ROLIE: Resource Oriented Lightweight Indicator Exchange

John P. Field

Senior Technologist, Security Architect

EMC

Agenda

- What is ROLIE?
- What motivated the draft?
- How does ROLIE relate to IODEF, RID, & RID/T?
- Next Steps
- Discussion

What is ROLIE?

- A resource-oriented approach to cyber security information sharing.
  - Cf. http://datatracker.ietf.org/doc/draft-field-mile-rolie/
- Approaches the problem from the perspective of a RESTful ROA, rather than a message-based SOA.
  - 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.

What is REST?

- REST is not a protocol, it is an architectural style.
  - REpresentational State Transfer
- Design of distributed systems from the point of view of <u>resources</u> and their <u>representations</u>.
  - Identification and addressability of resources.
  - Uniform interface
  - Media types
  - Hypertext
    - …As the Embodiment of Application State (HATEOAS)

High Level Goals for ROLIE

- Make it easier to do simple sharing starting right now.
  - Anyone with a browser or feed reader can participate.
- Enable us to achieve more complex sharing over time.
  - Loose coupling ensures that additional capabilities can be added organically, and incrementally.
  - Avoids operational coordination between sharing parties.
- Leverage existing investments in Identity Management.
  - Avoid a requirement for distributed policy enforcement.
- Ensure participants are free to innovate independently.
  - And measure and manage their individual ROIs.

Use Cases for ROLIE

- Government agency sharing an 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.
- CSIRT consortiums collaborating on operational incident response in a sharing portal.
- Private sector organizations submitting cyber security compliance reports to a government agency.

Selected Technical Drivers for ROLIE

- Ease of Adoption
  - For both client, and server.
- Improved Scalability and Reduced Complexity.
  - E.g. Search and Update Use Cases
- Identity-based authorization enforcement at the source.
  - Interoperable policy definitions via XACML profile

Ease of Adoption

- The SOA approach to sharing inherently assumes symmetric deployment architecture.
  - All participants must deploy and maintain a functionally equivalent infrastructure.
    - Both messaging and policy management.
  - Non-trivial investment is needed to participate, regardless of the specific role to be played.
    - >200 pages of specifications, not including the normative references, or the sharing agreements.
  - How to calculate ROI?

