Remediation

Terms (for this Presentation)

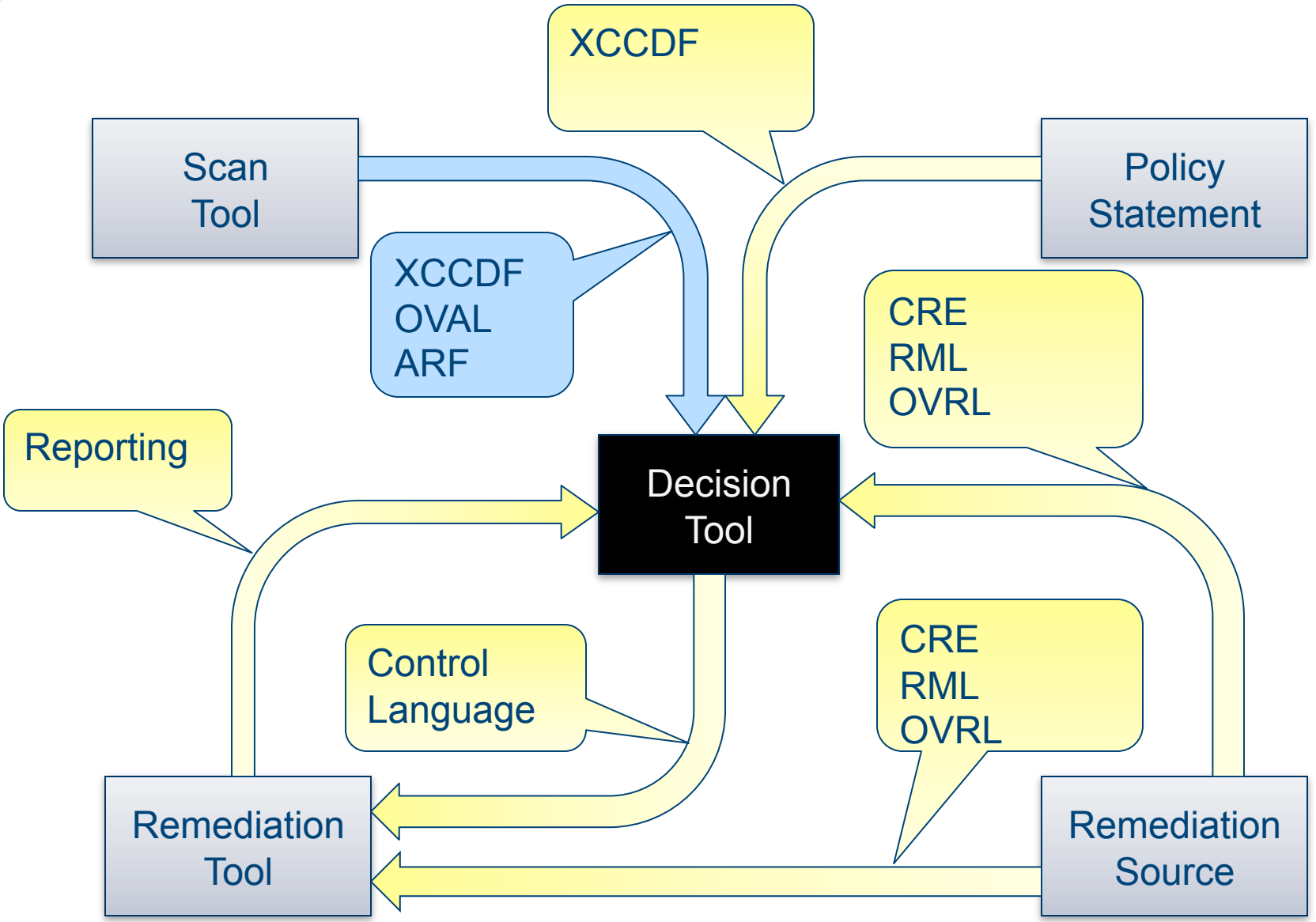
- Vulnerability – a software flaw, mis-configuration, or non-compliant setting that enables unauthorized access or use of a device
- Remediation – a change to the system configuration or installed software files in response to a vulnerability

Use Cases

- Remediate one or more computing assets for all vulnerabilities found
- Remediate one or more computing assets for a subset of vulnerabilities found
- Apply one or more remediations to one or more computing assets regardless of their current state
- Question : What use cases are we missing?

