

The bright future of the Extensible Configuration Checklist format (XCCDF), the Open Vulnerability Assessment Language (OVAL) and its friends

- Slides are online at OVALtools.org
- Please register for our announce and/or discussion mailing lists at OVALtools.org



About

- This talk...
 - Intended to make you aware of the growing movement of OVAL and XCCDF
 - Including what's happening at NUCIA.UNOmaha.edu
 - Based on
 - Stephen Quinn & Peter Mell's talk on Technical Control Automation
 - **Jay Beale's OVAL talk**
 - Robert Martin's paper
 - OVAL & XCCDF talk from RSA2006
 - OVAL and XCCDF websites
 - These slides and source documents are online at:
 - OVALtools.org
 - There are also mailing lists – please signup!
- This speaker...
 - Matt Payne, CISSP & NUCIA.UNOmaha.edu Fellow



Agenda

- Managing risk: certification and accreditation
 - Yesterday, today, and tomorrow
- Semi-Automation not automation
- OVAL and XCCDF Overview
- Future Visions
- What's easy for a computer is not easy for a person
 - Need for a DSL
- What you can do!





Managing risk: certification and accreditation

- “Risk Management – The fine art of getting to feel good.” – BB 7/8/5
- **Certification and Accreditation (C&A):**
 - “a process for managing risk”
 - “...process, set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) and security posture...throughout the life cycle of the system”
 - Wikipedia on DITSCAP
 - <http://tinyurl.com/n48yz>
 - FYI DITSCAP has been replaced by DIACAP

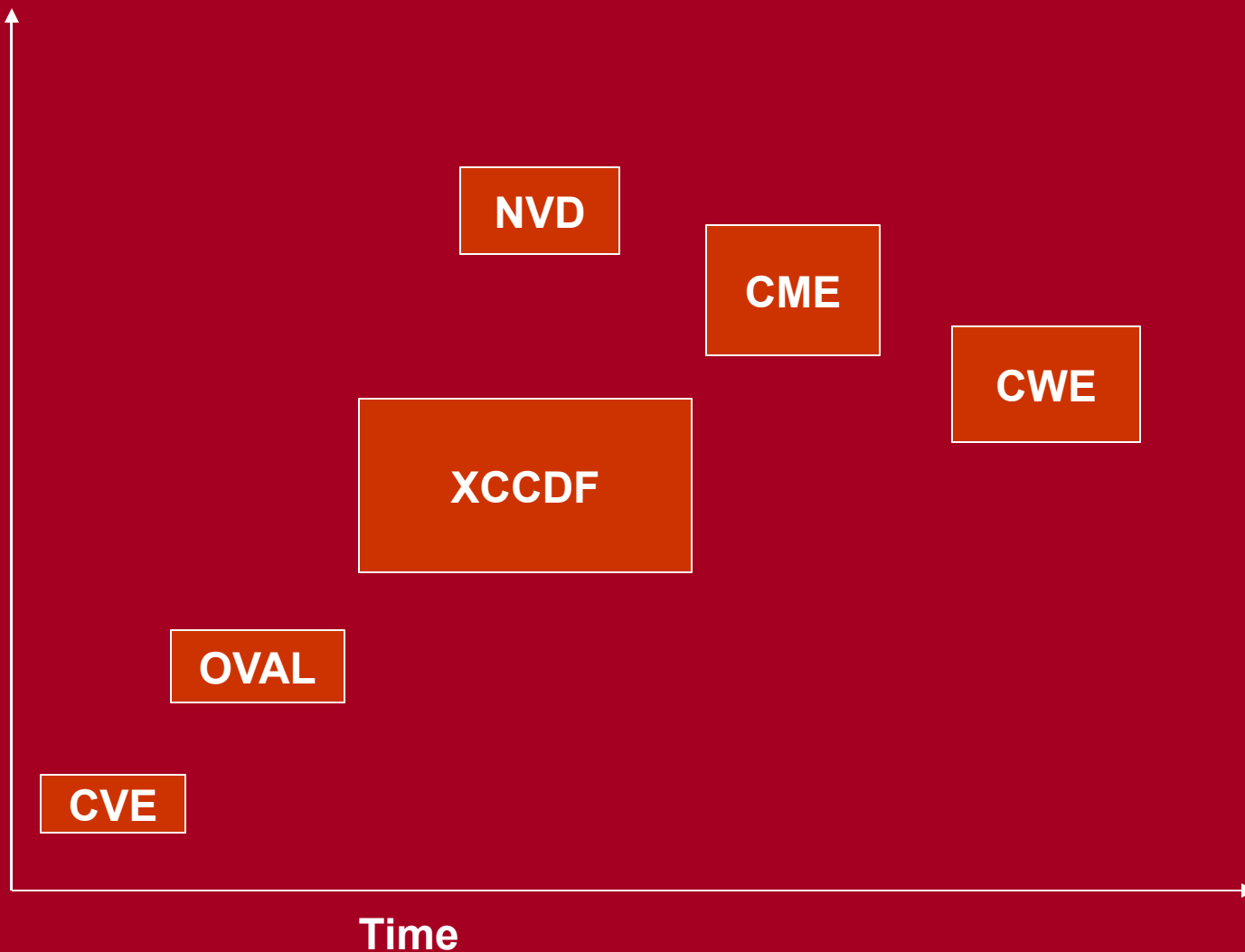
C&A Yesterday, today, and tomorrow

- Yesterday
 - Pondering, slow, driven by subject matter experts
- Today
 - Mandates for faster turnaround
 - Guidance is mainly prose based: STIGS, NIST, SNAC, etc
 - Proprietary one off tools such as the GOLD Disk and friends
 - Documents are static (created/updated every 3 years)
 - Little situational awareness
- Tomorrow
 - Pondering, fast, builds subject matter experts
 - Driven by open standards and COTS that compete on performance and features
 - Guidance is mainly based on open standards: XCCDF and OVAL
 - Better situational awareness; the SSAA is expressed in XCCDF!
 - Documents have a dynamic component



Evolution of Open Standards

Expressiveness





NIST Checklist Program

Encourage Vendor Development and Maintenance of Security Guidance.

Currently Hosts 95 separate guidance documents for over 143 IT products.

In English Prose and automation-enabling formats (i.e. .inf files, scripts, etc.)

Need to provide configuration data in standard, consumable format.

<http://checklists.nist.gov>

NIST 800-68 alpha

- **SP 800-68**
 - Guidance for Securing Microsoft Winc
 - October 2005
- **NIST 800-68 alpha content at**
 - <http://checklists.nist.gov/NIST-800-68-alpha>
 - aka <http://tinyurl.com/oxztm>



Semi-Automation not automation

- Open standards improve innovation
 - All us to focus on the knowledge and wisdom
 - Not data formats
- Danger! We do not want to set it and forget it!
- XCCDF, OVAL and friends create tools for making baselines not destinations!
- We want to spend time managing risk not reworking what we already know.
- Semi-Automation will improve situational awareness enabling many things....

Your Key to Security

Getting better all the time...



A NIST Vision

Config

Standards

**Integration
Projects**



**Couple
patches
and
Config
checking**

Patches



Involved Organizations



Standards



Integration Projects



IT Security Vendors



DOD COTS Products

Some left out?

The Coming Wave in C&A

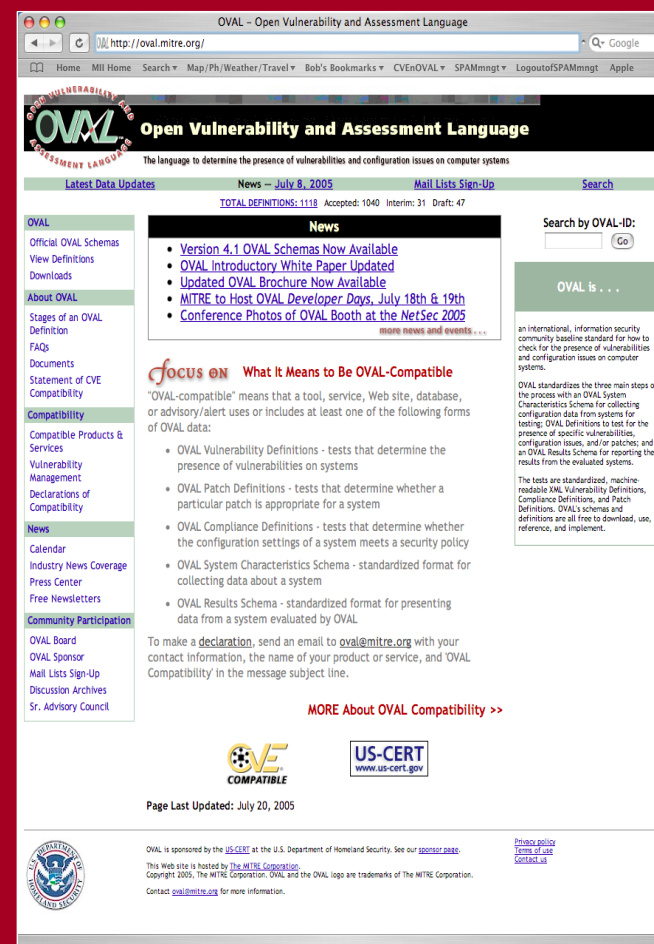
- The big picture -- It's all about reducing risk. Increasing knowledge is one way of reducing risk.
- The good!
 - OVAL+XCCDF+CVE+CME+CWE and the coming revolution in certification and accreditation (C&A) with Smart data led by NSA and MITRE.
- The bad!
 - Checklists can have problems
- The challenge
 - Benefits of automation without the pitfalls



