Asset Reporting Format (ARF) and Asset Identification

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

John Wunder
MITRE Corporation

6th Annual IT Security Automation Conference

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

Background

- DoD CND R&T PMO developed ARF 0.41 to support internal DoD use-cases
- NIST, in conjunction with DoD CND R&T PMO and MITRE, considering additional use cases relevant to SCAP and other industry practices, developed ARF 1.0 (DRAFT) to replace ARF 0.41

Agenda

- Introduction to Asset Identification
- Introduction to ARF
- Timeline and Ways to Participate

Agenda

➡ Introduction to Asset Identification

- Introduction to ARF
- Timeline and Ways to Participate

Asset Identification

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

Asset Identification

Or,

Asset Identification

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?

- Device
- Person
- Organization
- Network
- System
- Software
- Circuit
- But third 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

How it works

Assets may be identified using a combination of

zero to many **canonical identifiers** and/or

some set of **identifying information**

Canonical 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

Identifying Information

- Sometimes, assigned identifiers are unavailable or are not shared
- But, some information that is **collectable** or **discoverable** about an asset is available
  - Devices: hostname, IPv4 address, MAC address
  - People: Full name, location, organization
  - Organizations: Name, type
- Some amount of certainty of an accurate identification

How it works

Assets may be identified using a combination of

zero to many **canonical identifiers** and/or

some set of **identifying information**

Examples

Canonical IDs:

- Asset1234@MITRE

Canonical IDs:

- Asset1234@Tool1
- Asset4321@Tool2

Canonical IDs:

- Asset1234@Tool1
- Asset4321@Tool2

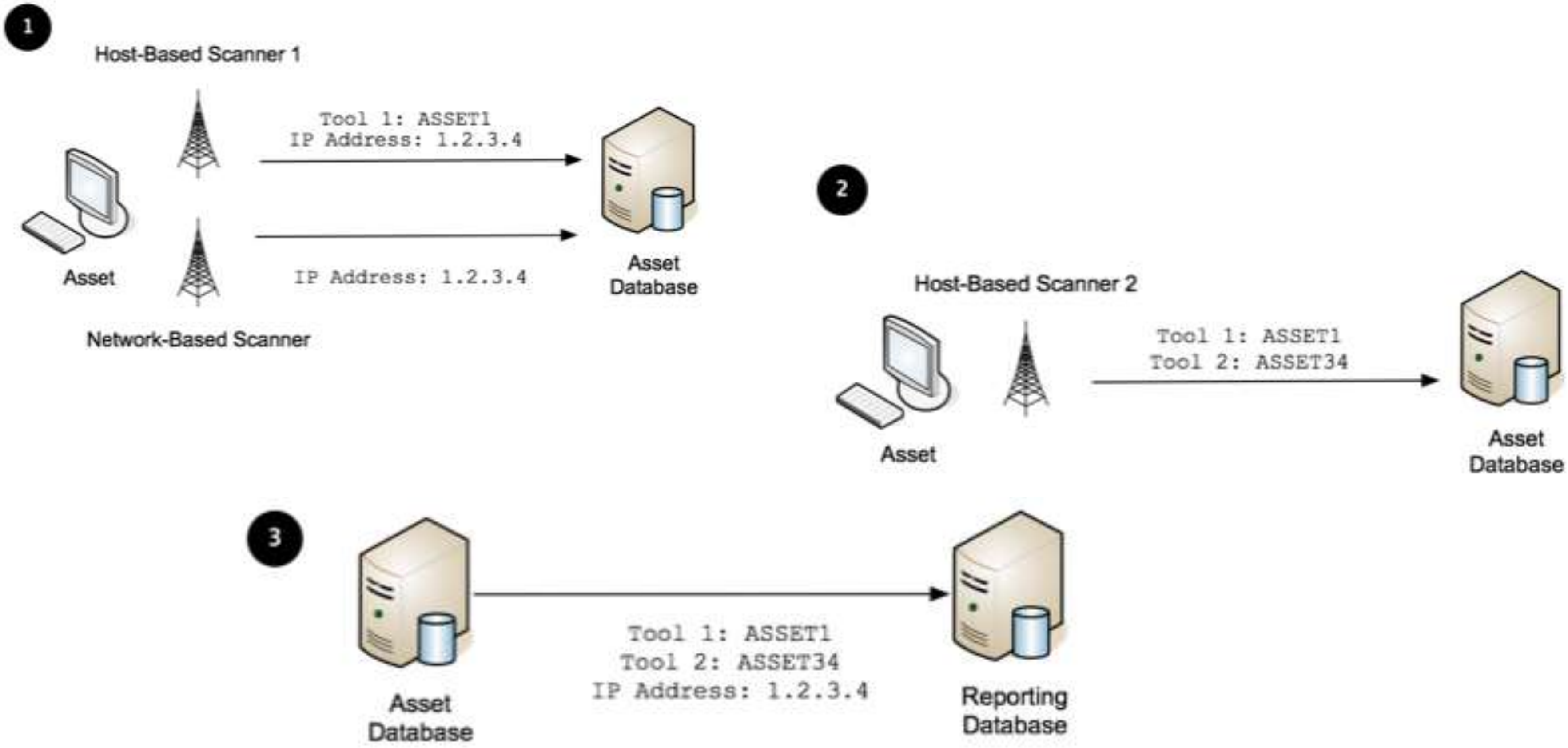
Identifying Information:

