicable benchmarks of type STIG (metadata) against a set of target hosts
- Allow tools to auto-select a profile within a benchmark
- Define allowed schemas and values for facts

Uses

- XCCDF
  - Automatable (OVAL)
  - Non-automatable (OCIL)
    - Target might be a person defined by applicable role or other attribute
    - This has other implications
- Remediation

- Scoring
  - Some applicability factors could later be used to tailor environmental scoring
  - The same CCE might have different CCSS values in profiles for domain controller and member server
- Simple declaration of facts
  - intrusion set characteristics: CVE-XXXX-YYYY & CCE-ZZZZ-Z
  - CVSS=9 when CVE-XXXX-YYYY & CPE:/o:microsoft:windows_xp

SCAP Language Statement

- Build on CPE Language
  - Add to the language, DO NOT change CPE
- Fact-ref could be defined by any SCAP approved schema
  - CPE
  - Asset model (workstation)
  - Network model (internet facing)
  - Organization model (finance org)
  - Person model (system admin)
- Check-ref defines specific methods to evaluate fact-ref
  - OVAL definition
  - OCIL definition (limit to OCIL docs until complexities of mixed content are addressed)
  - CPE matching (assumes trusted source of CPEs)
  - Data resource (identifier and system URI)
- Logical combination of facts still processed to create a result
- Not all fact-refs will be facts that are automatically discoverable
  - Examples: CIA requirement level (DoD MAC level), organization, role
  - Implies content will be processed by a system that has access to additional data (e.g., CMDB)
  - If fact can’t be evaluated then process as if it were true

Questions

- Valid use case?
- Other solutions?
  - Build support directly into XCCDF?
- Separate supporting spec?
  - Where might it live?
  - How would it be included in SCAP?