OVAL Concept

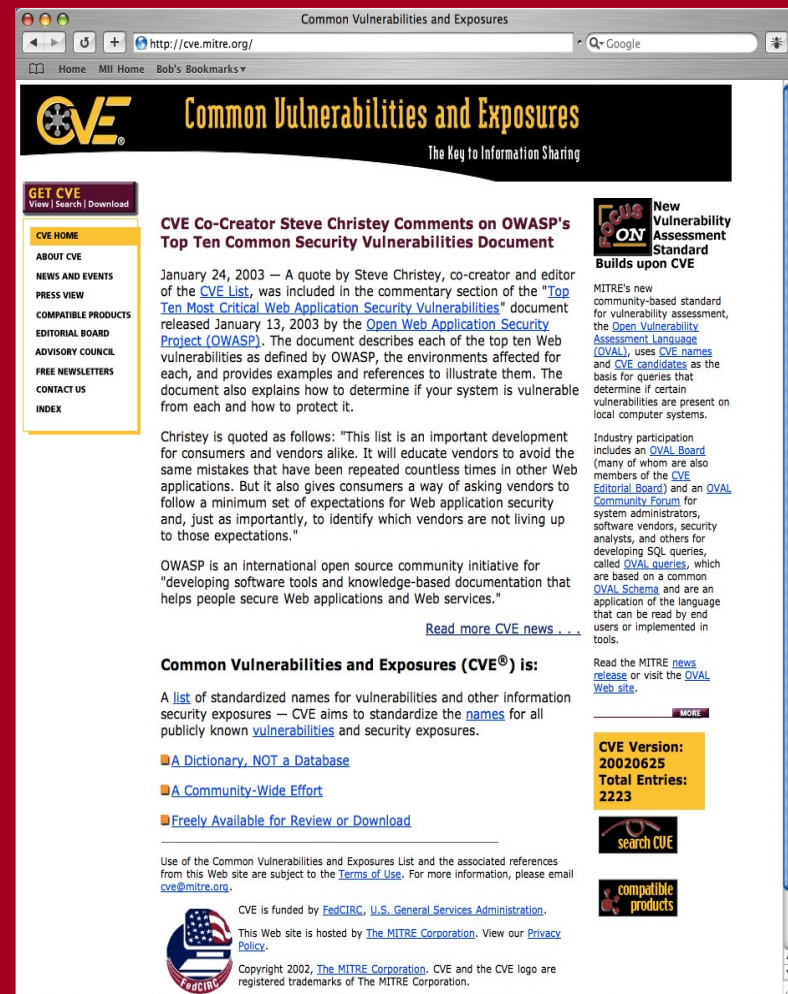
- The Open Vulnerability and Assessment Language Initiative

- Community-based collaboration
- Precise definitions to test for each vulnerability, misconfiguration, policy, or patch
- Standard schema of security-relevant configuration information
- OVAL schema and definitions freely available for download, public review, and comment
- Security community suggests new definitions and schema
- OVAL board considers proposed schema modifications



The Common Vulnerabilities and Exposures (CVE) Initiative

- An international security community activity led by MITRE focused on developing a list that provides common names for publicly known information security vulnerabilities and exposures.
- Key tenets
 - One name for one vulnerability or exposure
 - One standardized description for each vulnerability or exposure
 - Existence as a dictionary rather than a database
 - Publicly accessible for review or download from the Internet
 - Industry participation in open forum (editorial board)
- The CVE list and information about the CVE effort are available on the CVE web site at [cve.mitre.org]

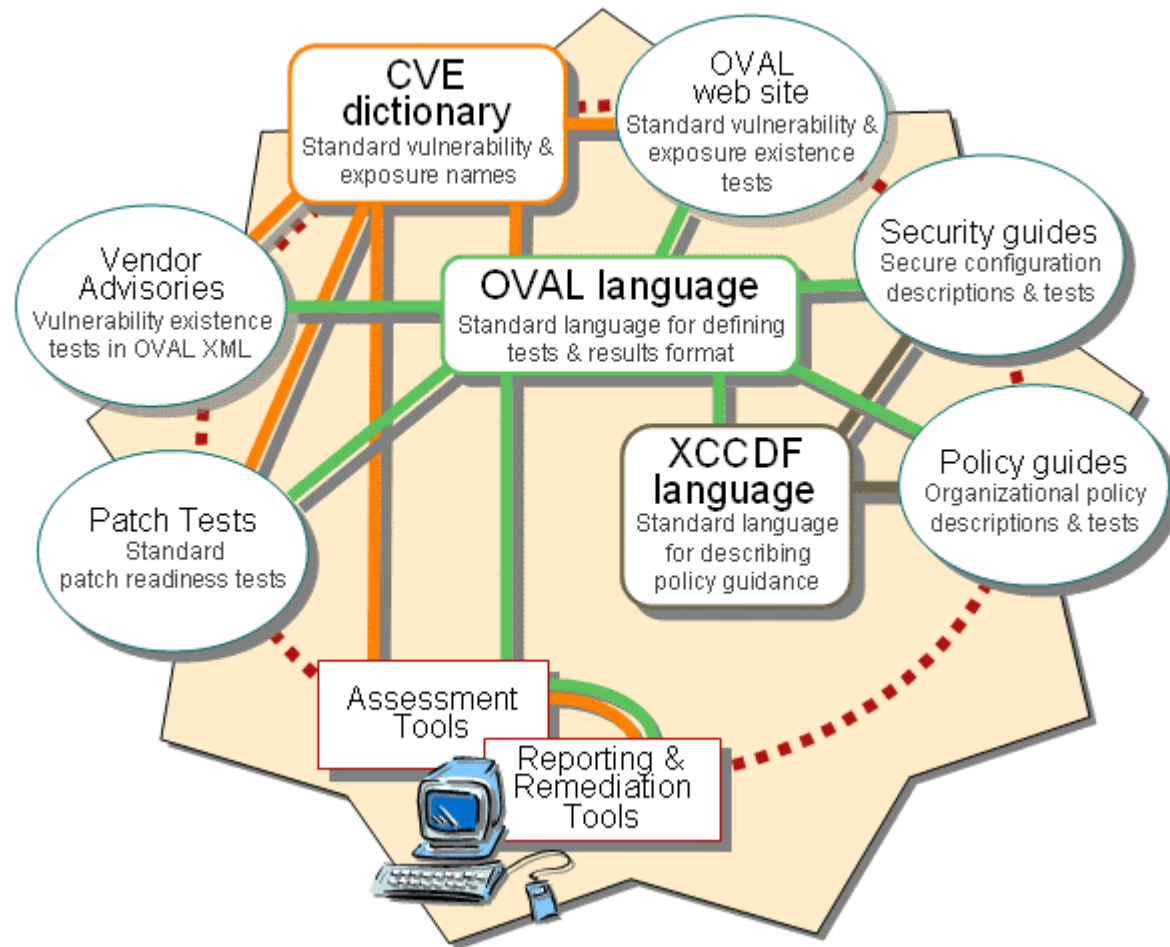


One of Bob Martin's Future Visions

Transformational Vulnerability Management Through Standards

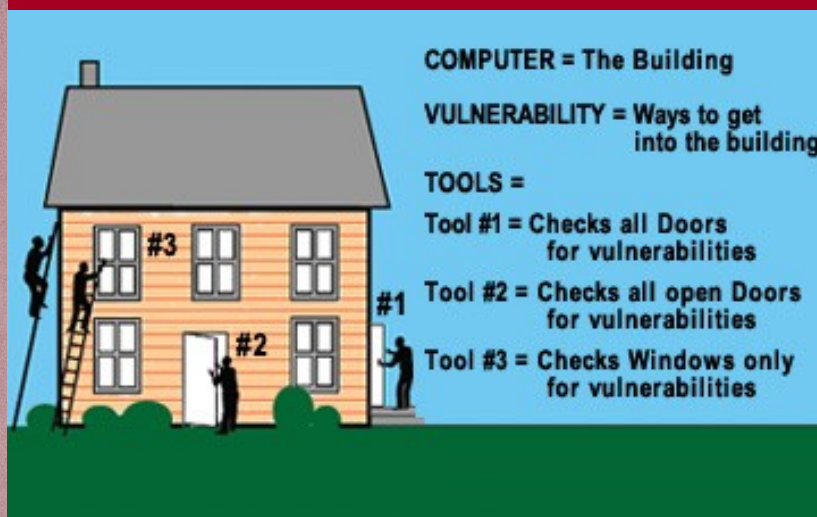
- Robert A. Martin in CrossTalk
- May 2005
- tinyurl.com/jr5qv

Standards for Enabling Automation in Information Security



Checklists can have problems

- From the OVAL Introduction document:



- Remember! You can not test for the absence of flaws
- e.g. using a chain saw to come in through the wall.
- Checklists should be a baseline – a beginning; not a destination!



