RID IETF Draft Update

Kathleen M. Moriarty

INCH Working Group

3 August 2005

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

RID Updates

- Purpose
- RID and INCH
- Generalizing RID draft
  - Communication flow for all IODEF documents
  - Schema changes
  - Transport in a separate document
- Communication Mechanism for RID Documents
- RIDPolicy

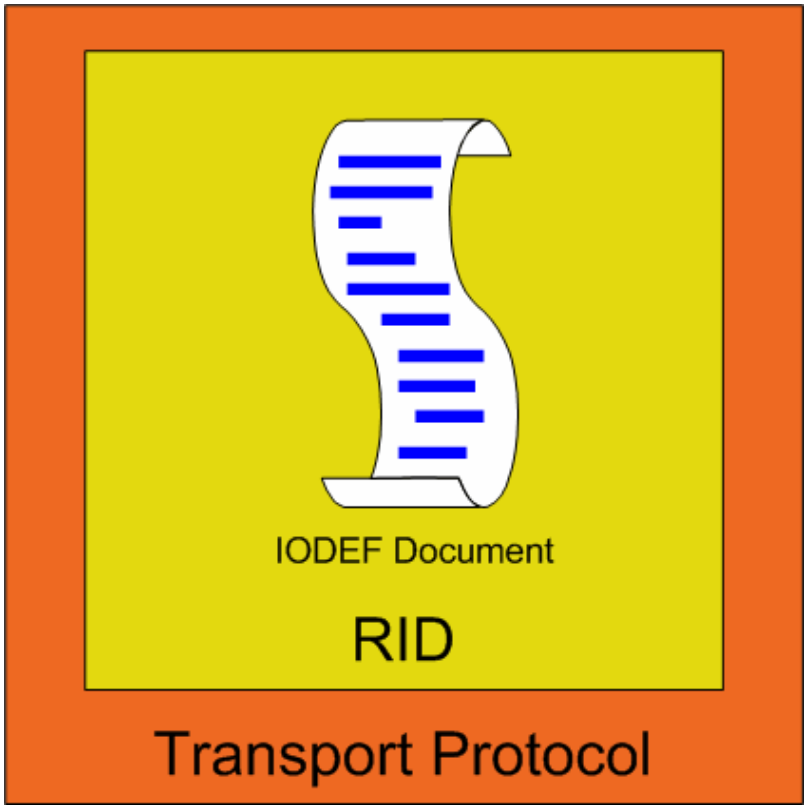
Real-time Inter-network Defense (RID)

- 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 and intrusion detection
  - Method to stop attack traffic close to the source
- The generalization of RID specifies
  - Communication flow to facilitate RID messaging
- Major document updates include
  - RID no longer an extension of IODEF using the AddtionalData class
    - Separate schema which acts as an XML wrapper for IODEF documents
  - Text changes
  - New message types
    - Ability to send an incident report with no required action
    - Ability to request information about an incident
- Are there any other cases that are not yet covered?

