Resource-Oriented Lightweight Information Exchange (ROLIE)

draft-ietf-mile-rolie-03

IETF 96 - MILE Working Group

Dave Waltermire, Stephen Banghart, John Field

Background: ROLIE as a Solution

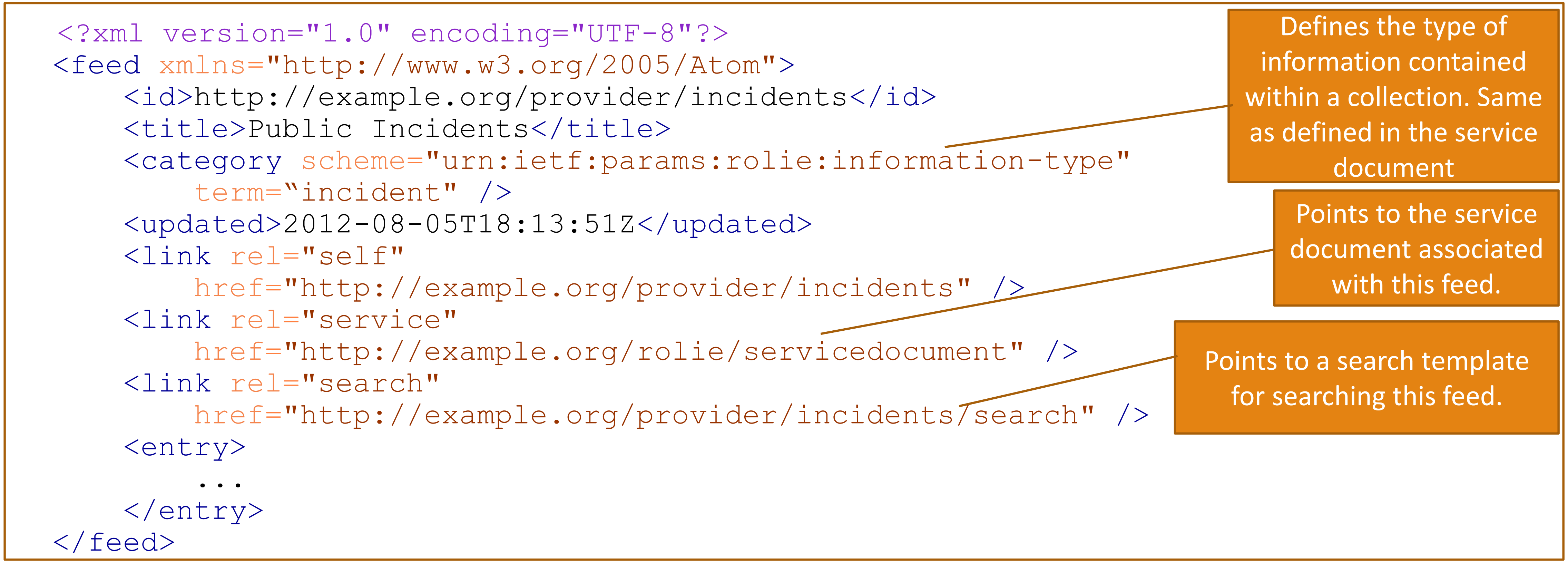
- The Resource-Oriented Lightweight Resource Exchange (ROLIE)
- A profile of the Atom Publication Protocol (RFC 5023) and the Atom Syndication Format (RFC 4287).
- Allows collections of security information resources to be discovered without prior knowledge of the information.
- Provides a mechanism to characterize different types of security information resources
- Creates system for producers to push content with granular access controls
- Originally meant for IODEF exchange, repurposed as a general security information exchange

