RID Draft Update
Migrating to IODEF

Kathleen M. Moriarty

IETF INCH Working Group

04 March 2004

This work was sponsored by the Air Force under Air Force Contract Number F19628-00-C-0002.

RID Updates

- Purpose
- RID and INCH
- Messaging Format Changes
  - Packet based to XML
- Define Extensions to IODEF Model
- Communication Mechanism for RID Documents
- Security Considerations
  - Consortiums
  - Privacy

Real-time Inter-network Defense (RID)

- Trace Security Incidents to the Source
- Stop or Mitigate the Effects of an Attack or Security Incident
- Facilitate Communications between Network Providers
- Integrate with existing and future network components
  - Systems to trace traffic across a network
    - NetFlow, Hash Based IP Traceback, IP Marking, etc.
    - Intrusion Detection Systems
    - Network devices such as routers and firewalls
- Provide secure means to communicate RID messages
  - Consortiums agree upon use and abuse guidelines
  - Consortiums provide a key exchange method
    - Trusted PKI, certificate repository, cross certifications

RID and INCH

- RID is used to communicate security incident handling information between CSIRTs or NPs
- RID carries much of the same data as an IODEF document
- RID requires a few additional data elements
- Communication and proper transport of messages is in the RID specification
- RID is now reformatted to use the IODEF specification
  - Packet based format to IODEF document
- RID message types
  - Noted in a SOAP wrapper to an XML IODEF document

RID Extensions to IODEF

- AdditionalData Class from IODEF used to define Extensions
  - IPPacket Class
    - Allows hex packets to be stored in the RID message in a format that will be expected by the recipient of a RID message
    - Multiple packets may be sent in a single message
  - NPPath Class
    - Purpose is to identify the path of the trace and to avoid loops
  - TraceStatus Class
    - Method for providing approval status from upstream peer after a trace request is made

Communicating RID Messages

- SOAP Messaging Wrapper and XML Security
  - Method to transport messages
  - Provide integrity, authentication, authorization
  - XML digital signature, encryption, and public key infrastructure
- Public Key Infrastructure
  - Provided by consortiums linking network providers for RID messaging
- Message Types
  - Trace Request
  - Trace Authorization
  - Source Found
  - Relay Request
- RID Systems Must Track the Requests by
  - Incident Number
  - Packet Contents
  - Completion Status

Security Considerations

- Consortiums
  - Agreements between entities involved in RID peering
  - Provide a secure key exchange repository/system (PKI)
  - Peering agreements and policies between consortiums and across national boundaries or jurisdictions
- System use guidelines
  - Privacy considerations
  - Abuse policies
  - Use policies may vary across national network or consortium boundaries
    - Automated method to allow enforcement of use agreements
- RID server security policies
  - Network based access controls
  - Hardened systems
- Communication security considerations for the exchange of RID messages and the underlying protocols

Summary

- Many updates from the previous version
  - Moved from packet based format to a solution based on IODEF documents
  - Extended the AdditionalData Class to accommodate the needs of RID messaging
  - Security will use XML Digital Signature and XML Encryption
  - PKI at the core of the security model, but provided by a consortium
  - Topology examples to address implementers questions
  - Extended information on system use and privacy considerations
- Near Future Update will include
  - SOAP wrapper and more information on XML Security
  - Further specifications on automating a flag for system use adherence guidelines
  - May include additional examples of other message types
  - Any suggested revisions or clarifications
- http://www.ietf.org/internet-drafts/draft-moriarty-ddos-rid-05.txt