

---

# **RID IETF Draft Update**

**Kathleen M. Moriarty**

**INCH Working Group**

**29 March 2005**

**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

---

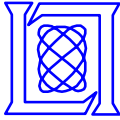
- **Purpose**
- **RID and INCH**
- **Generalizing RID draft**
  - **Communication flow for all IODEF documents**
  - **Transport in a separate document**
- **Message Format for RID**
- **Updates to the RID Extensions to IODEF Model**
- **Communication Mechanism for RID Documents**
- **RIDPolicy Comments**



# Real-time Inter-network Defense (RID)

---

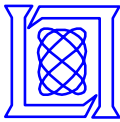
- **Facilitate Communication of IODEF documents between Network Providers (NPs) and CSIRTs**
- **\* Report incidents to NPs or CSIRTs**
- **Trace Security Incidents to the Source**
- **Stop or Mitigate the Effects of an Attack or Security Incident**
  - **Integrate with existing and future network components**
    - Intrusion Detection Systems**
    - Systems to trace traffic across a network**
    - Network devices such as routers and firewalls**
- **Provide secure means to communicate IODEF documents**
  - **Consortiums agree upon use and abuse guidelines**
  - **Consortiums provide Public Key Infrastructure to support encryption and digital signing requirements**



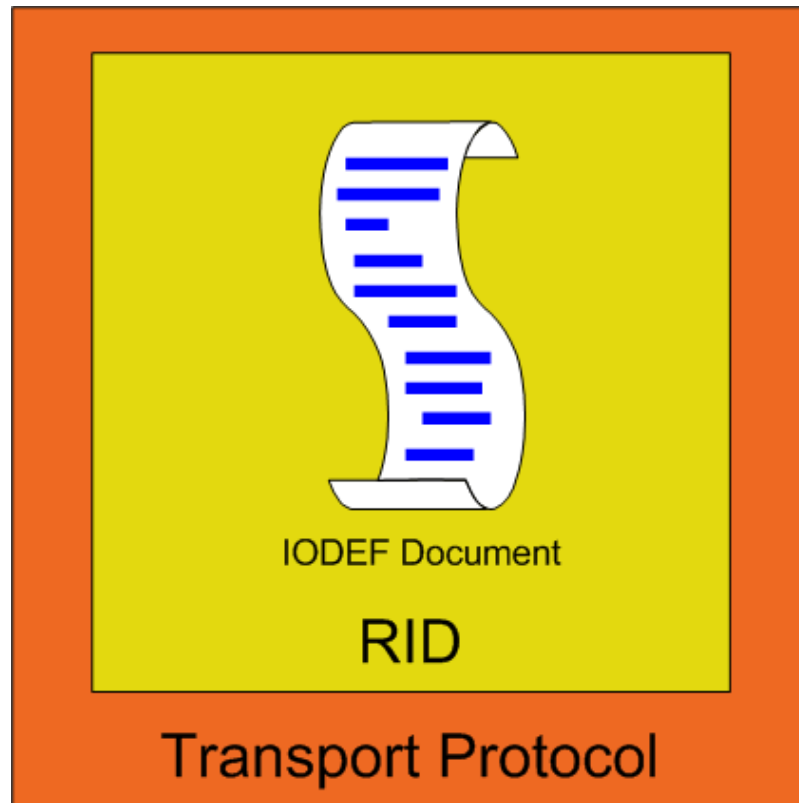
# Generalization of RID for IODEF

---

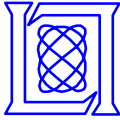
- **RID is used to communicate security incident handling information between CSIRTs or Network Providers (NPs)**
- **RID initially intended for:**
  - **Reporting and tracing security incident information to a RID system close to the attack source**
  - **Integration with traceback systems**
    - For the case where traffic may have been spoofed
  - **Method to stop attack traffic close to the source**
- **The generalization of RID will specify**
  - **Communication flow of all IODEF documents**
  - **This involves adding one more message type for the reporting of a security incident for statistics with no further actions to be taken**
    - Report message type added to RIDPolicy
- **Major document updates are text changes and the ability to send an incident report with no required action**
- **Are there any other cases that are not yet covered?**



