

Resource-Oriented Lightweight Information Exchange (ROLIE)

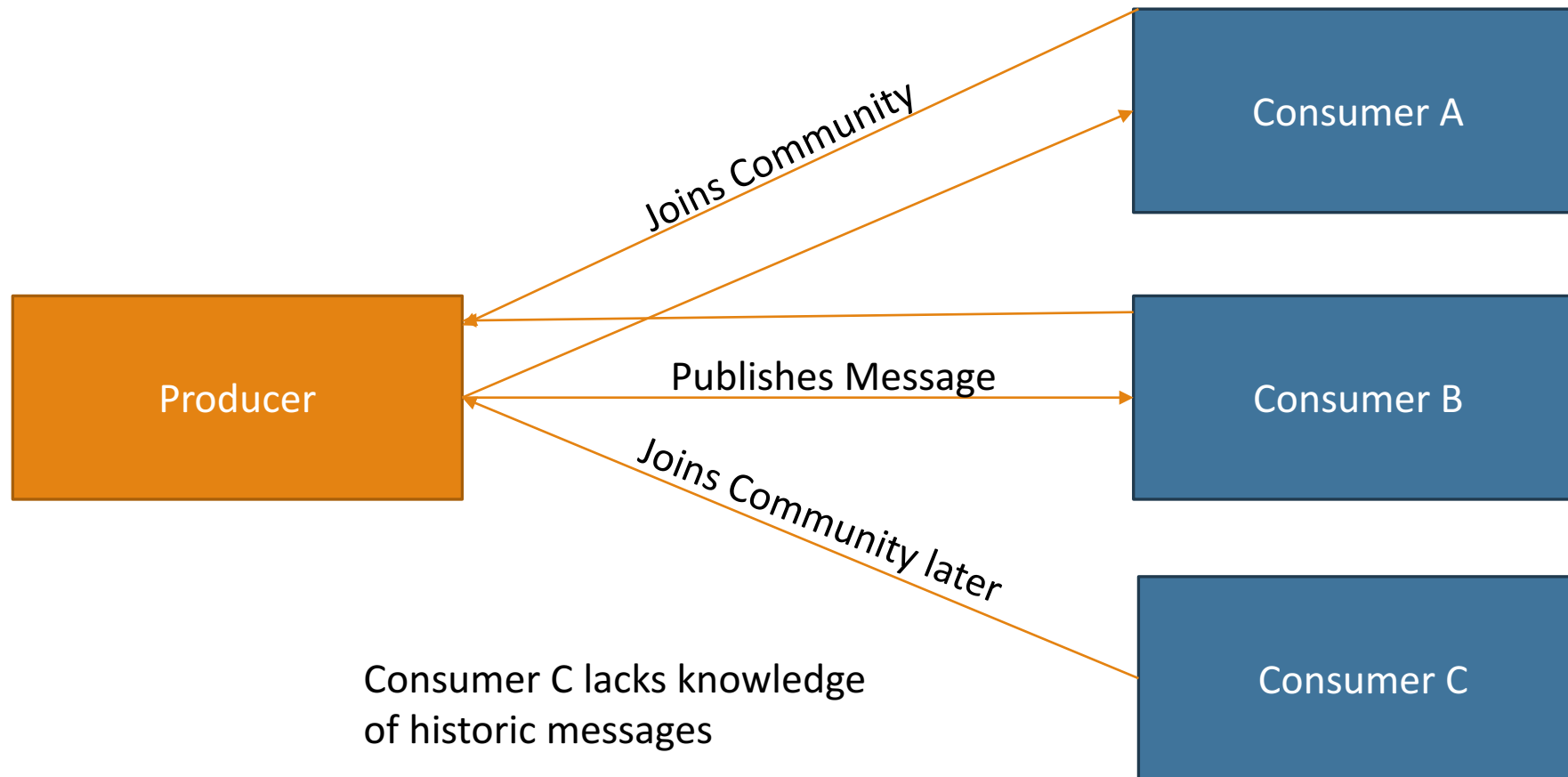
draft-ietf-mile-rolie-08

IETF 99 - SACM Working Group
Dave Waltermire, Stephen Banghart

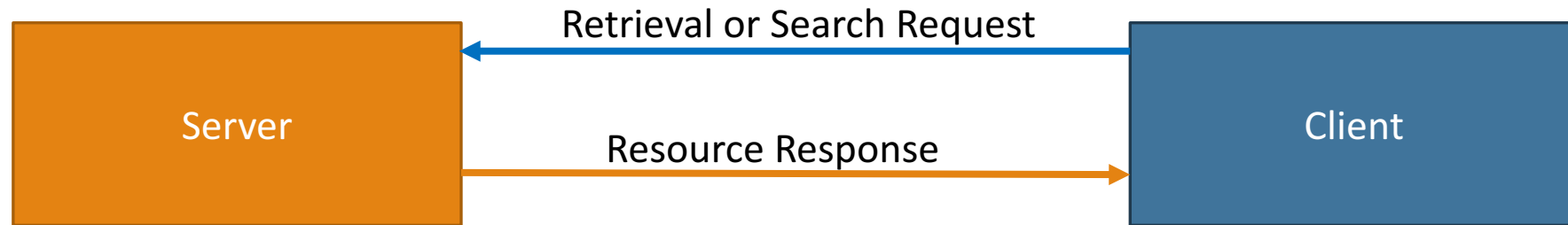
The Problem

- Organizations require many kinds of security information from many sources in many formats in many serializations– open world problem!
- Information distribution requires prior coordination and agreement on these factors
- Once information is negotiated and shared, there is no good way to negotiate historical information.