Derived Requirements

- Uniquely identify a remediation (Enumeration)
- Express data about the content of a remediation (Markup Language)
- Express how to perform a remediation in a machine readable form (OVRL)
- Develop a method of specifying which remediations should be applied to which assets in a given environment
- Develop a control language to express computing assets, remediations, and variables
- Express results of remediation
- Question : What requirements are we missing?


XCCDF
Scan Tool
Policy Statement
XCCDF
OVAL
ARF
CRE
RML
OVRL
Reporting
Decision Tool
Control Language
CRE
RML
OVRL
Remediation Tool
Remediation Source

Unique Identification

- Unique Identifier for a remediation
  - Current litmus test – CRE represents a set of actions to remediate a specific vulnerability
- Use lessons learned from CVE
- A CRE consists of a unique identifier and a description
- Question : Do we need a CRE identifier to support vendor interoperability and compliance reporting?
- Question : Should it allow for both global and local identifiers?
- Question : What should the identifiers look like?

CRE Markup Language

- Developing a Remediation Markup Language ("RML") specification
- Expresses metadata such as
  - CRE Description
  - When a CRE was created
  - Who created it
  - When a CRE was modified
  - Who modified it
- Question : What other metadata should we capture?

CRE Markup Language

- Conditions where the remediation is applicable
  - In response to a given CVE or CCE
  - On what platforms (CPE)
- Remediation Steps
  - Prose version for use in documents
  - Reference to a machine readable version
- References
- Question : What other data is valuable in “RML”

```
<cre>
    <entry name="CRE-5673-8" />
    <description lang="en_us">Install office 2000 patch KB921595</desc>
</cre>
<rml cre="CRE-5673-8">
    <creation date="" organization="">
    <modification date="" organization=""/>
    <platforms>
        <platform nametype="cpe" name="cpe:/a:microsoft:office:2000:sp3"/>
    </platforms>
    <initiators>
        <initiator nametype="cve" name="CVE-2008-3019"/>
        <initiator nametype="cve" name="CVE-2008-3018"/>
        <initiator nametype="cve" name="CVE-2008-3021"/>
        <initiator nametype="cve" name="CVE-2008-3020"/>
        <initiator nametype="cve" name="CVE-2008-3460"/>
        <initiator nametype="vendor_id" name="A#"/>
        <initiator nametype="microsoft_security_bulletin" name="MS08-044"/>
        <initiator nametype="microsoft_security_bulletin" name="MS08-039"/>
        <initiator nametype="US-CERT" name="TA08-225A"/>
    </initiators>
    <action_list>
        <action actiontype="prose" source="inline">
            Ensure that Office 2000 SP3 is installed, that there is 250 MB of free space available on the system,
            and that no office components are running.  Install patch KB921595.
        </action>
        <action actiontype="ovrl" source="ovrfile.xml" id="local.org.ovrl:1"/>
    </action_list>
</rml>
```

OVRL

- Functional description of a remediation
- Leverage “lessons learned” from OVAL and other SCAP specifications
- Reuse existing OVAL constructs where possible
  - Objects
  - Variables
  - States

OVRL

- Prerequisites for successful action
  - Disk Space
  - Existing software state
- Ordering
- What changes to make to the system
- Steps to take after making the modifications
  - Reboot
  - Restart service
- What to do when an action fails