- IPv4: 1.2.3.4
- Hostname: mm123123

Identifying Information:

- IPv4: 1.2.3.4
- Hostname: mm123123

Sample Usage (Reporting)



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

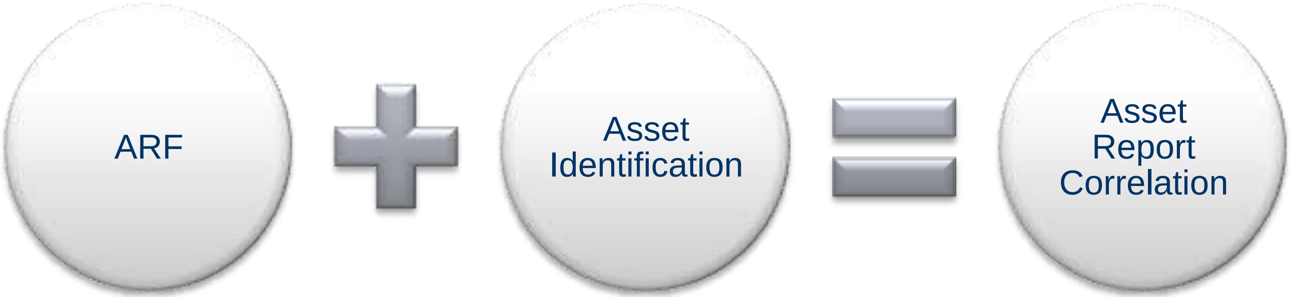
- Introduction to Asset Identification
- ➡ Introduction to ARF
- Timeline and Ways to Participate

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

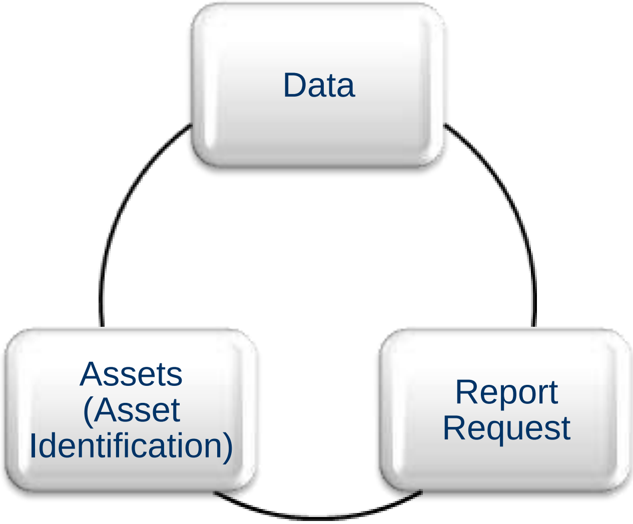
Purpose of ARF (con't)