Anatomy of a ROLIE Service Document

```
<?xml version="1.0" encoding="UTF-8"?>
<service xmlns="http://www.w3.org/2007/app"
    xmlns:atom="http://www.w3.org/2005/Atom">
  <workspace>
    <atom:title>Public Security Information Sharing</atom:title>
    <collection
        href="http://example.org/provider/vulns">
      <atom:title>Public Incident Information</atom:title>
      <categories fixed="yes">
        <atom:category
            scheme="urn:ietf:params:rolie:information-type"
            term=“incident"/>
      </categories>
    </collection>
  </workspace>
</service>
```

Defines the type of information contained within a collection

Anatomy of a ROLIE Feed



```
<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom">
    <id>http://example.org/provider/incidents</id>
    <title>Public Incidents</title>
    <category scheme="urn:ietf:params:rolie:information-type"
        term=“incident" />
    <updated>2012-08-05T18:13:51Z</updated>
    <link rel="self"
        href="http://example.org/provider/incidents" />
    <link rel="service"
        href="http://example.org/rolie/servicedocument" />
    <link rel="search"
        href="http://example.org/provider/incidents/search" />
    <entry>
        ...
    </entry>
</feed>
```

Defines the type of information contained within a collection. Same as defined in the service document

Points to the service document associated with this feed.

Points to a search template for searching this feed.

Anatomy of a Paged ROLIE Feed

```
<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom">
    ...
    <link rel="self" href="http://example.org/provider/incidents?pg=5"/>
    <link rel="first" href="http://example.org/provider/incidents?pg=1"/>
    <link rel="prev" href="http://example.org/provider/incidents?pg=4"/>
    <link rel="next" href="http://example.org/provider/incidents?pg=6"/>
    <link rel="last" href="http://example.org/provider/incidents?pg=10"/>
    ...
</feed>
```

Provides link relations for navigation through paged feed entries.

Anatomy of a ROLIE Entry

```
<?xml version="1.0" encoding="UTF-8"?>
<entry xmlns="http://www.w3.org/2005/Atom"
    xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0">
  <id>http://www.example.org/provider/incident/123456</id>
  <title>Sample Incident Report</title>
  <updated>2012-08-05T18:13:51Z</updated>
  <rolie:format ns="urn:ietf:params:xml:ns:iodef-2.0"/>
  <content type="application/xml"
      src="http://www.example.org/provider/incident/123456/data"/>
</entry>
```

Provides information about the data model of the content.

Content is linked to, not embedded.

The ROLIE extension system

- Use of an IANA table to provide information type extensibility
- Use of the atom:category element with the scheme “urn:ietf:params:rolie:information-type”
- Example Information Types:
  - incident
  - indicator
  - configuration-checklist
  - vulnerability
- Defined through a series of use case oriented drafts

Issue #26: Forward Slash Resource URLs

- Forward Slash Resource URL (Section 5.6)
- Provides compatibility with existing RID deployments by providing requirements around the “/” resource.
- RID compatibility part of the CSIRT Use Case, but probably not required for core ROLIE functionality

Proposal:

A. Keep in ROLIE Core
   - ➢ Not useful for non-incident/IODEF use cases; requires additional implementation

B. Move to the CSIRT Use Case Document
   - ➢ Limits requirement to implementations supporting incident/IODEF use cases

Section 5.3: / (forward slash) Resource URL

The "/" resource MAY be provided for compatibility with existing deployments that are using Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS [RFC6546]. Consistent with RFC6546 errata, a client requesting a GET on "/" MUST receive an HTTP status code 405 Method Not Allowed. An implementation MAY provide full support for RFC6546 such that a POST to "/" containing a recognized RID message type just works. Alternatively, a client requesting a POST to "/" MAY receive an HTTP status code 307 Temporary Redirect. In this case, the location header in the HTTP response will provide the URL of the appropriate RID endpoint, and the client may repeat the POST method at the indicated location. This resource could also leverage the new draft by reschke that proposes HTTP status code 308 (cf: draft-reschke-http-status-308-07.txt).

