SCAP Content Generation

Andrew Buttner & Jon Baker

September 22, 2008

Overview

- standards are only effective if there is content
- content creation is our biggest challenge
  - labor
  - knowledge
  - responsibility

Goals

1) separate content from tools
2) tools available to support generation
3) content created by those with knowledge
4) accessible repositories

MITRE

Successful content is now separated ...

```
<?xml version="1.0" encoding="UTF-8" ?>
<oval_definitions xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-definitions-5#unix unix-definitions-schema.xsd http://oval.mitre.org/XMLSchema/oval-definitions-5 oval-definitions-schema.xsd
        http://oval.mitre.org/XMLSchema/oval-definitions-5#solaris solaris-definitions-schema.xsd http://oval.mitre.org/XMLSchema/oval-common-5 oval-common-schema.xsd"
        xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-
        def="http://oval.mitre.org/XMLSchema/oval-definitions-5">
<generator>
 <oval:product_name>The OVAL Repository</oval:product_name>
 <oval:schema_version>5.4</oval:schema_version>
 <oval:timestamp>2008-09-12T10:17:25.317-04:00</oval:timestamp>
 </generator>
<definitions>
<definition id="oval:org.mitre.oval:def:3270" version="1" class="vulnerability">
<metadata>
 <title>Security Vulnerability in the Solaris 10 Internet Protocol (ip(7P)) may Lead to a Denial of Service (DoS) Condition</title>
<affected family="unix">
 <platform>Sun Solaris 10</platform>
 </affected>
 <reference source="CVE" ref_id="CVE-2007-5716" ref_url="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5716" />
 <description>Unspecified vulnerability in the Internet Protocol (IP) functionality in Sun Solaris 10 allows local users to cause a denial of service (panic) via unspecified vectors, probably related to a UDP
        packet.</description>
 </metadata>
<criteria operator="OR" comment="Software Section">
<criteria operator="AND" comment="Solaris 10 (SPARC) meets Sun Alert 103087">
 <extend_definition comment="Solaris 10 (SPARC) is installed" definition_ref="oval:org.mitre.oval:def:1440" />
 <criterion comment="Patch 118833-04 or later installed" test_ref="oval:org.mitre.oval:tst:5394" />
 <criterion negate="true" comment="Patch 127111-02 or later installed" test_ref="oval:org.mitre.oval:tst:5429" />
 </criteria>
<criteria operator="AND" comment="Solaris 10 (x86) meets Sun Alert 103087">
 <extend_definition comment="Solaris 10 (x86) is installed" definition_ref="oval:org.mitre.oval:def:1926" />
 <criterion comment="Patch 118855-03 or later installed" test_ref="oval:org.mitre.oval:tst:5577" />
 <criterion negate="true" comment="Patch 127112-02 or later installed" test_ref="oval:org.mitre.oval:tst:5048" />
 </criteria>
 </criteria>
 </definition>
<definition id="oval:org.mitre.oval:def:1926" version="1" class="inventory">
<metadata>
 <title>Solaris 10 (x86) is installed</title>
<affected family="unix">
 <platform>Sun Solaris 10</platform>
 </affected>
 <reference source="CPE" ref_id="cpe:/o:sun:sunos:5.10::ix86" />
 <description>The operating system installed on the system is Sun Solaris 10 for x86.</description>
 </metadata>
<criteria>
 <criterion comment="Solaris 10 Installed" test_ref="oval:org.mitre.oval:tst:3680" />
 <criterion comment="ix86 architecture" test_ref="oval:org.mitre.oval:tst:3912" />
 </criteria>
 </definition>
<definition id="oval:org.mitre.oval:def:1440" version="1" class="inventory">
<metadata>
 <title>Solaris 10 (SPARC) is installed</title>
<affected family="unix">
 <platform>Sun Solaris 10</platform>
 </affected>
 <reference source="CPE" ref_id="cpe:/o:sun:sunos:5.10::sparc" />
 <description>The operating system installed on the system is Sun Solaris 10 for SPARC.</description>
 </metadata>
<criteria>
 <criterion comment="Solaris 10 Installed" test_ref="oval:org.mitre.oval:tst:3680" />
 <criterion comment="sparc architecture" test_ref="oval:org.mitre.oval:tst:3237" />
 </criteria>
 </definition>
 </definitions>
```