- 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

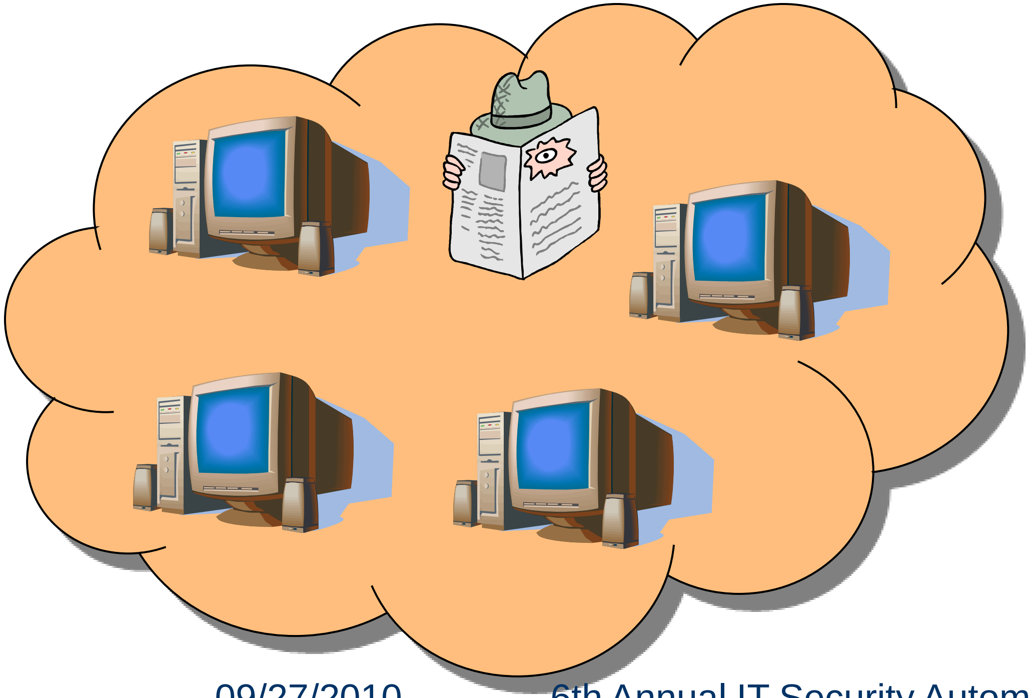
- Must be able to:
  - associate one or more assets with arbitrary payloads
  - define explicit relationships between payloads and assets
  - combine multiple ARF reports into a single ARF report
  - define reusable sets of data
  - reference data external to the ARF report

Use Cases

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

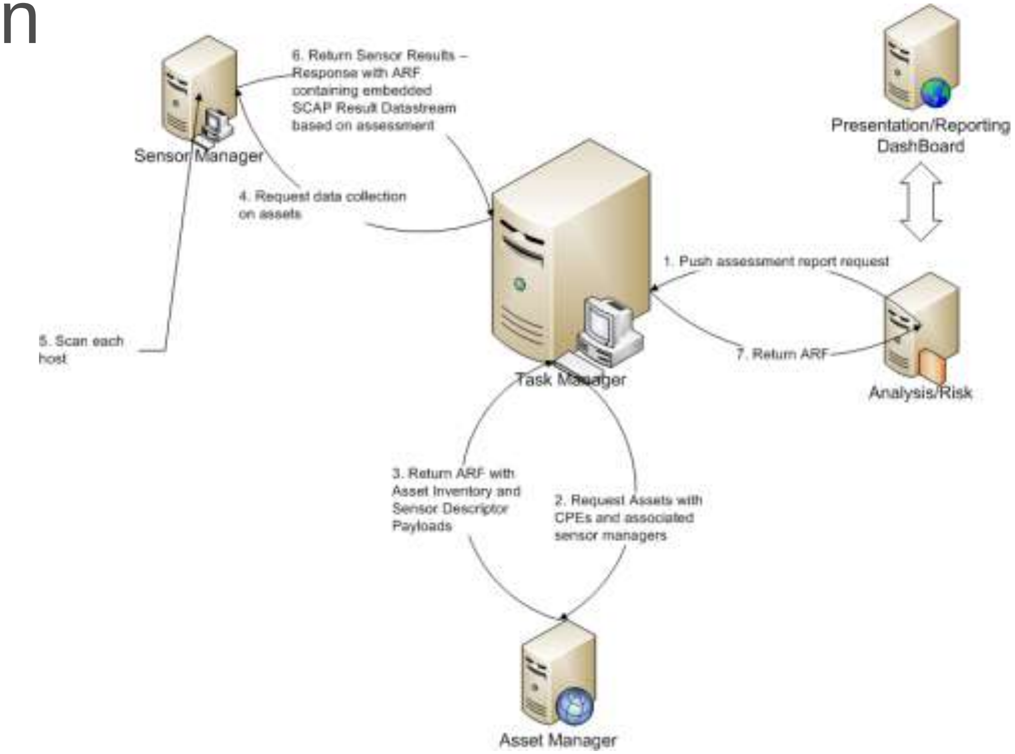
Use case: Asset Discovery and Inventory Management