Issue #29: Standalone Entries

- Atom entries can be a standalone document, with no surrounding feed.
- If a client navigates to an entry, how do they identify the feed the entry belongs to to find additional entries?

Proposal:

- Provide a pointer to the containing feed through a link with relation “collection” as per RFC 6573
- Add to Link Relations Section (Section 6.3)

Issue #3: rolie:format (rolie:data-model)

Provides an indicator of the format used to express the content pointed to by the atom:content element in a ROLIE-based atom:entry.

Proposal: Create a new extension element with the following attributes:

- ns: Provides a globally unique identifier for the namespace of the data model
- version (Optional) : The version of the data model
- schema (Optional) : An IRI to the relevant schema resource
- schema-type (Optional): The type of the schema (e.g. XML Schema, RelaxNG, JSON-LD)

QUESTIONS:

- Will all content models have an associated namespace?
- Should we create an IANA registry linking allowed namespaces to information types?
- Some data model versions are encoded in the namespace. What if the version is not?
- If the data model is constrained by a schema, is there value in referencing the schema used?
- Most schema formats do not have an associated media type. What vocabulary should we use?

Issue #4: Schema for “rolie” namespace

- Need to define a schema describing use of “rolie:format” element once we settle on the structure of the element
- Placeholder for the schema in section 9
- Atom uses the Relax NG Compact Schema format. [1]
- QUESTION: Use Relax NG compact schema for consistency or use XML schema?

[1] http://relaxng.org/compact-20021121.html

Issue #30: Data Model Enumeration

- The ROLIE extension system allows documents to create additional information-type entries in the IANA table.
- Each information-type could have an explicit enumeration of data-models that can describe that information type.
- Can provide guidance on data model selection but may discourage flexibility
- QUESTION: Should the information-types have explicitly listed data-models that express that type?

