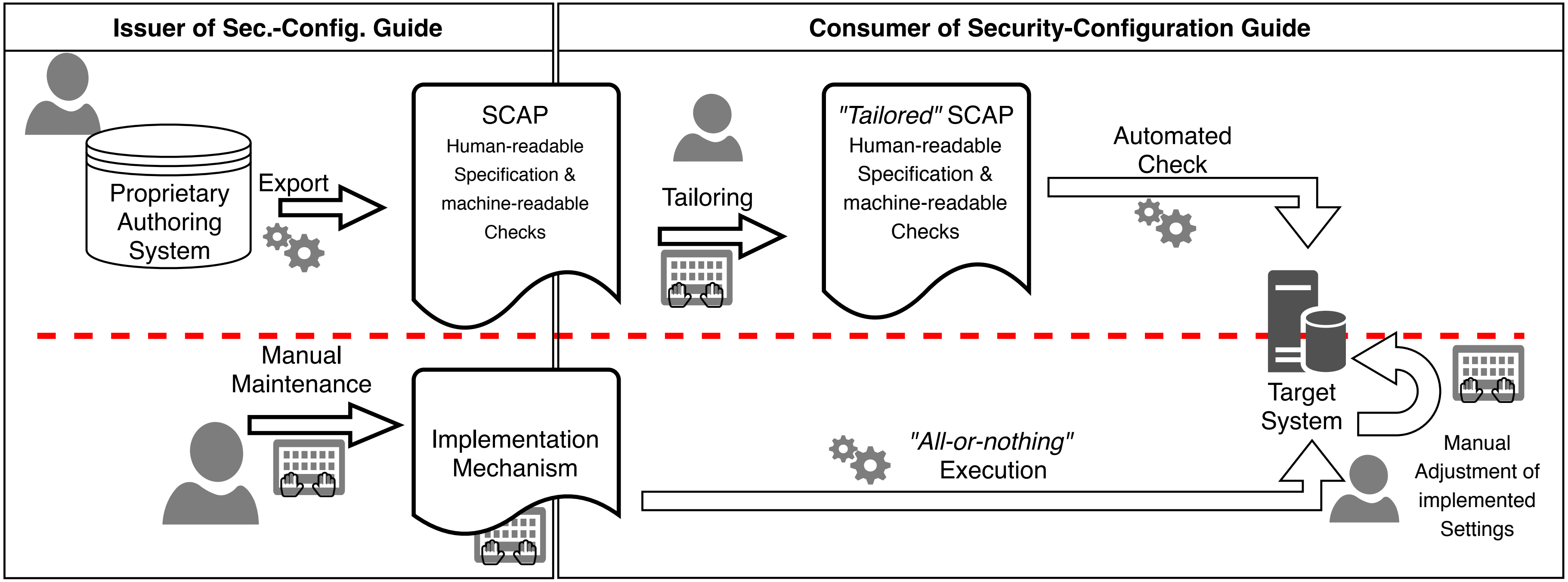
Towards deriving automated implementation & verification mechanisms from a single machine-readable requirements specification

Using Windows Hardening as proof-of-concept

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

Patrick Stöckle, Technical University of Munich | Chair of Software and Systems Engineering

Status Quo for almost all SCAP Baselines
(with some OpenScap baselines as notable exception)



Issuer of Sec.-Config. Guide
Consumer of Security-Configuration Guide
Proprietary Authoring System
Export
SCAP
Human-readable Specification & machine-readable Checks
Tailoring
"Tailored" SCAP
Human-readable Specification & machine-readable Checks
Automated Check
Manual Maintenance
Implementation Mechanism
"All-or-nothing" Execution
Target System
Manual Adjustment of implemented Settings

