ROLIE:
Resource-Oriented Lightweight Indicator Exchange

John P. Field
Security Architect
Pivotal

Agenda

- Motivation for ROLIE
- Use Case Examples
- Review of questions raised since draft -02
- Additional Discussion

What is ROLIE?

- A Resource-Oriented, Lightweight approach to enabling cyber security information sharing.
  - REST is the architecture of the World Wide Web.
    - Cf. Chapter 5, “Architectural Styles and the Design of Network-based Software Architectures”
    - Roy Fielding, Univ. Cal. Irvine, 2000.

Motivation for ROLIE

- The cyber security challenge is an asymmetric conflict; the attackers exhibit:
  - Loosely coupled collaboration patterns
  - High degree of technical agility
  - Continuous evolution / adaptability of tactics & methods
- Message-based architectures function optimally when deployed and operated symmetrically.
- The REST architectural style is naturally asymmetric and has proven to be agile, economical, and scalable.
  - Loose coupling through *uniform interface* and *content-type* negotiation enables continuous incremental improvement.

ROLIE Use Case: Feed

Example request for an Incident Feed:

```
GET /csirt/private/incidents HTTP/1.1
Host: www.example.org
Accept: application/atom+xml
```

ROLIE Use Case: Feed

```
HTTP/1.1 200 OK
Date: Fri, 24 Aug 2012 17:20:11 GMT
Content-Length: 2882
Content-Type: application/atom+xml;type=feed;charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.w3.org/2005/Atom file:/C:/schemas/atom.xsd
                        urn:ietf:params:xml:ns:iodef-1.0 file:/C:/schemas/iodef-1.0.xsd" xml:lang="en-US">

    <generator version="1.0" xml:lang="en-US">emc-csirt-iodef-feed-service</generator>
    <id xml:lang="en-US">http://www.example.org/csirt/private/incidents</id>
    <title type="text" xml:lang="en-US">Atom formatted representation of a feed of IODEF documents</title>
    <updated xml:lang="en-US">2012-05-04T18:13:51.0Z</updated>
    <author>
        <email>csirt@example.org</email>
        <name>EMC CSIRT</name>
    </author>

    <!-- By convention there is usually a self link for the feed -->
    <link href="http://www.example.org/csirt/private/incidents" rel="self"/>

    <entry>
        <id>http://www.example.org/csirt/private/incidents/123456</id>
        <title>Sample Incident</title>
        <link href="http://www.example.org/csirt/private/incidents/123456" rel="self"/>       <!-- by convention
        <link href="http://www.example.org/csirt/private/incidents/123456" rel="alternate"/>  <!-- required by At
        <published>2012-08-04T18:13:51.0Z</published>
        <updated>2012-08-05T18:13:51.0Z</updated>
        <!-- The category is based upon IODEF purpose and restriction attributes -->
        <category term="traceback" scheme="purpose" label="trace back" />
        <category term="need-to-know" scheme="restriction" label="need to know" />
        <summary>A short description of this incident, extracted from the IODEF Incident class, <description> ele
    </entry>

    <entry>
        <!-- ...another entry... -->
    </entry>

</feed>
```

ROLIE Use Case: Entry

Example request for an Entry:

```
GET /csirt/private/incidents/123456
Host: www.example.org
Accept: application/atom+xml
```

ROLIE Use Case: Entry

```
HTTP/1.1 200 OK
Date: Fri, 24 Aug 2012 17:30:11 GMT
Content-Length: 4965
Content-Type: application/atom+xml;type=entry;charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<entry>
  <id>http://www.example.org/csirt/private/incidents/123456</id>
  <title>Sample Incident</title>
  <link href="http://www.example.org/csirt/private/incidents/123456" rel="self"/>       <!-- by convention -->
  <link href="http://www.example.org/csirt/private/incidents/123456" rel="alternate"/>  <!-- required by Atom
  <published>2012-08-04T18:13:51.0Z</published>
  <updated>2012-08-05T18:13:51.0Z</updated>
  <!-- The category is based upon IODEF purpose and restriction attributes -->
  <category term="traceback" scheme="purpose" label="trace back" />
  <category term="need-to-know" scheme="restriction" label="need to know" />
  <summary>A short description of this incident, extracted from the IODEF Incident class, <description> elemen

  <!-- Refer to section 5.9 for the list of supported (cyber information-specific) link relationships -->
  <!-- Typical operations that can be performed on this IODEF message include edit -->
  <link href="http://www.example.org/csirt/private/incidents/123456" rel="edit"/>

  <!-- the next and previous are just sequential access, may not map to anything related to this IODEF Inciden
  <link href="http://www.example.org/csirt/private/incidents/123457" rel="next"/>
  <link href="http://www.example.org/csirt/private/incidents/123455" rel="previous"/>

  <!-- navigate up to the full collection.  Might also be rel="collection" as per IANA registry -->
  <link href="http://www.example.org/csirt/private/incidents" rel="up"/>

  <content type="application/xml">
    <iodef:IODEF-Document lang="en" xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef:Incident purpose="traceback" restriction="need-to-know">

        ...

      </iodef:Incident>
    </iodef:IODEF-Document>
  </content>
</entry>
```

