Asset Summary Reporting

Mark Davidson
MITRE Corporation

Adam Halbardier
Booz Allen Hamilton
Supporting NIST

Who is contributing

- National Institute of Standards and Technology (NIST)
- MITRE Corporation
- Department of Defense Computer Network Defense Research and Technology (DoD CND R&T)

Agenda

- History of ASR
- Current Work Effort
- Requirements
- Core Concepts
- Use Cases
- Reporting Categories – Predefined
- Reporting Categories – Undefined
- Prototype

ASR – History

- ASR began as DoD Assessment Summary Results.
  - Currently in production use
  - Current version is 0.41.
- DoD ASR Goals
  - Exchange security assessment results & device inventories of IT assets
  - Contain summarized information about many assets
  - Developed by MITRE

ASR – Current Effort

- ASR as NIST Asset Summary Results
  - Currently under development
  - Next iteration will be 1.0
- Goals
  - Summarize any information about any set of assets
  - Support SCAP/Continuous Monitoring use cases
  - Support uses outside of SCAP/CM
  - Allow complexity/size options

ASR – Requirements

- Support use cases from
  - FISMA (Cyberscope)
  - Continuous Monitoring
  - SAIR III
- ASR must be
  - extensible and adaptable
  - industry agnostic
  - compatible with other security automation specifications

ASR – Core Concepts

- Population Characteristics
  - Describes asset population from which the ASR is generated
- System-Ident
  - Analagous to a key-value pair
  - Ident means identifier
  - Ex: system="http://cve.mitre.org/"
    ident="CVE-2011-3686"

ASR – Core Concepts (cont'd)

- System-Ident (cont'd)
  - Metadata (optional)
  - Result (optional)
  - System-ident (optional)

ASR – Use Cases

- FIPS 199
- OS List & Count
- Patch SLAs

ASR – Use Case: FIPS 199

- For each sub-organization provide a count of systems that are FIPS 199 “low”, “medium”, and “high” category (Cyberscope 1a-c).

ASR – Use Case: FIPS 199

Org Unit	FIPS 199 Score
Accounting	High
Accounting	Medium
Accounting	Low
Sales	High
Sales	High
Sales	Low
Engineering	Medium
Engineering	Medium
Engineering	High

System=OrgUnit; Ident=Accounting
System=FIPS199; Ident=High; Count=1
System=FIPS199; Ident=Med; Count=1
System=FIPS199; Ident=Low; Count=1

System=OrgUnit; Ident=Sales
System=FIPS199; Ident=High; Count=2
System=FIPS199; Ident=Med; Count=0
System=FIPS199; Ident=Low; Count=1

System=OrgUnit; Ident=Engineering
System=FIPS199; Ident=High; Count=2
System=FIPS199; Ident=Med; Count=0
System=FIPS199; Ident=Low; Count=1

ASR – Use Case: OS List & Count

- Provide a list of operating systems, identified by CPE, and a count of assets running each operating system (Cyberscope 3 Data Feed).

ASR – Use Case: OS List & Count

Asset ID	OS
100	cpe:/o:microsoft:windows_7
111	cpe:/o:microsoft:windows_7
200	cpe:/o:microsoft:windows_7
222	cpe:/o:redhat:enterprise_linux
300	cpe:/o:redhat:enterprise_linux
333	cpe:/o:redhat:enterprise_linux
400	cpe:/o:redhat:enterprise_linux
444	cpe:/o:redhat:enterprise_linux
500	cpe:/o:redhat:enterprise_linux
555	cpe:/o:redhat:enterprise_linux

System=http://cpe.mitre.org/;
Ident=cpe:/o:microsoft:windows_7;
count=3

System=http://cpe.mitre.org/;
Ident=cpe:/o:redhat:enterprise_linux;
count=7

ASR – Use Case: Patch SLAs

- Provide percentage of systems that have exceeded patch duration threshold

ASR – Use Case: Patch SLAs

Asset ID	PatchSLA	PatchAge
100	15 Days	5 Days
111	15 Days	10 Days
200	15 Days	30 Days
222	30 Days	15 Days
300	30 Days	15 Days
333	30 Days	45 Days
400	30 Days	15 Days
444	30 Days	45 Days
500	30 Days	15 Days
555	30 Days	15 Days

System=PatchSLA; Ident=15_Days; Count=3
  System=PatchAge; ident=lte_15Days;
    count=2
  System=PatchAge; ident=gt_15Days;
    count=1

System=PatchSLA; Ident=30_Days; Count=7
  System=PatchAge; ident=lte_30Days;
    count=5
  System=PatchAge; ident=gt_30Days;
    count=2

ASR – Revisiting System-Ident

- A system is a category of identifiers
- An ident is a single identifier within a category of identifiers, or system
- Certain system-ident pairs are predefined in the ASR specification
- All other system-idents must be mutually agreed upon by producer and consumer

ASR – Predefined Categories

- Certain reporting categories, if used, must be used in a specific manner:
  - SCAP Standards
    - CPE, CVE, CCSS, CVSS, OCIL, OVAL, XCCDF
  - Others
    - Patches

ASR – Undefined Categories

- An undefined reporting category is any category that is not predefined by the specification
- Guidelines are given for using undefined categories

ASR - Prototype

- Process
  - Input SCAP results
    - XCCDF benchmarks
  - Configurable Output Parameters
  - Output ASR
- Uses
  - Simulate large (100,000+) asset populations
  - Test ASR schema

Get Involved

- Contact any of the following people
  - Adam Halbardier – adam.halbardier@nist.gov
  - Mark Davidson - mdavidson@mitre.org
  - Dave Waltermire – dave.waltermire@nist.gov
- Join the asset-dev@nist.gov mailing list (contact Dave Waltermire to be added)
- Ask about getting involved in the working group

Questions & Answers / Feedback

Adam Halbardier (Booz Allen Hamilton)
Supporting NIST
adam.halbardier@nist.gov - (310) 297-5444

Mark Davidson (MITRE Corporation)
mdavidson@mitre.org - (781) 271-3611

Dave Waltermire (NIST)
david.waltermire@nist.gov - (301) 975-3390