ROLIE: Resource Oriented Lightweight Indicator Exchange

John P. Field
Senior Technologist, Security Architect
Pivotal Services @ EMC

Agenda

- What is ROLIE?
- What motivated the draft?
- Discussion

What is ROLIE?

- RESTful, resource-oriented approach to cyber security information sharing.
  - An Atom feed binding for cyber security information, rather than p2p message-based.
- Enables
  - Loose coupling, ease of adoption
  - Dynamic discovery,
  - Leveraging of existing Identity Management infrastructure.

High Level Goals for ROLIE

- Make it easier to do simple sharing.
  - Anyone with a feed reader can participate.
- Avoid operational coordination between sharing parties.
- Leverage existing investments in Identity Management.
- Avoid requirements for distributed policy enforcement.
- Loose coupling, scalability

Goal: Ease of Sharing

- Non-trivial investment is needed to participate, regardless of the specific role to be played.
- Avoid the need for a symmetry in deployment architecture.
- For many use cases and participant roles, an identity-based authorization of a RESTful feed is sufficient, and appropriate.

Use Case Examples

- RID Query
  - a SOAP RPC-style invocation
  - Compute burden falls on server, rather than on client.
  - With REST style, client does the “Big Data” crunching
- RID Report
  - a SOAP Doc-centric style invocation
  - Ensuring distributed transactional integrity requires complex logic, state on server.
  - With REST style, server does not maintain application state

Business Use Cases for ROLIE

- Government agency sharing indicator repository broadly with citizens and the private sector.
- Private sector organizations publishing cyber intelligence feed to subscribing customers.
- Private sector organizations accepting incident reports from their partners and customers.

Relationship to existing RFCs

- ROLIE is complementary to the existing RFCs.
  - Use IODEF or IODEF+RID as the resource representation.
    - Media Type: Application/Atom+XML; IODEF+RID
  - Other representations also possible.
  - Use of HTTP return codes to drive client requests between existing "/" resource, and any other URLs.
    - e.g. 300 Multiple Choices, 301 Moved Permanently, 302 Found, 303 See Other, 307 Temporary Redirect, 308 Permanent Redirect (draft-reschke-http-status-308)

Summary

- 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.

Discussion

- Questions or comments?

Thank You

jfield@pivotal.io