Enterprise Asset Reporting

Adam Halbardier
Booz Allen Hamilton
Supporting NIST

Agenda

- Overview of Asset Identification, ARF, and ASR
- Approach for cross organizational reporting
- Discussion

Agenda

- Overview of Asset Identification, ARF, and ASR
- Approach for cross organizational reporting
- Discussion

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.).

What is Asset Identification, ARF, ASR

- What is Asset Identification
  - NIST Interagency Report (IR) 7693
  - A specification governing the method and format to define and produce aggregate reports about 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 Asset Identification, ARF, ASR (con't)

- What is ASR
  - NIST Interagency Report (IR) 7848
  - A specification governing the method and format to define and produce aggregate reports about assets

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?

- 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

How it works

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

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

Examples

Synthetic IDs:
- Asset1234@MITRE

Synthetic IDs:
- Asset1234@MITRE
- Asset4321@Tool2

Synthetic IDs:
- Asset1234@MITRE
- Asset4321@Tool2

Literal Identifiers:
- IPv4: 1.2.3.4
- Hostname: mm123123

Literal Identifiers:
- IPv4: 1.2.3.4
- Hostname: mm123123

Purpose of ARF

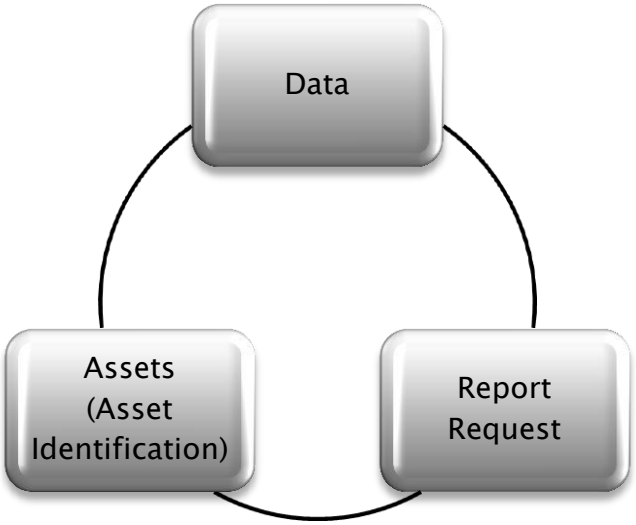
- Define a data model to house data about:
  - Assets
  - Asset identification information
  - Requests for asset information
  - The relationships between the components above
- Define a specification to report about assets in support of numerous use cases in government and industry at various levels 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