OVRL

- Question : Should we use the OVAL schema, extend the OVAL schema, or create OVRL analogs?
- Question : How should we approach “undo” functionality?

```
<objects>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:local.test:obj:1" version="1">
        <hive>HKEY_LOCAL_MACHINE</hive>
        <key>System\CurrentControlSet\Control\Lsa</key>
        <name>NoLMHash</name>
    </registry_object>
</objects>
<states>
    <registry_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:local.test:ste:1" version="1">
        <type>reg_dword</type>
        <value datatype="int">1</value>
    </registry_state>
</states>
<actions>
    <registry_action id="ovrl:local.test:act:1" version="1"
                     comment="Set HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash to type REG_DWORD and value 1">
        <object object_ref="oval:local.test:obj:1"/>
        <state state_ref="oval:local.test:ste:1"/>
    </registry_action>
</actions>
<definitions>
    <definition id="ovrl:local.test:def:1" version="1" >
        <metadata>
            <title>Set LAN Manager Hash Value Not Stored on Next Password Change</title>
            <affected family="windows">
                <platform>Microsoft Windows XP</platform>
            </affected>
            <reference source="CRE" ref_id="CRE-XXXX-X"/>
            <description>Network security: Do not store LAN Manager hash value on next password change</description>
        </metadata>
        <action_list>
            <action action_ref="ovrl:local.test.act:1"/>
        </criteria>
    </definition>
```

Policy Specification

- Specify a security policy for an organization
  - Identify the allowed/preferred remediations for a given vulnerability
- Allow for application of remediations without performing an evaluation first
- Deploy different remediation policies to multiple organizational assets/capabilities
- Question : Should we investigate the use of XCCDF for this purpose?

Remediation Applicability

- Use of a “Control Language”
- Express the assets to apply remediations to
  - IP Range
  - Active Directory Membership
  - Machine Names
- Express the remediations to apply (vs. following pre-deployed policy)
- Express variables for use in remediations
- Express Restrictions, Delays, additional options

Remediation Applicability

- Question : Do we need other control languages?
- Question : If so should we have one large specification or multiple smaller ones?
- Question : Are there existing specifications we should be looking at to use as control languages?

```xml
<?xml version="1.0" encoding="utf-8"?>
<content xmlns="http://RCL" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <targetlist id="RCL:TL:01" >
        <target id="192.168.0.1" idtype="ipv4_addr" />
        <remediation_group id="RCL:RG:01"/>
        <option_group id="RCL:OG:01"/>
    </targetlist>

    <targetlist id="RCL:TL:02" >
        <target id="cpe:/a:microsoft:office:xp:sp3" idtype="cpe"/>
        <target id="cpe:/a:microsoft:office_project:2002:sp1" idtype="cpe"/>
        <remediation_group id="RCL:RG:02"/>
        <option_group id="RCL:OG:01"/>
    </targetlist>

    <remediationgroup id="RCL:RG:01">
        <remediation id="CRE-2008-001" idtype="CRE" />
        <remediation id="CRE-2007-043" idtype="CRE" />
    </remediationgroup>

    <remediationgroup id="RCL:RG:02">
        <remediation id="CRE-2008-003" idtype="CRE" />
    </remediationgroup>

    <optiongroup id="RCL:OG:01">
        <option name="AllowUndo" value="true" />
        <option name="AllowApplicationDelay" value="true" />
        <option name="RebootBehavior" value="NONE" />
        <option name="AllowRebootDelay" value="FALSE" />
    </optiongroup>

</content>
```

Returning Result

- Question : Is it valuable to return results from the remediation engine itself? (success/ failure/error)
- Question : What types of results and what level of reporting is desirable?

```
<content xmlns="http://CRRF" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <target id="192.168.0.1" idtype="ipv4_addr" targetlist="RCL:TL:01">
        <remediation id="CRE-2008-001" idtype="CRE" status="success" />
        <remediaiton id="CRE-2007-043" idtype="CRE" status="success"/>
    </target>
    <target id="host.domain.com" idtype="fqdn" targetlist="RCL:TL:02">
        <remediation id="CRE-2008-003" idtype="CRE" status="success" />
    </target>
    <target id="192.168.0.2" idtype="ipv4_addr" targetlist="RCL:TL:02">
        <remediation id="CRE-2008-003" idtype="CRE" status="failure" notes="Failed beacuse of x"/>
    </target>
</content>
```

Conclusion

- More information will be forthcoming on the emerging specs mailing list
- Actively seeking feedback
- Currently working on schemas and specifications
- Currently working on a reference implementation for OVRL

Contact Information

Matthew Kerr

matt.kerr@g2-inc.com

Matthew Wojcik

woj@mitre.org

David Waltermire

david.waltermire@nist.gov