Robert A. Martin Writes:

- Obtaining capabilities that:
 - can import the OVAL XML results for remediation,
 - organizational status reporting,
 - generating certification and accreditation reports,
 - the DoD will have created a focused, efficient, timely, and effective enterprise incident management and remediation process
 - by adopting information security products, services, and methodologies that support the CVE naming standard and use OVAL test definitions and results schemas.
 - By also adopting the XCCDF standard, the DoD will be able to take the improvements in these areas on to a fuller set of policy and configuration management arenas.
- Collectively these changes will dramatically improve the insight and oversight of the security and integrity of the systems and networks...

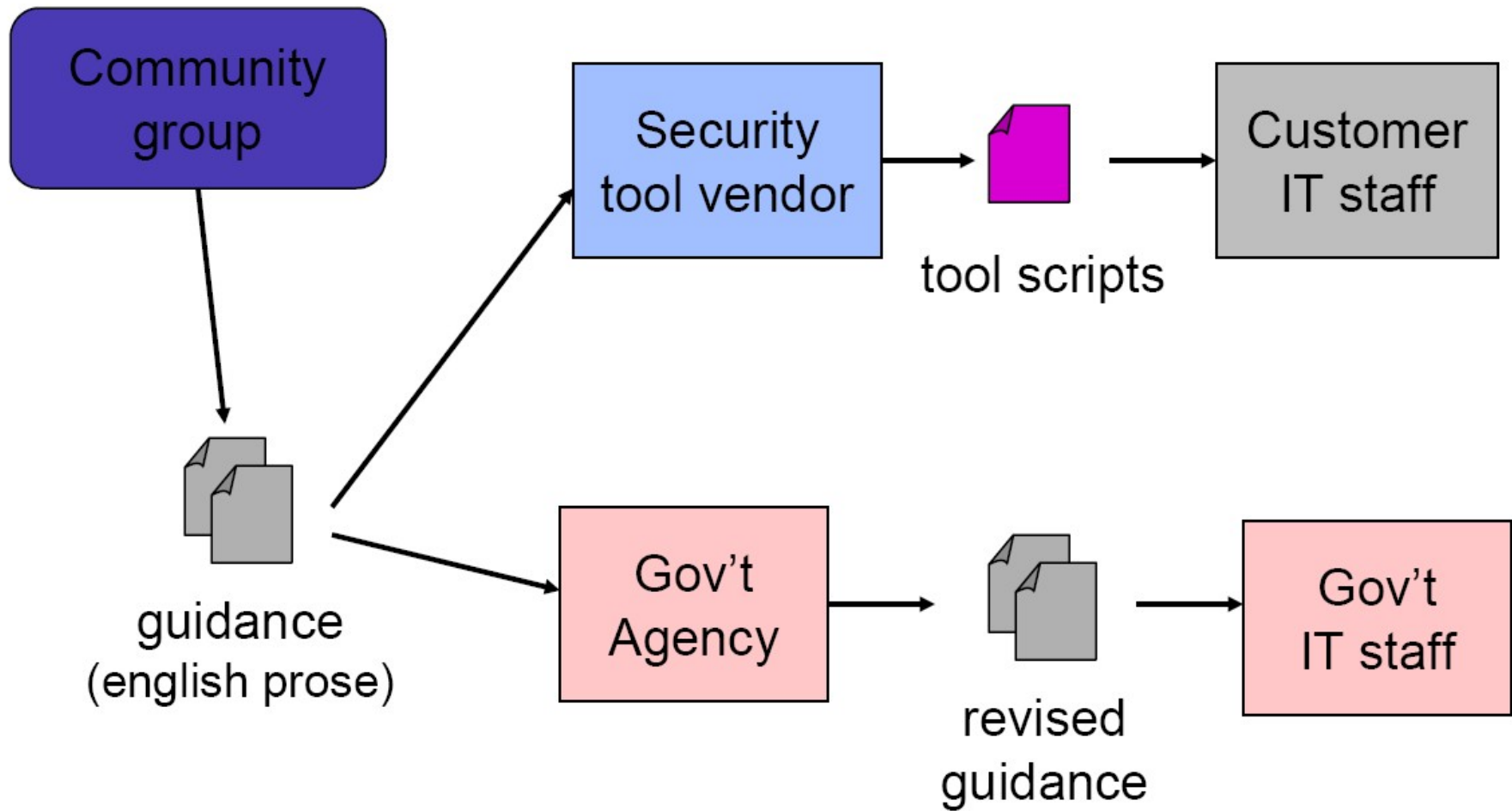


What is XCCDF?

- XCCDF is a way to solve serious problems in the way information assurance is practiced.
- XCCDF is poised to become part of the common language of information assurance.
- XCCDF is a big part of the IA professional's future
 - No more knowledge and wisdom trapped in Microsoft office!