- Reporting on newly discovered assets
- Maintaining inventory records of assets
- Communicating about assets between data stores



Use case: Vulnerability Management

- Endpoint scan results
- Aggregate reporting of vulnerability / remediation


6. Return Sensor Results – Response with ARF containing embedded SCAP Result Datastream based on assessment
Sensor Manager
Presentation/Reporting DashBoard
4. Request data collection on assets
1. Push assessment report request
5. Scan each host
7. Return ARF
Task Manager
Analysis/Risk
3. Return ARF with Asset Inventory and Sensor Descriptor Payloads
2. Request Assets with CPEs and associated sensor managers
Asset Manager

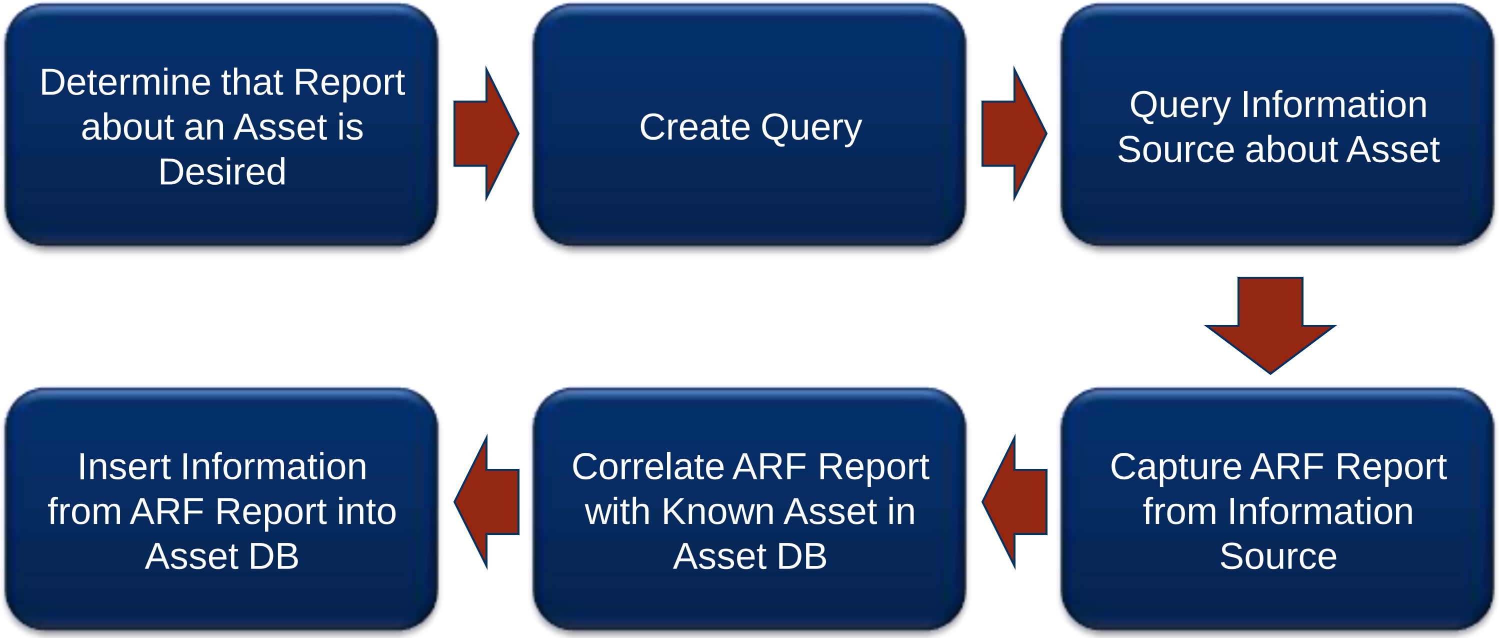
Use case: Compliance Assessment

- 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

Sample Workflow



Determine that Report about an Asset is Desired

Create Query

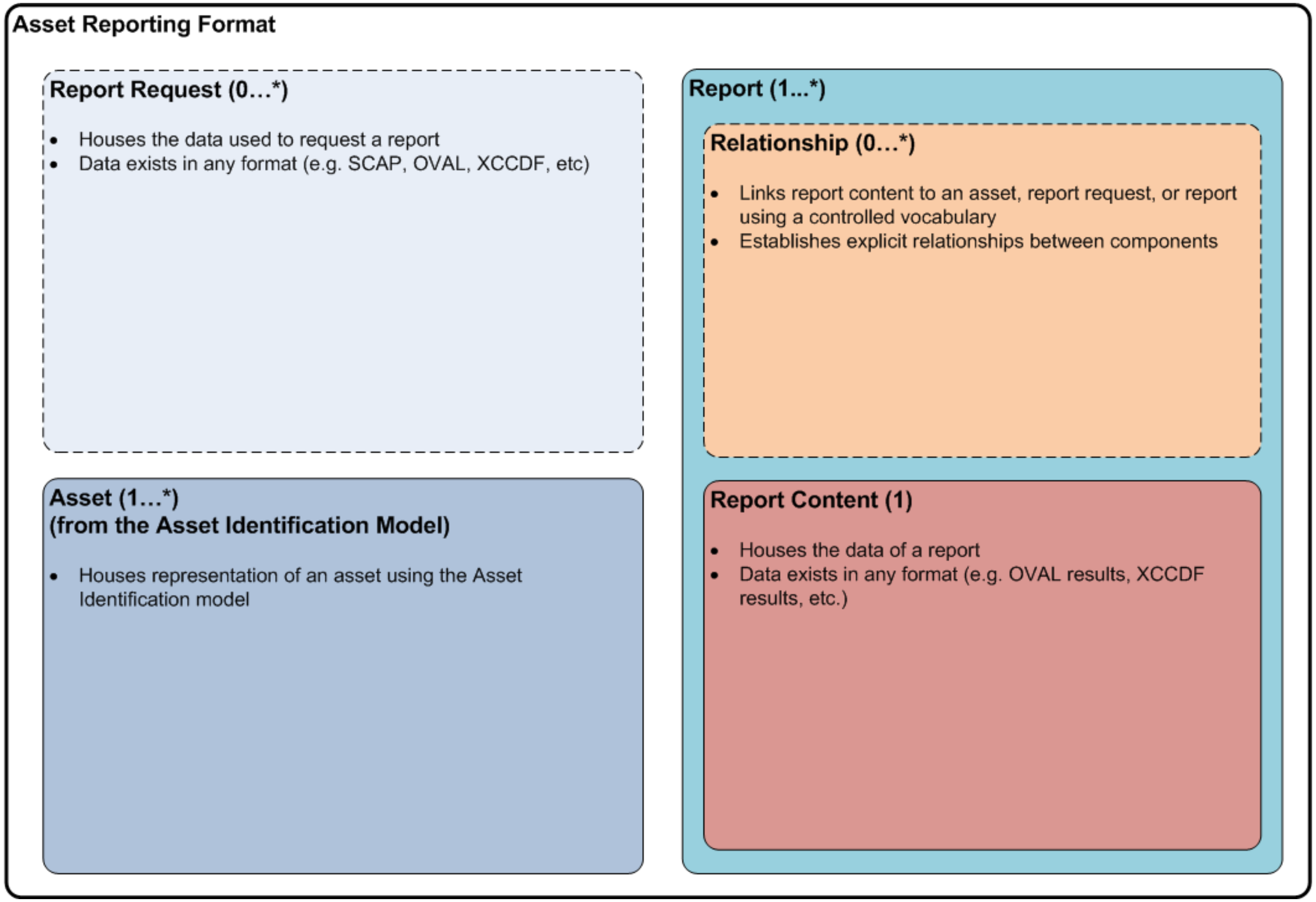
Query Information Source about Asset

Capture ARF Report from Information Source

Correlate ARF Report with Known Asset in Asset DB

Insert Information from ARF Report into Asset DB

ARF Data Model Outline



Asset Reporting Format

Report Request (0…*)

