The eXtensible Configuration and Checklist Document Format (XCCDF)

Chris Calabrese <chris_calabrese@yahoo.com>

Introduction

Every system administrator has local policies and standards that their systems are supposed to comply with, and there are many security-audit tools to check compliance. However, many of these tools don't allow easy customization to local policy, or to drop-in new third-party policy definitions.

XCCDF is an XML-based format that addresses these problems by providing a unified way to describe

- System configuration policies/benchmarks/standards such those from the Center for Internet Security (www.cisecurity.org) or the NSA's Security Configuration Guides (www.nsa.gov/snac)
- How software can evaluate systems for policy compliance using Mitre's Open Vulnerability Assessment Language (oval.mitre.org) or similar schemes
- How people and/or software can fix systems that don't comply
- How well a particular system conforms to a policy for reporting purposes

What you can do with XCCDF

Security people

- Leverage existing policy/benchmark/standard bits when developing new policies (think XML-includes) or tailoring a policy for a particular environment
- Avoid writing your own custom auditing/configuration scripts

System administrators

- Makes it easy to customize 3rd party policies/benchmarks/standards for the local environment
- Avoid writing your own custom auditing/configuration scripts

Auditors

- Audit to local standards using your software tools – instead of by hand

Tool developers

- Concentrate on developing the tools, not the policies
- Enable your tools to be used by all administrators/auditors whether they buy into your default policies or now

XML Object Model

All XCCDF documents contain exactly one Benchmark object. A *Benchmark*, in turn, holds one or more *Rules*, *Values*, and/or *Groups*. *Groups* are containers that hold other *Rules*, *Values*, and/or *Groups*.

Simple example

The following is a trivial example to give the flavor of an XCCDF document:

```
<?xml version="1.0. ?>
 <cdf:Benchmark id="bench-example"
  xmlns:cdf="http://www.cisecurity.org/xccdf/0.10.1">
  <cdf:title>Trivial XCCDF Benchmark</cdf:title>
  <cdf:description xml:lang="en">
   Illustrate the structure of an XCCDF document.
   </cdf:description>
  <cdf:platform>MyLinuxDistro</cdf:platform>
  ...
  <cdf:Rule id="ssh-running" selected="1">
   <cdf:title>Is SSH running?</cdf:title>
   <cdf:description>
    This Rule tests whether SSH is running on
    TCP/<cdf:sub value="sshport"/>
    </cdf:description>
  <cdf:requires>sshport</cdf:requires>
  <cdf:check system="http://oval.mitre.org/XMLSchema/oval/">
   <cdf:check-export value-id="sshport" export-name="var2./>
   <cdf:check-content-ref href="authchecks.oval.xml" name="DEFN208"/>
   </cdf:check>
  </cdf:Rule>
 ...
 <cdf:Value id="sshport" selected="1"
  type="number" operator="equals" allowChanges="1">
  <cdf:title>SSH Port Number</cdf:title>
  <cdf:question>SSH Port Number</cdf:question>
  <cdf:description xml:lang="en">
   This is the TCP port number on which SSH may listen.
   </cdf:description>
  <cdf:default>22</cdf:default>
  <cdf:value>2222</cdf:value>
  </cdf:Value>
 ...
 </cdf:Benchmark>
```

Benchmark tailoring

As eluded to above, benchmark tailoring is done through the following mechanisms:

Selection / deselection

- Any *Group* or *Rule* may be selected or deselected.
- Deselected items are not applied during compliance testing.

Value settings

- A user can supply new settings to any *Value* object

Extensions

- New *Groups*, *Rules*, and *Values* can be created that extend another *Group*/*Rule*/*Value*
- Think object inheritance

Who is behind XCCDF

The main players in the development of XCCDF are the US National Security Agency's Information Assurance Directorate (www.nsa.gov/ia), the Center for Internet Security (www.cisecurity.org), and MITRE (www.mitre.org).

Getting Involved

The XCCDF draft-spec is not available to the public at this time pending release review by the NSA.

You can get involved, and get a copy of the draft-spec, however, by subscribing to the XCCDF mailing list. Do this by sending an email request to xccdf-dev-subscribe@lists.cisecurity.org.

Author Bio

Chris Calabrese comes to the XCCDF project through his role as the Center for Internet Security's HP-UX Benchmark team-leader/editor. In the day-time, he's part of the Information Security Engineering team at "very large healthcare company."

Chris has been involved in information security for "a long time" and has given several security-related talks at SANS, a (non-security-related) talk at USENIX, and contributed security-related articles to both *;login,* and USENIX's now-defunct *Computing Systems* journal.

Chris holds a MS/Comp-Sci from New York University.