Uncompleted work on ROLIE Core

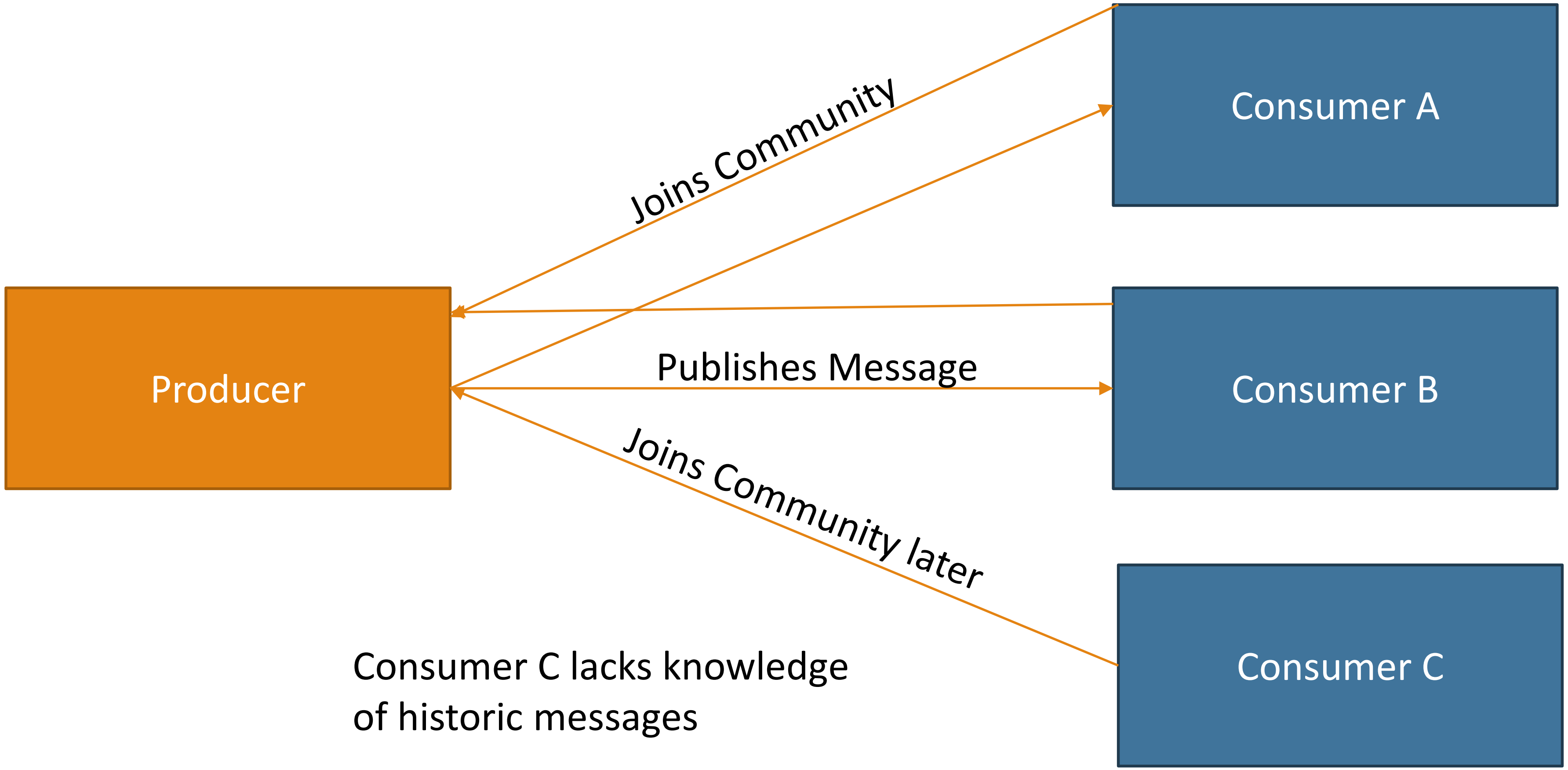
- Security Considerations [Issue #22]
- IANA Considerations
  - Sub registry for urn:ietf:params:rolie for the information-type category scheme
- Appendix Use Case cleanup [Issue #20]
- Complete full rolie:format proposal/specification
- Flesh out TLS requirements (Section 5.3) [Issue #27]
- User Authentication/Authorization Requirements (Section 5.4/5.5) [Issue #9]
  - XACML
  - http-auth
  - Oauth
- Better specification for use of open search [Issue #28]

Looking Forward

- ROLIE draft at revision 3, more feedback is needed
- The CSIRT Use Case document is being worked on
  - Contains much of the original text from ROLIE addressing CSIRT use cases
  - Currently being recast to align with the new ROLIE core
  - Will need WG adoption once complete
- Other extension documents for information types need to be considered
  - Software management information (e.g., SWID tags)
  - Configuration checklist information (e.g., SCAP)
  - Vulnerability records and bulletins

