



RID IETF Draft Update

Kathleen M. Moriarty

INCH Working Group

11 November 2004

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

"Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the United States Government."

MIT Lincoln Laboratory



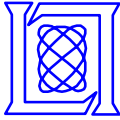
RID Updates

- **Purpose**
- **RID and INCH**
- **Messaging Format for RID**
- **Define Extensions to IODEF Model**
- **New Extension for Policy and Trace Continuance**
- **Communication Mechanism for RID Documents**
- **Security Considerations**



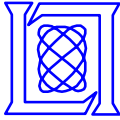
Real-time Inter-network Defense (RID)

- **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**
 - Intrusion Detection Systems
 - NetFlow, Hash Based IP Traceback, IP Marking, etc.
 - 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 Network Providers (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 message types**
 - **XML IODEF document with RID extensions**
 - **SOAP Wrapper**
 - Message Type distinguished in SOAP wrapper**



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**

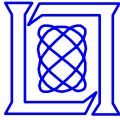
Method for providing approval status from upstream peer after a trace request is made
 - **RIDPolicy**

Method to determine via RID messages if trace should be continued between NPs
Policy negotiations for RID messages
- **Reliability of the trace type requested**
 - Some NPs may have multiple choices for traceback
 - Method needed to decide which of several methods should be used by the percentage from the originator of request
- **Level of trace required**
 - RID systems need to reference the IODEF expectation class to determine how fast of a trace mechanism should be used
 - The start time and end time can be used to determine if a fast method of tracing or a slow and more detailed trace mechanism can be used



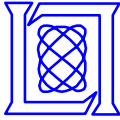
RID Policy

- **RID Policy**
 - Ensures policy information is transferred between participating RID peers
 - Policy information in RID to prevent policy related issues from relying on the transport mechanism for enforcement
 - Message type is specified in the RIDPolicy class
- **RIDPolicy Information**
 - **Extension to define the type of trace**
 - IODEF Method and Impact class information should be considered for the type of traffic requested for trace and the success of an attack
 - Explicit statement for the type of trace requested in case it does not fit into the category of attack traffic and can be linked to a CVE or other identifier
 - **Identifies where the traffic may have policy issues**
 - Client to NP
 - NP to client
 - Within a consortium
 - Between peers
 - Between consortiums
 - Across national boundaries
- **Purpose is to try to prevent abuse of the system**
 - Address security, confidentiality, and privacy concerns listed in the draft
 - New extension created to address issues raised at IETF-59
- **Any comments on RIDPolicy?**



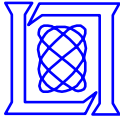
Communicating RID Messages

- **SOAP Messaging Wrapper and XML Security**
 - Method to transport messages
 - Policy negotiated in RID message and not wrapper
 - Provide integrity, authentication, authorization
 - XML digital signature, encryption, and public key infrastructure
 - Encryption of RID for privacy and security reasons should be via XML encryption and not through the security provided by a wrapper or higher level protocol
- **Public Key Infrastructure**
 - Provided by consortiums linking network providers for RID messaging
- **Message Types**
 - Trace Request
 - Trace Authorization
 - Source Found
 - Relay Request
- **Outstanding question on Source Found Message for Not Found Status**
 - Proposed change of Source Found to Result Message from MEW
 - NULL IP in source found indicates NOT found – preferred option
 - Needs to be documented in draft for implementers
- **RID Systems Must Track the Requests by**
 - Incident Number
 - Packet Contents
 - Completion Status



Message Transport

- **Transport via HTTPS, BEEP, or Email?**
- **Mailing list seems to prefer HTTPS**
 - Solution is available and easy to implement
 - Provides the security mechanisms necessary to secure and authenticate the message transport
 - Protocol not designed for this purpose, but can get through firewalls
- **Email**
 - Some positive and negative comments
 - Has necessary security and reliability
 - May not be as fast as a direct communication protocol
- **BEEP**
 - May be more appropriate for RID implementation
 - Provides the security mechanisms necessary to secure and authenticate the message transport
 - Has not been implemented yet, may be a better choice at a later time
- **Stunnel**
- **SOAP Wrapper and transport will be fully defined in a separate document**



Security Considerations

- **Consortiums discussed in previous draft release**
 - Agreements between entities involved in RID peering
 - Provide a secure key exchange repository/system (PKI)
 - Peering agreements and policies between consortiums, across national boundaries, or jurisdictions
 - Policy enforced through RID messages by stating level and type of trace
- **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

- **Updates from the previous version**
 - **Extended the AdditionalData Class to accommodate the needs of RID messaging and RIDPolicy**
 - Extended information on system use and privacy considerations
 - RID message numbers
 - **PKI at the core of the security model, but provided by a consortium**
 - **XML Schema for RID extensions**
 - **Digital signature on example**
- **Near Future Updates will include**
 - **Separate document for SOAP wrapper and transport**
 - **Any suggested revisions or clarifications**
- **<http://www.ietf.org/internet-drafts/draft-ietf-inch-rid-01.txt>**