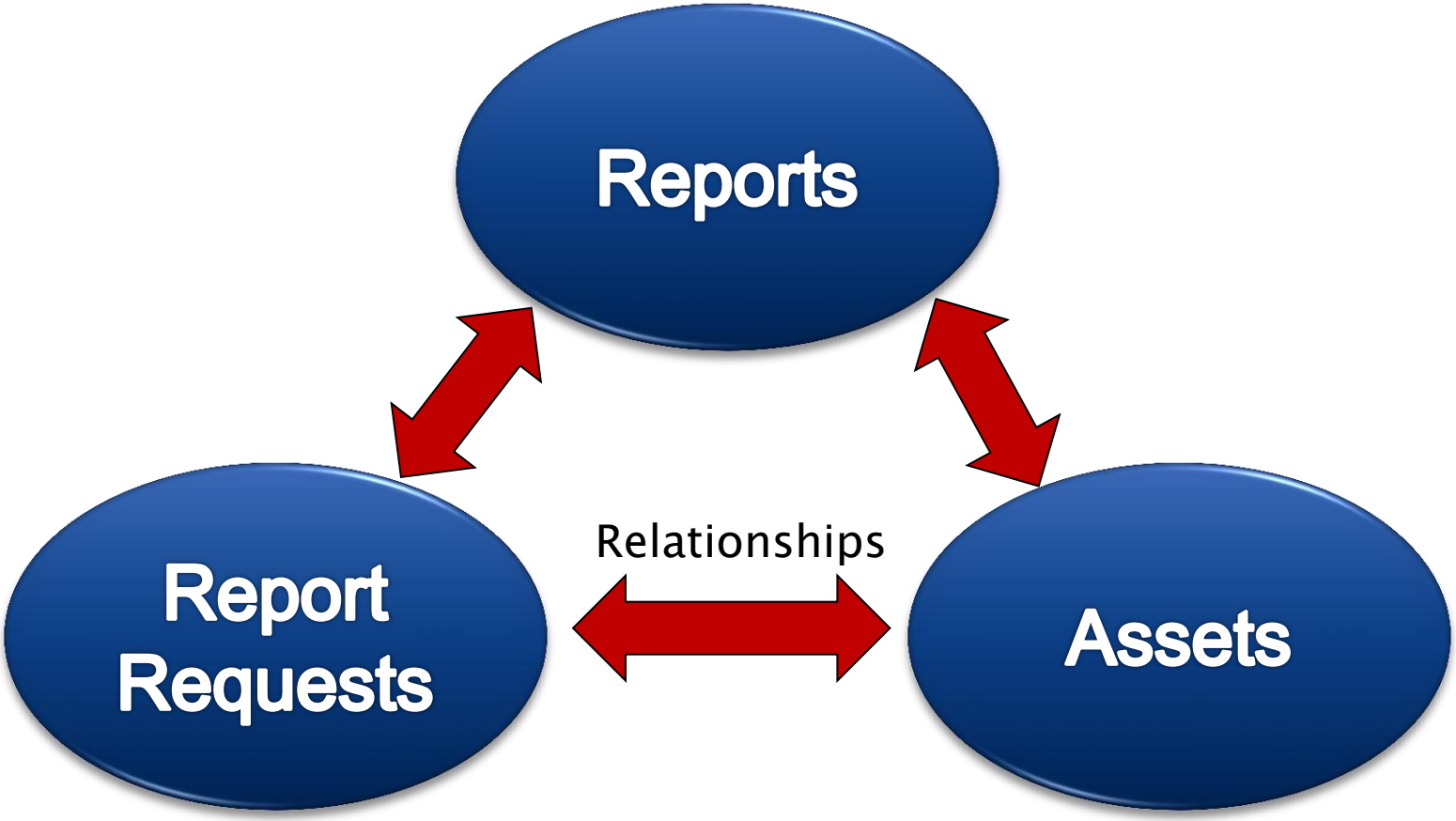
- Define the report transport data model
- Define the relationships between asset report components, while leaving the low-level data models to other specifications