RID Envelope for IODEF



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

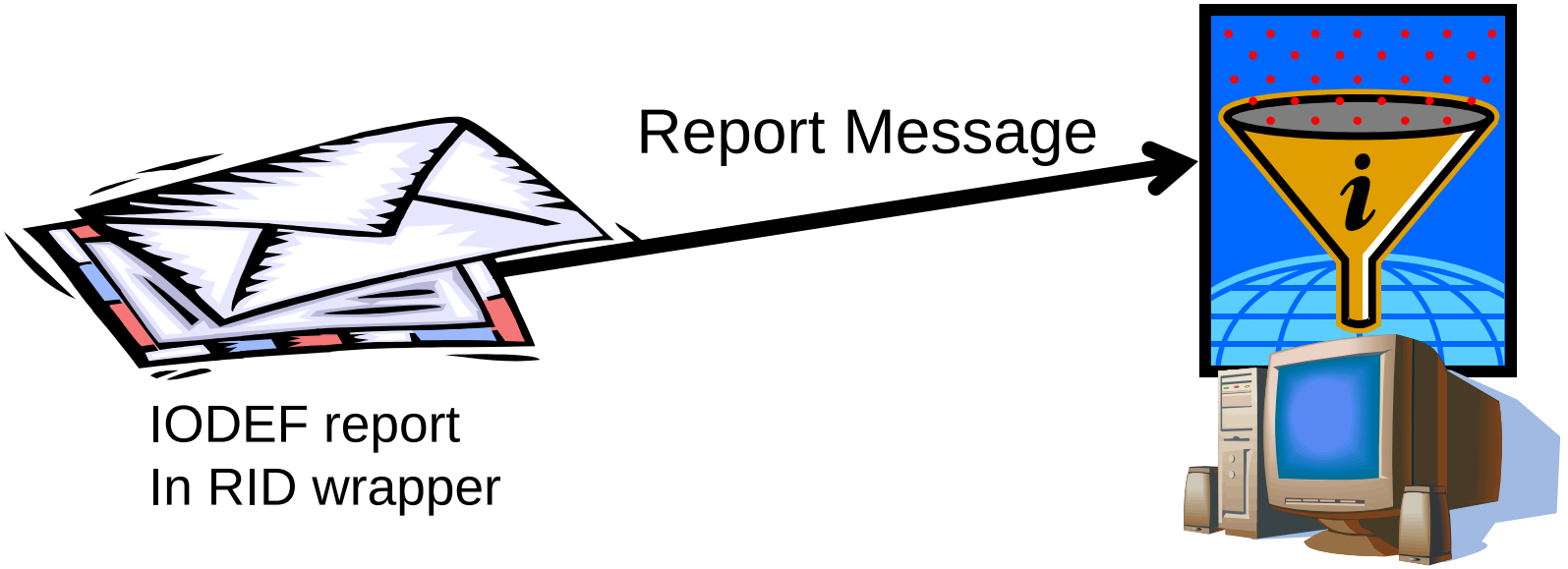
Communicating RID Messages

- 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
  - 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
  - * IncidentQuery
    - Request a report on a particular incident or type of incident
- RID Systems Must Track the Requests by
  - * Incident Number and Instance ID
    - The incident@ID is referenced in RIDPolicy from the data model
    - Format: CSIRTname-IncidentID-Instance
  - Packet Contents
  - Completion Status

Schema Updates

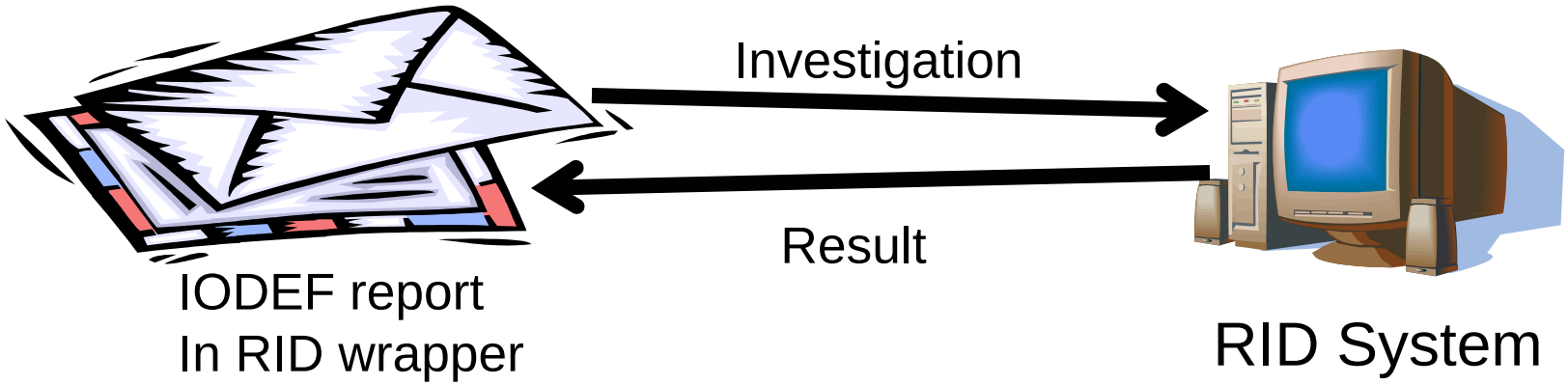
- **RID Schema**
  - **Envelope for the IODEF document**
  - **Separated out from IODEF extension**
    - **Facilitates transport requirements**
    - **Enables easy access to necessary document data to prevent the need to parse the entire document received**
    - **RIDPolicy class can easily be pulled into the SOAP header**
- **Enumerated lists added for all relevant elements**
  - **Lists values changed from decimal type to string for readability of document where possible**