ROLIE Use Case: Repository

Example request to a Repository:

```
GET /csirt/repository/ddos
Host: www.example.org
Accept: application/atom+xml
```

ROLIE Use Case: Repository

```
HTTP/1.1 200 OK
Date: Fri, 24 Aug 2012 17:20:11 GMT
Content-Length: nnnn
Content-Type: application/atom+xml;type=feed;charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.w3.org/2005/Atom file:/C:/schemas/atom.xsd
                        urn:ietf:params:xml:ns:iodef-1.0 file:/C:/schemas/iodef-1.0.xsd"
    xml:lang="en-US">

    <generator version="1.0" xml:lang="en-US">emc-csirt-iodef-feed-service</generator>
    <id xml:lang="en-US">http://www.example.org/csirt/repository/ddos</id>
    <title type="text" xml:lang="en-US">Atom formatted representation of a feed of known ddos resources.</title>
    <updated xml:lang="en-US">2012-05-04T18:13:51.0Z</updated>
    <author>
        <email>csirt@example.org</email>
        <name>EMC CSIRT</name>
    </author>

    <!-- By convention there is usually a self link for the feed -->
    <link href="http://www.example.org/csirt/repository/ddos" rel="self"/>

    <entry>
        <id>http://www.example.org/csirt/repository/ddos/123456</id>
        <title>Sample DDOS Incident</title>
        <link href="http://www.example.org/csirt/repository/ddos/123456" rel="self"/>          <!-- by convention -->
        <link href="http://www.example.org/csirt/repository/ddos/123456" rel="alternate"/>     <!-- required by Atom
        <link href="http://www.example.org/csirt/repository/ddos/987654" rel="related"/>       <!-- link to a related
        <link href="http://www.cyber-agency.gov/repository/indicators/1a2b3c" rel="related"/> <!-- link to a related
        <published>2012-08-04T18:13:51.0Z</published>
        <updated>2012-08-05T18:13:51.0Z</updated>
        <!-- The category is based upon IODEF purpose and restriction attributes -->
        <category term="traceback" scheme="purpose" label="trace back" />
        <category term="need-to-know" scheme="restriction" label="need to know" />
        <category term="ddos" scheme="ttp" label="tactics, techniques, and procedures"/>
        <summary>A short description of this DDOS attack, extracted from the IODEF Incident class, <description> elem
    </entry>

    <entry>
        <!-- ...another entry... -->
    </entry>

</feed>
```

Issues raised since draft -02

1. IANA link registrations, versus fully qualified private link types are sufficient.
   - Suggestion: Use IANA registrations, since the list of terms could be expanded further in the future.
   - Response: Agree, this is the best way to ensure interoperability. Individual sharing consortia can always choose to use fully qualified links in their community, in addition to the globally standardized ones.
2. Should we require atom categories that correspond to IODEF expectation class and/or IODEF impact class?
   - Suggestion: That would be helpful, if you could prepare that. Perhaps as an appendix.
   - Response: OK, the reason I raised the question is that I was not sure as to how CSIRTs might be using expectation and impact. The category could enable easier retrieval if that access pattern is common.
3. Should we include specific requirements for Archive and Paging?
   - Suggestion: Well, we MAY do so, I think. Server may provide paged feeds as defined by RFC 5005.
   - Response: Makes perfect sense to reference 5005.

Issues raised since draft -02

4. Requirements input on use cases involving RID schema in the Atom member entry content model for link rel=report.
   - Suggestion: Not essential. Having said that, if somebody could provide such inputs, that would be helpful.
   - Response: Motivation was to ensure that we optimize the usage/data access patterns. Goal is to enable requestors to minimize round trips.
5. Should we include a MILE media type parameter?
   - Suggestion: “no”. If we wish to negotiate the content, we have many other ways to do so, so I do not see the needs to include a MIME media type for this purpose.
   - Response: Agreed. Media type should remain generic, application/atom+xml. More specialized media type might have some benefits, but would also limit interoperability with clients that do not recognize the specialized type. The overall goal of the draft is to enable the broadest possible interactions.

Issues raised since draft -02

6. An atom:category for IODEF expectation, and/or impact?
   - Clarification: Is this required.
   - Response: Not required. Motivation was again to ensure that we optimize for common usage/data access patterns. Goal is to enable requestors to minimize round trips.

Conclusion

- Additional Questions or Comments?

Thank You

jfield@pivotal.com