atsec information security

Common Criteria

XML-based Security Targets for tool-supported evaluations

8th ICCC 2007 - Rome, Italy

David Ochel, Alejandro Masino
atsec information security

Objectives

- Understand automation potential in CC evaluations
- Realize how XML can help with automation
- Learn about atsec's approach to XML Security Targets (STs)

Agenda

- Why automation?
  - Potential for evaluation and ST creation
  - Examples
- Why XML?
- atsec's approach
  - Available work and tools
  - Examples
  - Outlook

the information security provider

Why automation?

- Evaluation

> **check — ** to generate a **verdict** by a simple comparison. Evaluator expertise is not required. The statement that uses this verb describes what is mapped.
>
> (CEM 3.1R1)

- ST creation
  - – Reproduction of already provided text
  - – Use of pre-defined structures

Automation potential: correspondence evaluation

- “Formal” checks for consistency/completeness
  - between ST and CC

    …that the statement of security requirements identifies all operations on the security requirements. (ASE_REQ.1-4)
  - within evidence piece

    …that the security objectives rationale traces all security objectives for the TOE back to threats countered by the objectives and/or OSPs enforced by the objectives. (ASE_OBJ.2-2)
  - between evidence pieces

    …that the tracing links the SFRs to the corresponding TSFIs. (ADV_FSP.1-5)
- …vs. “intelligent” examination of accuracy

Automation potential: Security Target creation

- Fixed structure for content
  - – Layout is always the same
- Reproduction of SFRs
  - – from CC Part 2/PPs
- Internal correspondence/consistency
  - – many consistency checks can be automated

XML ST: Objectives

- ST author's dreams
  - Automatically derive SFRs from Part 2
  - Support consistency/completeness checks, dependency checks, and rationale generation
  - Focus on content, not on layout
  - Support subsequent evidence creation (e.g., RCR analysis)
- ST evaluator's dreams
  - Perform automated consistency/dependency checks
  - Facilitate correspondence analysis with design, testing, guidance

Why XML?

- Source human readable/editable
- Structure independent from presentation
- Flexible markup language
- Platform/application/vendor-independent
- Easy version control

What was available?

- CC Part 1-3 and CEM (2.3 and 3.1)
- Security Target DTD
  - (work from Miguel Bañón, Spain)

atsec’s tool base

- Tool base
  - XML editors:
    - for example, oXygen — commercial
  - Rendering engine:
    - XEP — commercial
  - Programmatic framework:
    - Java — open source
  - Version management:
    - Subversion — open source
- XML framework
  - extend on existing DTD

ST creation: tool logic

- Create XML template
- Retrieve author-defined SFR templates from Part 2
- Generate report
  - generate “full” XML (e.g., create tables for rationale)
  - create PDF representation
  - warn author about (potential) inconsistencies

