The OVAL Repository

Matthew N. Wojcik

MITRE

© 2004 The MITRE Corporation. All rights reserved

Background

- A primary aim of the OVAL project is to promote the availability and sharing of open, machine-readable security content, specifically in the area of machine state information.
- Two main tools
  - The language specifies how to describe what to test for (definitions), what was actually found (system characteristics), and the outcome of analysis (results).
  - The Repository is an open collection of tests written and maintained by the community. Its aim is to reduce duplication of effort, spread the burden, and tap into a broad pool of expertise.

Goal: Primary-source vendors publishing machine-readable security content

© 2004 The MITRE Corporation. All rights reserved

Early History – 2002-2003

- MITRE created Repository web pages for content download and review, and OVAL Discussion List (aka Community Forum) for email discussion of content
- Initially all content created by MITRE
  - Windows and Solaris, shifting to Windows and Red Hat
- Limited community participation
  - Only occasional feedback on the list
  - With no tools to consume content except Definition Interpreter, hard to build interest—chicken and egg problem
  - With little feedback, hard to judge content quality

© 2004 The MITRE Corporation. All rights reserved

2004-September 2005

- Repository grows, increasing interest
  - 500+ “query” mark in January 2004
  - 1000+ definitions in January 2005
- Transition to XML eases use, boosts adoption
- OVAL Compatibility program
  - 2004: Declarations
  - 2005: Tools available
  - November 2005: First products officially OVAL Compatible
- Somewhat increased feedback on content
- ThreatGuard submissions starting mid-2005
  - Solaris, HP-UX, Mozilla Suite & Firefox, Windows

© 2004 The MITRE Corporation. All rights reserved

October 2005-Present

- ThreatGuard submitting definitions for all new MS Security bulletins beginning in October 2005
- MITRE switches from content authorship to Repository management
  - More work than anticipated
- Significantly increased discussion of Repository content
  - Driven by availability of more tools
- OVAL 5 IDs greatly facilitate multiple repositories
- June 2006: Red Hat announces availability of OVAL patch definitions for all RHEL 3 & 4 errata: www.redhat.com/oval
- MITRE continues to engage other primary-source vendors

© 2004 The MITRE Corporation. All rights reserved

Repository Management Tasks

- Process new submissions
  - Language validation
  - Check for inadvertent changes to existing definitions
  - Content review (in theory!)
- Respond to change suggestions
  - Research, discuss, implement
  - Understand scope of changes and full impact on Repository
  - Moderate any disagreements
- Enact Repository policies
  - Definition status, versioning, change history, attribution
  - CVE Compatibility & feed references to CVE
- Documentation

© 2004 The MITRE Corporation. All rights reserved

Challenges of Repository Management

- Some automation, but much manual
  - Version 5 set back automation
- Timeliness vs. Review
  - Want new submissions available ASAP
  - Comprehensive review is very slow
- Some issues beyond domain expertise of OVAL team
  - That's the whole point of community process!
  - ...but it makes intelligent review or moderation difficult
- Slow adoption of cooperative model
- Some changes have such broad impact they must be approached cautiously (and are hard to implement!)

© 2004 The MITRE Corporation. All rights reserved

Submitting New Content

- New content must be valid OVAL 5
  - Schematron validation
  - Well-formed content makes *everything* easier
- Re-use existing elements where appropriate
  - Tests, objects, states, variables, definitions
  - Copy and edit if close match
- Use Repository metadata
  - Status: INITIAL SUBMISSION
  - Version: 0
  - Contributor: Give yourself credit!
- Use appropriate references
  - CVEs whenever possible—use CVE Description if vuln def
- Co-ordinate with MITRE and Discussion list!
  - ID service
  - Avoid duplication of effort

© 2004 The MITRE Corporation. All rights reserved

Submitting Changes

- Understand the scope!
  - Where is the {test, object, state, variable, definition} used?
  - Is the change appropriate globally, or to some uses?
- Simple changes best sent to Discussion List
  - Easier for MITRE to make changes than vet submission file
- Valid OVAL Doc for complex or wide-reaching changes
  - Start with the most recent version
  - Discuss on list to ensure acceptance!
  - Consult MITRE for proper use of metadata
- Deprecation
  - Discuss with MITRE

© 2004 The MITRE Corporation. All rights reserved

Discussion

- How can we spread the burden?
  - Volunteers for content review
  - More groups involved in definition creation
  - Signup facility?
- Primary-souce content
  - Will there be demand for Repository definitions if software vendor supplies OVAL content?
  - Should Repository policy allow?
  - What added value is required?
  - How do we support extended definitions?
- Future of the Repository
  - As more collections of content come online, is there a need for “The OVAL Repository”?
  - Definition types?

© 2004 The MITRE Corporation. All rights reserved