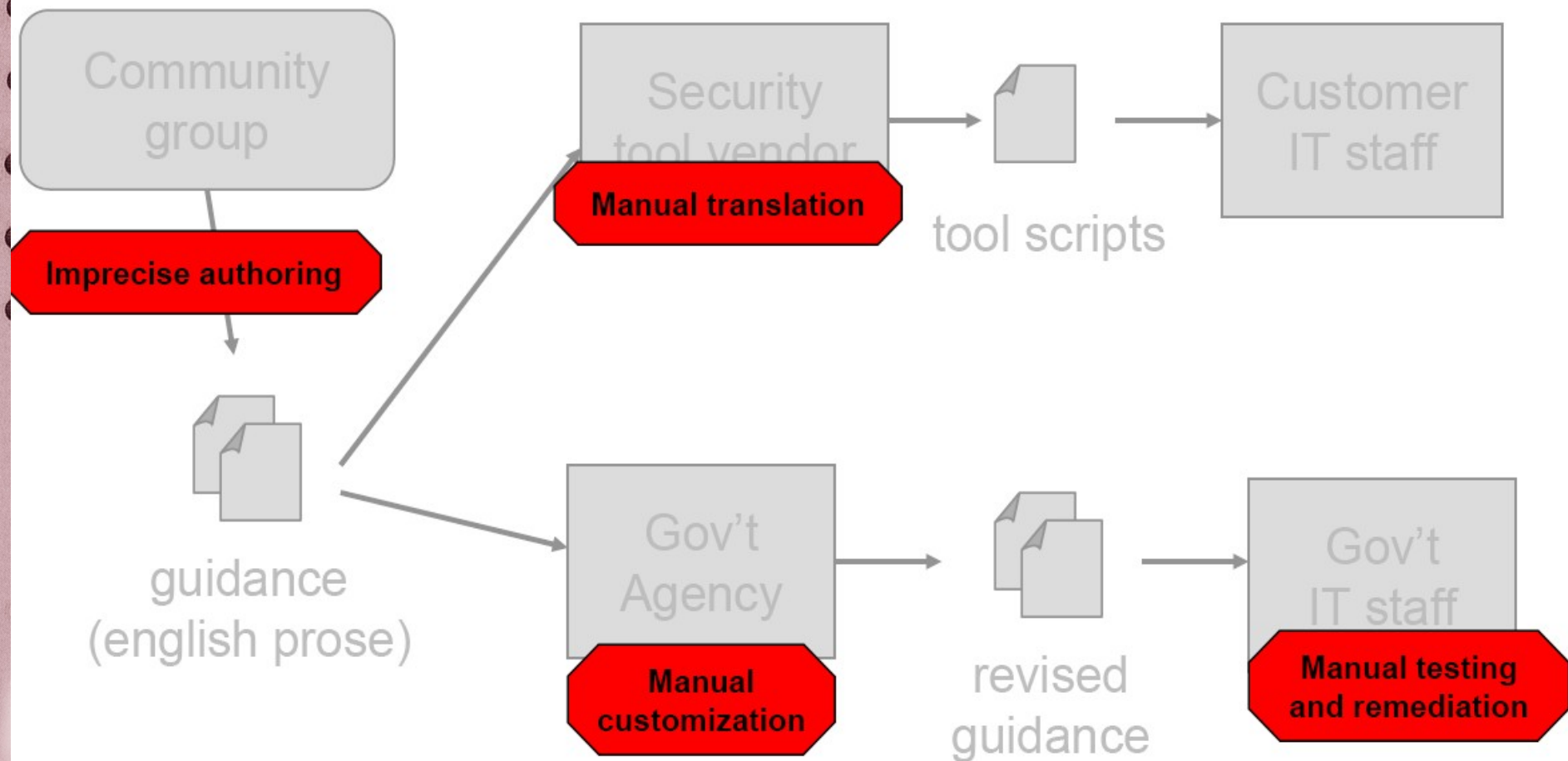
Your Key to Security

Scenario 1, Community Guidance - Today

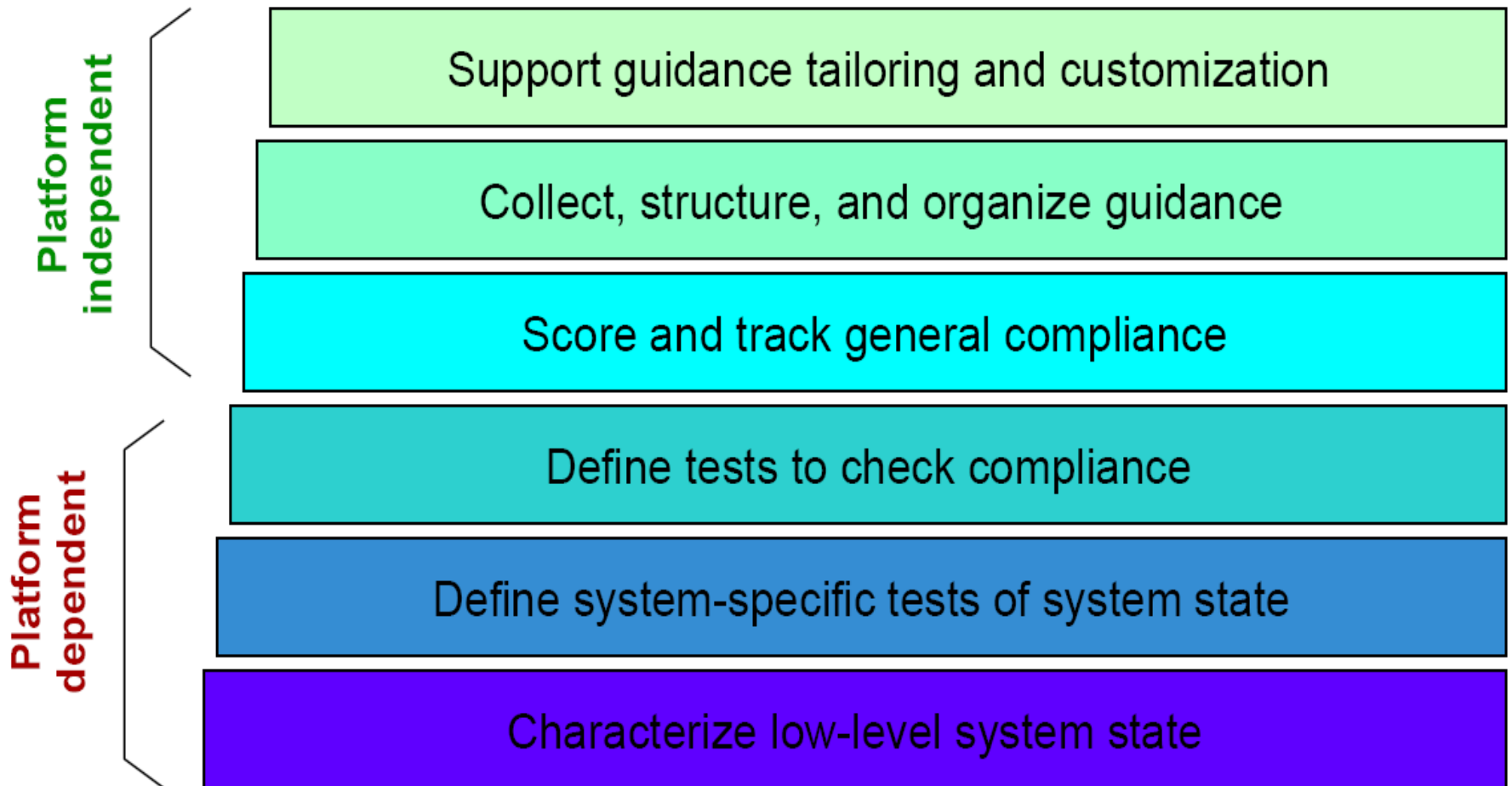


Scenario 1, Community Guidance - Today

What can go wrong?



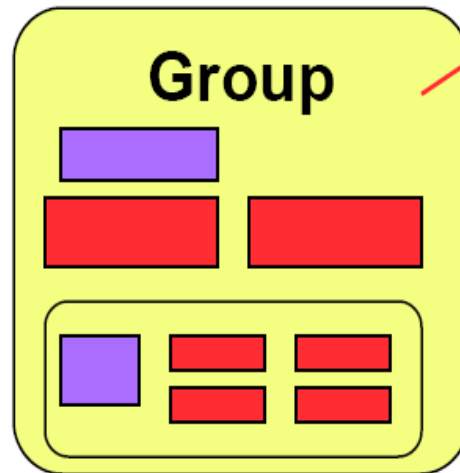
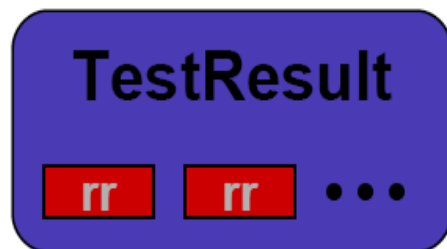
We need a language or languages to address these areas:



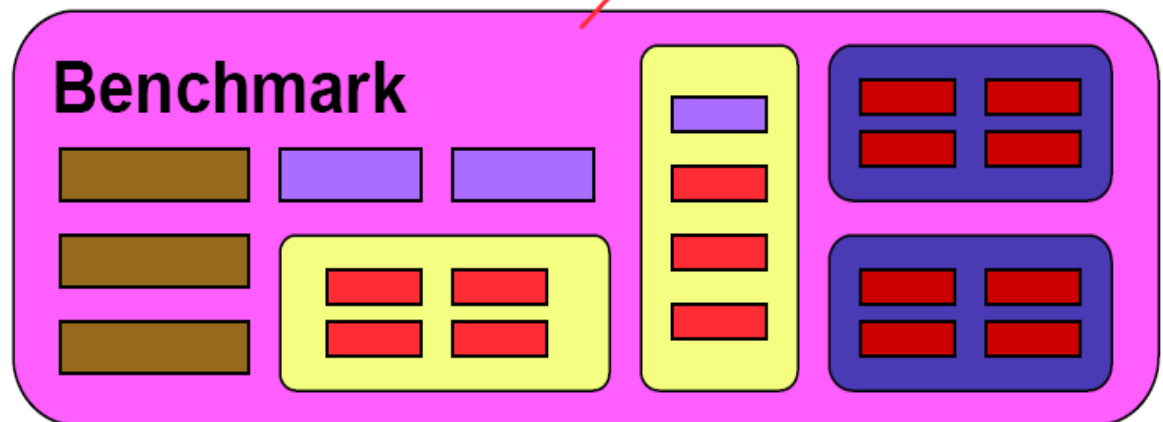
Two such languages are in development:



XCCDF defines the following object types:



Groups can contain Values and Rules, and can be nested.



A Benchmark can contain some of everything

Why XCCDF?

- “The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and **thereby foster more widespread application of good security practices.**”



XCCDF Will do...

- “XCCDF is a specification **language for writing security checklists, benchmarks, and related kinds of documents.**
- An XCCDF document represents a **structured collection of security configuration rules for some set of target systems.**
- The specification is **designed to support:**
 - **information interchange**
 - **document generation**
 - **organizational and situational tailoring**
 - **automated compliance testing**
 - **and compliance scoring.**
- The specification also defines a data model and format for storing results of benchmark compliance testing.”



Your Key to Security

Who does XCCDF?

- Development of the XCCDF specification is being led by NSA, with contributions from other agencies and organizations.
- Development of the OVAL specification is led by Mitre -- <http://oval.mitre.org/>
 - Mitre is a federally funded research center (FFRC)
 - Mitre also produces a BSD licensed OVAL scanner.
- Currently the Center for Internet Security has the only XCCDF system available.
 - This system is free but not open source. “free beer”
 - http://en.wikipedia.org/wiki/Free_beer
- Tailoring will cost you thousands of dollars!
- Other organizations are following with their own XCCDF efforts.
 - The OVALtools.org group is considering building an XCCDF system.
- XCCDF and OVAL have large boards made up of government, industry, and academia.

