Extended Incident Handling Working Group
Internet-draft
Intended-status: Informational
draft-moriarty-post-inch-rid-11.txt
Expires: September 30, 2010

Kathleen M. Moriarty
EMC

March 30, 2010

Real-time Inter-network Defense

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 30, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Abstract

Network security incidents, such as system compromises, worms, viruses, phishing incidents, and denial of service, typically result in the loss of service, data, and resources both human and system. Network providers and Computer Security Incident Response Teams need to be equipped and ready to assist in communicating and tracing security incidents with tools and procedures in place before the occurrence of an attack. Real-time Inter-network Defense outlines a proactive inter-network communication method to facilitate sharing incident handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms across for a complete incident handling solution. Combining these capabilities in a communication system provides a way to achieve higher security levels on networks. Policy guidelines for handling incidents are recommended and can be agreed upon by a consortium using the security recommendations and considerations.

TABLE OF CONTENTS

1. Normative and Informative

The XML schema [4] and transport requirements contained in this document are normative, all other information provided is intended as informative. More specifically, the following sections of this document are intended as informative: 1, 2, 3, the subsections of 4 including the introduction to 4, 4.1, and 4.2.
The following sections of this document are normative:
The sub-sections of 4 including 4.3, 4.4, 4.5, section 5, and section 6.

Note: The documented procedures represent the consensus of another group and are included to further describe environments where this schema can be used. The documented procedures are not required for conformance to this specification.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2 Introduction

Incident handling involves the detection, reporting, identification, and mitigation of an attack, whether it be a system compromise, socially engineered phishing attack, or a denial of service attack. When an attack is detected, the response may include simply filing a report, notification to the source of the attack, a request for mitigation, or the request to locate the source. One of the more difficult cases is that in which the source of an attack is unknown, requiring the ability to trace the attack traffic iteratively upstream through the network for the possibility of any further actions to take place. In cases with accurate records of an active session between the victim system and the attacker or source system are available, the source is easy to identify. The problem of tracing incidents becomes more difficult when the source is obscured or spoofed, logs are deleted, and the number of sources is overwhelming. If the source of an attack is known or identified, it may be desirable to request actions be taken to stop or mitigate the effects of the attack.

Current approaches to mitigating the effects of security incidents are aimed at identifying and filtering or rate-limiting packets from attackers who seek to hide the origin of their attack by source address spoofing from multiple locations. Measures can be taken at network provider (NP) edge routers providing ingress, egress, and broadcast filtering as a recommended best practice in

[RFC2827].

Network providers have devised solutions, in-house or commercial, to trace attacks across their backbone infrastructure to either

identify the source on their network or on the next upstream network in the path to the source. Techniques, such as collecting packets as traffic traverses the network, have been implemented to provide the capability to trace attack traffic after an incident has occurred. Other methods use packet-marking techniques or flow-based traffic analysis to trace traffic across the network in real time. The single-network trace mechanisms use similar information across the individual networks to trace traffic. Problems may arise when an attempt is made to have a trace continued through the next upstream network since the trace mechanism and management may vary.

In the case in which the traffic traverses multiple networks, there is currently no established communication mechanism for continuing the trace. If the next upstream network has been identified, a phone call might be placed to contact the network administrators in an attempt to have them continue the trace. A communication mechanism is needed to facilitate the transfer of information to continue traces accurately and efficiently to upstream networks. The communication mechanism described in this paper, Real-time Inter-network Defense (RID), takes into consideration the information needed by various single network trace implementations and the requirement for network providers to decide if a trace request should be permitted to continue. The data in RID messages is represented in an Extensible Markup Language (XML) [1] document using the Incident Object Description Exchange Format (IODEF) and RID. By following this model, integration with other aspects of the network for incident handling is simplified. Finally, methods are incorporated into the communication system to indicate what actions need to be taken closest to the source in order to halt or mitigate the effects of the attack at hand. RID is intended to provide a method to communicate the relevant information between Computer Security Incident Response Teams (CSIRTs) while being compatible with a variety of existing and possible future detection tracing and response approaches.

Security and privacy considerations are of high concern since potentially sensitive information may be passed through RID messages. RID messaging takes advantage of XML security and privacy policy information set in the RID schema. The RID schema acts as an XML envelope to support the communication of IODEF documents for exchanging or tracing information security incidents. RID messages are encapsulated for transport, which is defined in a separate document. The authentication, integrity, and authorization features each layer has to offer is used to achieve necessary level of security.

1.3 Attack Types and RID Messaging

RID messaging is intended for use in coordinating incident handling to locate the source of an attack and stop or mitigate the effects of the attack. The attack types include system or network

compromises, denial of service attacks, or other malicious network traffic. RID is essentially a messaging system coordinating attack detection, tracing mechanisms, and the incident handling responses to locate the source of traffic. If a source address is spoofed, a more detailed trace of a packet (RID TraceRequest) would be required to locate the true source. If the source address is valid, the incident handling may only involve the use of routing information to determine what network provider is closest to the source (RID Investigation request) and can assist with the remediation. The type of RID message used to locate a source is determined by the validity of the source address. RID message types are discussed in section 4.3.

DoS [11] attacks are characterized by large amounts of traffic destined for particular Internet locations and can originate from a single or multiple sources. An attack from multiple sources is known as a distributed denial-of-service attack (DDoS). Because DDoS attacks can originate from multiple sources, tracing such an attack can be extremely difficult or nearly impossible. Many TraceRequests may be required to accomplish the task and may require the use of dedicated network resources to communicate incident handling information to prevent a DoS against the RID system and network used for tracing and remediation. Provisions are suggested to reduce the load and prevent the same trace from occurring twice on a single-network backbone discussed in section 4 on communication between NPs. The attacks can be launched from systems across the Internet unified in their efforts or by compromised systems enlisted as "zombies" that are controlled by servers, thereby providing anonymity to the controlling server of the attack. This scenario may require multiple RID traces, one to locate the zombies and an additional one to locate the controlling server. DDoS attacks do not necessarily spoof the source of an attack since there are a large number of source addresses, which make it difficult to trace anyway. DDoS attacks can also originate from a single system or a subset of systems that spoof the source address in packet headers in order to mask the identity of the attack source. In this case, an iterative trace through the upstream networks in the path of the attack traffic may be required.

RID traces may also be used to locate a system used in an attack to compromise another system. Compromising a system can be accomplished through one of many attack vectors, using various techniques from a remote host or through local privilege escalation attempts. The attack may exploit a system or application level vulnerability that may be the result of a design flaw or a configuration issue. A compromised system, as described above, can be used to later attack other systems. A single RID

Investigation request may be used in this case since it is probable that the source address is valid. Identifying the sources of system compromises may be difficult since an attacker may access the compromised system from various sources. The attacker may also

take measures to hide their tracks by deleting log files or by accessing the system through a series of compromised hosts. Iterative RID traces may be required for each of the compromised systems used to obscure the source of the attack. If the source address is valid, an Investigation request may be used in lieu of a full RID TraceRequest.

Once an attack has been reported, CSIRTs may want to query other CSIRTs if they have detected an attack or simply report that one has taken place. The Report message can be used to file a report without an action take and an IncidentQuery can be used to ask if an attack has been seen by another CSIRT.

System compromises may result from other security incident types such as worms, Trojans, or viruses. It is often the case that an incident goes unreported even if valid source address information is available because it is difficult to take any action to mitigate or stop the attack. Incident handling is a difficult task for an NP and even at some client locations due to network size and resource limitations.

2. RID Integration with Network Provider Technologies

For the purpose of this document, a network provider (NP) shall be defined as a backbone infrastructure manager of a network. The network provider's Computer Security Incident Response Team shall be referred to as the CSIRT. The backbone may be that of an organization providing network (Internet or private) access to commercial, personal, government, or educational institutions, or the backbone provider of the connected network. The connected network provider is an extension meant to include Intranet and Extranet providers as well as instances such as a business or educational institute's private network.

NPs typically manage and monitor their networks through a centralized network management system (NMS). The acronym NMS will be used to generically represent management servers on a network used for the management of network resources. An Incident Handling System (IHS) is used to communicate RID messages and may be integrated with an NMS as well as other components of the network. The components of the network that may be integrated through the RID messaging system include attack or event detection, network tracing, and network devices to stop the effects of an attack.

The detection of security incidents may rely on manual reporting, automated intrusion detection tools, and variations in traffic types or levels on a network. Intrusion detection systems (IDS) may be integrated into the IHS to create IODEF documents or RID

messages to facilitate security incident handling. Detection of a security incident is outside the scope of this paper; however, it should be possible to integrate detection methods with RID messaging.

RID messaging in an IHS is intended to be flexible in order to accommodate various traceback systems currently in use as well as those that may evolve with technology. RID is intended to communicate the necessary information needed by a trace mechanism to the next upstream NP in the path of a trace. Therefore, a RID message must carry the superset of data required for all tracing systems. If possible, the trace may need to inspect packets to determine a pattern, which could assist reverse path identification. This may be accomplished by inspecting packet header information such as the source and destination IP addresses, ports, and protocol flags to determine if there is a way to distinguish the packets being traced from other packets. A description of the incident along with any available automated trace data should trigger an alert to the NP's CSIRT for further investigation. The various technologies used to trace traffic across a network are described in section 3.1.

Another area of integration is the ability to mitigate or stop attack traffic once a source has been located. Any automated solution should consider the possible side effects to the network. A change control process or a central point for configuration management might be used to ensure that the security of the network and necessary functionality are maintained and that equipment configuration changes are documented. Automated solutions may depend upon the capabilities and current configuration management solutions on a particular network. The solutions may be based on HTTPS or or appropriate protocols defined in the transport specification.

3. Characteristics of Attacks

The goal of tracing a security incident may be to identify the source or to find a point on the network as close to the origin of the incident as possible. A security incident may be defined as a system compromise, a worm or Trojan infection, or a single- or multiple-source denial-of-service attack. Incident tracing can be used to identify the source(s) of an attack in order to halt or mitigate the undesired behavior. The communication system, RID, described in this paper can be used to trace any type of security incident and allows for actions to be taken when the source of the attack or a point closer to the source is known or has been identified. The purpose of tracing an attack would be to halt or mitigate the affects of the attack through methods such as filtering or rate-limiting the traffic close to the source or by using methods such as taking the host or network offline. Care must also be taken to ensure the system is not abused and to use proper analysis in determining if attack traffic is, in fact, attack traffic at each NP along the path of a trace.

