ROLIE: Resource-Oriented Lightweight Indicator Exchange

John P. Field
Senior Technologist, Security Architect
EMC
Agenda

• Motivation for ROLIE
• Use Case Examples
• Review of changes since draft -00
• 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.
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 17:30:11 GMT
Content-Length: 2882
Content-Type: application/atom+xml;type=feed; charset=utf-8

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:emc-atom="http://example.org/csirt/private/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/remote/incidents</id>
<title xml:lang="en-US">Atom formatted representation of a feed of IODEF documents</title>
<updated xml:lang="en-US">2012-08-04T18:13:51.0Z</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/remote/incidents" rel="self"/>

<entry>
  <id>http://www.example.org/csirt/private/remote/incidents/123456</id>
  <title>Sample Incident</title>
  <link href="http://www.example.org/csirt/private/remote/incidents/123456" rel="alternate" />
  <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="traceback" />
  <category term="need-to-know" scheme="restriction" label="need to know" />
  <summary>A short description of this incident, extracted from the IODEF Incident class, </summary>
  <description>

</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

<!-- by convention -->
<link href="http://www.example.org/csirt/private/incidents/123456" rel="self"/>
<link href="http://www.example.org/csirt/private/incidents/123456" rel="alternate"/>  <!-- required by Atom
<published>2012-08-04T18:13:51.02</published>
<updated>2012-08-05T18:13:51.02</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"/>

A short description of this incident, extracted from the IODEF Incident class, <description> element

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/atom+xml"

<iodef:iodef-document lang="en" xmlns:iodef="urn:iietf: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
Change Summary since draft -00

• The latest draft includes feedback received since the draft -00
  – Incorporated feedback from IETF 85 in Atlanta.
  – Some discussion, suggestions and questions occurred on list, plus some off-list conversations.
• The changes focused on improving clarity of goal, and scope.
• AFAICT, no fundamental disagreements on the basic approach being proposed.
Specific changes since draft -00 (1 / 3)

• Fixed a small number of typographical errors and a few misspellings throughout.
• Added a number of missing internal cross references to improve readability.
• Updated the text in the Introduction section for improved brevity and clarity of goal.
• Added new non-normative text describing the use of HTTP 4xx status codes for authorization.
Specific changes since draft -00 (2 / 3)

• Added a new non-normative example illustrating a persistent repository use case.
• Added new normative text recommending use of SAML2 for authentication of interactive end users who are members of a sharing consortium.
• Added new normative text describing requirements for user authorization.
Specific changes since draft -00 (3 / 3)

• Added non-normative appendix describing a suggested approach to a XACML profile.
Generalizing beyond MILE?

• The current draft is specifically focused only on MILE use cases.
  – e.g., incidents and indicators, etc.

• It has been suggested that the approach described may apply to use cases being considered in SACM, and elsewhere.

• Generalization to other WG use cases would require engagement from those team(s).
Conclusion

• Questions or Comments?
Thank You

johnp.field@emc.com