» Source: tinyurl.com/9cabh

OVAL Board Members

- Academic/Educational
 - CERIAs/Purdue University
 - Pascal Meunier
- Other Security Experts
 - Bastille Linux
 - Center for Internet Security
 - CERT
 - DISA
 - NSA
- This list is incomplete.
 - Source:
tinyurl.com/9mlmh
- Operating Systems/Software Vendors
 - IBM
 - Microsoft
 - RedHat
 - Debian
 - Cisco
 - Adobe
- Tool Vendors
 - CSC, Harris, Symantec



The Current OVAL Board



Others are being added all the time...

Where is XCCDF?

Soon XCCDF will be in more and more places!

Extensible Configuration Checklist Description Format (XCCDF), with its associated standards and tools, is part of a fast-growing movement:

- Semi-automation of system scans and scoring
- Interoperable, vendor-neutral data
- Semi-automated document generation
- Current Repository:
 - <http://checklists.nist.gov/repository/index.html>



Your Key to Security

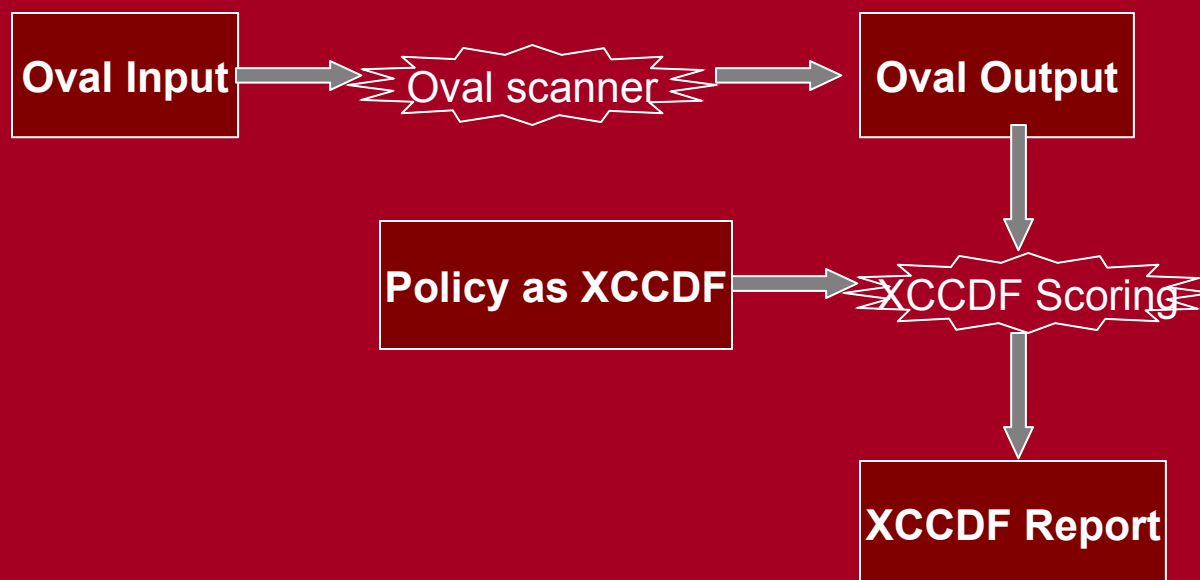
When?

- The XCCDF movement is very new.
- The OVAL movement is a bit older
 - And more accepted.
- NUCIA hopes to have some XCCDF tools in Beta test later this year.
 - Please email Payne@MattPayne.org for more info

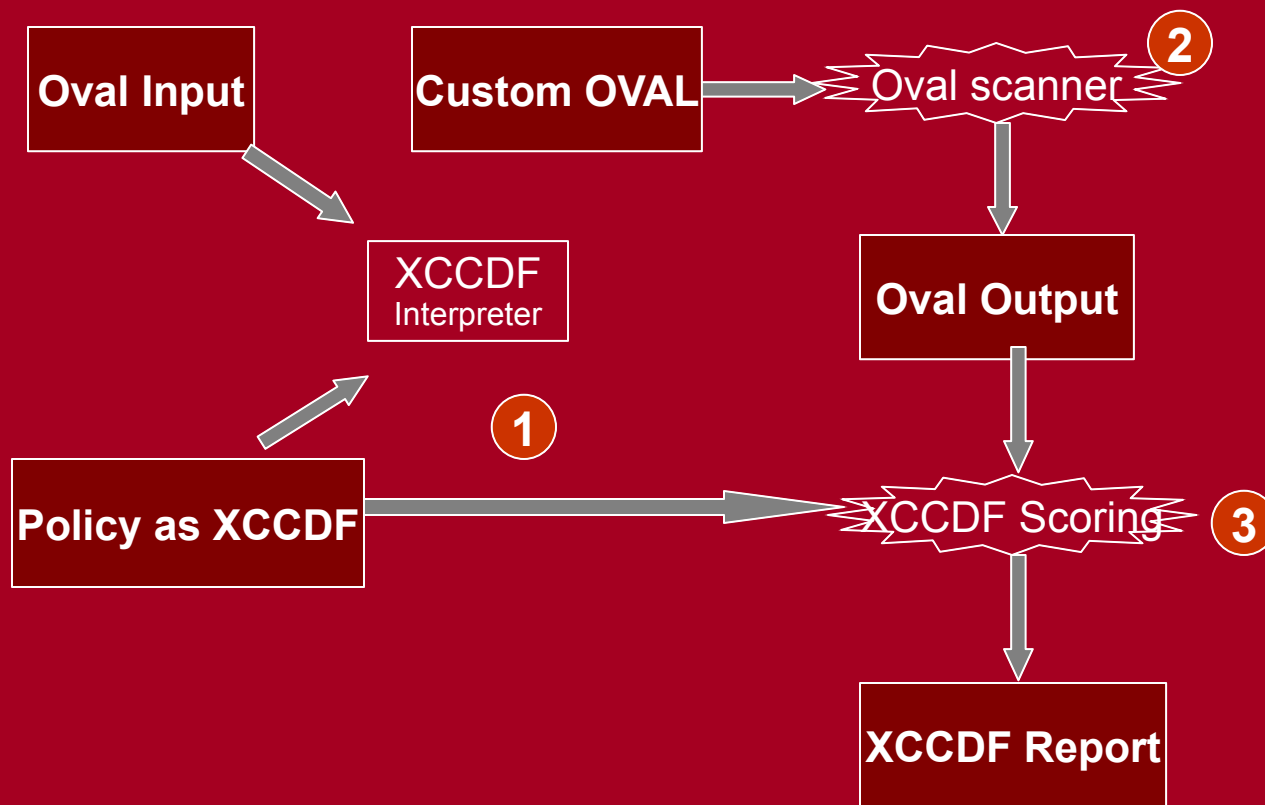


Your Key to Security

How: A simple way...



How: Drive OVAL w/ XCCDF



Sample XCCDF Report

Compliance Validation Report - Mozilla Firefox

File Edit View Go Bookmarks Tools Help del.icio.us

file:///C:/Documents%20and%20Settin... Go wikipedia free beer

J2SE API post to del.icio.us https://hecate.gds.uno... TinyURL! Sub with Bloglines

Start Stumbling...

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools

Gmail - Inbox... Google Calen... OVAL - Open... WGratis versus... Compliance...

Summary

Computer Name: lappy
Benchmark: Windows XP Professional Benchmark
Profile: SP2 Legacy Standalone
Scan Time: 05/18/2006 10:02:27

Description	Items		Score	
	Passed	Failed	Actual	Max
1 Service Packs and Security Updates	1	1	10.000	20.000
1.1 Major Service Pack and Security Update Requirements	1	0	10.000	10.000
1.2 Minor Service Pack and Security Update Requirements	0	1	0.000	10.000
2 Auditing and Account Policies	9	15	8.333	20.000
2.1 Major Auditing and Account Policies Requirements	1	1	5.000	10.000
2.2 Minor Auditing and Account Policies Requirements	8	14	3.333	10.000
2.2.1 Audit Policy (minimums)	0	7	0.000	2.500
2.2.2 Account Policy	2	4	0.833	2.500
2.2.3 Account Lockout Policy	0	3	0.000	2.500
2.2.4 Event Log Settings - Application, Security, and System Logs	6	0	2.500	2.500
2.2.4.1 Application Log	2	0	0.833	0.833
2.2.4.2 Security Log	2	0	0.833	0.833
2.2.4.3 System Log	2	0	0.833	0.833
3 Security Settings	20	22	8.000	20.000
3.1 Major Security Settings	2	2	5.000	10.000
3.2 Minor Security Settings	18	20	3.000	10.000
3.2.1 Security Options	18	12	3.000	5.000
3.2.2 Additional Registry Settings	0	8	0.000	5.000

Find: beer Find Next Find Previous Highlight all Match case

Done 0.968s Open Notebook Adblock

Your Key to Security

Free CIS Benchmarks

- <http://www.cisecurity.org/index.html>
- Which ones use XCCDF?
 - Windows XP
 - Not Apache!
 - Not too much else in XCCDF yet...