Tracing security incidents can be a difficult task since attackers

go to great lengths to obscure their identity. In the case of a security incident, the true source might be identified through an existing established connection to the attacker's point of origin. However, the attacker may not connect to the compromised system for a long period of time after the initial compromise or may access the system through a series of compromised hosts spread across the network. Other methods of obscuring the source may include targeting the host with the same attack from multiple sources using both valid and spoofed source addresses. This tactic can be used to compromise a machine and leave a difficult task of locating the true origin for the administrators. Security incidents, including DDoS attacks, can be difficult or nearly impossible to trace because of the nature of the attack. Some of the difficulties in tracing attacks include the following:

- O the attack originates from multiple sources;
- O the attack may include various types of traffic meant to consume server resources, such as a SYN flood attack without a significant increase in bandwidth utilization;
- O the type of traffic could include valid destination services, which cannot be blocked since they are essential services to business, such as DNS servers at an NP or HTTP requests sent to an organization connected to the Internet;
- O the attack may utilize varying types of packets including TCP, UDP, ICMP, or other IP protocols;
- O the attack may be from 'zombies', which then require additional searches to locate a controlling server as the true origin of the attack;
- O the attack may use a very small number of packets from any particular source, thus making a trace after the fact nearly impossible.

If the source(s) of the attack cannot be determined from IP address information or tracing the increased bandwidth utilization, it may be possible to trace the traffic based on the type of packets seen by the client. In the case of packets with spoofed source addresses, it is no longer a trivial task to identify the source of an attack. In the case of an attack using valid source addresses, methods such as the traceroute utility can be used to fairly accurately identify the path of the traffic between the source and destination of an attack. If the true source has been identified, actions should be taken to halt or mitigate the effects of the attack by reporting the incident to the NP or the upstream NP

closest to the source. In the case of a spoofed source address, other methods can be used to trace back to the source of an attack. The methods include packet filtering, packet hash comparisons, IP marking techniques, ICMP traceback, and packet flow analysis. As

in the case of attack detection, tracing traffic across a single network is a function that can be used with RID in order to provide the networked ability to trace spoofed traffic to the source, while RID provides all the necessary information to accommodate the approach used on any single network to accomplish this task. RID can also be used to report attack traffic close to the source where the IP address used was determined to be valid or simply to report that an incident occurred.

3.1 Integrating Trace Approaches

There have been many separate research initiatives to solve the problem of tracing upstream packets to detect the true source of attack traffic. Upstream packet tracing is currently confined to the borders of a network or an NP's network. Traces require access to network equipment and resources, thus potentially limiting a trace to a specific network. Once a trace reaches the boundaries of a network, the network manager or NP adjacent in the upstream trace must be contacted in order to continue the trace. NPs have been working on individual solutions to accomplish upstream tracing within their own network environments. The tracing mechanisms implemented thus far have included proprietary or custom solutions requiring specific information such as IP packet header data, hash values of the attack packets, or marked packets. Hash values are used to compare a packet against a database of packets that have passed through the network in the case of "Hash Based IP Traceback" [7]. Other research solutions involve marking packets as explained in "ICMP Traceback Messages" [8], "Practical Support for IP Traceback" [10], the IP Flow Information eXport (IPFIX) protocol [RFC3917], and IP Marking [6]. The single network traceback solutions were considered in developing RID to determine the information needed to accomplish an inter-network trace where different solutions may be in place.

3.2 Superset of Packet Information for Traces

In order for network traffic to be traced across a network, an example packet from the attack must be sent along with the TraceRequest or Investigation request. According to the research for Hash-based IP Traceback, all of the non-changing fields of an IP header along with 8 bytes of payload are required to provide enough information to uniquely trace the path of a packet. The non-changing fields of the packet header and the 8 bytes of payload are the superset of data required by most single-network tracing systems used; limiting the shared data to the superset of the packet header and 8 bytes of payload prevents the need for sharing potentially sensitive information that may be contained in the data portion of a packet.

The RecordItem class in the IODEF is used to store a hexadecimal formatted packet including all packet header information plus 8 bytes of payload or the entire packet contents.

The above trace systems do not require a full packet, but it may be useful in some cases, so the option is given to allow a full packet to be included in the data model.

If a subset of a packet is used, the following guidelines should be used to provide compatibility between RID systems. The complete header MUST be provided so that all systems expect a full packet header and the packet can be properly parsed. The full content may be provided, but at least 8 bytes must be included to conduct a network trace. RID requires the first 28 bytes of an IP v4 packet in order to perform a trace. The required number of bytes provides the IP header in an IP v4 packet, which is 10 bytes long; the TCP/UDP/ICMP header is also 10 bytes long, plus an additional 8 bytes of payload to distinguish the packet for tracing purposes. RID requires 48 bytes for an IP v6 packet in order to distinguish the packet in a trace. The input mechanism should be flexible enough to allow intrusion detection systems or packet sniffers to provide the information. The system creating the RID message should also use the packet information to populate the Incident class information in order to avoid human error and also allow a system administrator to override the automatically populated information.

4. Communication Between Network Providers

Note: The introduction and sub-sections 4.1 and 4.2 are informative, with the exception of references to IODEF/RID Transport, [RFCYYYY]. Sub-sections 4.3, 4.4, 4.5 are normative.

Expediting the communication between CSIRTs is essential when responding to a security-related incident, which may cross network access points (Internet backbones) between providers. As a result of the urgency involved in this inter-NP security incident communication, there must be an effective system in place to facilitate the interaction. This communication policy or system should involve multiple means of communication to avoid a single point of failure. Email is one way to transfer information about the incident, packet traces, etc. However, e-mail may not be received in a timely fashion or be acted upon with the same urgency as a phone call or other communication mechanism.

Each NP should dedicate a phone number to reach a member of the CSIRT. The phone number could be dedicated to inter-NP incident communications and must be a hotline that provides a 24x7 live response. The phone line should reach someone who would have either the authority and expertise or the means to expedite the necessary action to investigate the incident. This may be a difficult policy to establish at smaller NPs due to resource limitations, so another solution may be necessary. An outside

group may be able to serve this function if given the necessary access to the NPs network. The outside resource should be able to mitigate or alleviate the financial limitations and any lack of experienced resource personnel.

A technical solution to trace traffic across a single NP may include homegrown or commercial systems in which RID messaging must accommodate the input requirements. The IHS used on the NP's backbone by the CSIRT to coordinate the trace across the single network requires a method to accept and process RID messages and relay trace requests to the system, as well as to wait for responses from the system to continue the RID request process as appropriate. In this scenario, each NP would maintain its own RID/IHS and integrate with a management station used for network monitoring and analysis. An alternative for NPs lacking sufficient resources may be to have a neutral third party with access to the NP's network resources who could be used to perform the incident handling functions. This could be a function of a central organization operating as a CSIRT for the Internet as a whole or within a consortium that may be able to provide centralized resources. Consortiums would consist of a group of NPs and/or CSIRTs that agree to participate in the RID communication protocol with an agreed-upon policy and communication protocol facilitating the secure transport of IODEF/RID XML documents. Transport for RID messages is specified in the IODEF/RID Transport [RFCYYYY] document.

One goal of RID is to prevent the need to permit access to other network's equipment through the use of a standard messaging mechanism to enable IHSs to communicate incident handling information to other networks in a consortium or in neighboring networks. The third party mentioned above may be used in this technical solution to assist in facilitating incident handling and possibly traceback through smaller NPs. The RID messaging mechanism may be a logical or physical out-of-band network to ensure the communication is secure and unaffected by the state of the network under attack. The two management methods would accommodate the needs of larger NPs to maintain full management of their network, and the third party option could be available to smaller NPs who lack the necessary human resources to perform incident handling operations. The first method enables the individual NPs to involve their network operations staff to authorize the continuance of a trace or other necessary response to a RID communication request through their network via a notification and alerting system. The out-of-band logical solution for messaging may be permanent virtual circuits configured with a small amount of bandwidth dedicated to RID communications between NPs.

The network used for the communication should consist of out-of-band or protected channels (direct communication links) or encrypted channels dedicated to the transport of RID messages. The communication links would be direct connections between network

peers who have agreed upon use and abuse policies through the use of a consortium. Consortiums might be linked through policy comparisons and additional agreements to form a larger web or iterative network of peers that correlates to the traffic paths

available over the larger web of networks. The maintenance of the individual links is the responsibility of the two network peers hosting the link. Contact information, IP addresses of RID systems and other information must be coordinated between bilateral peers by a consortium and may use existing databases, such as the Routing Arbitor. The security, configuration, and confidence rating schemes of the RID messaging peers must be negotiated by peers and must meet certain overall requirements of the fully connected network (Internet, government, education, etc.) through the peering and/or a consortium-based agreement.

RID messaging established with clients of an NP may be negotiated in a contract as part of a value-added service or through a service level agreement. Further discussion is beyond the scope of this document and may be more appropriately handled in network peering or service level agreements.

Procedures for incident handling need to be established and well known by anyone that may be involved in incident response. The procedures should also contain contact information for internal escalation procedures, as well as for external assistance groups such as a CSIRT, CCCERT, GIAC, and the FBI.

4.1 Inter-Network Provider RID Messaging

In order to implement a messaging mechanism between RID communication or IHS systems, a standard protocol and format is required to ensure inter-operability between vendors. The messages would have to meet several requirements in order to be meaningful as they traverse multiple networks. RID provides the framework necessary for communication between networks involved in the incident handling, possible traceback, and mitigation of a security incident. Several message types described in section 4.3 are necessary to facilitate the handling of a security incident. The message types include the Report, IncidentQuery, TraceRequest, RequestAuthorization, Result, and the Investigation request message. The Report message is used when an incident is to be filed on a RID system or associated database, where no further action is required. An IncidentQuery message is used to request information on a particular incident. A TraceRequest message is used when the source of the traffic may have been spoofed. In that case, each network provider in the upstream path who receives a trace request will issue a trace across the network to determine the upstream source of the traffic. The RequestAuthorization and Result messages are used to communicate the status and result of a TraceRequest or Investigation. The Investigation request message would only involve the RID communication systems along the path to the source of the traffic and not the use of network trace systems.