# RID Envelope for IODEF



- All IODEF documents are enveloped in RID
- Facilitates communication of IODEF documents and sets purpose
  - Reporting
  - Investigation where source is known
  - Trace request
- The transport protocol will be defined in a separate document
  - SOAP and HTTPS



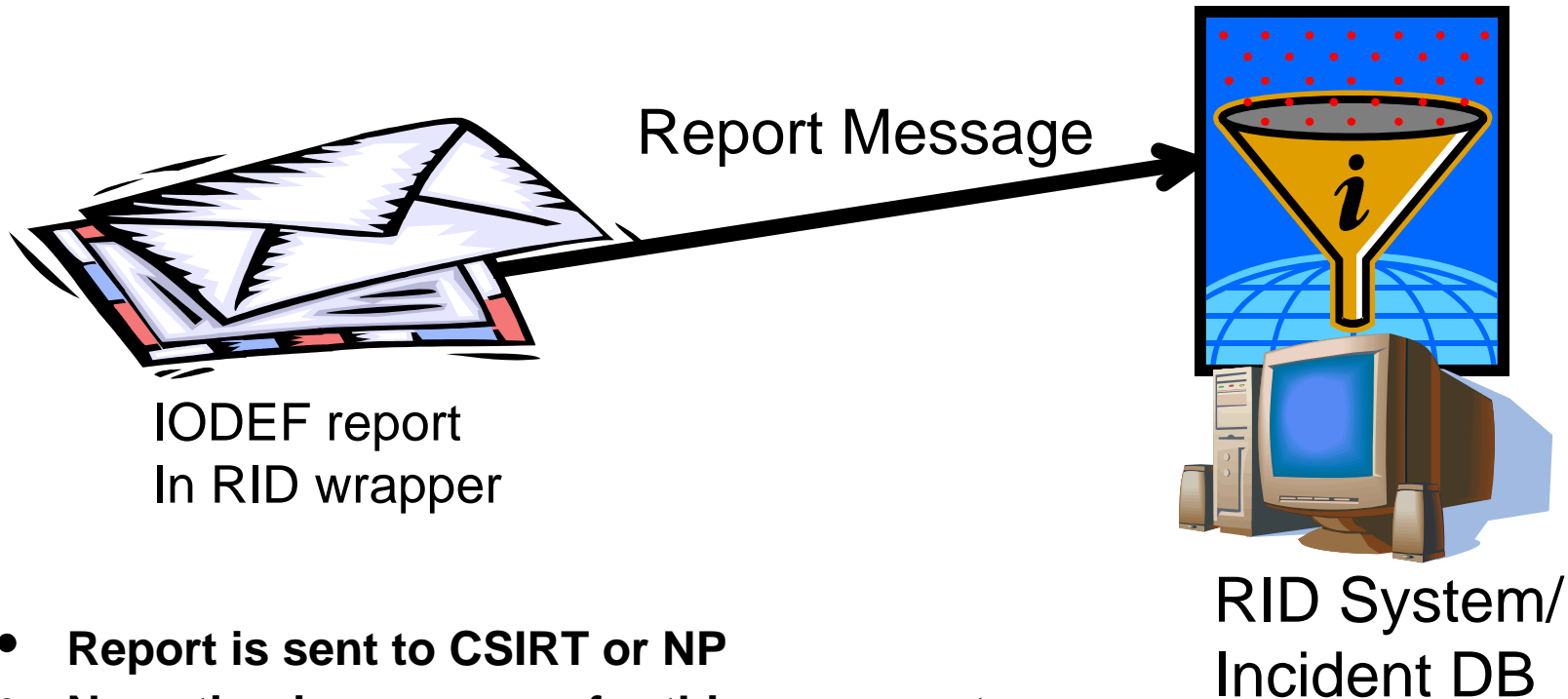
# Communicating RID Messages

---

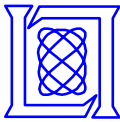
- RID serves as the message wrapper for all IODEF documents
- RID defines the communication flow of all IODEF documents using the defined RID message types
- **Message Types**
  - **Trace Request**  
Requires integration with traceback systems to identify upstream source
  - **Trace Authorization**  
Traceback approval status in upstream provider's network
  - **Result**