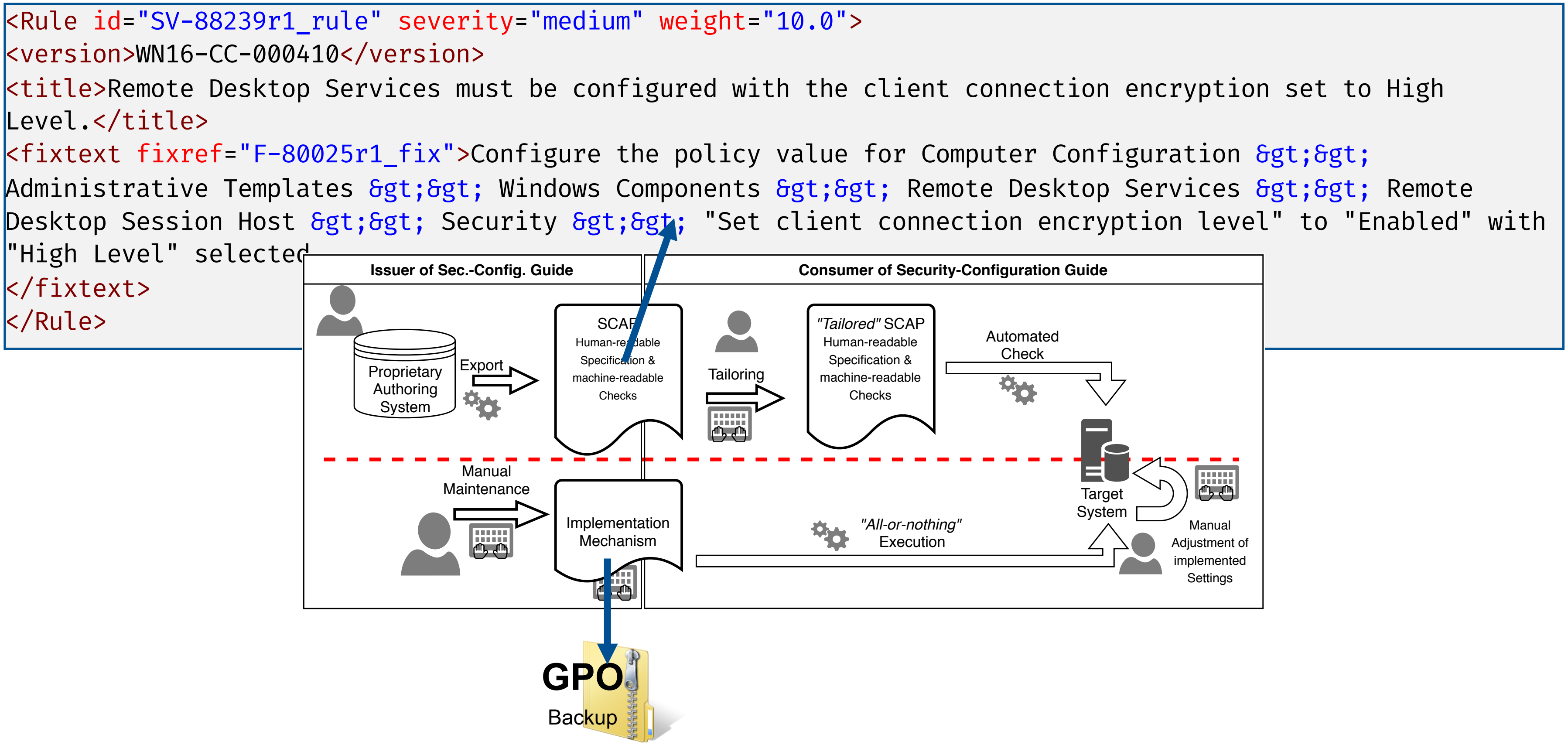
Implementations and checks are created **and maintained** independently from each other

Implementations not part of SCAP content authoring/maintenance

- Is the implementation valid? Right GPO path, etc.
- Is the check really verifying the implementation?

Relation Implementation ↔ Check is not clear

Status Quo for almost all SCAP Baselines
(with some OpenScap baselines as notable exception)