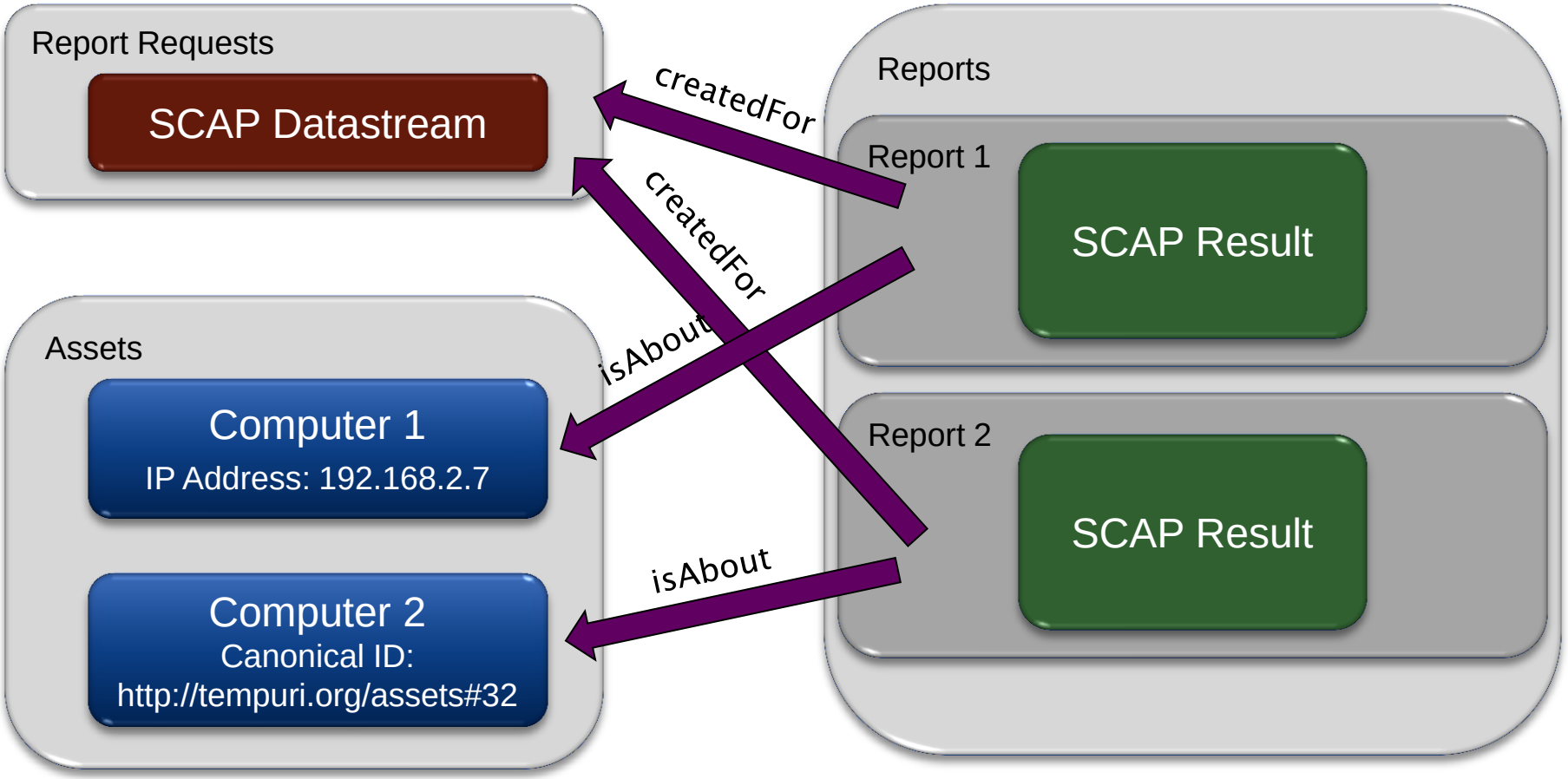
High-level Requirements

- 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

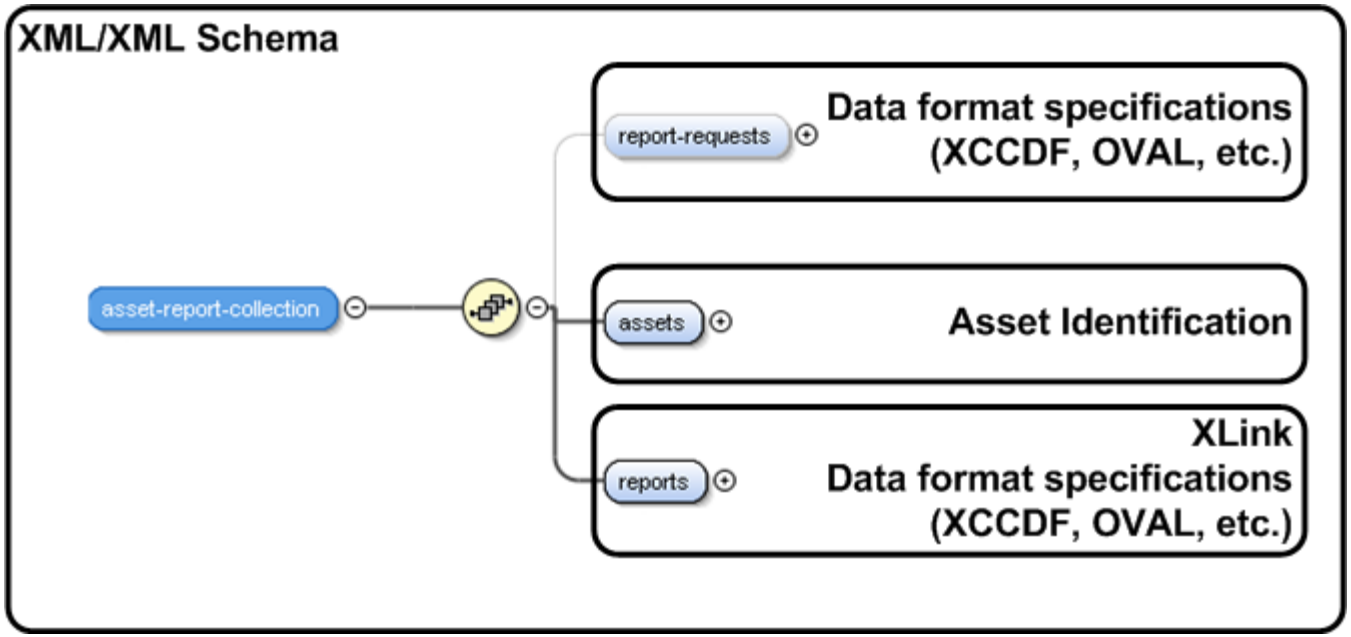
ARF Model



Example


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

ARF's Relationship to Other Specifications



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

ASR – Goals

- 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
- ASR must be
  - extensible and adaptable
  - industry agnostic
  - compatible with other security automation specifications