The Investigation request leverages the bilateral relationships or a consortium's inter-connections to mitigate or stop problematic traffic close to the source. Routes could determine the fastest path to a known source IP address in the case of a Investigation

request. A message sent between RID systems for a TraceRequest or an Investigation request to stop traffic at the source through a bordering network would require the information enumerated below:

1. Enough information to enable the network administrators to make a decision about the importance of continuing the trace.
2. The incident or IP packet information needed to carry out the trace or investigation.
3. Contact information of the origin of the RID communication. The contact information could be provided through the autonomous system number [RFC1930] or NIC handle information listed in the Registry for Internet Numbers or other Internet databases.
4. Network path information to help prevent any routing loops through the network from perpetuating a trace. If a RID system receives a TraceRequest containing its own information in the path, the trace must cease and the RID system should generate an alert to inform the network operations staff that a tracing loop exists.
5. A unique identifier for a single attack should be used to correlate traces to multiple sources in a DDoS attack.

Use of the communication network and the RID protocol must be for pre-approved, authorized purposes only. It is the responsibility of each participating party to adhere to guidelines set forth in both a global use policy for this system and one established though the peering agreements for each bilateral peer or agreed-upon consortium guidelines. The purpose of such policies is to avoid abuse of the system; the policies shall be developed by a consortium of participating entities. The global policy may be dependent on the domain it operates under; for example, a government network or a commercial network such as the Internet would adhere to different guidelines to address the individual concerns. Privacy issues must be considered in public networks such as the Internet. Privacy issues are discussed in the security section along with other requirements that must be agreed upon by participating entities.

RID requests must be legitimate security-related incidents and not used for purposes such as sabotage or censorship. An example of such abuse of the system would include a request to rate-limit legitimate traffic to prevent information from being shared between users on the Internet (restricting access to online versions of papers) or restricting access from a competitor's product in order to sabotage a business.

The RID system should be configurable to either require user input or automatically continue traces. This feature would enable a network manager to assess the available resources before continuing

a trace. A trace initiated from a TraceRequest may cause adverse effects on a network. If the confidence rating is low, it may not be in the NP's best interest to continue the trace. The confidence ratings must adhere to the specifications for selecting the

percentage used to avoid abuse of the system. TraceRequests must be issued by authorized individuals from the initiating network, set forth in policy guidelines established through peering or SLA.

4.2 RID Network Topology

The most basic topology for communicating RID systems would be a direct connection or a bilateral relationship as illustrated below.

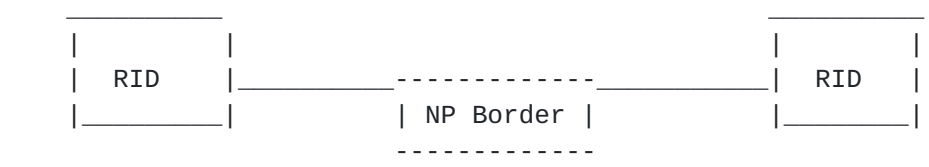


Figure 1: Direct Peer Topology

Within the consortium model, several topologies might be agreed upon and used. One would leverage bilateral network peering relationships of the members of the consortium. The peers for RID would match that of routing peers and the logical network borders would be used. This approach may be necessary for an iterative trace where the source is unknown. The model would look like the above diagram; however, there may be an extensive number of inter-connections of bilateral relationships formed. Also within a consortium model, it may be useful to establish an integrated mesh of networks to pass RID messages. This may be beneficial when the source address is known, and an interconnection may provide a faster route to reach the closest upstream peer to the source of the attack traffic. An example is illustrated below.

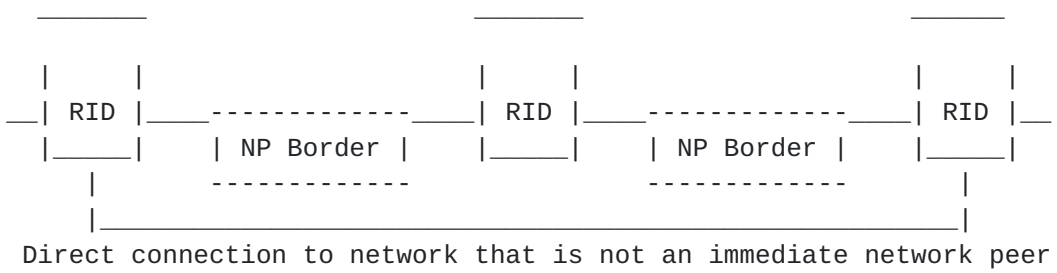


Figure 2: Mesh Peer Topology

By using a fully meshed model in a consortium, broadcasting RID requests would be possible, but not advisable. By broadcasting a request, RID peers that may not have carried the attack traffic on their network would be asked to perform a trace for the potential of deceasing the time in which the true source was identified. As a result, many networks would have utilized unnecessary resources for a TraceRequest that may have also been unnecessary.

4.3 Message Formats

The following section describes the six RID message types which are based on the IODEF model [RFC5070]. The messages are generated and received on RID communication systems on the NP's network. The messages may originate from IODEF messages from intrusion detection servers, CSIRTS, analysts, etc. A RID message uses the IODEF framework with the RID extension, which is encapsulated for transport [RFCYYYY]. Each RID message type, along with an example, is described in the following sections. The IODEF-RID schema is introduced in section 4.3.3 to support the RID message types in section 4.3.1.

4.3.1 RID Data Types

RID is derived from the IODEF data model and inherits all of the data types defined in the IODEF model. One data type is added by RID, BOOLEAN.

4.3.1.1 Boolean

A boolean value is represented by the BOOLEAN data type.

The BOOLEAN data type is implemented as "xs:Boolean" [9] in the schema.

4.3.2 RID Messages and Transport

The six RID message types follow:

1. TraceRequest. This message is sent to the RID system next in the upstream trace. It is used to initiate a TraceRequest or to continue a TraceRequest to an upstream network closer to the source of the origin of the security incident. The TraceRequest would trigger a traceback on the network to locate the source of the attack traffic.

2. RequestAuthorization. This message is sent to the initiating RID system from each of the upstream NPs' RID systems to provide information on the request status in the current network.

3. Result. This message is sent to the initiating RID system through the network of RID systems in the path of the trace as notification that the source of the attack was located. The Result message is also used to provide the notification of actions taken for an Investigation request.

4. Investigation. This message type is used when the source of the traffic is believed to be valid. The purpose of the Investigation message request is to leverage the existing peer relationships in order to notify the network provider closest to the source of the

valid traffic of a security-related incident for any necessary actions to be taken.

5. Report. This message is used to report a security incident, for which no action is requested. This may be used for the purpose of correlating attack information by CSIRTS, statistics and trending information, etc.

6. IncidentQuery. This message is used to request information about an incident or incident type from a trusted RID system. The response is provided through the Report message.

When a system receives a RID message, it must be able to determine the type of message and parse it accordingly. The message type is specified in the RIDPolicy class. The RIDPolicy class may also be used by the transport protocol to facilitate the communication of security incident data to trace, investigate, query, or report information security incident information.

4.3.3 IODEF-RID Schema

There are three classes included in the RID extension required to facilitate RID communications. The RequestStatus class is used to indicate the approval status of a TraceRequest or Investigation request; the IncidentSource class is used to report whether or not a source was found and to identify the source host(s) or network(s); and the RIDPolicy class provides information on the agreed policies and specifies the type of communication message being used.

The RID schema acts as an envelope for the IODEF schema to facilitate RID communications. The intent in maintaining a separate schema and not using the AdditionalData extension of IODEF is the flexibility of sending messages between RID hosts. Since RID is a separate schema that includes the IODEF schema, the RID information acts as an envelope, and then the RIDPolicy class can be easily extracted for use by the transport protocol. The security requirements of sending incident information across the network require the use of encryption. The RIDPolicy information is not required to be encrypted, so separating out this data from the IODEF extension removes the need for decrypting and parsing the entire IODEF and RID document to determine how it should be handled at each RID host.

The purpose of the RIDPolicy class is to specify the message type for the receiving host, facilitate the policy needs of RID, and provide routing information in the form of an IP address of the destination RID system.

The policy information and guidelines are discussed in section 6.5. The policy is defined between RID peers and within or between

consortiums. The RIDPolicy is meant to be a tool to facilitate the defined policies. This MUST be used in accordance with policy set between clients, peers, consortiums, and/or regions. Security, privacy, and confidentiality MUST be considered as specified in

this document.

The RID Schema is defined as follows:

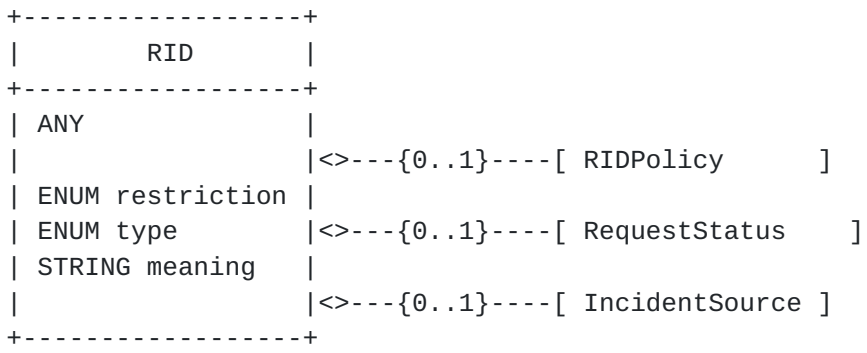


Figure 3: The RID Schema

The aggregate classes that constitute the RID schema in the iodef-rid namespace are as follows:

RIDPolicy
Zero or One. The RIDPolicy class is used by all message types to facilitate policy agreements between peers, consortiums or federations as well as to properly route messages.

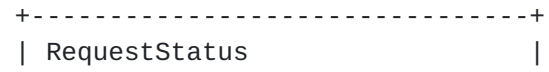
RequestStatus
Zero or One. This is used only in Request Authorization messages to report back to the originating RID system if the trace will be continued by each RID system that received a TraceRequest in the path to the source of the traffic.

IncidentSource
Zero or One. The IncidentSource class is used in the Result message only. The IncidentSource provides the information on the identified source host or network of an attack trace or investigation.

Each of the three listed classes may be the only class included in the RID class, hence the option for zero or one. In some cases, RIDPolicy MAY be the only class in the RID definition when used by the transport protocol [RFCYYYY] as that information should be as small as possible and may not be encrypted. The RequestStatus message MUST be able to stand alone without the need for an IODEF document to facilitate the communication, limiting the data transported to the required elements per RFCYYYY.

4.3.3.1 RequestStatus Class

The RequestStatus class is an aggregate class in the RID class.