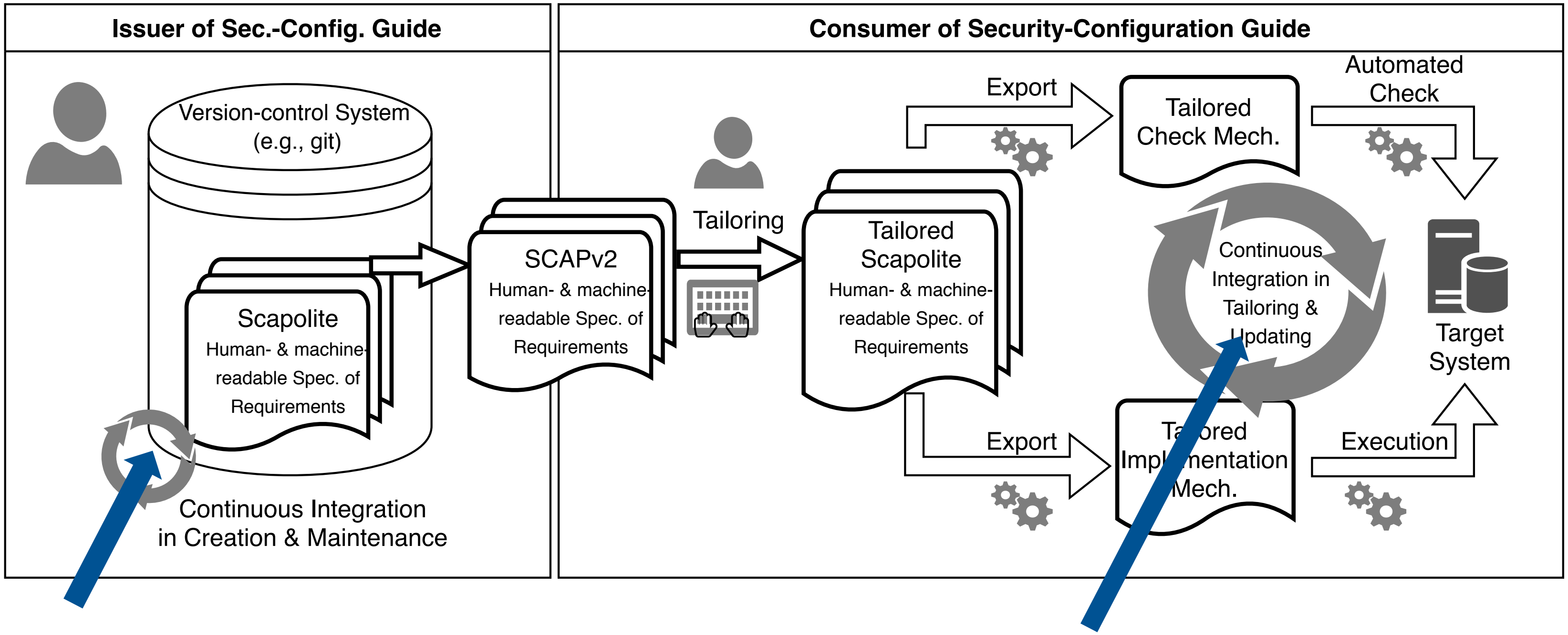


```
<Rule id="SV-88239r1_rule" severity="medium" weight="10.0">
<version>WN16-CC-000410</version>
<title>Remote Desktop Services must be configured with the client connection encryption set to High
Level.</title>
<fixtext fixref="F-80025r1_fix">Configure the policy value for Computer Configuration &gt;&gt;
Administrative Templates &gt;&gt; Windows Components &gt;&gt; Remote Desktop Services &gt;&gt; Remote
Desktop Session Host &gt;&gt; Security &gt;&gt; "Set client connection encryption level" to "Enabled" with
"High Level" selected
</fixtext>
</Rule>
```

Issuer of Sec.-Config. Guide
Consumer of Security-Configuration Guide
Proprietary Authoring System
Export
SCAP Human-readable Specification & machine-readable Checks
Tailoring
"Tailored" SCAP Human-readable Specification & machine-readable Checks
Automated Check
Target System
Manual Maintenance
Implementation Mechanism
"All-or-nothing" Execution
Manual Adjustment of implemented Settings
GPO
Backup

Example: IASE Microsoft Windows Server 2016 STIG Benchmark

Goal


Issuer of Sec.-Config. Guide
Consumer of Security-Configuration Guide
Version-control System (e.g., git)
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