Message-Oriented Publish/Subscribe Model



Message-Oriented Request/Response Model



What if the resource or search term is unknown?

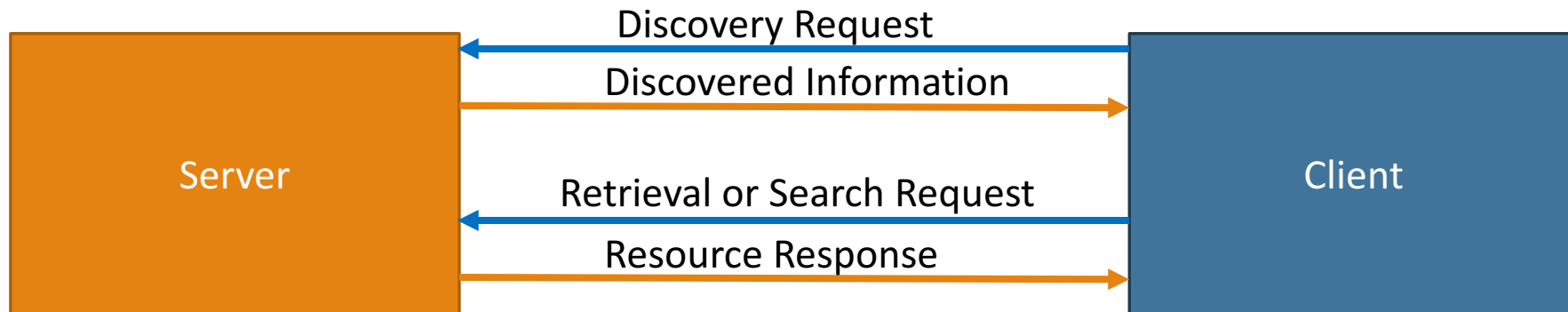
The Goals of ROLIE

- Provide metadata to allow clients to discover and search information resources
- Minimize the retrieval of unneeded information and reduce round trips
- Provide granular control of access to resources in order to support public and private information exchange
- Enable automatic machine communication and information processing

ROLIE as a Solution

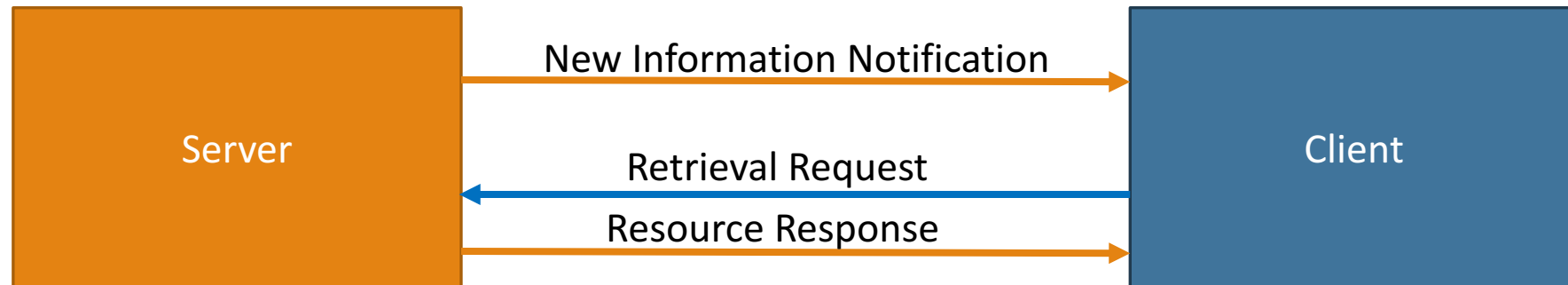
- The Resource-Oriented Lightweight Resource Exchange (ROLIE) is a profile of the Atom Publication Protocol and the Atom Syndication Format.
- Allows collections of security information resources to be discovered without prior knowledge of the information.
- Provides an extensible mechanism to characterize different types of security information resources

Resource-Oriented Discovery Model



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

Resource-Oriented Publication/Subscription



Publication/Subscription protocol (e.g., XMPP) can be used with the Resource-Oriented approach to provide notifications of new information.

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">
  <app:workspace>
    <atom:title>Public Security Information Sharing</atom:title>
    <app:collection
      href="http://example.org/provider/vulns">
      <atom:title>Public Vulnerabilities</atom:title>
      <app:categories fixed="yes">
        <atom:category
          scheme="urn:ietf:params:rolie:information-type"
          term="vulnerability"/>
      </app:categories>
    </app:collection>
  </app:workspace>
</app:service>
```

Defines the type of information
contained within a collection

Anatomy of a ROLIE Feed

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

Anatomy of a Paged ROLIE Feed

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

Provides link relations for navigation through paged feed entries.

Anatomy of a ROLIE Entry

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

Provides information about the data model of the content.

Content is linked to, not embedded.

The ROLIE extension system

- The Atom Category element provides a flexible extension point for characterizing information and for declaring information types.
- List of officially supported information types registered in IANA table by extensions.
- Example: “ROLIE CSIRT Extension” document creates IANA table entries for:
 - Information Types: Incidents, Indicators

ROLIE Software Descriptor Extension

- Establishes the “software descriptor” information type
 - Identifies and characterizes software, software installers/packages, and software patches.
 - Software descriptors do not characterize installation records, running software, or configuration state
- Lists ISO 2015 SWID Tags as a data format that expresses this information type

Looking Forward

- ROLIE draft -08 version recently posted in MILE. WGGLC finished, sheparding process starting.
- ROLIE Software descriptor extension WG adoption
 - Draft version -02 with minor edits soon, mostly changes to reflect changes in -07 and -08 of core draft
- ROLIE Checklist extension review and updates

Discussion