RequestStatus

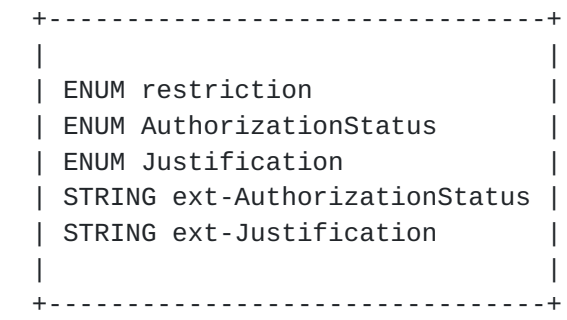


Figure 4: The RequestStatus Class

The RequestStatus class has five attributes:

restriction
Optional. ENUM. This attribute indicates the disclosure guidelines to which the sender expects the recipient to adhere. This guideline provides no real security since it is the choice of the recipient of the document to honor it. This attribute follows the same guidelines as restriction used in IODEF.

AuthorizationStatus
Required. ENUM. The listed values are used to provide a response to the requesting CSIRT of the status of a TraceRequest in the current network.

1. Approved. The trace was approved and will begin in the current NP.
2. Denied. The trace was denied in the current NP. The next closest NP can use this message to filter traffic from the upstream NP using the example packet to help mitigate the effects of the attack as close to the source as possible. The RequestAuthorization message must be passed back to the originator and a Result message used from the closest NP to the source to indicate actions taken in the IODEF History class.
3. Pending. Awaiting approval and a time-out period has been reached which resulted in this pending status and RequestAuthorization message being generated.
4. ext-value. An escape value used to extend this attribute. See [RFC 5070] IODEF Section 5.1.

Justification
Optional. ENUM. Provide a reason for a denied or pending message.
1. SystemResource. A resource issue exists on the systems that would be involved in the request.
2. Authentication. The enveloped digital signature [RFC3275] failed to validate.

3. AuthenticationOrigin. The detached digital signature for the original requestor on the IP packet failed to validate.
4. Encryption. Unable to decrypt the request.
5. Other. There were other reasons this request could not be

processed.

6. ext-value. An escape value used to extend this attribute. See [RFC5070] IODEF Section 5.1.

ext-AuthorizationStatus
Optional. STRING. A means by which to extend the AuthorizationStatus attribute. See [RFC5070] IODEF Section 5.1.

ext-Justification
Optional. STRING. A means by which to extend the Justification attribute. See [RFC5070] IODEF Section 5.1.

4.3.3.2 IncidentSource Class

The IncidentSource class is an aggregate class in the RID class.

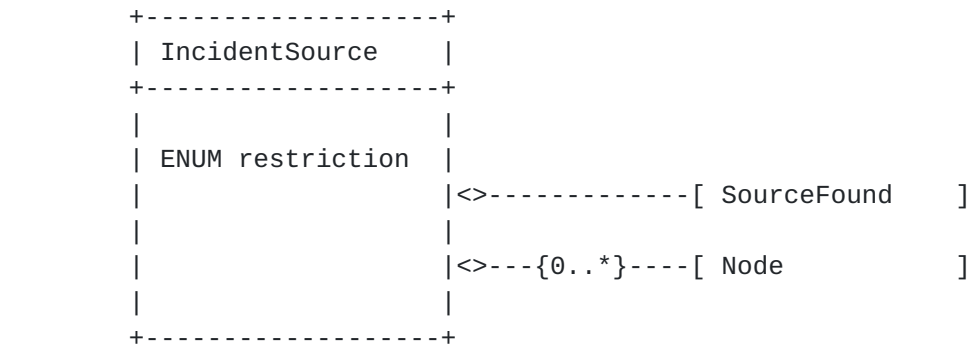


Figure 5: The IncidentSource Class

The elements that constitute the IncidentSource class follow:

SourceFound
One. Boolean. The Source class indicates if a source was identified. If the source was identified, it is listed in the Node element of this class.

True. Source of incident was identified.
False. Source of incident was not identified.

Node
One. The Node class is used to identify a host or network device, in this case to identify the system communicating RID messages.

The base definition of the class is reused from the IODEF specification IODEF 3.16.

The IncidentSource class has one attribute.

restriction
Optional. ENUM. This attribute indicates the disclosure guidelines to which the sender expects the recipient to adhere. This guideline provides no real security since it is the choice of the recipient of the document to honor it. This attribute follows the same guidelines as restriction used in IODEF.

4.3.3.3 RIDPolicy

The RIDPolicy class facilitates the delivery of RID messages and is also referenced for transport in the transport document [RFCYYYY].

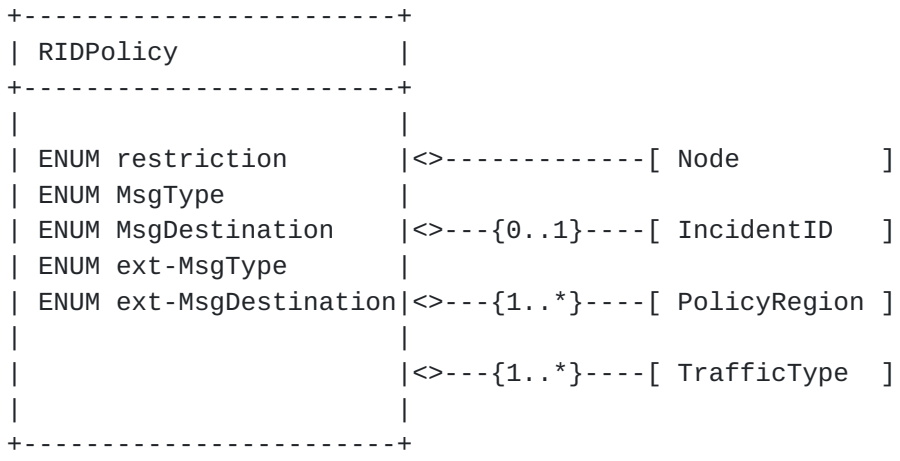


Figure 6: The RIDPolicy Class

The aggregate elements that constitute the RIDPolicy class are as follows:

Node
One. The Node class is used to identify a host or network device, in this case to identify the system communicating RID messages.

The base definition of the class is reused from the IODEF specification IODEF 3.16.

IncidentID
Zero or one. Global reference pointing back to the IncidentID defined in the IODEF data model. The IncidentID includes the name of the CSIRT, an incident number, and an instance of that incident. The instance number is appended with a dash separating the values and is used in cases for which it may be desirable to group incidents. Examples of incidents that may be grouped would be botnets, DDoS attacks, multiple hops of compromised systems found during an investigation, etc.

PolicyRegion
One or many. Required. The values for the attribute region are used to determine what policy area may require consideration before a trace can be approved. The PolicyRegion may include multiple selections from the attribute list in order to fit all possible policy considerations when crossing regions, consortiums, or networks.

region
One. ENUM.

1. ClientToNP. An enterprise network initiated the request.
2. NPToClient. An NP passed a RID request to a client or an enterprise attached network to the NP based on the service level agreements.
3. IntraConsortium. A trace that should have no restrictions within the boundaries of a consortium with the agreed-upon use and abuse guidelines.
4. PeerToPeer. A trace that should have no restrictions between two peers but may require further evaluation before continuance beyond that point with the agreed-upon use and abuse guidelines.
5. Between-Consortiums. A trace that should have no restrictions between consortiums that have established agreed-upon use and abuse guidelines.
6. AcrossNationalBoundaries. This selection must be set if the trace type is anything but a trace of attack traffic with malicious intent. This must also be set if the traffic request is based upon regulations of a specific nation that would not apply to all nations. This is different from the inter-consortium since it may be possible to have multiple nations as members of the same consortium, and this option must be selected if the traffic is of a type that may have different restrictions in other nations.
7. ext-value. An escape value used to extend this attribute. See [RFC5070] IODEF Section 5.1.

TrafficType

One or many. Required. The values for the attribute type are meant To assist in determining if a trace is appropriate for the NP receiving the request to continue the trace. Multiple values may be selected for this element; however, where possible, it should be restricted to one value which would most accurately describe the traffic type.

type

One. ENUM.

1. Attack. This option should only be selected if the traffic is related to a network-based attack. The type of attack MUST also be listed in more detail in the IODEF Method and Impact classes for further clarification to assist in determining if the trace can be continued. ([RFC5070] section 3.9 and 3.10.1)
2. Network. This option MUST only be selected when the trace is related to NP network traffic or routing issues.
3. Content. This category MUST be used only in the case in which the request is related to the content and regional restrictions on accessing that type of content exist. This is not malicious traffic but may include determining what sources or destinations accessed certain materials available on the

Internet, including, but not limited to, news, technology, or inappropriate content.

4. OfficialBusiness. This option MUST be used if the traffic being traced is requested or affiliated with any government or

other official business request. This would be used during an investigation by government authorities or other government traces to track suspected criminal or other activities.

5. Other. If this option is selected, a description of the traffic type MUST be provided so that policy decisions can be made to continue or stop the trace. The information should be provided in the IODEF message in the Expectation class or in the History class using a HistoryItem log.
6. ext-value. An escape value used to extend this attribute. See [RFC5070] IODEF Section 5.1.

The RIDPolicy class has five attributes

restriction
Optional. ENUM. This attribute indicates the disclosure guidelines to which the sender expects the recipient to adhere. This guideline provides no real security since it is the choice of the recipient of the document to honor it. This attribute follows the same guidelines as restriction used in IODEF.

MsgType
Required. ENUM. The type of RID Message sent. The six types of messages are described in Section 4.3.1 and can be noted as one of the six selections below.

1. TraceRequest. This message may be used to initiate a TraceRequest or to continue a TraceRequest to an upstream network closer to the source of the origin of the security incident.

2. RequestAuthorization. This message is sent to the initiating RID system from each of the upstream RID systems to provide information on the request status in the current network.

3. Result. This message indicates that the source of the attack was located and the message is sent to the initiating RID system through the RID systems in the path of the trace.

4. Investigation. This message type is used when the source of the traffic is believed to be valid. The purpose of the Investigation request is to leverage the existing peer or consortium relationships in order to notify the NP closest to the source of the valid traffic that some event occurred, which may be a security-related incident.

5. Report. This message is used to report a security incident, for which no action is requested in the IODEF expectation class. This may be used for the purpose of correlating attack information by CSIRTS, statistics and trending information,

etc.

6. IncidentQuery. This message is used to request information

from a trusted RID system about an incident or incident type.