ASR – Core Concepts

- Data source
  - Identifies the asset pool from which the report is generated
- Record set
  - A collection of 1 or more records to report
- Record set type
  - A description of how to construct a record set
- Namespace Qualified Attributes
  - Well-defined attributes associated with a record

ASR – Record

- Record
  - A particular set of information, usually used as the basis for a count
  - Records are composed of namespace qualified attributes that are well defined
  - Each record may contain a count of assets for the record, as well as a list of assets enumerating that count

Example – Record Set

```
<asr:summary-report xmlns:ex="com.example" xmlns:asr="http://scap.nist.gov/schema/asset-summary-reporting/1.0"
xmlns:asr-attr="http://scap.nist.gov/schema/asset-summary-reporting/1.0/attr" page-number="1" last-page="true"
report-id="d1e1">
    <asr:metadata timestamp="2011-11-08T14:27:44.97Z"/>
    <asr:record-set id="asr:com.example:rset:1" data-source-ref="asr:com.example:dsrc:1" record-
            set-type="ex:cve-report-small">
        <asr:record asr-attr:cve-id="CVE-2011-2013" asr-attr:inventory-finding="EXISTS"
        asr-attr:count="50"/>
        <asr:record asr-attr:cve-id="CVE-2011-2013" asr-attr:inventory-
                finding="NOT_EXISTS" asr-attr:count="170"/>
        <asr:record asr-attr:cve-id="CVE-2011-2013" asr-attr:inventory-
                finding="NOT_APPLICABLE" asr-attr:count="30"/>
    </asr:record-set>
    <asr:data-source id="asr:com.example:dsrc:1" resource="VulnDb.abc.com" population-
    size="250"/>
</asr:summary-report>
```

Example – Record Set Type

Record Set Type Name: {com.example}cve-report-small

Description: To report on the number of computers affected by a CVE. Attributes

- asr-attr:cve-id – MUST include. This is the CVE ID being reported on. Type: XML schema “string”.
- asr-attr:inventory-finding – MUST include. This is a status of the CVE for each asset in the count. Value must be one of “EXISTS”, “NOT_EXISTS”, “NOT_APPLICABLE”, “NOT_REPORTED”, “ERROR”, or “UNKNOWN”. Type: XML schema “string”.
- asr-attr:count – MUST include. Asset list is associated with this attribute. This count is the number of assets with the CVE related to the asset via the inventory-finding. Type: XML schema nonNegativeInteger.

Permit attributes not explicitly described here: no

Require asset list: not permitted

Require identifier list: not permitted

ASR – Paging

- An ASR record set may span multiple pages when necessary
  - Reduces risk of resending a large, single report
  - Reduces memory load of creating large, single reports

Agenda

- Overview of Asset Identification, ARF, and ASR
- Approach for cross organizational reporting
- Discussion

Enterprise Reporting Goals

- Support the request and response of data calls across the Federal government (FISMA/Cyberscope reporting)
- Communicate threat and incident information
- Enable standardized security reporting within an enterprise

Leverage GRC Report Exchange

- An Internet Engineering Task Force (IETF) working document out of the Managed Incident Lightweight Exchange (MILE) working group
- Defines workflows and formats for sending, requesting, and acknowledging reports
- Provides mechanisms to define policy around the security and handling of messages

Message Types

- Report – a GRC report
- Request – request a GRC report
- Query – request information about a GRC report
- Acknowledgement – request/query status
- Result – response to request/query

Report Registration

- GRC Report Exchange requires IANA registration of a report schema, before use
- Proposal: register ARF 1.1 as a GRC Report Exchange report type

Advantages of Leveraging ARF

- ARF enables asset reporting of arbitrary information types
- For detailed reporting of individual assets, ARF:
  - provides the high-level relationships to connect data to assets
  - leverages standardized asset identification
- For enterprise/aggregate asset reporting, ARF can embed ASR

Transport Protocol

- Proposal: use HTTP/TLS, similar to the Real-time Inter-network Defense (RID) transport proposal in RFC 6546