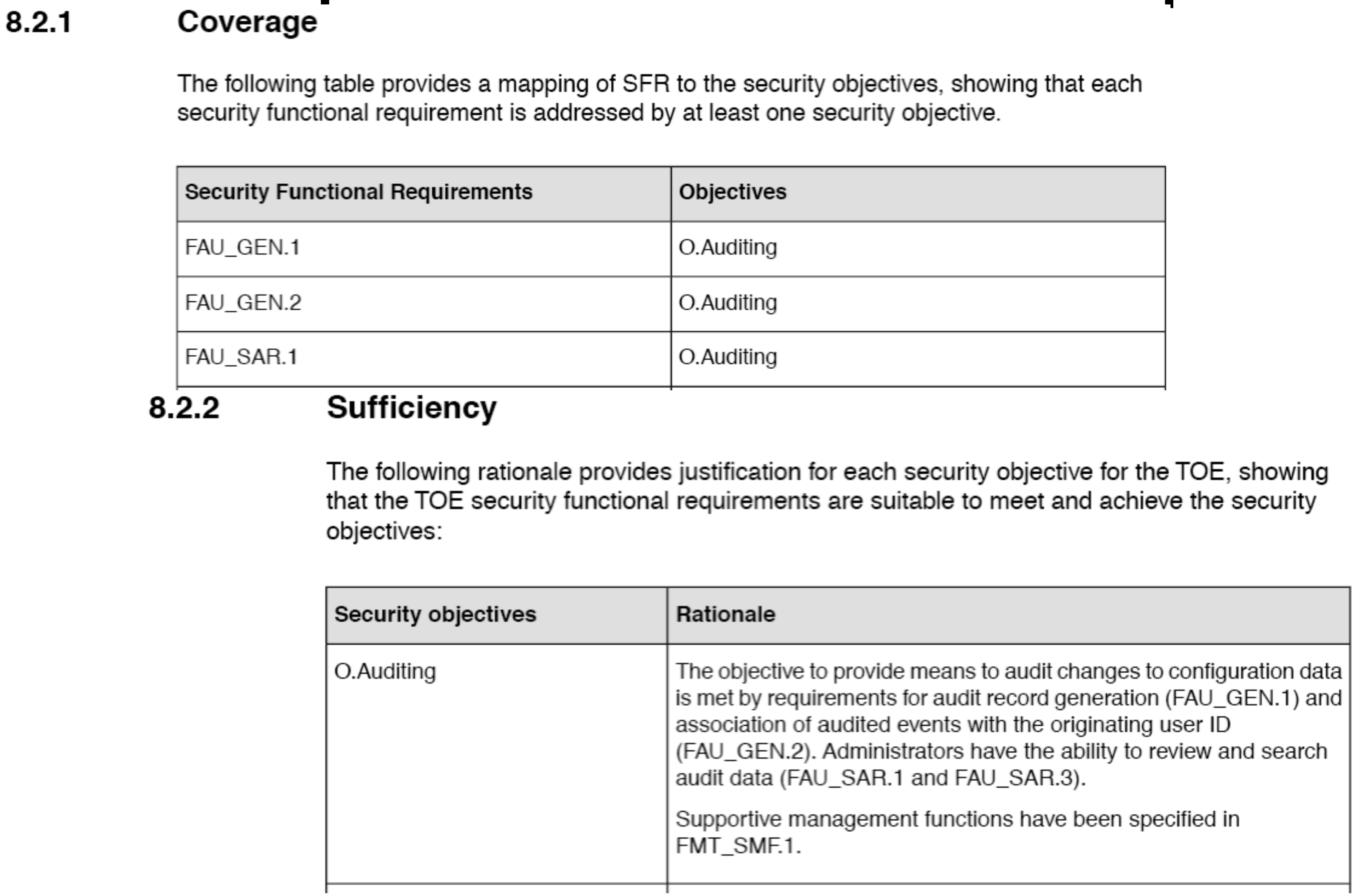
Example: XML SFR

```xml
<sfr-component id="fmt_msa.1" name="Management of security attributes">
    <sfr-element id="fmt_msa.1.1">
        The TSF shall enforce the
            <fe-assignment done="yes">
                <fe-assignmentitem> Example Security Policy</fe-assignmentitem>
            </fe-assignment>
        to restrict the ability to
            <fe-selection exclusive="NO" done="yes">
                <fe-selectionitem> change_default </fe-selectionitem>
                <fe-selectionitem> query </fe-selectionitem>
                <fe-selectionitem> modify </fe-selectionitem>
                <fe-selectionitem> delete </fe-selectionitem>
            </fe-selection>
        the security attributes
            <fe-assignment done="yes">
                <fe-assignmentitem>access control lists</fe-assignmentitem>
            </fe-assignment>
        to
            <fe-assignment done="yes">
                <fe-assignmentitem>authorized administrators</fe-assignmentitem>
            </fe-assignment>.
    </sfr-element>
</sfr-component>
```

Example: XML objective

```
<objective id="O.Auditing">
    <description>
        <p>The TOE shall provide accounting information for security-
   relevant configuration changes to the TOE.</p>
    </description>
    <addressed-by sfr-id="fau_gen.1"/>
    <addressed-by sfr-id="fau_gen.2"/>
    <addressed-by sfr-id="fau_sar.1"/>
    <addressed-by sfr-id="fau_sar.3"/>
    <addressed-by sfr-id="fmt_smf.1"/>
    <rationale>
        <p>The objective to provide means to audit changes to configuration
   data is met by requirements for audit record generation (FAU_GEN.1) and
   association of audited events with the originating user ID (FAU_GEN.2).
   Administrators have the ability to review and search audit data
   (FAU_SAR.1 and FAU_SAR.3).</p>
        <p>Supportive management functions have been specified in
   FMT_SMF.1.</p>
    </rationale>
</objective>
```

Example: ST rationale output



8.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement is addressed by at least one security objective.

Security Functional Requirements	Objectives
FAU_GEN.1	O.Auditing
FAU_GEN.2	O.Auditing
FAU_SAR.1	O.Auditing

8.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the TOE security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.Auditing	The objective to provide means to audit changes to configuration data is met by requirements for audit record generation (FAU_GEN.1) and association of audited events with the originating user ID (FAU_GEN.2). Administrators have the ability to review and search audit data (FAU_SAR.1 and FAU_SAR.3). Supportive management functions have been specified in FMT_SMF.1.

Project status

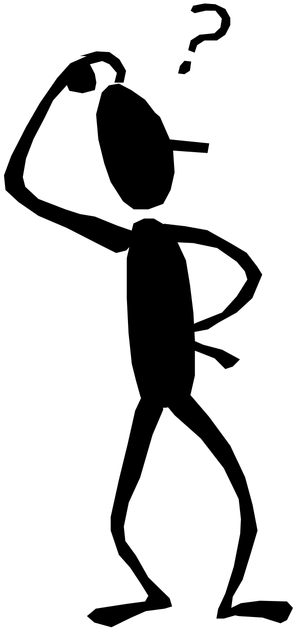
- ST is complete :)
- Some automation features implemented
- ST evaluation was mostly manual

- Some open issues
  - table editing
  - vendor compatibility

Next objectives?

- Extend DTD to cover PPs (already CC 3.1-compatible)
- Develop GUI for ST creation
- Make ST DTD public domain/ move to XML schema?
- Automate evaluation consistency checks
- Support different presentation formats (e.g., DocBook, Word)

Questions?



david@atsec.com