7. ext-value. An escape value used to extend this attribute. See [RFC5070] IODEF Section 5.1.

MsgDestination
Required. ENUM. The destination required at this level may either be the RID messaging system intended to receive the request or the source of the incident in the case of an Investigation request where the RID system that can assist to stop or mitigate the traffic may not be known and the message has to traverse RID messaging systems by following the routing path to the closest RID system to the source of the attack traffic. The Node element lists either the RID system or the IP of the source, and the meaning of the value in the Node element is determined by the MsgDestination element.

1. RIDSystem. The address listed in the Node element of the RIDPolicy class is the next upstream RID system that will receive the RID message.

2. SourceOfIncident. The address listed in the Node element of the RIDPolicy class is the incident source. The IP address is used to determine the path of RID systems that will be used to find the closest RID system to the source of an attack in which the IP used by the source is believed to be valid and an Investigation message is used. This is not to be confused with the IncidentSource class as the defined value here is from an initial trace or investigation request, not the source used in a Result message.
3. ext-value. An escape value used to extend this attribute. See [RFC5070] IODEF Section 5.1.

ext-MsgType
Optional. STRING. A means by which to extend the MsgType attribute. See [RFC5070] IODEF Section 5.1.

ext-MsgDestination
Optional. STRING. A means by which to extend the MsgDestination attribute. See RFC5070] IODEF Section 5.1.

4.3.4 RID Namespace

The RID schema declares a namespace of "iodef-rid-1.0" and registers it per [2]. Each IODEF-RID document MUST use the "iodef-rid-1.0" namespace in the top-level element RID-Document. It can be referenced as follows:

<RID-Document

```
      version="1.00" lang="en-US"
      xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
      xsi:schemaLocation="http://iana.org/iodef/ietf-inch-rid-1.0.xsd"
```

where the string "http://iana.org/iodef/ietf-inch-rid-1.0.xsd" is the URL to the schema.

4.4 RID Messages

The IODEF model is followed as specified in [RFC5070] for each of the RID message types. The RID schema is used in combination with IODEF documents to facilitate RID communications. Each message type varies slightly in format and purpose; hence, the requirements vary and are specified for each. All classes, elements, attributes, etc., that are defined in the IODEF-Document are valid in the context of a RID message; however, some listed as optional in IODEF are mandatory for RID as listed for each message type. The IODEF model MUST be fully implemented to ensure proper parsing of all RID messages.

Note: The implementation of the RID system may obtain some of the information needed to fill in the content required for each message type automatically from packet input to the system or default information such as that used in the EventData class.

4.4.1 TraceRequest

Description: This message or document is sent to the Network Management Station next in the upstream trace once the upstream source of the traffic has been identified.

The following information is required for TraceRequest messages and is provided through:

RID Information:
RIDPolicy
: RID message type, IncidentID, and destination policy information

IODEF Information:
Time Stamps (DetectTime, StartTime, EndTime, ReportTime)
Incident Identifier (Incident Class, IncidentID)
: Trace number - used for multiple traces of a single incident, must be noted.

Confidence rating of security incident (Impact and Confidence Class)
System Class is used to list both the Source and Destination
: Information used in the attack and must note if the traffic is spoofed, thus requiring an upstream TraceRequest in RID.

Expectation class should be used to request any specific actions
: to be taken close to the source.

Path information of nested RID systems, beginning with the
: request originator used in the trace using IODEF EventData

with category set to infrastructure
Event, Record, and RecordItem Classes to include example packets
and other information related to the incident. Note: Event

information included here requires a second instance of EventData from that used to convey NP path contact information.

Standards for Encryption and Digital Signatures [RFC3275], [5]:
Digital signature from initiating RID system, passed to all systems in upstream trace using XML digital signature.

A DDoS attack can have many sources, resulting in multiple traces to locate the sources of the attack. It may be valid to continue multiple traces for a single attack. The path information would enable the administrators to determine if the exact trace had already passed through a single network. The incident identifier must also be used to identify multiple TraceRequests from a single incident. If a single TraceRequest results in divergent paths of TraceRequests, a separate instance number MUST be used under the same IncidentID The IncidentID@instance of IODEF can be used to correlate related incident data that is part of a larger incident.

4.4.2 RequestAuthorization Message

Description: This message is sent to the initiating RID system from the next upstream NP's RID system to provide information on the request status in the current network.

The following information is required for RequestAuthorization messages and is provided through:

RID Information:
RIDPolicy
RID message type, IncidentID, and destination policy information
Status of TraceRequest
RequestStatus class in RID schema

Standards for Encryption and Digital Signatures [RFC3275],[5]:
Digital signature of responding NP for authenticity of Trace Status Message, from the NP creating this message using XML digital signature.

A message is sent back to the initiating RID system of the trace as status notification. This message verifies that the next RID system in the path has received the message from the previous system in the path. This message also verifies that the trace is now continuing, has stopped, or is pending in the next upstream. The pending status would be automatically generated after a 2-minute timeout without system predefined or administrator action taken to approve or disapprove the trace continuance. If a Request

is denied, the originator and sending peer (if they are not the same) MUST both receive the message. This enables the sending peer the option to take action to stop or mitigate the traffic as close

to the source as possible.

4.4.3 Result Message

Description: This message indicates that the trace or investigation has been completed and provides the result. The Result message includes information on whether or not a source was found and the source information through the IncidentSource class. The Result information MUST go back to the originating RID system that began the investigation or trace. An NP may use any number of incident handling data sources to ascertain the true source of an attack. All of the possible information sources may or may not be readily tied into the RID communications system.

The following information is required for Result messages and will be provided through:

RID Information:
RIDPolicy
RID message type, IncidentID, and destination policy information
Incident Source
The IncidentSource class of the RID schema is used to note if a source was identified and the source(s) address.

IODEF Information:
Time Stamps (DetectTime, StartTime, EndTime, ReportTime)
Incident Identifier (Incident Class, IncidentID)
Trace number - used for multiple traces of a single incident, must be noted.
Confidence rating of Security Incident (Impact and Confidence Class)
System Class is used to list both the Source and Destination Information used in the attack and must note if the traffic is spoofed, thus requiring an upstream TraceRequest in RID.
History Class atype attribute is used to note any actions taken.
History class also notes any other background information including notes about the confidence level or rating of the result information.
Path information of nested RID systems, beginning with the request originator used in the trace using IODEF EventData with category set to infrastructure
The last NP listed is the NP, which located the source of the traffic (the NP sending the Result message)

Event, Record, and RecordItem Classes to include example packets and other information related to the incident [optional]
Note: Event information included here requires a second

instance of EventData from that used to convey NP path contact information.

Standards for Encryption and Digital Signatures [RFC3275]:

Digital signature of source NP for authenticity of Result Message, the NP creating this message using XML digital signature.

A message sent back to the initiating RID system to notify the associated CSIRT that the source has been located. The actual source information may or may not be included, depending on the policy of the network in which the client or host is attached. Any action taken by the NP to act upon the discovery of the source of a trace should be included. The NP may be able to automate the adjustment of filters at their border router to block outbound access for the machine(s) discovered as a part of the attack. The filters may be comprehensive enough to block all Internet access until the host has taken the appropriate action to resolve any security issues or to rate-limit the ingress traffic as close to the source as possible.

Security and privacy considerations discussed in sections 6 and 7 must be taken into account.

Note: The History Class has been expanded in IODEF to accommodate all of the possible actions taken as a result of a RID TraceRequest or Investigation request using the iodef:atype or action type attribute. The History class should be used to note all actions taken close to the source of a trace or incident using the most appropriate option for the type of action along with a description. The atype attribute in the Expectation class can also be used to request an appropriate action when a TraceRequest or Investigation request is made.

4.4.4 Investigation Message Request

Description: This message type is used when the source of the traffic is believed to be valid. The purpose of the Investigation message request is to leverage the existing bilateral peer relationships in order to notify the network provider closest to the source of the valid traffic that some event occurred, which may be a security-related incident.

The following information is required for Investigation messages and is provided through:

RID Information:
RID Policy
RID message type, IncidentID, and destination policy information

IODEF Information:
Time Stamps (DetectTime, StartTime, EndTime, ReportTime)

Incident Identifier (Incident Class, IncidentID)
Trace number - used for multiple traces of a single incident, must be noted.

Confidence rating of security incident (Impact and Confidence Class)
System Class is used to list both the Source and Destination Information used in the attack and must note if the traffic is spoofed, thus requiring an upstream TraceRequest in RID.
Expectation class should be used to request any specific actions to be taken close to the source.
Path information of nested RID systems, beginning with the request originator used in the trace using IODEF EventData with category set to infrastructure
Event, Record, and RecordItem Classes to include example packets and other information related to the incident. Note: Event information included here requires a second instance of EventData from that used to convey NP path contact information.

Standards for Encryption and Digital Signatures [RFC3275]:
Digital signature from initiating RID system, passed to all systems in upstream trace using XML digital signature.

Security considerations would include the ability to encrypt [3] the contents of the Investigation message request using the public key of the destination RID system. The incident number would increase as if it were a TraceRequest message in order to ensure uniqueness within the system. The relaying peers would also append their AS or RID system information as the request message was relayed along the web of network providers so that the Result message could utilize the same path as the set of trust relationships for the return message, thus indicating any actions taken. The request would also be recorded in both the state table of the initiating and destination NP RID system. The destination NP is responsible for any actions taken as a result of the request in adherence to any service level agreements or internal policies. The NP should confirm the traffic actually originated from the suspected system before taking any action and confirm the reason for the request. The request may be sent directly to a known RID System or routed by the source address of the attack using the message destination of RIDPolicy, SourceOfIncident.

Note: All intermediate parties must be able to view RIDPolicy information in order to properly direct RID messages.

4.4.5 Report Message

Description: This message or document is sent to a RID system to provide a report of a security incident. This message does not require any actions to be taken, except to file the report on the receiving RID system or associated database.

The following information is required for Report messages and will be provided through:

RID Information:
RID Policy
RID message type, IncidentID, and destination Policy information

The following data is recommended if available and can be provided through:

IODEF Information:
Time Stamps (DetectTime, StartTime, EndTime, ReportTime)
Incident Identifier (Incident Class, IncidentID)
Trace number - used for multiple traces of a single incident, must be noted.
Confidence rating of security incident (Impact and Confidence Class)
System Class is used to list both the Source and Destination Information used in the attack.
Event, Record, and RecordItem Classes to include example packets and other information related to the incident [optional].