- Houses the data used to request a report
- Data exists in any format (e.g. SCAP, OVAL, XCCDF, etc)

Asset (1…*)
(from the Asset Identification Model)

- Houses representation of an asset using the Asset Identification model

Report (1...*)

Relationship (0…*)

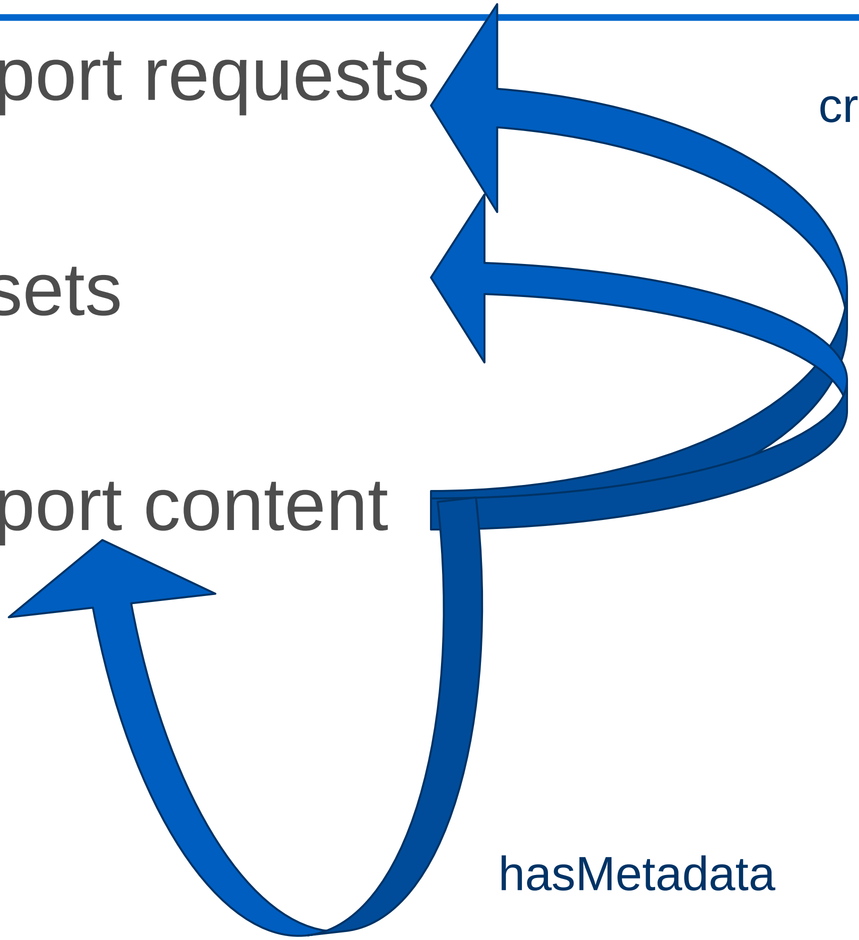
- Links report content to an asset, report request, or report using a controlled vocabulary
- Establishes explicit relationships between components

Report Content (1)

- Houses the data of a report
- Data exists in any format (e.g. OVAL results, XCCDF results, etc.)