Message Example: Report

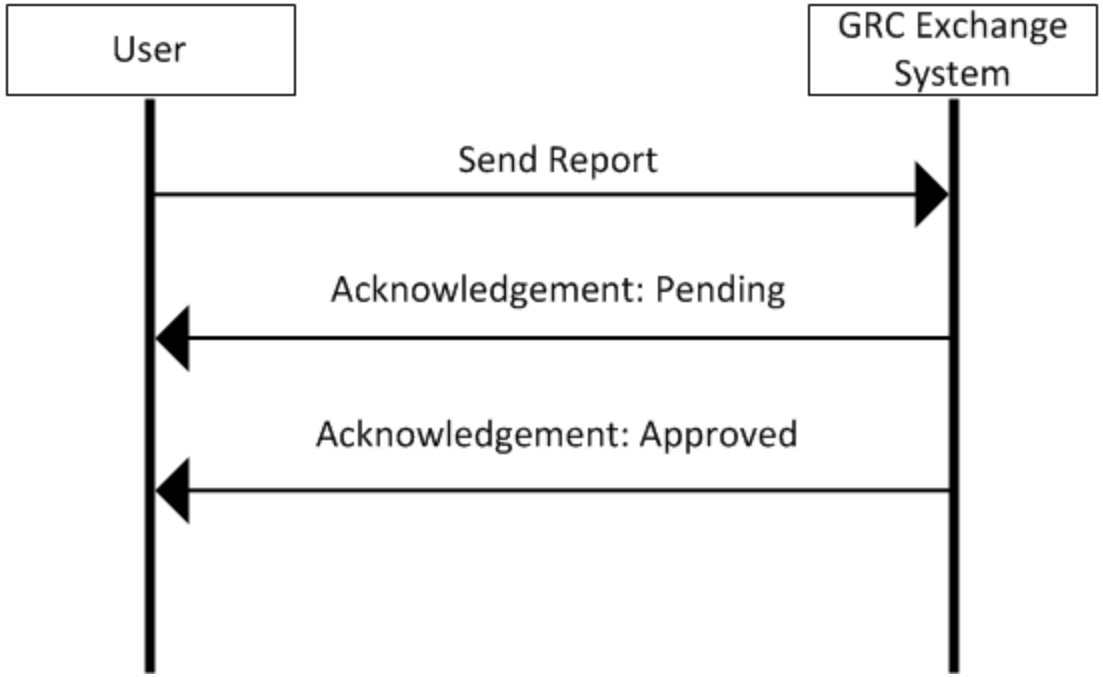
- See external XML message

```
<?xml version="1.0" encoding="UTF-8"?>
<grc-exchange:GRC-Exchange xmlns:grc-exchange="urn:ietf:params:xml:ns:grc-exchange-1.0"
 xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.2"
 xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:sch="http://purl.oclc.org/dsdl/schematron"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:grc-exchange-1.0 file:/C:/NIST/Conferences/GRC-Exchange-0.7.6.xsd"
 lang="en-US">
 <grc-exchange:GRCPolicy MsgType="Report" MsgDestination="GRCSystem">
  <grc-exchange:PolicyRegion region="ClientToSP"/>
 </grc-exchange:GRCPolicy>
 <grc-exchange:GRCDocument XMLSchemaID="http://scap.nist.gov/schema/asset-reporting-format/1.1" Version="1.0">
  <grc-exchange:ReportType type="Filing"/>
  <grc-exchange:XMLDocument dtype="xml">
   <asset-report-collection xmlns="http://scap.nist.gov/schema/asset-reporting-format/1.1"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://scap.nist.gov/schema/asset-reporting-format/1.1 http://scap.nist.gov/schema/asset-reporting-format/1.1/asset-reporting-format_1.1.0.xsd">
    <reports>
     <report id="id3">
      <content>
       <summary-report xmlns="http://scap.nist.gov/schema/asset-summary-reporting/1.0"
        xmlns:asr-attr="http://scap.nist.gov/schema/asset-summary-reporting/1.0/attr"
        xmlns:rec-set-type-def="http://scap.nist.gov/schema/asr/record-set-type-def"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://scap.nist.gov/schema/asset-summary-reporting/1.0 http://scap.nist.gov/schema/asset-summary-reporting/1.0/asset-summary-reporting_1.0.xs
        http://scap.nist.gov/schema/asset-summary-reporting/1.0/attr http://scap.nist.gov/schema/asset-summary-reporting/1.0/asset-summary-reporting-attr_1.0.xsd"
        report-id="report-id1" page-number="1" last-page="true">
        <record-set id="asr:gov.nist:rset:1" record-set-type="rec-set-type-def:compliance"
         data-source-ref="asr:gov.nist:dsrc:1"
```