Standards for Encryption and Digital Signatures [RFC3275]:
Digital signature from initiating RID system, passed to all systems receiving the report using XML digital signature.

Security considerations would include the ability to encrypt [3] the contents of the Report message request using the public key of the destination RID system. Senders of a Report message should note that the information may be used to correlate security incident information for the purpose of trending, pattern detection, etc., and may be shared with other parties unless otherwise agreed upon with the receiving RID system. Therefore, sending parties of a report message may obfuscate or remove destination addresses or other sensitive information before sending a report message. A Report message may be sent either to file an incident report or in response to an IncidentQuery and data sensitivity must be considered in both cases. The NP path information is not necessary for this message as it will be communicated directly between two trusted RID systems.

4.4.6 IncidentQuery

Description: The IncidentQuery message is used to request incident information from a trusted RID system. The request can include the incident number, if known, or detailed information about the incident. If the incident number is known, the report message containing the incident information can easily be returned to the trusted requestor using automated methods. If an example packet or other unique information is included in the IncidentQuery, the

return report may be automated; otherwise, analyst intervention may be required.

The following information must be used for an IncidentQuery message

and is provided through:

RID Information:
RID Policy
RID message type, IncidentID, and destination Policy information

IODEF Information [optional]:
Time Stamps (DetectTime, StartTime, EndTime, ReportTime)
Incident Identifier (Incident Class, IncidentID)
Trace number - used for multiple traces of a single incident, must be noted.
Confidence rating of security incident (Impact and Confidence Class)
System Class is used to list both the Source and Destination Information used in the attack.
Event, Record, and RecordItem Classes to include example packets and other information related to the incident [optional].

Standards for Encryption and Digital Signatures [RFC3275]:
Digital signature from initiating RID system, passed to all systems receiving the IncidentQuery using XML digital signature. If a packet is not included, the signature may be based on the RIDPolicy class.

The proper response to the IncidentQuery message is a Report message. Multiple incidents may be returned for a single query if an incident type is requested. In this case, the receiving system would send an IODEF document containing multiple incidents or all instances of an incident. The system sending the reply may pre-set a limit to the number of documents returned in one report. The recommended limit is 5 to prevent the documents from becoming too large. Other transfer methods may be suited better than RID for large transfers of data. The Confidence rating may be used in the IncidentQuery message to select only incidents with an equal or higher confidence rating than what is specified. This may be used for cases when information is gathered on a type of incident but not on specifics about a single incident. Source and destination information may not be needed if the IncidentQuery is intended to gather data about a specific type of incident as well.

4.5 RID Communication Exchanges

The following section outlines the communication flows for RID and also provides examples of messages. The proper response to a TraceRequest is a RequestAuthorization message. The RequestAuthorization message lets the requestor know if the trace will continue through the next upstream network. If there is a

problem with the request, such as a failure to validate the digital signature or decrypt the request, a RequestAuthorization message MUST be sent to the requestor and the downstream peer (if they are not one in the same) providing the reason why the message could not

be processed. Assuming the trace continued, additional TraceRequests with the response of a TraceAuthorization message would occur passing the request upstream in the path to the source of the traffic related to the incident. Once a source is found, a Result message is sent to the originator of the trace, as determined by the NP path information provided through the document instance of EventData, where contact is set to infrastructure. The NP path information is also used when sending the RequestAuthorization messages to the first entry (the trace originator) and the last nested entry (the downstream peer). The Result message is encrypted [3] for the originator providing information about the incident source and any actions taken. If the originator fails to decrypt or authenticate the Result message, a RequestAuthorization message is sent in response, otherwise no return message is sent. If a RequestAuthorization message is sent with the RequestStatus set to denied, a downstream peer receiving this message may choose to take action to stop or mitigate the traffic at that point in the network, as close to the source as possible. If the downstream peer chooses this option, they would send a Result message to the trace originator.

Note: for each example listed below, [RFC3330] addresses were used. Assume each IP address listed is actually a separate network range held by different NPs. Addresses were used from /27 network ranges.

4.5.1 Upstream Trace Communication Flow

The diagram below outlines the RID TraceRequest communication flow between RID systems on different networks tracing an attack.

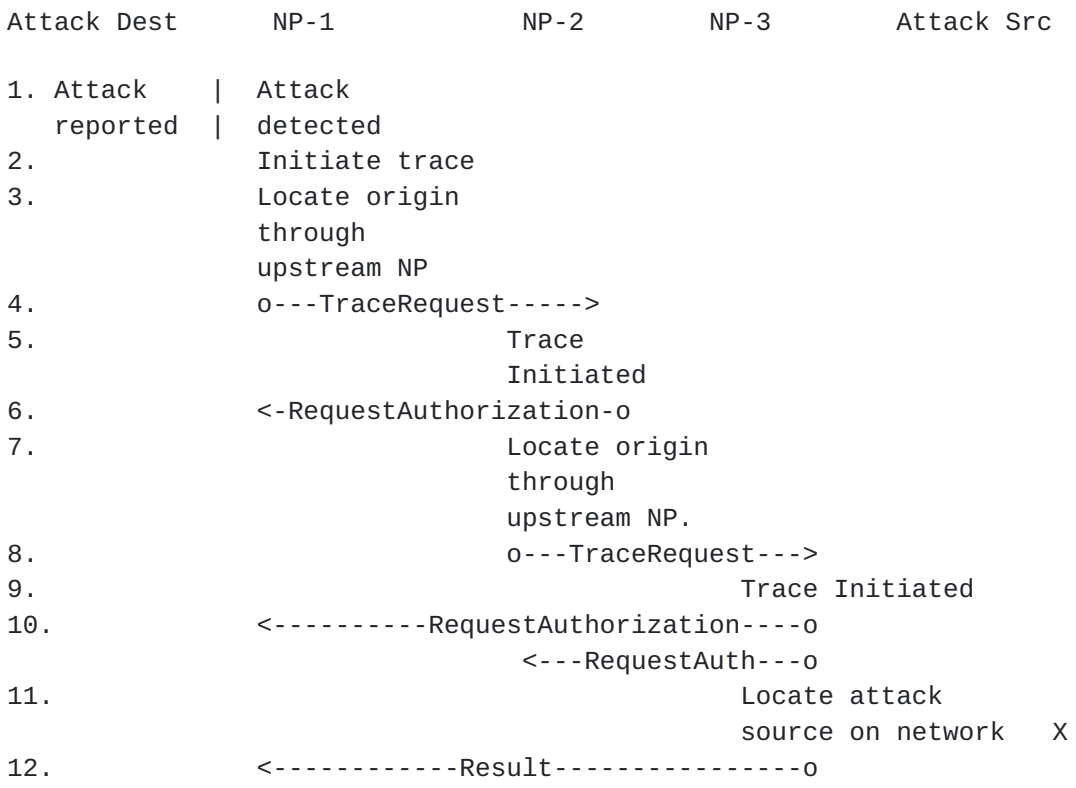


Figure 7: TraceRequest Communication Flow

Before a trace is initiated, the RID system should verify if an instance of the trace or a similar request is not active. The traces may be resource intensive, therefore providers need to be able to detect potential abuse of the system or unintentional resource drains. Information such as the source and destination information, associated packets, and the incident may be desirable to maintain for a period of time determined by administrators.

The communication flow demonstrates that a RequestAuthorization message is sent to both the downstream peer and the original requester. If a TraceRequest is denied, the downstream peer has the option to take an action and respond with a Result message. The originator or the request may follow up with the downstream peer of the NP involved using an Investigation request to ensure an action is taken if no response is received. Nothing precludes the originator of the request from initiating a new trace request bypassing the NP, which denied the request if a trace is needed

beyond that point. Another option may also be for the initiator to send an Investigation request to an NP upstream of the NP which denied the request if enough information was gathered to discern the true source of the attack traffic from the incident handling

information.

4.5.1.1 RID TraceRequest Example

The example listed is of a TraceRequest based on the incident report example from the IODEF document. The RID extension classes were included as appropriate for a TraceRequest message using the RIDPolicy class. The example given is that of a CSIRT reporting a DoS attack in progress to the upstream NP. The request asks the next NP to continue the trace and have the traffic mitigated closer to the source of the traffic.

```
<iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="TraceRequest"
                       MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="IntraConsortium"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.3</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#207-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
</iodef-rid:RID>
<!-- IODEF-Document accompanied by the above RID -->
<iodef:IODEF-Document version="1.00"
                      xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef:Incident restriction="need-to-know" purpose="traceback">
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#207-1
    </iodef:IncidentID>
    <iodef:DetectTime>2004-02-02T22:49:24+00:00</iodef:DetectTime>
    <iodef:StartTime>2004-02-02T22:19:24+00:00</iodef:StartTime>
    <iodef:ReportTime>2004-02-02T23:20:24+00:00</iodef:ReportTime>
    <iodef:Description>Host involved in DOS attack</iodef:Description>
    <iodef:Assessment>
      <iodef:Impact severity="low" completion="failed" type="dos"/>
    </iodef:Assessment>
    <iodef:Contact role="creator" type="organization">
      <iodef:ContactName>Constituency-contact for 192.0.2.35
      </iodef:ContactName>
      <iodef:Email>Constituency-contact@192.0.2.35</iodef:Email>
    </iodef:Contact>
    <iodef:EventData>
      <iodef:Flow>
        <iodef:System category="source">
```

```
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.35
            </iodef:Address>
          </iodef:Node>
```

```
          <iodef:Service>
            <iodef:port>38765</iodef:port>
          </iodef:Service>
        </iodef:System>
        <iodef:System category="target">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.67
            </iodef:Address>
          </iodef:Node>
          <iodef:Service>
            <iodef:port>80</iodef:port>
          </iodef:Service>
        </iodef:System>
      </iodef:Flow>
      <iodef:Expectation severity="high" action="rate-limit-host">
        <iodef:Description>
          Rate limit traffic close to source
        </iodef:Description>
      </iodef:Expectation>
      <iodef:Record>
        <iodef:RecordData>
          <iodef:Description>
            The IPv4 packet included was used in the described attack
          </iodef:Description>
          <iodef:RecordItem dtype="ipv4-packet">450000522ad9
             0000ff06c41fc0a801020a010102976d0050103e020810d9
             4a1350021000ad6700005468616e6b20796f7520666f7220
             6361726566756c6c792072656164696e6720746869732052
             46432e0a
          </iodef:RecordItem>
        </iodef:RecordData>
      </iodef:Record>
    </iodef:EventData>
    <iodef:History>
      <iodef:HistoryItem>
        <iodef:DateTime>2001-09-14T08:19:01+00:00</iodef:DateTime>
        <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
          CSIRT-FOR-OUR-DOMAIN#207-1
        </iodef:IncidentID>
        <iodef:Description>
          Notification sent to next upstream NP closer to 192.0.2.35
        </iodef:Description>
      </iodef:HistoryItem>
    </iodef:History>
  </iodef:Incident>
</iodef:IODEF-Document>

<!-- Digital signature accompanied by above RID and IODEF -->
```

```
<Envelope xmlns="urn:envelope"
          xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0"
          xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0">
  <iodef:IODEF-Document>
```

```
    <iodef:Incident>
      <iodef:EventData>
        <iodef:Record>
          <iodef:RecordData>
            <iodef:RecordItem type="ipv4-packet">450000522ad9
             0000ff06c41fc0a801020a010102976d0050103e020810d9
             4a1350021000ad6700005468616e6b20796f7520666f7220
             6361726566756c6c7920726164696e6720746869732052
             46432e0a
            </iodef:RecordItem>
          </iodef:RecordData>
        </iodef:Record>
      </iodef:EventData>
    </iodef:Incident>
  </iodef:IODEF-Document>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod
         Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
         20010315#WithComments"/>
      <SignatureMethod
         Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm=
           "http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod
           Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>KiI5+6SnFAs429VNwsoJjHPplmo=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>
      VvyXqCzjoW0m2NdxNeToXQcqcSM80W+JMW+Kn01cS3z3KQwCPeswzg==
    </SignatureValue>
    <KeyInfo>
      <KeyValue>
        <DSAKeyValue>
          <P>/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9j
             QTxeEu0ImbzRMqzVDZkVG9xD7nN1kuFw==</P>
          <Q>li7dzDacuo67Jg7mtqEm2TRuOMU=</Q>
          <G>Z4Rxsnqc9E7pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/XPaF5
             Bpsy4pNWMOHCBiNU0NogpsQW5QvnlMpA==</G>
          <Y>VFWTD4I/aKni4YhDyYxAJozmj1iAzPLw9Wwd5B+Z9J5E7lHjcAJ+bs
             HifTyYdnj+roGzy4o09YntYD8zneQ7lw==</Y>
        </DSAKeyValue>
      </KeyValue>
    </KeyInfo>
```

```
  </Signature>
</Envelope>
```

