Towards deriving automated implementation & verification mechanisms from a single machine-readable requirements specification

Using Windows Hardening as proof-of-concept

Patrick Stöckle | Dr. Bernd Grobauer

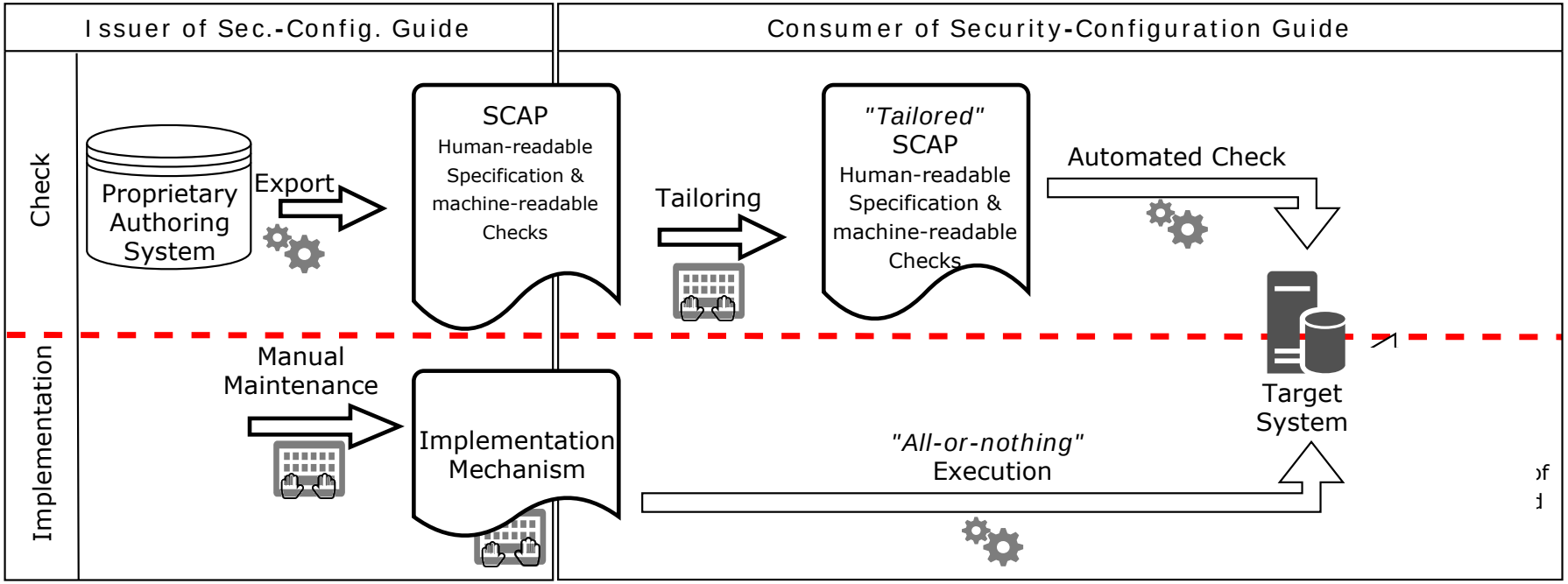
patrick.stoeckle@tum.de | bernd.grobauer@siemens.com

