Virtual Room #1

Hosted By: **Wendell Piez**, IT Security Specialist, *NIST/ITL/CSD*

(OSCAL Webpage)

Disclaimer: Portions of the event may be recorded and audience Q&A or comments may be captured. The recorded event may be edited and rebroadcasted or otherwise made publicly available by NIST. By attending this event, you acknowledge and consent to having your conversation recorded.

oscal2022@nist.gov
conferences@nist.gov

OSCAL Tools

Open-source XSLT for OSCAL

(and more)

Wendell Piez

NIST / ITL / CSD

XML/XSLT

One resource among many

Too many OSCAL Tools sites is a good problem to have….

… we do need a way to make the work available …

Today we talk about https://github.com/usnistgov/oscal-tools

Other OSCAL Tools initiatives are listed on https://pages.nist.gov/OSCAL/tools/

Origins and purpose

Started as a repository for code not normative for OSCAL, but supporting it
Built internally to support various efforts and as demonstrations
But was also made generalized and customizable
So why not make it available

- Show what can be done
- Catalyze other initiatives coding to OSCAL

Did anyone mention web sites with git repositories in back?

… a static web site is also a platform for demonstration …

Current and planned scope

XSLTs for styling OSCAL began as spinoffs from NIST project work / proofs-of-concept

Repository is also useful as a clearing house for utilities

Has also hosted other (NIST) projects before they find permanent homes – and might do so again

Aspiring to an "always finished, always growing" maintenance model

XSLT for download

Why XSLT? (Long topic)
tldr: XSLT 3.0 is not your grandma's XSLT
Performance, versatility, safety features

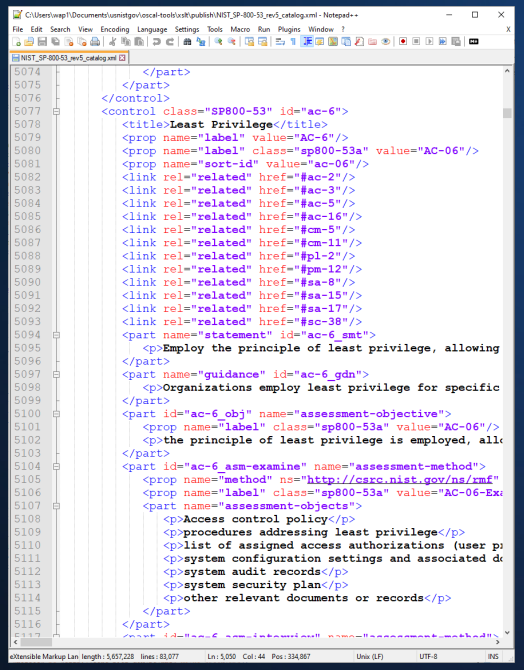
XML Stylesheet Language Transformations
W3C Recommendation 8 June 2017

Record of success encapsulating and managing the "static presentation" problem
Declarative language suitable for a library supporting local customizations
Works in wide range of architectures / environments
Scalable – both throughput and complexity
Delivers functionality on a commodity freeware stack
Produces well-understood, useful outputs
HTML, CSS, PDF… CSV, plain text, structured code …

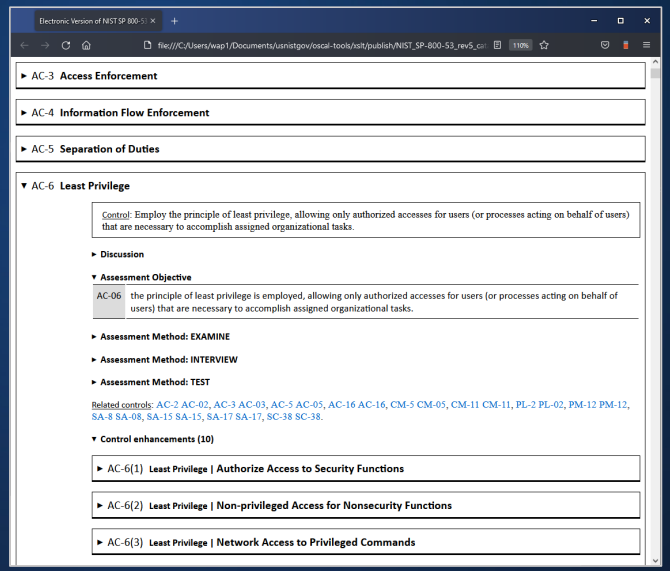
NIST National Institute of Standards and Technology U.S. Department of Commerce
ITL INFORMATION TECHNOLOGY LABORATORY