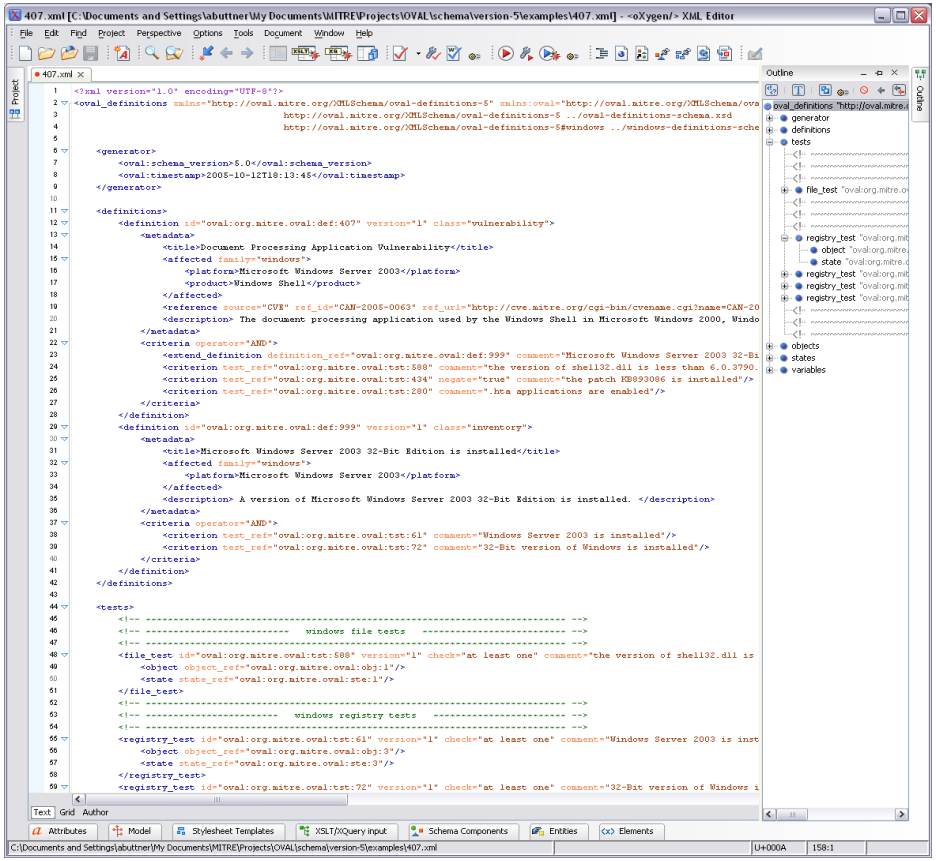
Facilitate Creation

- Ideally – a variety of commercial applications designed to help the content writer