Technical University of Munich | Siemens AG

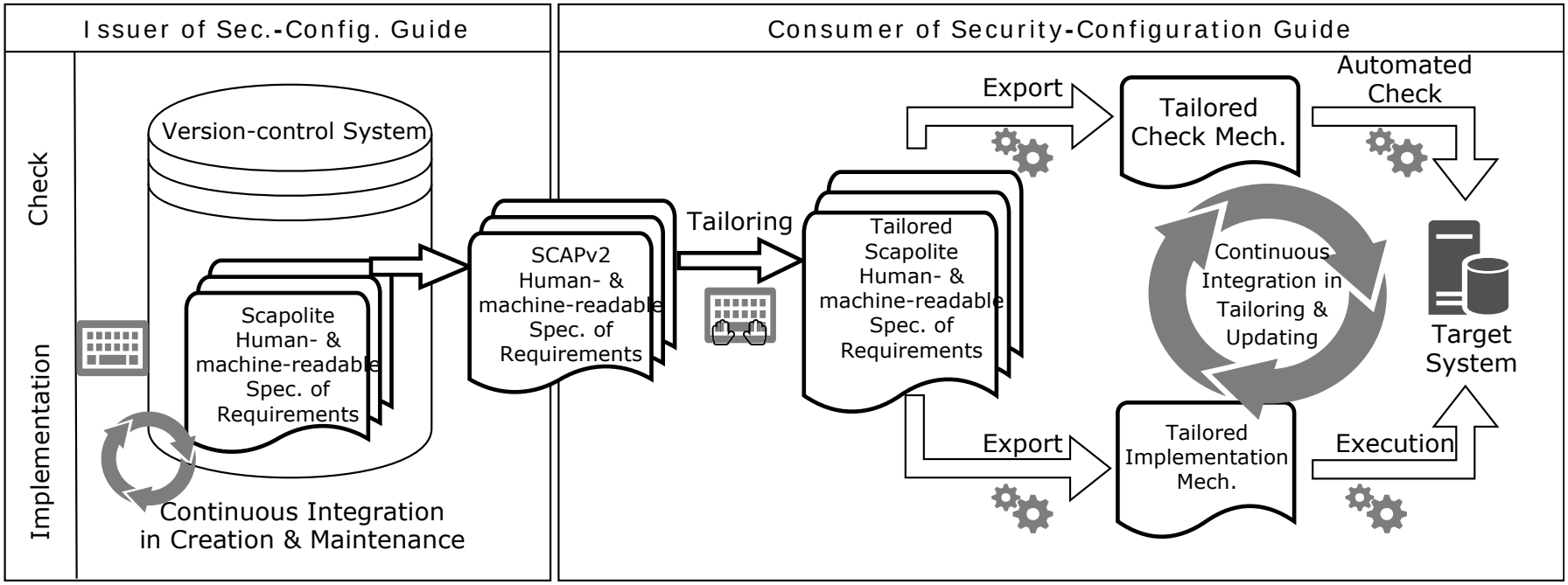
Chair of Software and Systems Engineering | CT RDA ITS

presented @NIST SCAP v2 Workshop April 30th to May 2nd 2019

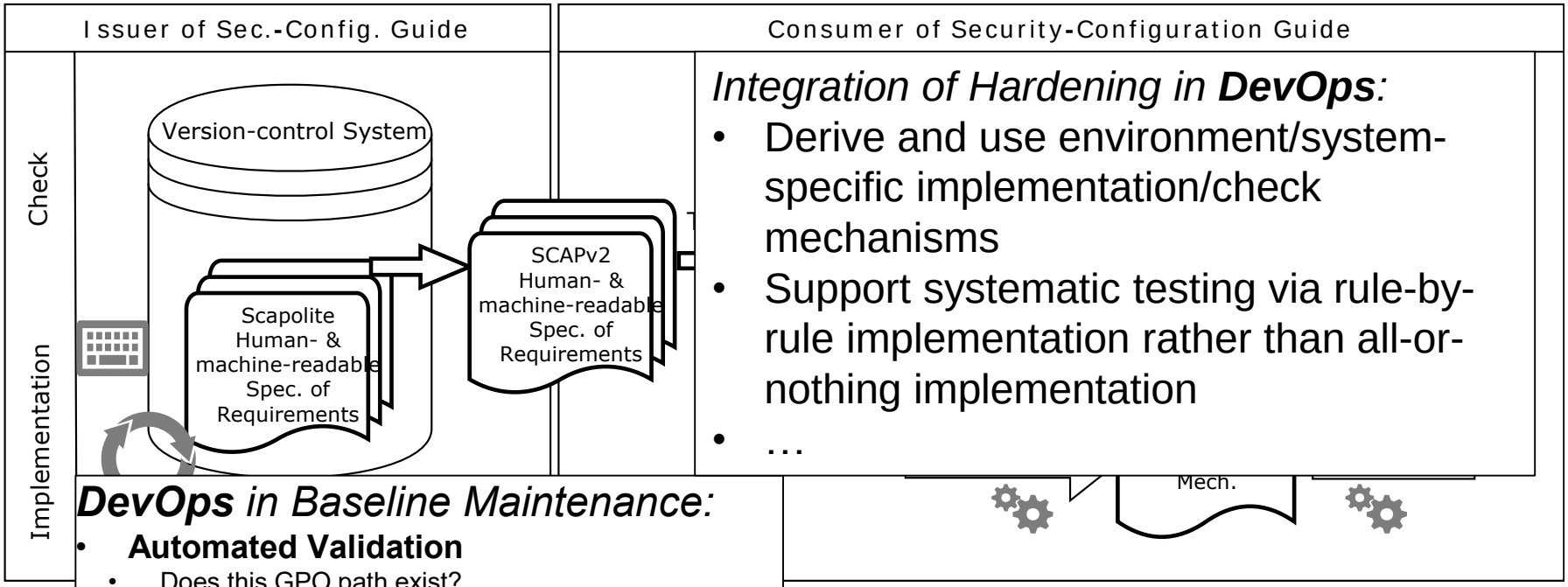
Status Quo for almost all SCAP Baselines