Formal presentation for web and print

Interpreting semantic encoding for human readers



```
          </part>
        </part>
      </control>
      <control class="SP800-53" id="ac-6">
        <title>Least Privilege</title>
        <prop name="label" value="AC-6"/>
        <prop name="label" class="sp800-53a" value="AC-06"/>
        <prop name="sort-id" value="ac-06"/>
        <link rel="related" href="#ac-2"/>
        <link rel="related" href="#ac-3"/>
        <link rel="related" href="#ac-5"/>
        <link rel="related" href="#ac-16"/>
        <link rel="related" href="#cm-5"/>
        <link rel="related" href="#cm-11"/>
        <link rel="related" href="#pl-2"/>
        <link rel="related" href="#pm-12"/>
        <link rel="related" href="#sa-8"/>
        <link rel="related" href="#sa-15"/>
        <link rel="related" href="#sa-17"/>
        <link rel="related" href="#sc-38"/>
        <part name="statement" id="ac-6_smt">
          <p>Employ the principle of least privilege, allowing
        </part>
        <part name="guidance" id="ac-6_gdn">
          <p>Organizations employ least privilege for specific
        </part>
        <part id="ac-6_obj" name="assessment-objective">
          <prop name="label" class="sp800-53a" value="AC-06"/>
          <p>the principle of least privilege is employed, all
        </part>
        <part id="ac-6_asm-examine" name="assessment-method">
          <prop name="method" ns="http://csrc.nist.gov/ns/rmf"
          <prop name="label" class="sp800-53a" value="AC-06-Exa
          <part name="assessment-objects">
            <p>Access control policy</p>
            <p>procedures addressing least privilege</p>
            <p>list of assigned access authorizations (user pr
            <p>system configuration settings and associated da
            <p>system audit records</p>
            <p>system security plan</p>
            <p>other relevant documents or records</p>
          </part>
        </part>
```



▸ AC-3 **Access Enforcement**

▸ AC-4 **Information Flow Enforcement**

▸ AC-5 **Separation of Duties**

▾ AC-6 **Least Privilege**

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

▸ **Discussion**

▾ **Assessment Objective**

AC-06	the principle of least privilege is employed, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

▸ **Assessment Method: EXAMINE**

▸ **Assessment Method: INTERVIEW**

▸ **Assessment Method: TEST**

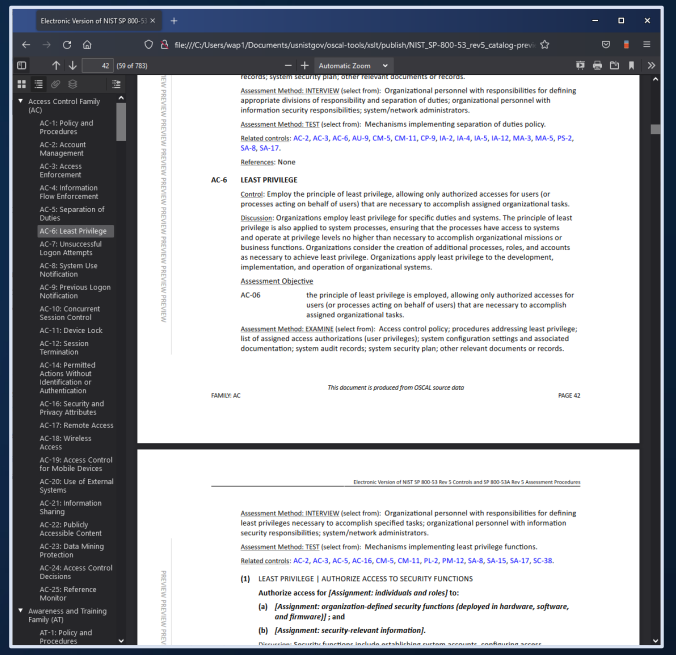
Related controls: AC-2 AC-02, AC-3 AC-03, AC-5 AC-05, AC-16 AC-16, CM-5 CM-05, CM-11 CM-11, PL-2 PL-02, PM-12 PM-12, SA-8 SA-08, SA-15 SA-15, SA-17 SA-17, SC-38 SC-38.

▾ **Control enhancements (10)**

▸ AC-6(1) **Least Privilege | Authorize Access to Security Functions**

▸ AC-6(2) **Least Privilege | Non-privileged Access for Nonsecurity Functions**

▸ AC-6(3) **Least Privilege | Network Access to Privileged Commands**



AC-6 **LEAST PRIVILEGE**

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

Assessment Objective

AC-06 the principle of least privilege is employed, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Assessment Method: EXAMINE (select from): Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

This document is produced from OSCAL source data

FAMILY: AC PAGE 42

Elapsed runtimes for 5.5MB OSCAL catalog:
(1189 controls and enhancements)

- HTML: 0.6sec
- PDF: 17.1sec (1.1 sec transformation, 16sec layout)
  Commodity tools / no optimization
  This PDF has 766pp.

XSLT core use case: producing human-readable pages from XML source data

Other capabilities

CSS for OSCAL authoring or lightweight browser display

XSLT UUID refresher utility

- assigns new (random) UUIDs

XSLT OSCAL "blank" document generator

- catalog, profile, SSP, SAP, or SAR (so far)
- valid but empty; fresh timestamp

… and more to come …

Link checkers

Network discovery

Semantic analysis, mapping, exposition

(Please contribute ideas)

usnistgov Pages site

https://pages.nist.gov/oscal-tools/

Web site accompanying the software repository
Just finalized! February 2022
Expected to grow
- Updates to current projects
- New projects
- Cover/describe projects in other repositories

client-side XSLT

CSX demonstrations

https://pages.nist.gov/oscal-tools/demos/csx/

Started as experiments in a personal repo, then grew

Demonstrates a concept: XSLT transformations in the browser

But this time, you provide the data

(It is processed for display and shown, but not passed anywhere.)

Further work / feedback

What should we be doing?

Github Issues
Public Gitter chat channel
We also have an oscal/xslt-etc 'room' in Gitter

Web site – tutorials; hints and ideas?

Tools – for online or offline use?