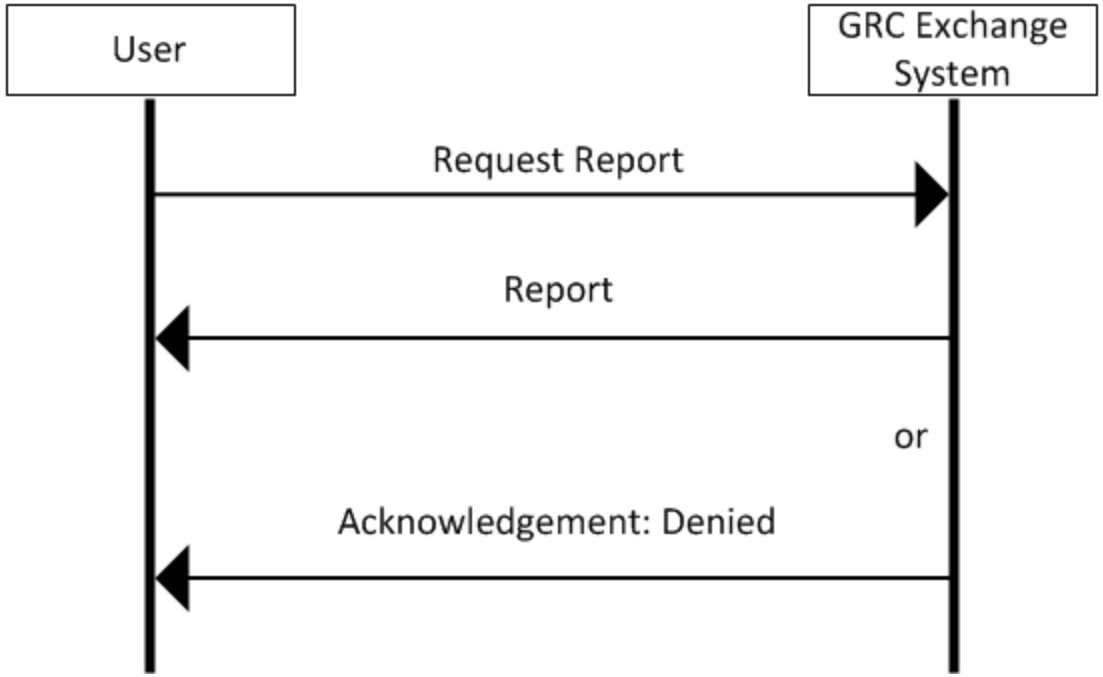
Message Example: Acknowledgement

```
<grc-exchange:GRC-Exchange>
   <grc-exchange:GRCPolicy MsgType="Acknowledgment"
MsgDestination="GRCSystem">
      <grc-exchange:PolicyRegion region="ClientToSP"/>
   </grc-exchange:GRCPolicy>
   <grc-exchange:RequestStatus AuthorizationStatus="Approved"/>
</grc-exchange:GRC-Exchange>
```