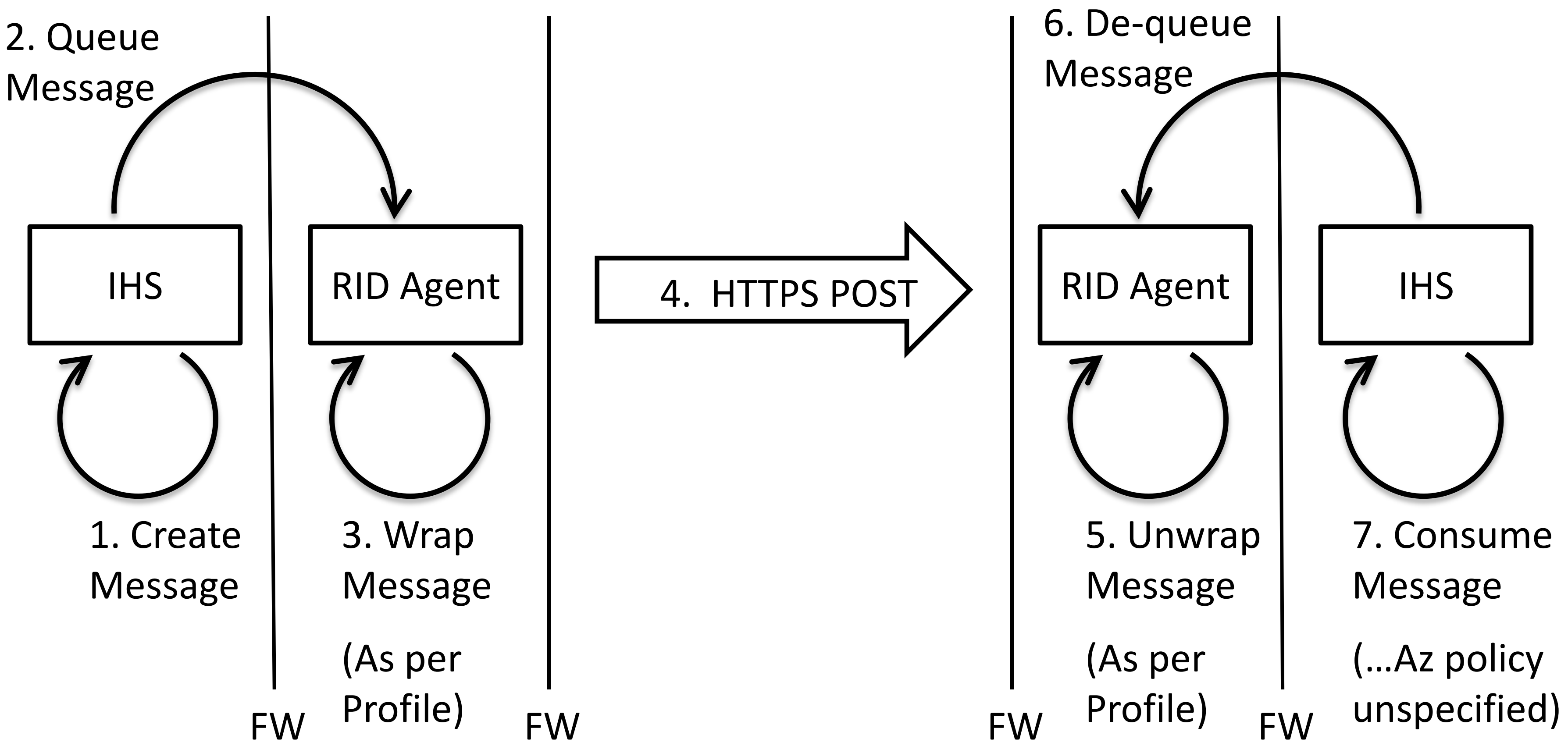
Improved Scalability and Complexity

- The existing protocols are patterned on SOAP Web Services, albeit without a SOAP header.
  - Conversational state management in a distributed system is known to have scalability limitations and inherent complexity.
- Use Case Examples
  - RID Query – a SOAP RPC-style invocation
    - compute burden falls on server, rather than on client.
      - Potential challenges with provider resource management .
  - RID Report – a SOAP Doc-centric style invocation
    - Update semantics underspecified.
      - Ensuring transactional integrity requires complex logic.

Sharing Agreements & Security Profiles

- CSIRT needs assurance that sensitive information will be used appropriately, e.g. “acceptable use”.
- Existing standards appropriately defer policy details to the **Sharing Agreements**.
- Sharing Agreements must define **Security Profiles** and their associated controls.
  - Implemented using XML security.
- Responsibility for enforcement is shared – and distributed – between the source and destination RID agent, and IHS.
  - MAC with labels, versus DAC.

Distributed Message –based Security



2. Queue Message

6. De-queue Message

IHS

RID Agent

4. HTTPS POST

RID Agent

IHS

1. Create Message

3. Wrap Message

(As per Profile)

5. Unwrap Message

(As per Profile)

7. Consume Message

(…Az policy unspecified)

Need to coordinate the encryption and decryption with the logical authorization policy enforcement.

Security Profile Management

- Implementers must build management tools to administer the Security Profiles.
  - e.g. Administration of:
    - Consortiums, Security Profiles, Counter-parties, XPath expressions, Algorithms / Modes, Key Management, for self and peers.
- All necessary and appropriate, but not easy to build, test, and operate.
- Orthogonal to existing Identity Management infrastructure.
- For some use cases, and some participant roles, identity-based authorization may provide a viable alternative.

Interoperable Profiles

- In practice, end-to-end security requires a machine-readable Security Profile, with a set of message-level crypto protections.
  - No interoperable standard exists for this.
- In addition, RID agent (cryptographic) enforcements MUST be correlated with the logical access controls provided in the IHS.
  - No interoperable standard exists for this.
- An alternative is to just use TLS for the channel security and a XACML profile for endpoint enforcement.

ROLIE Authorization

- ROLIE specifies authorization enforcement only at the source system.
  - No responsibility for additional enforcement at destination.
  - Leverage existing investments in identity management for authorization enforcement.
- XACML profile for interoperable policy management.
  - Can ensure consistency of enforcement in IHS.
- Improved audit trail
  - individual accountability end-to-end.
- XML object security still supported, if and as needed.
  - Negotiate Media Type: Accept and Content Type headers

XACML Profile

- XACML ABAC is based on predicate logic expressions constructed from the attributes of four variables:
  - Subject, Resource, Action, & Environment.
- Example:
  - Subject Attributes, e.g. from SAML Assertion
  - Resource: URI and/or XPath into XML content
  - Action: HTTP verb
  - Environment: Other, such as Geo, Alert-level, etc.
- Can be used to achieve interoperable policy expressions on a per-user, or per-role basis.

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)

Next Steps

- Deploy our current POC implementation to allow potential adopters to further explore the merits of the approach.
- Revise the -00 internet draft based on the feedback received to date.
- Begin work on an -00 internet draft for a ROLIE XACML profile.

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

johnp.field@emc.com