Report Message



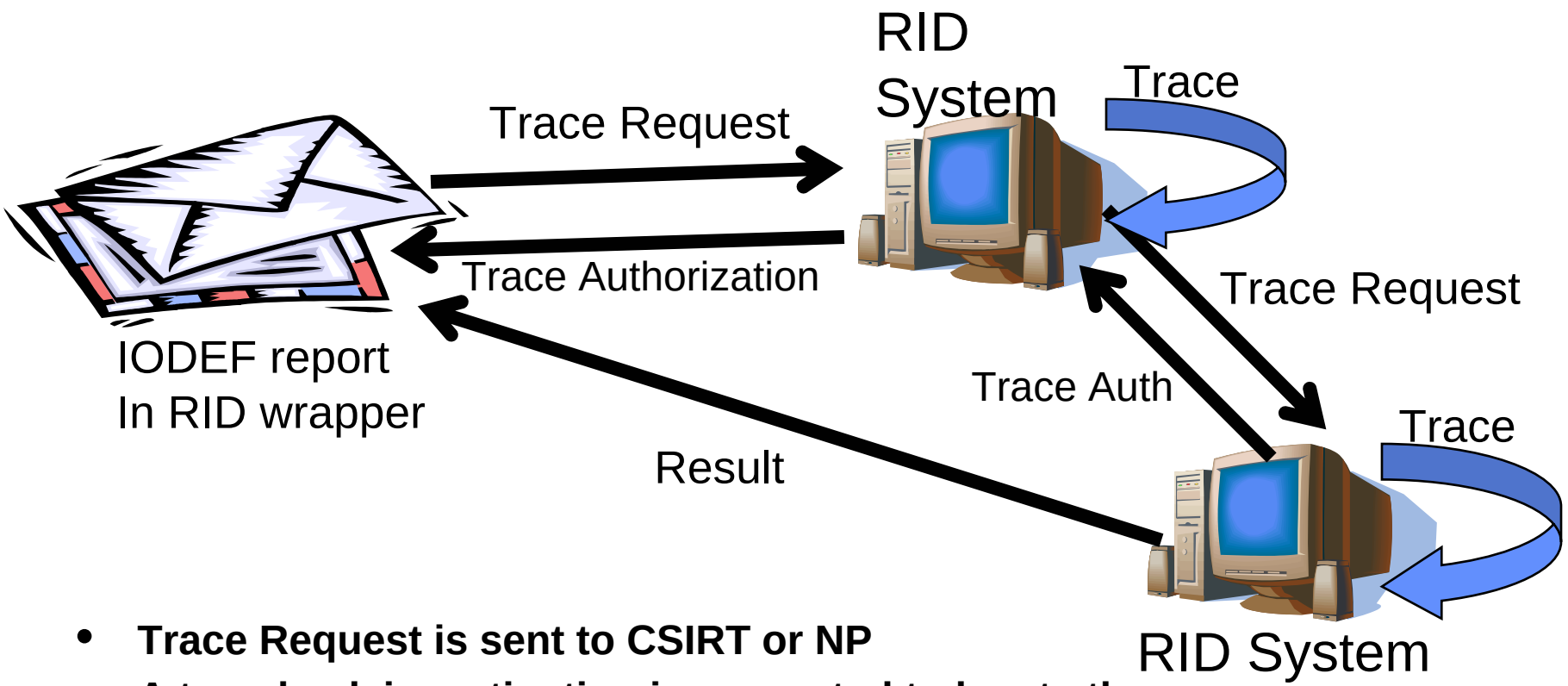
- **Report is sent to CSIRT or NP**
- **No action is necessary for this message type**
- **Used for statistics and generating trending information**
- **Transport will use TCP (HTTPS), so there is no response necessary**