Objects To Be Related

- Report requests
- Assets
- Report content



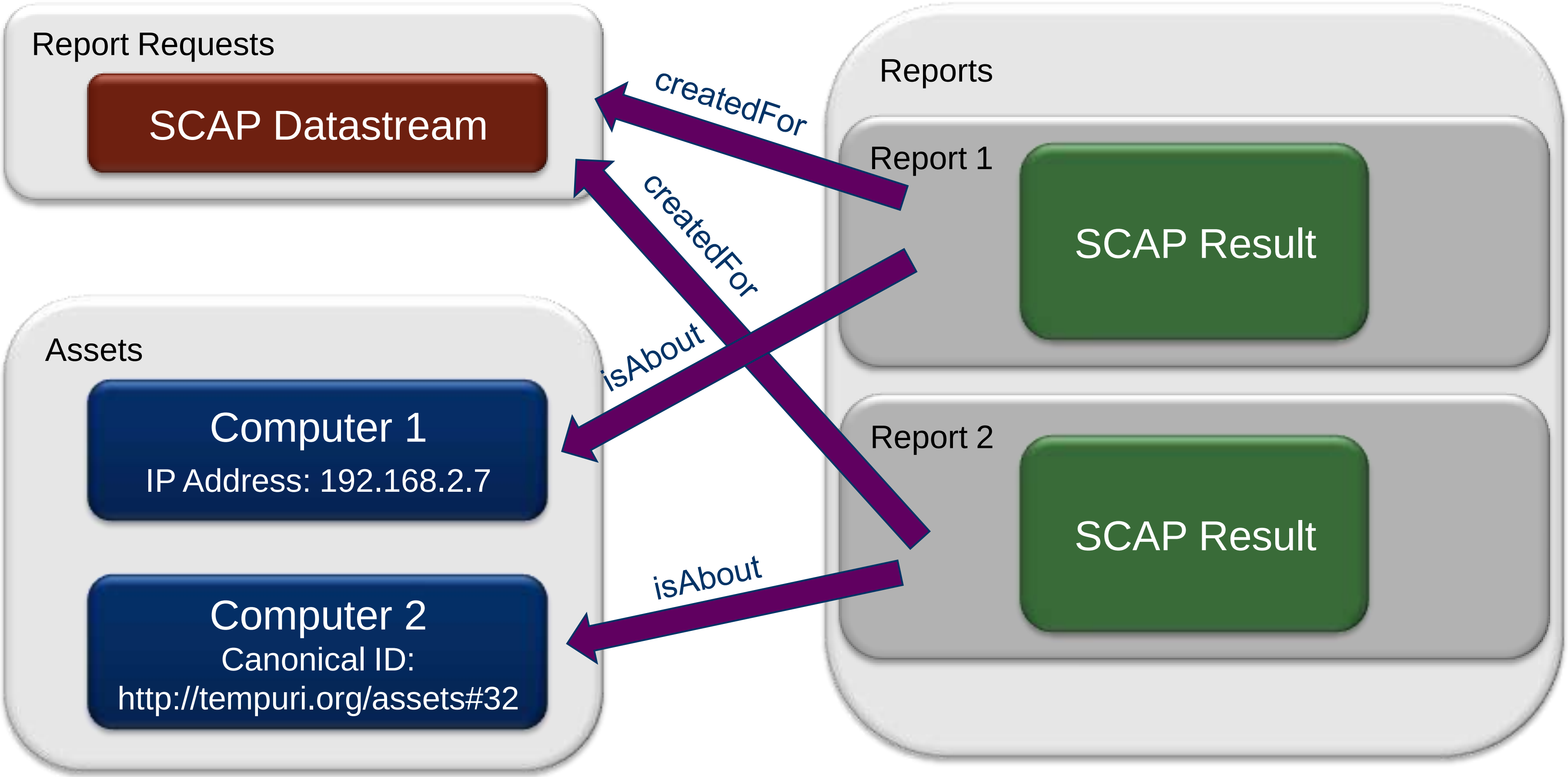
createdFor

isAbout
hasSource
retrievedFrom
createdBy
emittedBy

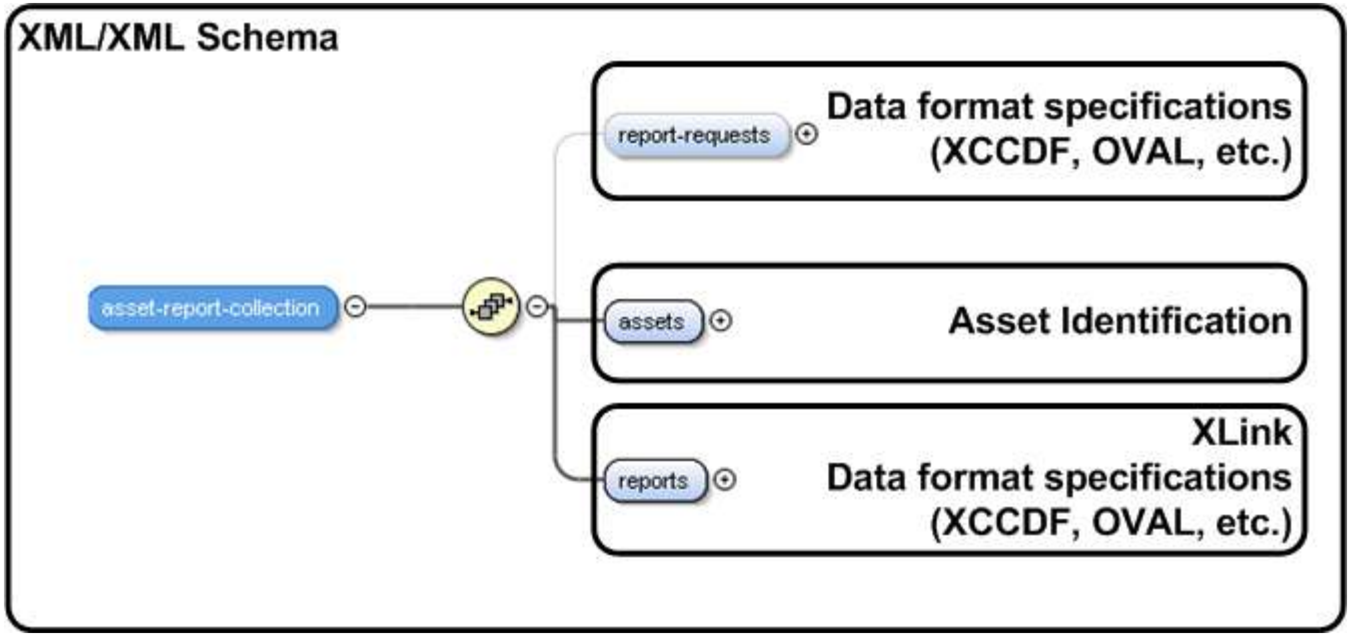
hasMetadata

http://scap.nist.gov/vocabulary/arf/relationships/1.0#

Example


Report Requests
SCAP Datastream
Reports
createdFor
createdFor
Report 1
SCAP Result
Assets
isAbout
Computer 1
IP Address: 192.168.2.7
Report 2
SCAP Result
isAbout
Computer 2
Canonical ID:
http://tempuri.org/assets#32

ARF's Relationship to Other Specifications


XML/XML Schema
asset-report-collection
report-requests
Data format specifications (XCCDF, OVAL, etc.)
assets
Asset Identification
reports
XLink
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

- Introduction to ARF
- Introduction to Asset Identification
- ➡ Timeline and Ways to Participate

Timeline

- After workshop, changes will be incorporated into ARF and Asset Identification and drafts will be released
- Drafts will enter NIST 30 day public review period
- Specifications final in Winter 2010
- Inclusion in SCAP 1.2

Get Involved

- Contact any member of the working group
  - Adam Halbardier – adam.halbardier@nist.gov
  - John Wunder – jwunder@mitre.org
  - Dave Waltermire – dave.waltermire@nist.gov
  - Mark Johnson – mark.johnson@nist.gov
- Email to emerging-specs@nist.gov
- Ask about getting involved in the working group
- Submit comments on NIST IR 7693 and 7694
- Come to the workshop on Wednesday

Additional Resources

NIST Websites:

- SCAP Homepage: http://scap.nist.gov
- SCAP Validated Tools: http://nvd.nist.gov/scapproducts.cfm
- SCAP Validation Homepage: http://nvd.nist.gov/validation.cfm
- National Checklist Program: http://checklists.nist.gov
- National Vulnerability Database: http://nvd.nist.gov
- NIST Computer Security Resource Center (CRSC) http://csrc.nist.gov/publications/PubsSPs.html

Questions & Answers / Feedback

John Wunder

MITRE Corporation

jwunder@mitre.org

(781) 271-4602

Adam Halbardier

Booz Allen Hamilton

Supporting National Institute of Standards and Technology (NIST)

adam.halbardier@nist.gov

(310) 297-5444