Asset Reporting Format (ARF) and Asset Identification

Adam Halbardier
Booz Allen Hamilton
National Institute of Standards and Technology (NIST)

John Wunder
MITRE Corporation

Security Automation Developer Days – Spring 2011
What is ARF and Asset Identification

- **What is Asset Identification**
  - NIST Interagency Report (IR) 7693
  - A specification governing the method and format to identify and represent assets

- **What is ARF**
  - NIST Interagency Report (IR) 7694
  - A specification governing the formatting of reports about assets
  - Defines how tools should report on information about assets
What is an Asset

Anything that has value to an organization, including, but not limited to, an organization, person, computing device, Information Technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g. locks, cabinets, keyboards, etc.).
Who contributed to ARF and Asset Identification

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

- Overview of Asset Identification
- Overview of ARF
- Where we’re going
Agenda

Overview of Asset Identification

- Overview of ARF
- Where we’re going
Asset Identification

How do you associate information about an asset with the asset itself?
Asset Identification

Or,
How do you uniquely identify an asset and represent that identification?
Use Cases

- Reporting
  - E.g. assessments, remediations, events
- Tasking
  - E.g. assessments, remediations
- Contextual Information
  - E.g. owning organization, location, network, etc
- Federation of asset databases
- Correlation of sensed data
What types of assets are we looking at?

- Person
- Organization
- System
- Software
- Database
- Network
- Service
- Data
- Computing Device
- Circuit
- Website
- (3rd parties can extend it)
What do you get?

- Correlation of data across the management domain, including from varying...
  - Sensor types
  - Timeframes
  - Result types
  - Vendors
Are we there yet?

- Automated security specifications use varying mechanisms to identify assets
  - Incompatible specifications
  - Inconsistent implementations
  - Incomplete information
How can we get there?

- Single specification to identify assets
- May be used by specification authors as identification elements
  - OVAL
  - XCCDF
  - OCIL
  - Digital event reporting
  - Remediation
Assets may be identified using some set of identifying information, including both literal identifiers and synthetic identifiers.
Many tools assign identifiers to assets they manage

Assets may be identified using an **assigned identification element** in the context of a namespace

**Ex:**
- Namespace: VendorProduct1
- Identifier: Asset3544
Literal Identifiers

- Information that is **collectable** or **discoverable** about an asset is also useful for identification
  - Devices: hostname, IPv4 address, Motherboard GUID
  - People: Full name, location, organization
  - Organizations: Name, type
How it works

Assets may be identified using some set of identifying information, including both literal identifiers and synthetic identifiers.
Examples

Synthetic IDs:
- Asset1234@MITRE

Synthetic IDs:
- Asset1234@MITRE
- Asset4321@Tool2

Literal Identifiers:
- IPv4: 1.2.3.4
- Hostname: mm123123

Synthetic IDs:
- Asset1234@MITRE
- Asset4321@Tool2

Literal Identifiers:
- IPv4: 1.2.3.4
- Hostname: mm123123
What it means for you: **End Users**

- More complete and accurate information about each asset
  - Better metrics
  - Improved knowledge of security posture
  - Better return on investment
What it means for you: Vendors

- Simpler and Cheaper Implementation
  - Single identification element to implement across the various specifications
- Normalized data to support fusion and correlation
  - But no rules on extra features your product can offer
- Single path for feedback on problems
- Built-in extension mechanisms for value-added capabilities
What it means for you: Specification Authors

- Focus on core competency
  - Reuse asset identification
- Automatic compatibility of identification with other specifications
Agenda

- Overview of Asset Identification

- Overview of ARF

- Where we’re going
Purpose of ARF

- Define a data model to house data about:
  - Assets
  - Asset identification information
  - Requests for asset information
  - The relationships between the components above

- Define a specification to report about assets in support of numerous use cases in government and industry at various levels of detail
Purpose of ARF (con’t)

- Enable asset report correlation
  - Leverage the Asset Identification specification to identify the subjects of reports enabling different reports about the same assets to be correlated across and enterprise
Scope of ARF

- Define the report transport data model
- Define the relationships between asset report components, while leaving the low-level data models to other specifications
High-level Requirements

Must be able to:

- associate one or more assets with arbitrary payloads
- define explicit relationships between payloads and assets
- combine multiple ARF reports into a single ARF report
- define reusable sets of data
- reference data external to the ARF report
Use Cases

- Vulnerability Management
- Asset Discovery and Inventory Management
- Compliance Assessment
- Digital Event Analysis
Use case: Vulnerability Management

- Endpoint scan results
- Aggregate reporting of vulnerability / remediation
Use case: Asset Discovery and Inventory Management

- Reporting on newly discovered assets
- Maintaining inventory records of assets
- Communicating about assets between data stores
Use case: Compliance Assessment

- United States Government Configuration Baseline (USGCB) / Federal Desktop Core Configuration (FDCC)
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX) Compliance
- Payment Card Industry (PCI) Compliance
- Organizational policies (e.g. STIGs, NSA SCG)
Use case: Digital Event Analysis

- Report on digital events at the host level
- Aggregate digital event messages across organization
ARF Model

Reports

Report Requests

Assets
Example

Report Requests
- SCAP Datastream

Assets
- Computer 1
  IP Address: 192.168.2.7
- Computer 2
  Canonical ID: http://tempuri.org/assets#32

Reports
- Report 1
  SCAP Result
- Report 2
  SCAP Result

(createdFor)
ARF’s Relationship to Other Specifications

![Diagram showing ARF's relationship to XML/JSON schema, data format specifications (XCCDF, OVAL, etc.), asset identification, and XLink with data format specifications (XCCDF, OVAL, etc.).]
XLink

- A W3C specification describing the method of establishing links in XML
- Used in ARF to reference remote content
Why Use ARF

- Adds higher-level, standardized layer on top of reports about assets
- Adds ability to correlate and fuse data by cutting across specification boundaries
- Leverages standardized asset identification language
- Ties requests and responses about assets together
Agenda

- Overview of Asset Identification
- Overview of ARF

Where we’re going
Status

- Concluded public comment period in January
- Incorporated feedback from public comment period and from the participants of the working group
- Preparing to begin the final release process
- Planning for inclusion in SCAP 1.2
Asset Summary Reporting (ASR)

- Documenting the requirements for a summary format
- Considering an asset population querying solution that could be applicable to summary reporting AND tasking, among other applications
- Developing the ASR data model
Get Involved

- Contact any of the following people
  - Adam Halbardier – adam.halbardier@nist.gov
  - John Wunder – jwunder@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 National Institute of Standards and Technology (NIST)
adam.halbardier@nist.gov
(310) 297-5444

John Wunder
MITRE Corporation
jwunder@mitre.org
(781) 271-4602