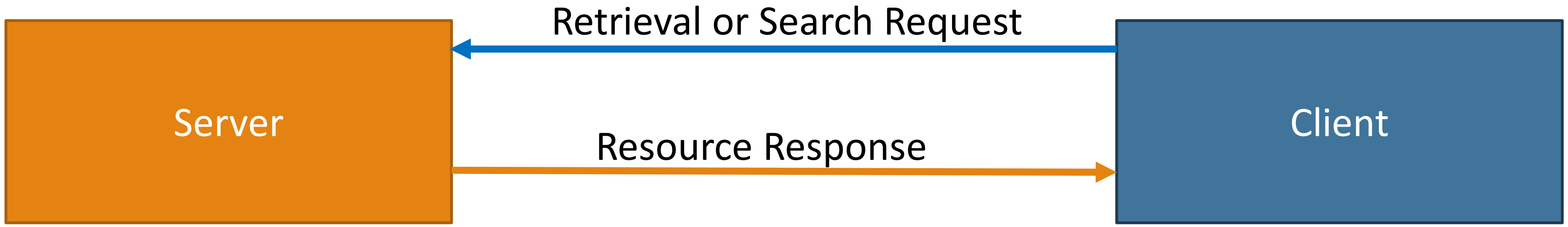
Backup Slides

Message-Oriented Publish/Subscribe Model



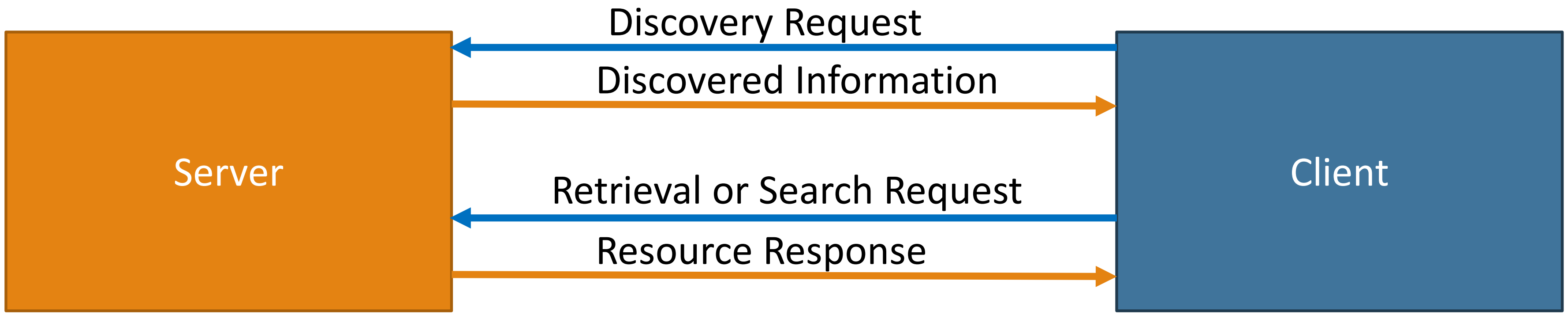
Consumer C lacks knowledge of historic messages

Message-Oriented Request/Response Model



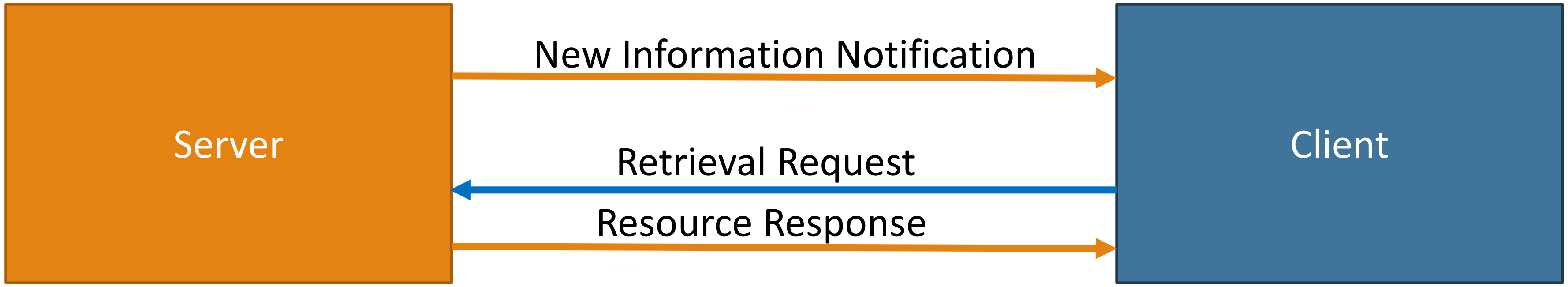
What if the resource or search term is unknown?

Resource-Oriented Discovery Model



Available resources can be
discovered, and interesting resources
can be searched and retrieved.

Resource-Oriented Publication/Subscription



Publication/Subscription model can be used with the Resource-Oriented approach to provide notifications of new information.