4.5.1.2 RequestAuthorization Message Example

The example RequestAuthorization message is in response to the TraceRequest message listed above. The NP that received the request is responding to approve the trace continuance in their network.

```
<iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="RequestAuthorization"
                       MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="IntraConsortium"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.67</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#207-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
  <iodef-rid:RequestStatus AuthorizationStatus="Approved"/>
</iodef-rid:RID>
```

4.5.1.3 Result Message Example

The example Result message is in response to the TraceRequest listed above. This message types only comes after a RequestAuthorization within the TraceRequest flow of messages. It may be a direct response to an Investigation request. This message provides information about the source of the attack and the actions taken to mitigate the traffic.

```
<iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="Result"
                       MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="IntraConsortium"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.67</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#207-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
  <iodef-rid:IncidentSource>
    <iodef-rid:SourceFound>true</iodef-rid:SourceFound>
    <iodef:Node>
```

```
      <iodef:Address category="ipv4-addr">192.0.2.37</iodef:Address>
    </iodef:Node>
  </iodef-rid:IncidentSource>
</iodef-rid:RID>
```

```
<!-- IODEF-Document accompanied by the above RID -->
<iodef:IODEF-Document version="1.00"
                      xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef:Incident restriction="need-to-know" purpose="traceback">
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#207-1
    </iodef:IncidentID>
    <iodef:DetectTime>2004-02-02T22:49:24+00:00</iodef:DetectTime>
    <iodef:StartTime>2004-02-02T22:19:24+00:00</iodef:StartTime>
    <iodef:ReportTime>2004-02-02T23:20:24+00:00</iodef:ReportTime>
    <iodef:Description>Host involved in DOS attack</iodef:Description>
    <iodef:Assessment>
      <iodef:Impact severity="low" completion="failed" type="dos"/>
    </iodef:Assessment>
    <iodef:Contact role="creator" type="organization">
      <iodef:ContactName>Constituency-contact for 192.0.2.35
      </iodef:ContactName>
      <iodef:Email>Constituency-contact@192.0.2.35</iodef:Email>
    </iodef:Contact>
    <iodef:EventData>
      <iodef:Contact role="admin" type="organization">
        <iodef:ContactName>Admin-contact for 192.0.2.35
        </iodef:ContactName>
        <iodef:Email>Admin-contact@10.1.1.2</iodef:Email>
      </iodef:Contact>
      <iodef:Flow>
        <iodef:System category="intermediate">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.35
            </iodef:Address>
          </iodef:Node>
        </iodef:System>
      </iodef:Flow>
      <iodef:EventData>
        <iodef:Contact role="admin" type="organization">
          <iodef:ContactName>Admin-contact for 192.0.2.3
          </iodef:ContactName>
          <iodef:Email>Admin-contact@192.0.2.3</iodef:Email>
        </iodef:Contact>
        <iodef:Flow>
          <iodef:System category="intermediate">
            <iodef:Node>
              <iodef:Address category="ipv4-addr">192.0.2.3
              </iodef:Address>
            </iodef:Node>
          </iodef:System>
        </iodef:Flow>
      </iodef:EventData>
```

```
    </iodef:EventData>
    <iodef:EventData>
      <iodef:Flow>
        <iodef:System category="source">
```

```
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.35
            </iodef:Address>
          </iodef:Node>
          <iodef:Service>
            <iodef:port>38765</iodef:port>
          </iodef:Service>
        </iodef:System>
        <iodef:System category="target">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.67
            </iodef:Address>
          </iodef:Node>
          <iodef:Service>
            <iodef:port>80</iodef:port>
          </iodef:Service>
        </iodef:System>
      </iodef:Flow>
      <iodef:Expectation severity="high" action="rate-limit-host">
        <iodef:Description>
          Rate limit traffic close to source
        </iodef:Description>
      </iodef:Expectation>
      <iodef:Record>
        <iodef:RecordData>
          <iodef:Description>
            The IPv4 packet included was used in the described attack
          </iodef:Description>
          <iodef:RecordItem dtype="ipv4-packet">450000522ad9
          0000ff06c41fc0a801020a010102976d0050103e020810d9
          4a1350021000ad6700005468616e6b20796f7520666f7220
          6361726566756c6c7920726164696e6720746869732052
          46432e0a
          </iodef:RecordItem>
        </iodef:RecordData>
      </iodef:Record>
    </iodef:EventData>
    <iodef:History>
      <iodef:HistoryItem>
        <iodef:DateTime>2004-02-02T22:53:01+00:00</iodef:DateTime>
        <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
          CSIRT-FOR-OUR-DOMAIN#207-1
        </iodef:IncidentID>
        <iodef:Description>
          Notification sent to next upstream NP closer to 192.0.2.35
        </iodef:Description>
      </iodef:HistoryItem>
      <iodef:HistoryItem action="rate-limit-host">
```

```
        <iodef:DateTime>2004-02-02T23:07:21+00:00</iodef:DateTime>
        <iodef:IncidentID name="CSIRT-FOR-NP3">
          CSIRT-FOR-NP3#3291-1
        </iodef:IncidentID>
```

```
        <iodef:Description>
          Host rate limited for 24 hours
        </iodef:Description>
      </iodef:HistoryItem>
    </iodef:History>
  </iodef:Incident>
</iodef:IODEF-Document>
```

4.5.2 Investigation Request Communication Flow

The diagram below outlines the RID Investigation Request communication flow between RID systems on different networks for a security incident with a known source address. The proper response to an Investigation request is a Result message. If there is a problem with the request, such as a failure to validate the digital signature or decrypt the request, a RequestAuthorization message is sent to the requestor. The RequestAuthorization message should provide the reason why the message could not be processed.