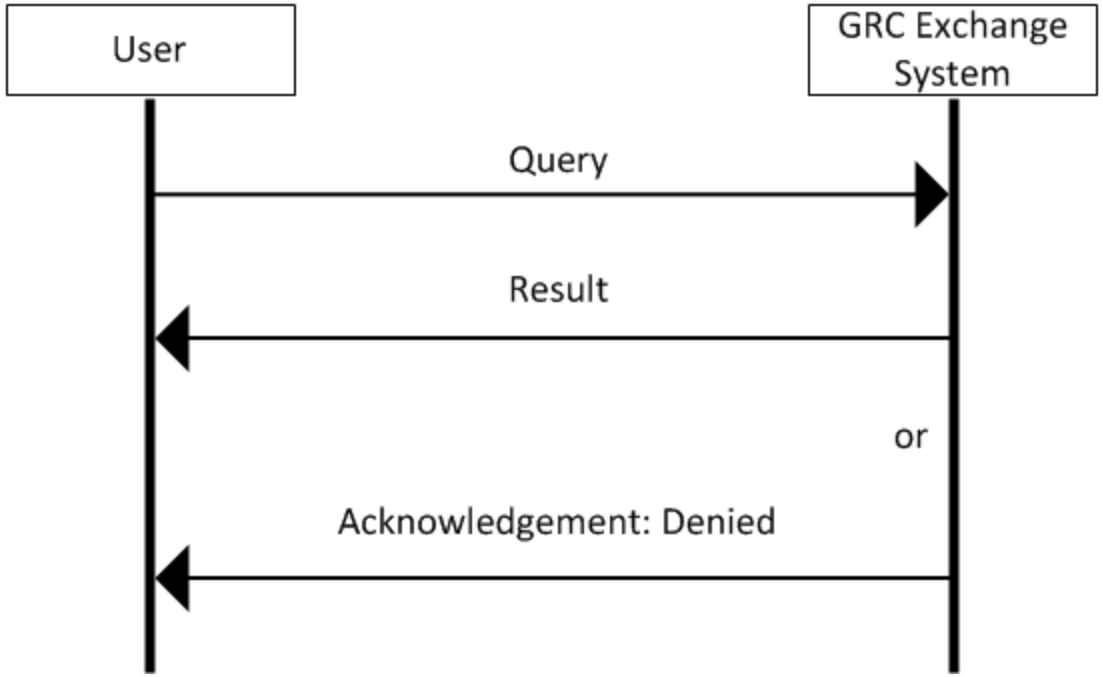
Workflow: Send Report



Workflow: Request Report



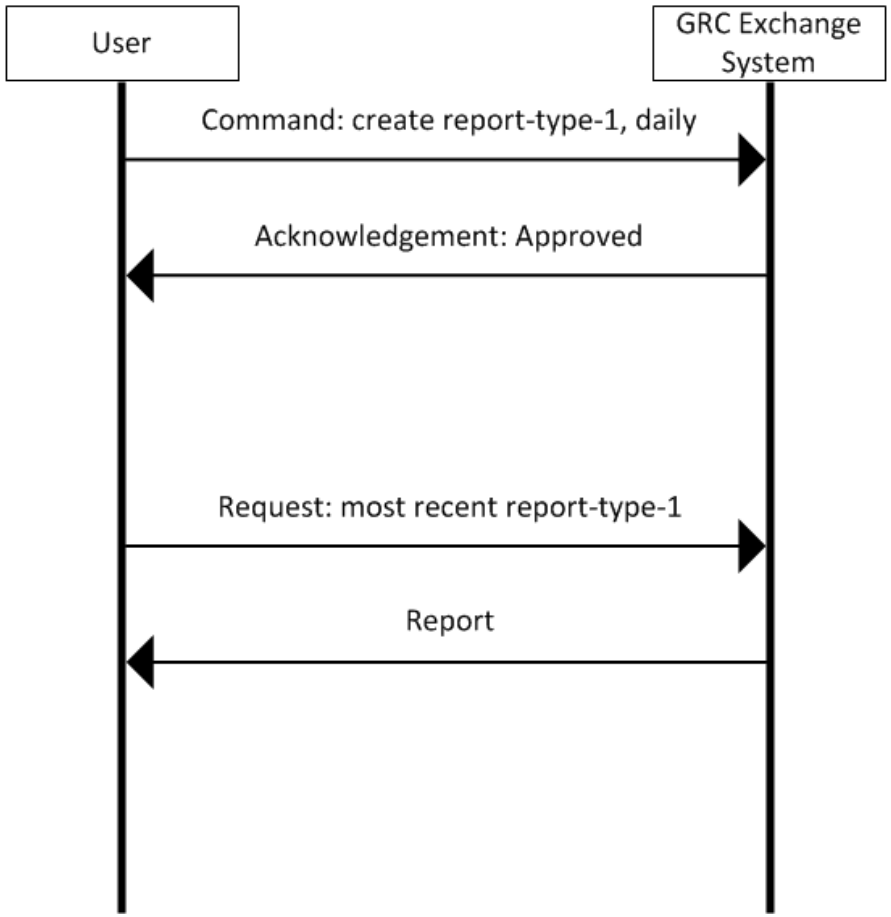
Workflow: Query



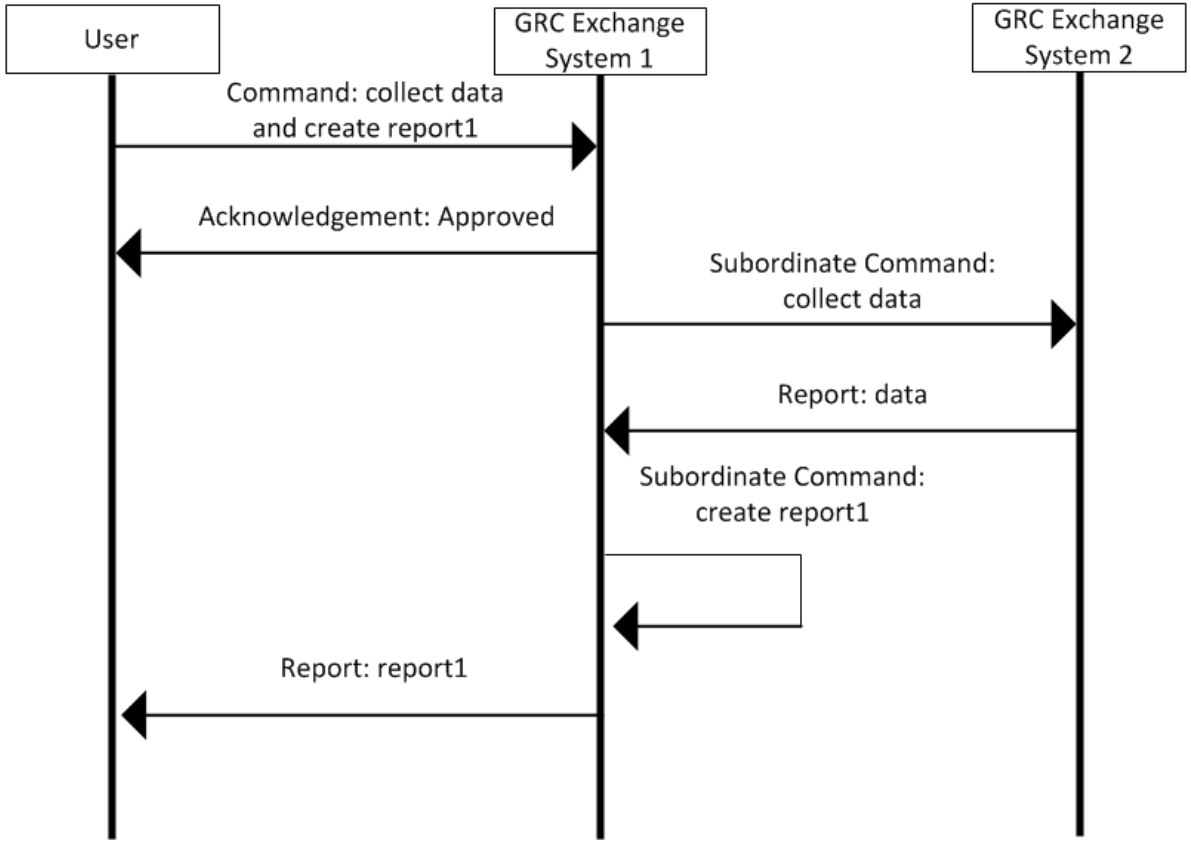
Proposal: Add Command Message to GRC Report Exchange

- Command message: send instructions
  - cause new data to be collected on-demand or on-schedule
  - cause new report to be constructed from existing data
  - cause new analysis on existing data
  - enable hierarchy and ordering of command messages

Workflow: Command



Workflow: Subordinate Command



Agenda

- Overview of Asset Identification, ARF, and ASR
- Approach for cross organizational reporting
- Discussion

Next Steps

- Define a transport protocol
- Register ARF with IANA as a GRC Exchange schema
- Develop request/query languages and register with IANA
- Add command message to GRC Report Exchange
- Finalize GRC Report Exchange
- Standardize several ASR report types (compliance, vulnerability, inventory, etc.)

Questions & Answers / Feedback

Adam Halbardier (Booz Allen Hamilton)

Supporting NIST

adam.halbardier@nist.gov - (310) 297-5444

Dave Waltermire (NIST)

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

Backup

ASR: XCCDF Record Set Type Definition

- xccdf-benchmark
- xccdf-profile (optional)
- xccdf-rule
- count

ASR: Inventory Record Set Type Definition

- cpe-name
- inventory-finding (EXISTS, NOT_EXISTS, etc.)
- count

ASR: Vulnerability Record Set Type Definition

- cve-id
- boolean-finding (TRUE, FALSE, etc.)
- count

ASR: Compliance Record Set Type Definition

- cce-id
- compliance-finding (PASS, FAIL, etc.)
- count