Goal


Issuer of Sec.-Config. Guide
Consumer of Security-Configuration Guide
Check
Implementation
Version-control System
Scapolite Human- & machine-readable Spec. of Requirements
Continuous Integration in Creation & Maintenance
SCAPv2 Human- & machine-readable Spec. of Requirements
Tailoring
Tailored Scapolite Human- & machine-readable Spec. of Requirements
Export
Tailored Check Mech.
Automated Check
Continuous Integration in Tailoring & Updating
Target System
Export
Tailored Implementation Mech.
Execution

Goal



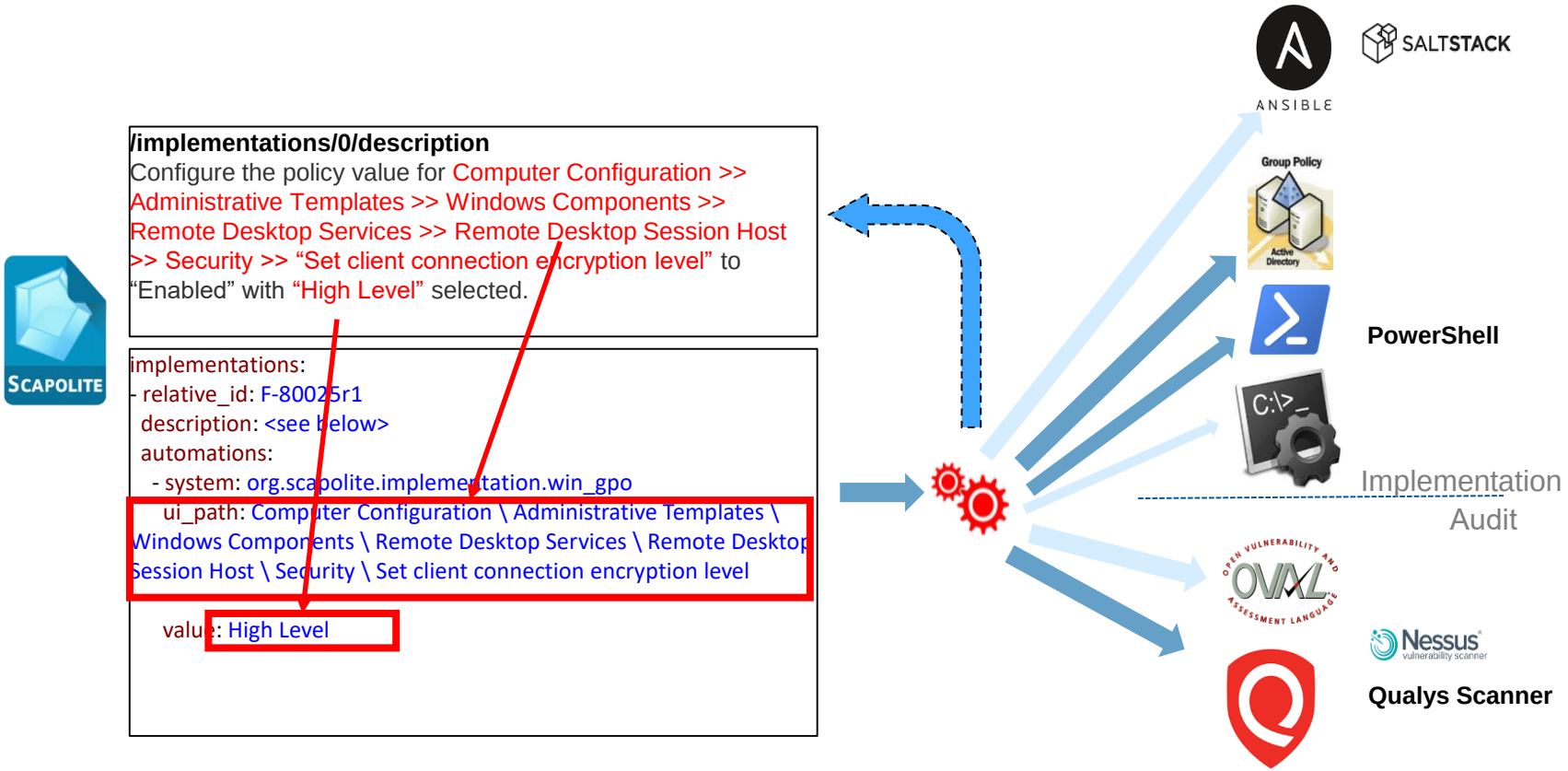
*Integration of Hardening in **DevOps**:*

- Derive and use environment/system-specific implementation/check mechanisms
- Support systematic testing via rule-by-rule implementation rather than all-or-nothing implementation
- …