- Today
  - XML tools
  - scripts
  - beta tools

MITRE

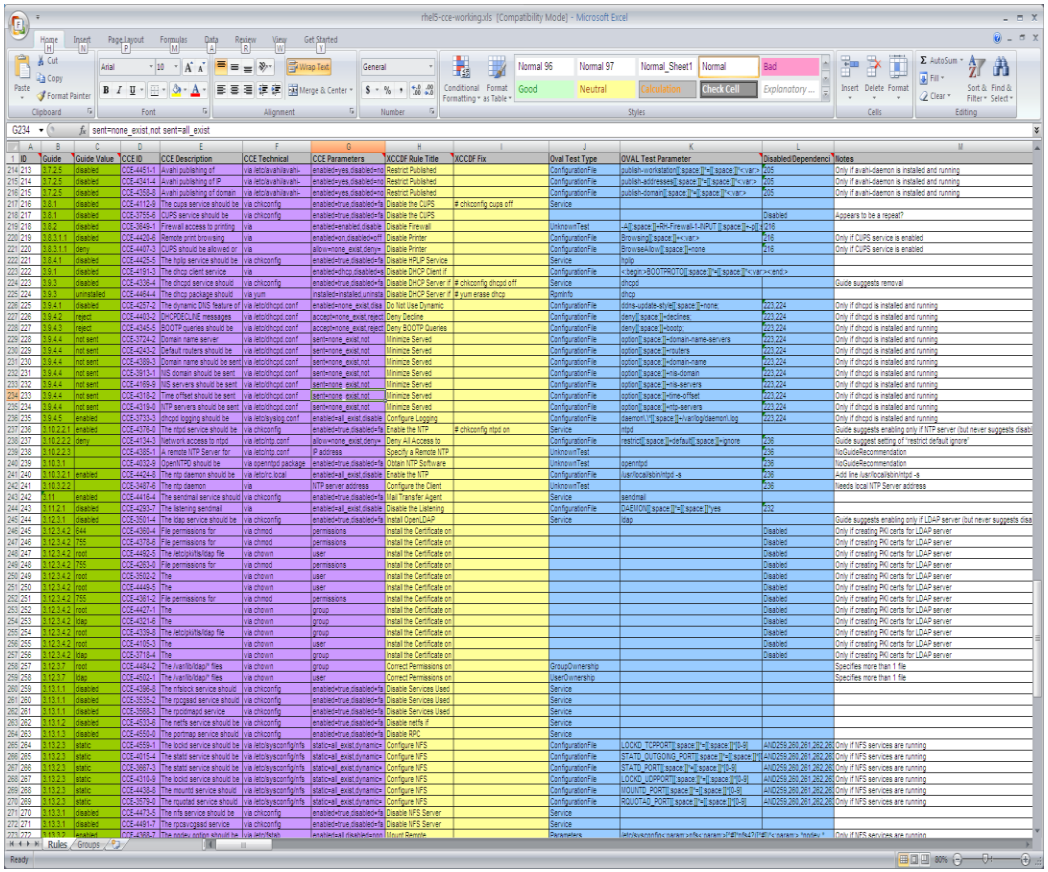
XML Tools



- color coding
- find / replace
- schema aware
- different views

- not XCCDF/OVAL aware
  - hyperlink ids?

Spreadsheet / Scripts



- remove XML knowledge
- simplify view
- auto generate

- still not perfect
  - new conditions?
  - data validation?
  - multi-user?
  - script maintenance?

MITRE

Multiple Benefits

- Spreadsheet can be used to support multiple efforts
  - CCE
  - XCCDF/OVAL
  - CPE
- Leverage work to help speed content development

Content Creation Tools

- Recommendation Tracker
- Benchmark Editor
- commercial editors

MITRE

Recommendation Tracker

Facilitate **consistent** guidance authoring through an established **standardized format** for **creating**, **developing**, and **tracking** all information pertinent to security guide and benchmark generation.

Codifies a proven guidance creation process.

https://sourceforge.net/projects/rectracker/

What does the RT do?

Provides structure to the guidance development process

- Clearly breaks out all key components to a Rule
- Leads users in a step-by-step fashion to produce clear guidance

Supports team collaboration

- User roles and task assignment
- Comments on key components
- Progress tracking

Enables offline development with synchronization

- Allow users to work in their environment of choice
- Facilitate team collaboration

Enables users to output guidance in standardized formats

- No additional burden to use standards

https://sourceforge.net/projects/rectracker/

MITRE

The Benchmark Editor

- Authoring standards based benchmarks is challenging
  - Requires training in the benchmark languages
  - Composed of numerous documents
  - Benchmark documents can be huge

- Open source development task lead by MITRE

Simplify authoring and maintaining standards based benchmarks

http://benchmarkeditor.mitre.org/

What can the Benchmark Editor do?

- Represents the Benchmark and all of its components as a single unit
- Parses Benchmarks into logical blocks
- Shows the complete structure of a Benchmark using a number of different views
- Automatically finds all references to or from any logical Element
- Allows any element to be opened and edited on a field-by-field basis
  - Users can modify the structure of the fields of a logical Element
  - Users can modify the values of fields within a logical Element
  - The tool always forces schema compliance
- All opened files can be searched for specific Elements
- Files can be edited by dragging and dropping Elements to copy, move, or create references between them

Benchmark Class

- This free, one-day seminar is designed to teach participants how to create Security Guidance that is:
  - Standards-Based
  - Structured
  - Automatable
- Share experience, knowledge, and tools to help vendors and security content developers produce good benchmarks more efficiently.

benchmarkcourse@mitre.org

Who Creates the Content?

- Primary Source Vendors
  - intimate knowledge
  - already doing the research
  - know when things change
- Researchers
  - vulnerability shops
  - configuration guide experts

Known Repositories

- Patches
  - Red Hat (http://www.redhat.com/oval)
  - Debian (http://www.debian.org/security/oval)
- Vulnerability
  - OVAL Repository (http://oval.mitre.org/repository)
    - Microsoft Windows
    - Sun Solaris
    - HP-UX
    - Cisco
- Benchmarks
  - NVD (http://nvd.nist.gov)

Summary

- Content is our biggest challenge
  - who, how, when
- It is a true community effort
  - with community wide benefits

MITRE