Your Key to Security

OVAL Scanners

- The MITRE OVAL definition interpreters are BSD licensed, while the content is basically freeware.
- Many other scanners are commercial
 - threatguard.com's
 - OEM kit
- You could create an infrastructure. One way you might do this:
 - Place an agent on each host that receives new definitions files, runs an interpreter, and sends back results.xml files.
 - A central console could receive and parse those results files, allowing you to check for vulnerabilities for which you don't yet have definitions.
 - Imagine if the central console pushed all the data covered by the schema, for each machine, into an SQL database.



OVAL Scanner

- Notes on MITRE's OVAL definition interpreter.
 1. Download version 5 of the interpreter from <http://oval.mitre.org/oval/download/interpreter/index.html> which is the most current version listed.
 2. Installed the interpreter to hdd.
 3. ran the commands

```
cd c:\program files\oval\ovaldi
ovaldi -m -o windows.definitions.xml -r results_file.xml
```
 4. checked the results vs the definitions
 5. created a simple, one-test, definitions file (windows.ie-installed.xml) that only checks to see if IE 6 is installed
 6. ran the command

```
ovaldi -m -o windows.ie-installed.xml -r simple_results.xml
```
 7. reviewed results



Your Key to Security


Why Host based?

- Host-based means that you can test for vulns that can't be checked by the network.
 - Network-based probably can't test for around half of the vulns we'd like to know about
- Host-based potentially means better accuracy.
 - Network-based has a much-reduced interaction.
- Host-based does present scalability problems.



OVAl Schema & Definitions

- XML, SQL, & Pseudo Code
- Schemas for:
 - Microsoft Windows
 - NT 4.0, 2000, XP, 98, & Server 2003
 - Sun Solaris 7, 8, 9
 - Red Hat Linux
- Draft Schemas
 - Hewlett-Packard UNIX (HP-UX)
 - Debian Linux
- Definitions for above and some applications
 - IIS 4.0 and 5.0; Internet Explorer 5.01, 5.5, and 6.0; and SQL Server 2000
- This was 2004!
- There's more now.



Open Vulnerability Assessment Language

The language to determine the presence of software vulnerabilities

[Latest Data Updates](#) News – [March 10, 2004](#) [Join the Community Forum](#) [Search](#)

[Get OVAL Vulnerability Definitions](#)
[Official OVAL Schema](#)
[Submit a Definition](#)
[Submission Guidelines](#)
[Downloads](#)
[About OVAL](#)
[Platforms Supported](#)
[How to Use OVAL](#)
[Stages of an OVAL Definition](#)
[Documents](#)
[FAQs](#)
[Statement of CVE Compatibility](#)
[News](#)
[Calendar](#)
[Industry News Coverage](#)
[Press Center](#)
[Press Releases](#)
[OVAL Board](#)
[Board Members](#)
[Board Discussion Archive](#)
[Board Meetings Archive](#)
[Community Forum](#)
[How to Participate](#)
[Discussion Archive](#)

OVAL Vulnerability Definition #566 Date Modified: 2004-03-09

OVAL-ID: OVAL566	CVE-ID: CAN-2003-0817	Platform(s): Microsoft Windows XP 64-Bit Edition, Version 2003 Microsoft Windows Server 2003 Microsoft Windows Server 2003 64-Bit Edition
Summary: CAN-2003-0817	Status: INTERIM	
Version: 0	Schema Version Used: 3	

Description:
Internet Explorer 5.01 through 6 SP1 allows remote attackers to bypass zone restrictions and read arbitrary files via an XML object.

Definition Synopsis:

- Vulnerable software exists
 - Internet Explorer 6 Service Pack 1 for Windows Server 2003 is installed
 - the version of mshtml.dll is less than 6.0.3790.94
 - the patch q824145 is not installed
- Vulnerable configuration
 - ActiveX controls and active scripting are enabled

Pseudocode **SQL** **XML**

Pseudocode

Your machine is vulnerable if ...

vulnerable software section:

```
Internet Explorer 6 Service Pack 1 for Windows Server 2003 is installed
-----
-- registry_test:
    • the hive 'HKEY_LOCAL_MACHINE' exists
    • the key 'SOFTWARE\Microsoft\Internet Explorer' exists
    • the name 'Version' exists
    • the value equals '6.00.3790.0000'

AND

the version of mshtml.dll is less than 6.0.3790.94
-----
-- file_test:
    • the file %WinDir%\System32\mshtml.dll exists
    • the version is less than '6.0.3790.94'

AND NOT

the patch q824145 is installed (Hotfix key)
-----
-- registry_test:
    • the hive 'HKEY_LOCAL_MACHINE' exists
    • the key 'SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\KB824245' exists
    • the name 'Installed' exists
    • the value equals 1

vulnerable configuration section:

AND

ActiveX controls and active scripting are enabled
-----
(
    local machine settings are being used and ActiveX controls and active scripting are enabled
    -----
)
```

CIS OVAL Packages: 2006

- Apache Level 1&2
- Solaris (Level-1) (All Versions)
- Oracle Level 1&2
- Cisco IOS Router/PIX
- HP-UX Level-1
- FreeBSD Level-1
- OS X Level-1
- Linux Level-1
- Wireless Networks
- BIND
- Automated Scanning Tool for the SANS/FBI "Top 20" List
- Windows XP Professional
- Win 2000 Professional (Level-2)
- Win 2000 Server (Level-2)
- Win 2000 (Level-1)
- Windows Server 2003
- SQL Server 2000
- Exchange Server
- Patchwork Utility for Windows NT

Source: tinyurl.com/7qlzj



NVD.NIST.GOV & CVE.MITRE.ORG & OVAL.MITRE.ORG

- **NVD contains:**
- 16193 CVE Vulnerabilities
- 53 US-CERT Alerts
- 1230 US-CERT Vuln Notes
- 1162 Oval Queries
- **Last updated:**
- 04/04/06
- **Publication rate:**
- 18 vulnerabilities / day

- OVAL-IDs Now Available for Most Recent Microsoft Security Bulletins
- FrSIRT Includes OVAL-IDs in Security Advisories
- Release Candidates of the Version 5.0 OVAL Schemas Now Available
- OVAL Interpreter Updated for Version 5.0 Release Candidates
- OVAL Presents Briefing at MISTI's FISMA Risk Management & Compliance Training Symposium on March 14th
- OVAL Initiative Surpasses 1,500+ Definitions



Sample OVAL output

OVAL Results

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address C:\Documents and Settings\Payne\Desktop\stylesheet\simple_results_fail.xml Go

System Information				
Host Name	lappy			
Operating System	Microsoft Windows XP Professional Service Pack 2			
Operating System Version	5.1.2600			
Architecture	INTEL32			
Interfaces				
Interface Name	Intel(R) PRO/Wireless 2200BG Network Connection			
IP Address	192.168.1.14			
MAC Address	00-0E-35-70-29-DA			
Interface Name	MS TCP Loopback interface			
IP Address	127.0.0.1			
MAC Address				
Schema Information				
Schema Name	Schema Version	Product Name	Product Version	Timestamp
Oval Schema	4.2			05/17/2006 23:09:09
System Characteristics Schema	4	OVAL Definition Interpreter	4.3	05/23/2006 10:21:01
Results Schema	4	OVAL Definition Interpreter	4.3	05/23/2006 10:21:01
Oval Test Results				
Vulnerable		Not Vulnerable		Unknown
OVAL ID	CVE ID	Description	Status	Version
OVAL1337	CVE-test-ie-bad	Microsoft Internet Explorer is installed, which is a bad idea.	ACCEPTED	1