***DevOps** in Baseline Maintenance:*

- **Automated Validation**
  - Does this GPO path exist?
    (If not, show alternative candidates)
  - Are the parameter values specified in the guidelines valid?
    (If not, show possible candidates)
- **Automated Testing:**
  - Execute implementation on test-system
  - Check test results before and after
  - …

Our Proof-of-Concept for Windows Hardening



Example

/implementations/0/description
Configure the policy value for **Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security >> "Set client connection encryption level"** to "Enabled" with **"High Level"** selected.

ui_path: Computer Configuration \ Administrative Templates \ Windows Components \ Remote Desktop Services \ Remote Desktop Session Host \ Security \ Set client connection encryption level
value: High Level
verification_status: Checked.

config: Computer
registry_key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
value_name: MinEncryptionLevel
action: DWORD:3

Registry Automation

string_value: Success
guid: '{0CCE923F-69AE-11D9-BED3-505054503030}'
name: Credential Validation
value: 1

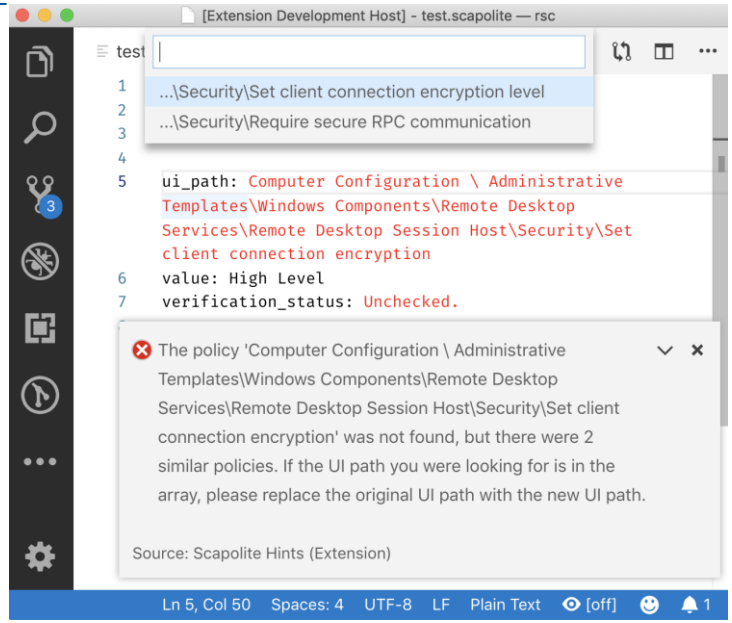
„audit.csv“ Automation

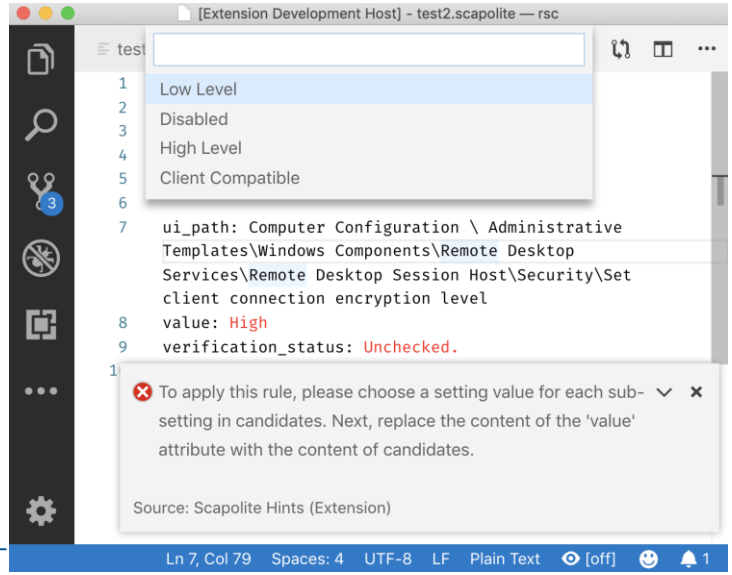
setting_name: SeAuditPrivilege
section: Privilege Rights
value:
- '*S-1-5-19'
- '*S-1-5-20'

„INF-File“ Automation

Example automations for other GPO settings

Verification





Conclusion

As consumers of baselines, what we do now is to

- Defined a format to specify GPO settings in a machine-readable way
- Use NLP to turn human-readable specifications into machine-readable specifications
- Generate required artefacts for DevOps approaches both in maintaining and using security baselines

What we would like to do

- Have CIS/IASE … specify required GPO settings in machine-readable way
- Use these machine-readable GPO settings

What we would like to have in SCAP v2

- More focus on automated implementation of security baselines
- Include machine-readable specification for the implementation

Contact

Patrick Stöckle
Patrick.Stoeckle@tum.de
https://www22.in.tum.de/stoeckle/
https://www.linkedin.com/in/patrick-stoeckle