    - \*Previously known as "Source Found"
    - \*Actions will be expanded in Data Model to support necessary options
  - **Investigation**
    - \*Previously Relay Request
    - Incident Investigation for attack mitigation with a known source
  - **\*Report**  
Statistics – no action necessary
- **RID Systems Must Track the Requests by**
  - **\* Incident Number and Instance ID**  
The **incident@ID** will be moved to RIDPolicy from the data model
  - **Packet Contents**
  - **Completion Status**



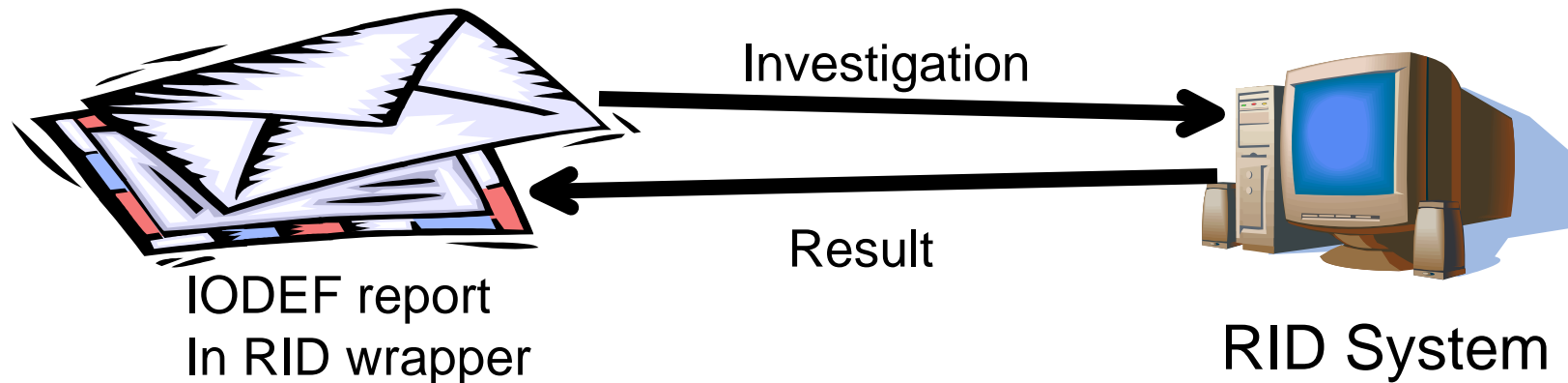
# Report Message



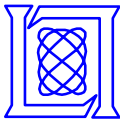
- Report is sent to CSIRT or NP
- No action is necessary for this message type
- Used for statistics and generating trending information
- Transport will use TCP (HTTPS), so there is no response necessary