Done My Computer



Your Key to Security

The XML before the XSLT

```

simple_results_fail.xml (-\Desktop\stylesheet) - GVIM
File Edit Tools Syntax Buffers Window Help
[Icons]
1 <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
2 +-- 2 lines: <?xml-stylesheet type="text/xsl" href="results_to_html.xsl"?>----
4
5 <generators>
6 +-- 4 lines: <oval>-----
10 <system_characteristics>
11 <product_name>OVAL Definition Interpreter</product_name>
12 <product_version>4.3</product_version>
13 <schema_version>4</schema_version>
14 <timestamp>20060523102101</timestamp>
15 </system_characteristics>
16 +-- 6 lines: <results>-----
22 </generators>
23
24 +-- 18 lines: <system_info>-----
42
43 <definitions>
44 <definition class="vulnerability" id="OVAL1337" instance="1">
45 <affected family="windows">
46 <windows:platform>Microsoft Windows XP</windows:platform>
47 <product>Internet Explorer</product>
48 </affected>
49 <description>Microsoft Internet Explorer is installed, which is a bad ide
a.</description>
50 <reference source="CUE">CUE-test-ie-bad</reference>
51 <status>ACCEPTED</status>
52 <version>1</version>
53 <criteria result="1">
54 <software operation="OR" result="1">
55 <criteria comment="Internet Explorer 6 is installed" negate="false"
result="1" test_ref="wrt-10027" version="1"/>
56 <criteria comment="Internet Explorer 7 in installed" negate="false"
result="0" test_ref="wrt-10028" version="1"/>
57 </software>
58 </criteria>

```

16,1

Top

Your Key to Security

OVAL Definition: Example

```
<definitions>
  <definition id="OVAL575">
    <affected family="windows">
      <windows:platform>Microsoft Windows 2000</windows:platform>
      <product>Microsoft Windows Workstation Service</product>
    </affected>
    <cveid status="CAN">2003-0812</cveid>
    <dates>
      <created date="2003-11-12" />
      <modified date="2004-03-09">Changed the status from INTERIM to ACCEPTED and the version
        from 0 to 1</modified>
    </dates>
    <description> Stack-based buffer overflow in a logging function for Windows Workstation Service
      (WKSSVC.DLL) allows remote attackers to execute arbitrary code via RPC calls that cause long
      entries to be written to a debug log file ("NetSetup.LOG"), as demonstrated using the
      NetAddAlternateComputerName API. </description>
    <status>ACCEPTED</status>
    <version>1</version>
    <criteria>
      <software operation="AND">
        <criterion test_ref="wrt-1" comment="Windows 2000 is installed" />
        <criterion test_ref="wft-8" comment="the version of wkssvc.dll is less than 5.00.2195.6862" />
        <criterion test_ref="wrt-86" negate="true" comment="the patch q828749 is installed (Hotfix key)"
          /> </software>
      <configuration>
        <criterion test_ref="wrt-71" comment="the workstation service is enabled" /> </configuration>
      </criteria>
    </definition> </definitions>
```

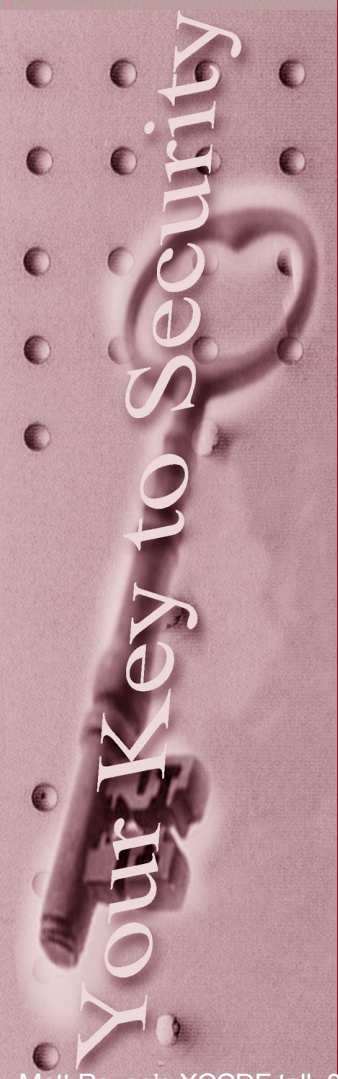

How are the CIS Benchmarks developed?

- The CIS Benchmarks are developed by teams of information security experts from the public, private, and academic sectors. Most development teams communication takes place via e-mail. Conference calls are held periodically to discuss in depth technical issues.

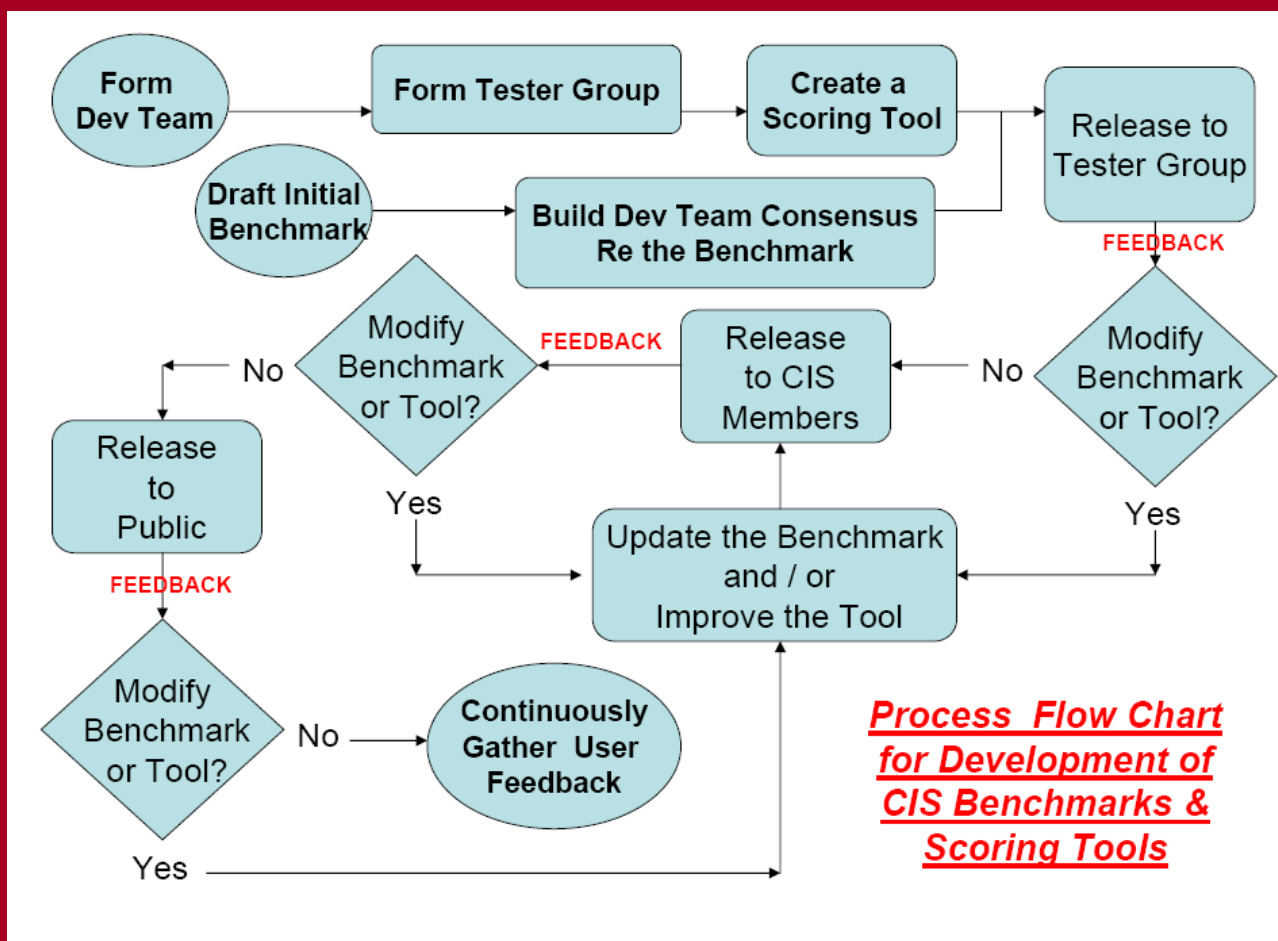
The phases of the Benchmark development process are as follows:

Initial Benchmark draft --> Core team consensus --> CIS members consensus --> Public release --> Maintenance of "broad end-user consensus" through periodic updates.

The objective is to provide consensus configuration Benchmarks that are user originated, continuously updated, and globally accepted. Participation by you and you colleagues is the key to success.



CIS Benchmark Dev Flow chart...



New CIS Benchmarks in Development

- **New Benchmarks and Scoring Tools in development:**
APPLICATIONS

OPERATING SYSTEMS

OS 400

Novell Netware

NETWORK DEVICES

Check Point FW-1/VPN-1 (Levels 1 & 2)

Cisco CAT Switches (Levels 1 & 2)

Juniper Routers (Levels 1 & 2)

Active Work Is Now Underway To Update These Released Benchmarks: Red Hat Linux
OS X



Your Key to Security

HELP WANTED!

- INDEPENDENT CONTRACTORS NEEDED FOR CONVERSION OF BENCHMARKS TO XCCDF FORMAT.