***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
  - …

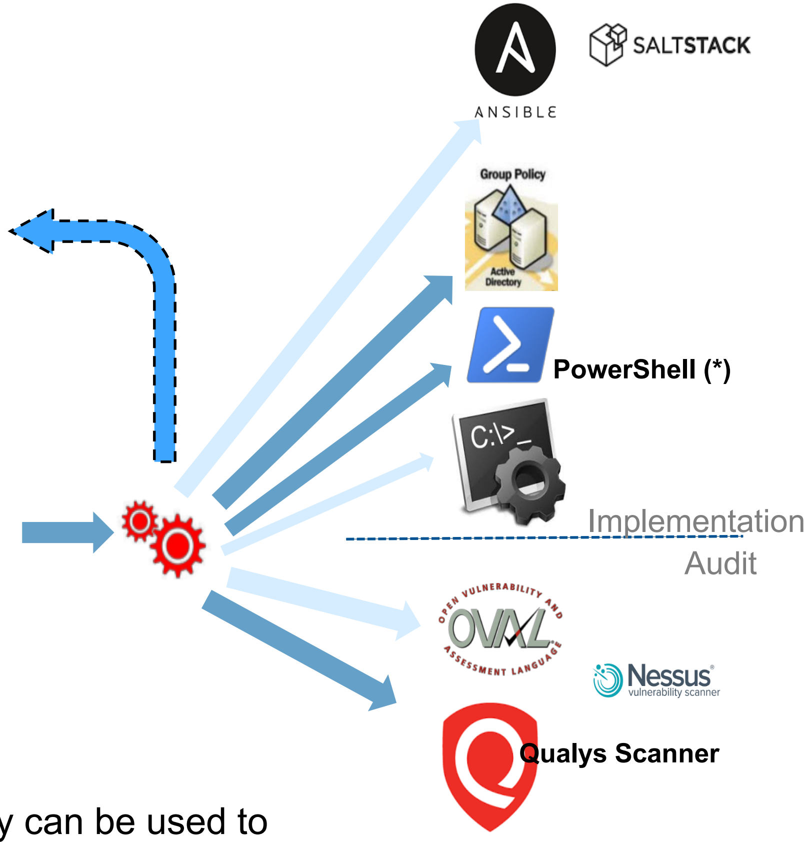
*Integration of Hardening in **DevOps**:*

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

Our Proof-of-Concept for Windows Hardening

/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.