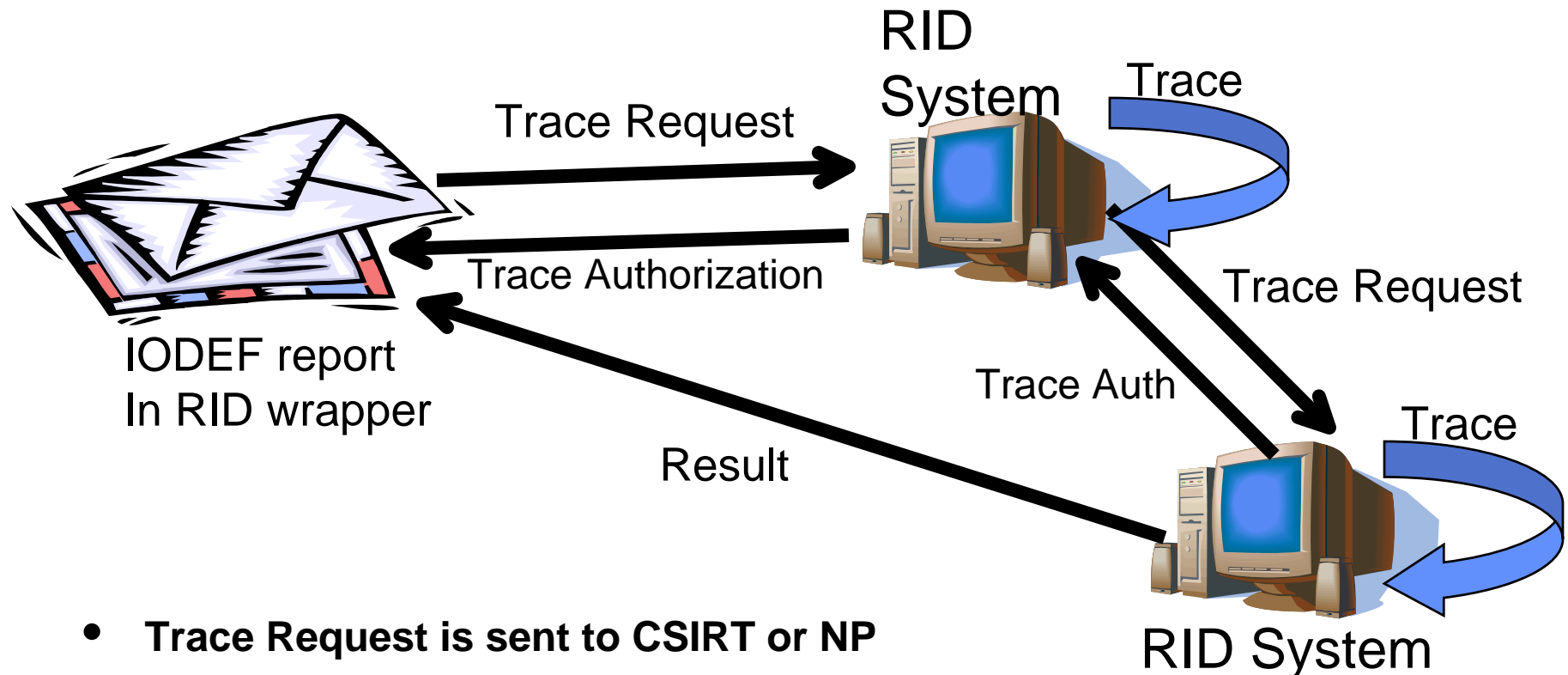
# Investigation Message



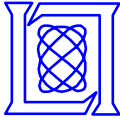
- **Investigation message is sent to CSIRT or NP**
- **An Investigation is requested where the source is known**
- **Purpose is to mitigate or stop the attack traffic**
- **A response via the Result message is required**
  - **Details the action(s) taken**



# Trace Request Message



- Trace Request is sent to CSIRT or NP
- A traceback investigation is requested to locate the source
- All upstream trace requests must decide if trace will be authorized
- Purpose is to mitigate or stop the attack traffic
- A response via the Result message is required
  - Details the action(s) taken



# Transport in a New Draft

---

- **Draft will define the transport protocol for all IODEF documents**
- **RID will define the message communication flow and the transport document will discuss SOAP and HTTPS for transport**
- **XML Security**
  - 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
- **SOAP Messaging Wrapper**
  - Method to transport messages
  - HTTPS will be the mandatory protocol for implementation
    - Not necessarily the most efficient transport for the IODEF messages, but was agreed upon by WG for ease of initial implementation
  - Other protocols may be added for optional support



# 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
    - \*Adding one for reporting/statistics
- **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?**



# Summary

---

- **Updates from the previous version**
  - Working on the generalization of RID to support transport of all IODEF documents
    - Many text updates are in progress
  - Update to the RIDPolicy class to change and add message types
  - DTD will be removed in the next revision
    - Pending on release of IODEF data model
    - Need to ensure documents flow
    - Need to update the text sections of document to eliminate DTD references
- **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>**