This conversion work is on the critical path for development of the CIS NG Scoring Tool, and is an urgent need.

The new tool is Java based and uses a new proposed XML standard called Extensible Configuration Checklist Description Format (XCCDF). This new format was originally developed at the National Security Agency and is currently being finalized by a consensus group of experts from government agencies, software vendors, and other private industry organizations.

In order to make the tool available as quickly as possible, all existing Benchmarks, as well as those currently in development, must be converted into the XCCDF format. We have an immediate need for several individuals to begin work on this key aspect of the tool development process.

The task requires:

- Experience with the development and use of XML files and associated tools.
- Experience with the subject matter of the Benchmark. For example, the person converting the Solaris Benchmark should have extensive background in Solaris.
- CIS is seeking work for hire arrangements with individuals who are interested and qualified to take on this work. The total amount of time to complete a Benchmark conversion is estimated at 60-100 man hours, based on initial analysis of the Windows XP Benchmark. Ample instruction and support during the course of the project will be provided.

If you are interested in learning more about this important project, please contact John Banghart by phone at: (703) 716-0199 or by email at jbanghart@cisecurity.org.



Your Key to Security

What Are the Scoring Tools?

- CIS Scoring Tools enable end users to verify the security configuration of systems prior to network deployment, monitor systems and network devices for ongoing conformity with the benchmarks, and demonstrate to auditors and business partners their compliance with the internationally accepted standard for security configuration. The Tools are host based and produce reports that guide users and system administrators to secure both new installations and production systems.

CIS Scoring Tools are available on the CIS web site for most of the CIS Benchmarks.

In addition, CIS is currently developing a Next Generation (NG) Scoring Tool -- one tool that enables users to compare the configuration of operating systems, applications, and network devices with all of the CIS Benchmarks.

The NG Tool is Java based. It electronically reads Benchmark files expressed in a new XML standard called Extensible Configuration Checklist Description Format (XCCDF). XCCDF is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for a set of target systems. For more information about XCCDF, go to <http://csrc.nist.gov/checklists/xccdf.html>.

CIS Members have access to Scoring Tools with added features not available to the general user community.

» Source: <http://www.cisecurity.org/bench.html>

- It would be nice if there were more than just the CIS tools!



Your Key to Security

Future Vision

- XCCDF 1.1
- XCCDF-P (platforms)
- New version of OVAL – 5.0
- The XCCDF editor movement
 - The main effort being led by committee and is tied to the XML view
 - The small effort at NUCIA
 - Not tied to the XML view
 - A Naked Objects GUI is in the works
 - Subscribe to the announce list at OVALtools.org



Your Key to Security

XCCDF-P

- Neal writes:
- Basically, the data model for XCCDF-P 1.1 is stripped down to the bone: only boolean Facts can exist, and Platform definitions are just boolean combinations of those Facts. This leads to somewhat funky constructs for some common cases, but it has some nice aspects to.

For example, the Fact for "my platform has MSIE 5.5 installed" would be:

```
<cdfp:Fact
name="urn:xccdf:fact:application:browser:msie:version:
5:5:">
  <cdfp:title>MSIE version 5.5</cdfp:title>
</cdfp:Fact>
```



Your Key to Security

A Vision of an XCCDF editor

- Allows the IA professional to create policy encoded as XCCDF
 - No need to know XML!
 - Output policy as RTF for inclusion in a MS-Word (or OpenOffice.org) document
 - Use macros to automatically update the Word document as needed
 - Reaches out to the OVAL repository
 - Via semantic search and direct lookup
- Extensible XCCDF scoring utility that's open source!
- Our goal – contribute to the state of the art in Certification and Accreditation (C&A)!
 - <http://tinyurl.com/n48yz>



Power of the Network Effect

- “The **network effect** is a characteristic that causes a **good** or **service** to have a **value** to a potential **customer** dependent on the number of customers already owning that good or using that service.”
- “One consequence of a network effect is that the purchase of a good by one **individual** indirectly benefits others who own the good - for example by purchasing a **telephone** a person makes other telephones more useful.”

– http://en.wikipedia.org/wiki/Network_effect



What's easy for a computer is not easy for a person: The Need for a DSL

- **A Digital Subscriber Line?**
- **No - a Domain Specific Language!**
 - DSLs make things easy within a specific knowledge domain
 - The language is works for the subject matter expert – not the other way around!
 - It's said that Ruby on Rails is a DSL for Database driven web sites.
 - It's said that the use of a DSL is the secret of Ruby on Rails success...
 - Wikipedia: <http://tinyurl.com/hlzar>



Hello World in OVAL

- From MITRE's **OVAL Definition Tutorial**
 - <http://tinyurl.com/k5hh2>
- XML is good for programs & programmers
- This is great Smart interoperable data
- This is not good for subject matter experts!
- Line counts:
 - 31 in XML
 - 10 in our DSL
- OVALdsl can be generated from OVAL XML
- OVAL XML can be generated from OVAL dsl

```

1.  <oval_definitions>
2.  <definitions>
3.  <definition id="oval:org.mitre.oval:obj:1">
4.    <metadata>
5.      <title>Hello World Example</title>
6.      <description> This definition is used to introduce the OVAL
          Language to individuals interested in writing OVAL Content.
        </description>
7.    </metadata>
8.    <criteria>
9.      <criteria test_ref="oval:org.mitre.oval:tst:1" comment="the
          value of the registry key equals Hello World"/>
10.    </criteria>
11.  </definition>
12. </definitions>
13. <tests>
14. <registry_test id="oval:org.mitre.oval:tst:1" check="all">
15.   <object object_ref="oval:org.mitre.oval:obj:1"/>
16.   <state state_ref="oval:org.mitre.oval:ste:1"/>
17. </registry_test>
18. </tests>
19. <objects>
20. <registry_object id="oval:org.mitre.oval:obj:1">
21.   <hive>HKEY_LOCAL_MACHINE</hive>
22.   <key>SOFTWARE\oval</key>
23.   <name>example</name>
24. </registry_object>
25. </objects>
26. <states>
27. <registry_state id="oval:org.mitre.oval:ste:1">
28.   <value>Hello World</value>
29. </registry_state>
30. </states>
31. </oval_definitions>

```


Hello World in a DSL for OVAL

1. **def** d = **new** Defn("vulnerability");
2. d.title = "Hello World Example";
3. d.description =
4. ""
5. This definition is used to introduce the OVAL Language
6. to individuals interested in writing OVAL Content.
7. "";
8. **def** t = d.criteria("AND","Software Section");
9. t.comment="the value of the registry key equals Hello World";
10. t.registry_object(hive:"HKEY_LOCAL_MACHINE",key:"SOFTWARE\\oval",name:"example") == t.registry_state(value:"Hello World");
- Line 10 does the work of lines 14-30 in XML!

Blank spaces improve readability....

```
def d = new Defn("vulnerability");  
d.title = "Hello World Example";  
d.description =  
""
```

This definition is used to introduce the OVAL Language to individuals interested in writing OVAL Content.

```
""",  
def t = d.criteria("AND","Software Section");  
t.comment="the value of the registry key equals Hello World";  
t.registry_object(hive:"HKEY_LOCAL_MACHINE",  
                  key:"SOFTWARE\\oval",  
                  name:"example")  
==  
t.registry_state(value:"Hello World");
```



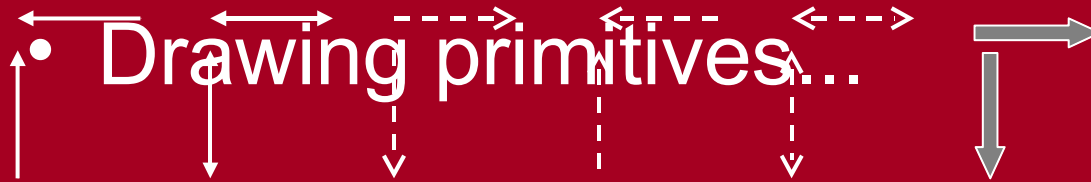
The bright future of the Extensible Configuration Checklist format (XCCDF) and its friends

- Slides are online at OVALtools.org
- **What you can do!**
 - Please register for our announce and/or discussion mailing lists at OVALtools.org
 - We need SMEs, Testers, and advisors!
 - Try our OVAL & XCCDF DSLs
 - Try our XCCDF & OVAL editor
 - Try our XCCDF interpreter
- Thank you!



Drawing Templates...

• Drawing primitives...



18-pt normal
18-pt bold
18-pt *italics*

18-pt
line-2

18-pt
line-2

18-pt

text

16-pt normal
16-pt bold
16-pt *italics*

16-pt B
line-2

16-pt B
line-2

text

8

14-pt normal
14-pt bold
14-pt *italics*

14-pt ln-1
line-2
line-3

line-1
line-2

text

8