Investigation Message



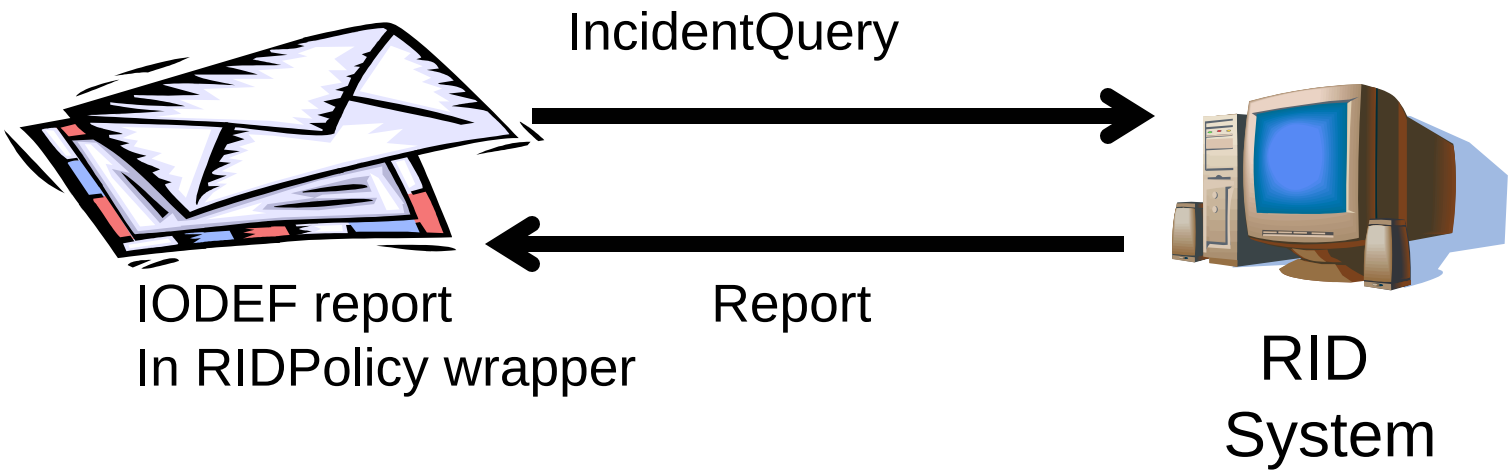
- **Investigation message is sent to CSIRT or NP**
- **An Investigation is requested where the source is known**
- **Purpose is to mitigate or stop the attack traffic**
- **A response via the Result message is required**
  - **Details the action(s) taken**

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**

IncidentQuery and Receive Report



- **IncidentQuery request is sent to CSIRT or NP**
- **Purpose is to obtain information on a particular incident or a type of incident**
- **A response via the Report message is provided**
- **Note: A report message can also be used by itself to provide new information on security incident to a RID system**

Transport in a New Draft

- SOAP Draft defines the transport protocol for RID documents
- RID will define the message communication flow and the transport document discusses SOAP and HTTPS for transport
- XML Security
  - Policy negotiated in RID message through the RIDPolicy, not in SOAP or other transport 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 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
  - Incident number is referenced in RIDPolicy to facilitate transport
- RIDPolicy Information
  - 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
  - Must be complimented with policies formed by consortiums/federations, or between peers
  - New extension created to address issues raised at IETF-59

- **Any comments on RIDPolicy?**

Summary

- Updates from the previous version
  - Continuing work on generalization of RID to support transport of all IODEF documents
    - Many text updates
    - DTD was removed
- Near Future Updates will include
  - RID Schema
    - Separate RID schema is an envelope for IODEF, not an extension
    - RIDPolicy class references global IODEF attribute for incidentID
    - Enumerated lists included for allowed values in schema definition
  - Added message types for incident query and response
  - Added information about IPFix
    - IETF flow analysis standard emerging
  - Pending on release of IODEF data model
    - Need to ensure documents flow
    - Need to update the text sections of document to eliminate DTD references
  - Separate document for SOAP wrapper and transport
- http://www.ietf.org/internet-drafts/draft-ietf-inch-rid-02.txt