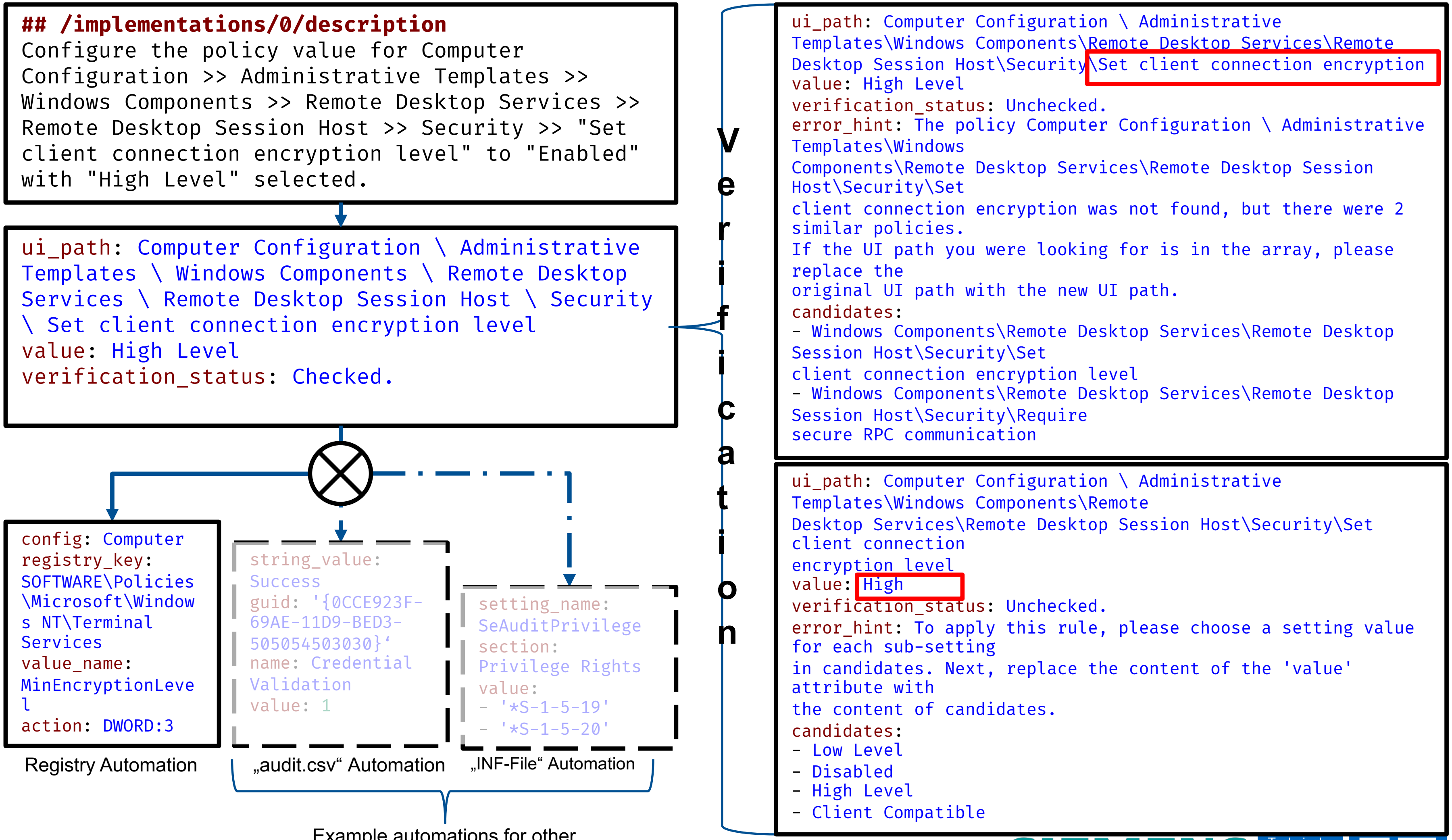
```
implementations:
- relative_id: F-80025r1
  description: <see below>
  automations:
    - system:
org.scapolite.implementation.win_gpo
      ui_path: Computer Configuration \
Administrative Templates \ Windows Components
\ Remote Desktop Services \ Remote Desktop
Session Host \ Security \ Set client
connection encryption level

      value: High Level
```



(*) Underlying PowerShell library can be used to

- Implement one rule
- Implement all rules
- Check one rule
- Check all rules

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\Window
s NT\Terminal
Services
value_name:
MinEncryptionLeve
l
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

```
ui_path: Computer Configuration \ Administrative
Templates\Windows Components\Remote Desktop Services\Remote
Desktop Session Host\Security\Set client connection encryption
value: High Level
verification_status: Unchecked.
error_hint: The policy Computer Configuration \ Administrative
Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Set
client connection encryption was not found, but there were 2
similar policies.
If the UI path you were looking for is in the array, please
replace the
original UI path with the new UI path.
candidates:
- Windows Components\Remote Desktop Services\Remote Desktop
Session Host\Security\Set
client connection encryption level
- Windows Components\Remote Desktop Services\Remote Desktop
Session Host\Security\Require
secure RPC communication
```

```
ui_path: Computer Configuration \ Administrative
Templates\Windows Components\Remote
Desktop Services\Remote Desktop Session Host\Security\Set
client connection
encryption level
value: High
verification_status: Unchecked.
error_hint: To apply this rule, please choose a setting value
for each sub-setting
in candidates. Next, replace the content of the 'value'
attribute with
the content of candidates.
candidates:
- Low Level
- Disabled
- High Level
- Client Compatible
```

Conclusion

- As consumers of CIS and IASE Windows baselines, what we do now is to
  - Use natural language processing to turn human-readable specifications of GPO settings into machine-readable specifications (86.5% fully automated, 13.5% require manual intervention)
  - Use machine-readable implementations to 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

- As users of SCAP, what we would like is to shift focus a little more on automated implementation than is currently the case
  - our Windows PoC shows that it is possible for certain systems;
  - including machine readable fix elements for Windows GPO settings is possible in SCAP as it is, we just need to agree on a definition for the „fix" system.
- Other systems will be harder to tackle, but for usage of SCAP(v2) in DevSecOps, there is no other way: we need machine-readable specifications of required security configurations.

Contact

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