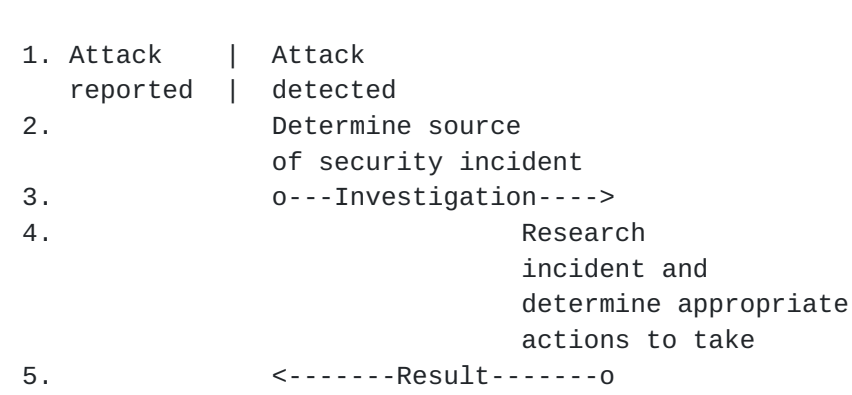


Figure 8: Investigation Communication Flow

4.5.2.1 Example Investigation Request

The following example only includes the RID-specific details. The IODEF and security measures are similar to the TraceRequest information, with the exception that the source is known and the receiving RID system is known to be close to the source. The source known is indicated in the IODEF document, which allows for incident sources to be listed as spoofed, if appropriate.

```
<iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="Investigation"
                       MsgDestination="SourceOfIncident">
    <iodef-rid:PolicyRegion region="PeerToPeer"/>
    <iodef:Node>
```

```
      <iodef:Address category="ipv4-addr">192.0.2.98</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
```

```
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#208-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
</iodef-rid:RID>
<!-- IODEF-Document accompanied by the above RID -->
<iodef:IODEF-Document version="1.00"
                      xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef:Incident restriction="need-to-know" purpose="other">
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#208-1
    </iodef:IncidentID>
    <iodef:DetectTime>2004-02-05T08:13:33+00:00</iodef:DetectTime>
    <iodef:StartTime>2004-02-05T08:13:31+00:00</iodef:StartTime>
    <iodef:EndTime>2004-02-05T08:13:33+00:00</iodef:EndTime>
    <iodef:ReportTime>2004-02-05T08:13:35+00:00</iodef:ReportTime>
    <iodef:Description>Host involved in DOS attack</iodef:Description>
    <iodef:Assessment>
      <iodef:Impact severity="low" completion="failed" type="recon"/>
    </iodef:Assessment>
    <iodef:Contact role="creator" type="organization">
      <iodef:ContactName>Constituency-contact for 192.0.2.35
      </iodef:ContactName>
      <iodef:Email>Constituency-contact@10.1.1.2</iodef:Email>
    </iodef:Contact>
    <iodef:EventData>
      <iodef:Flow>
        <iodef:System category="source">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.35
            </iodef:Address>
          </iodef:Node>
          <iodef:Service>
            <iodef:port>41421</iodef:port>
          </iodef:Service>
        </iodef:System>
        <iodef:System category="target">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.67
            </iodef:Address>
          </iodef:Node>
          <iodef:Service>
            <iodef:port>80</iodef:port>
          </iodef:Service>
        </iodef:System>
      </iodef:Flow>
      <iodef:Expectation severity="high" action="investigate">
        <iodef:Description>
```

```
          Investigate whether source has been compromised
        </iodef:Description>
      </iodef:Expectation>
    </iodef:EventData>
```

```
    <iodef:History>
      <iodef:HistoryItem>
        <iodef:DateTime>2004-02-05T08:19:01+00:00</iodef:DateTime>
        <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
          CSIRT-FOR-OUR-DOMAIN#208-1
        </iodef:IncidentID>
        <iodef:Description>
          Investigation request sent to NP for 192.0.2.35
        </iodef:Description>
      </iodef:HistoryItem>
    </iodef:History>
  </iodef:Incident>
</iodef:IODEF-Document>
```

4.5.2.2 RequestAuthorization Message Example

The example RequestAuthorization message is in response to the Investigation request listed above. The NP that received the request was unable to validate the digital signature used to authenticate the sending RID system.

```
<iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="RequestAuthorization"
                       MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="IntraConsortium"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.67</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#208-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
  <iodef-rid:RequestStatus AutorizationStatus="Denied"
                           Justification="Authentication"/>
</iodef-rid:RID>
```

4.5.3 Report Communication

The diagram below outlines the RID Report communication flow between RID systems on different networks.

```
     NP-1                          NP-2
  1. Generate incident information
     and prepare report message
  2.              o-------Report------->
  3.                             File report in database
```

Figure 9: Report Communication Flow

The Report communication flow is used to provide information on specific incidents detected on the network. Incident information may be shared between CSIRTS or participating RID hosts using this format. When a report is received, the RID system must verify that the report has not already been filed. The incident number and incident data, such as the hexidecimal packet and incident class information, can be used to compare with existing database entries. The Report message typically does not have a response. If there is a problem with the Report message, such as a failure to validate the digital signature [RFC3275] or decrypt the request, a RequestAuthorization message is sent to the requestor. The RequestAuthorization message should provide the reason why the message could not be processed.

4.5.3.1 Report Example

The following example only includes the RID-specific details. This report is an unsolicited report message that includes an IPv4 packet. The IODEF document and digital signature would be similar to the first example provided for this case.

```
<iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="Report" MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="PeerToPeer"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.130</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#209-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
</iodef-rid:RID>

<!-- IODEF-Document accompanied by the above RID -->
<iodef:IODEF-Document version="1.00"
                      xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef:Incident restriction="need-to-know" purpose="reporting">
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#209-1
    </iodef:IncidentID>
    <iodef:DetectTime>2004-02-05T10:21:08+00:00</iodef:DetectTime>
    <iodef:StartTime>2004-02-05T10:21:05+00:00</iodef:StartTime>
    <iodef:EndTime>2004-02-05T10:35:00+00:00</iodef:EndTime>
    <iodef:ReportTime>2004-02-05T10:27:38+00:00</iodef:ReportTime>
    <iodef:Description>Host illicitly accessed admin account
```

```
    </iodef:Description>
    <iodef:Assessment>
      <iodef:Impact severity="high" completion="succeeded"
                    type="admin"/>
```

```
      <iodef:Confidence rating="high"/>
    </iodef:Assessment>
    <iodef:Contact role="creator" type="organization">
      <iodef:ContactName>Constituency-contact for 192.0.2.35
      </iodef:ContactName>
      <iodef:Email>Constituency-contact@10.1.1.2</iodef:Email>
    </iodef:Contact>
    <iodef:EventData>
      <iodef:Flow>
        <iodef:System category="source">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.35
            </iodef:Address>
          </iodef:Node>
          <iodef:Service>
            <iodef:port>32821</iodef:port>
          </iodef:Service>
        </iodef:System>
        <iodef:System category="target">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.67
            </iodef:Address>
          </iodef:Node>
          <iodef:Service>
            <iodef:port>22</iodef:port>
          </iodef:Service>
        </iodef:System>
      </iodef:Flow>
    </iodef:EventData>
    <iodef:History>
      <iodef:HistoryItem>
        <iodef:DateTime>2004-02-05T10:28:00+00:00</iodef:DateTime>
        <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
          CSIRT-FOR-OUR-DOMAIN#209-1
        </iodef:IncidentID>
        <iodef:Description>
          Incident report sent to NP for 192.0.2.35
        </iodef:Description>
      </iodef:HistoryItem>
    </iodef:History>
  </iodef:Incident>
</iodef:IODEF-Document>
```

4.5.4 IncidentQuery Communication Flow

The diagram below outlines the RID IncidentQuery communication flow between RID systems on different networks.

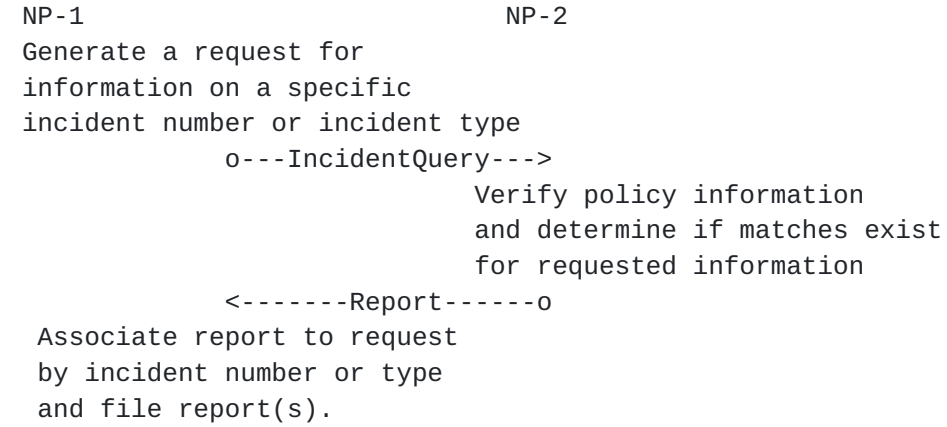


Figure 10: IncidentQuery Communication Flow

The IncidentQuery message communication receives a response of a Report message. If the Report message is empty, the responding host did not have information available to share with the requestor. The incident number and responding RID system, as well as the transport, assist in the association of the request and response since a report can be filed and is not always solicited. If there is a problem with the IncidentQuery message, such as a failure to validate the digital signature or decrypt the request, a RequestAuthorization message is sent to the requestor. The RequestAuthorization message should provide the reason why the message could not be processed.

4.5.4.1 IncidentQuery Example

The IncidentQuery request may be received in several formats as a result of the type of query being performed. If the incident number is the only information provided, the IODEF document and IP packet data may not be needed to complete the request. However, if a type of incident is requested, the incident number remains null and the IP packet data will not be included in the IODEF RecordItem class and the other incident information is the main source for comparison. In the case in which an incident number may not be the same between CSIRTS, either or both the incident number and/or IP packet information can be provided and used for comparison on the receiving RID system to generate a Report message(s).

```
<iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
```

```
              xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="IncidentQuery"
                       MsgDestination="RIDSystem">
```

```
    <iodef-rid:PolicyRegion region="PeerToPeer"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.3</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#210-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
</iodef-rid:RID>
```

5. RID Schema Definition

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
 xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0"
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 targetNamespace="urn:ietf:params:xml:ns:iodef-rid-1.0"
 elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:import namespace="urn:ietf:params:xml:ns:iodef-1.0"
 schemaLocation="urn:ietf:params:xml:ns:iodef-1.0"/>

<xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
 schemaLocation=
 "http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
<!-- ****************************************************************
*****************************************************************
***  Real-time Inter-network Defense - RID XML Schema             ***
***    Namespace - iodef-rid, August 2006                         ***
***    The namespace is defined to support transport of IODEF     ***
***     documents for exchanging incident information.            ***
*****************************************************************
-->
<!--RID acts as an envelope for IODEF documents to support the exchange
    of messages-->
<!--
====== Real-Time Inter-network Defense - RID ======
====  Suggested definition for RID messaging ======
 -->
<xs:annotation>
  <xs:documentation>XML Schema wrapper for IODEF</xs:documentation>
</xs:annotation>
<xs:element name="RID" type="iodef-rid:RIDType"/>
  <xs:complexType name="RIDType">
    <xs:sequence>
      <xs:element ref="iodef-rid:RIDPolicy" minOccurs="0"/>
      <xs:element ref="iodef-rid:RequestStatus" minOccurs="0"/>
      <xs:element ref="iodef-rid:IncidentSource" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
<!--Used in RequestAuthorization Message for RID-->
<xs:element name="RequestStatus" type="iodef-rid:RequestStatusType"/>
  <xs:complexType name="RequestStatusType">
     <xs:attribute name="AuthorizationStatus" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
          <xs:whiteSpace value="collapse"/>
            <xs:enumeration value="Approved"/>
```

```
            <xs:enumeration value="Denied"/>
            <xs:enumeration value="Pending"/>
            <xs:enumeration value="ext-value"/>
          </xs:restriction>
```

```
       </xs:simpleType>
     </xs:attribute>
     <xs:attribute name="ext-AuthorizationStatus"
                   type="xs:string" use="optional"/>
     <xs:attribute name="Justification">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
          <xs:whiteSpace value="collapse"/>
            <xs:enumeration value="SystemResource"/>
            <xs:enumeration value="Authentication"/>
            <xs:enumeration value="AuthenticationOrigin"/>
            <xs:enumeration value="Encryption"/>
            <xs:enumeration value="Other"/>
            <xs:enumeration value="ext-value"/>
          </xs:restriction>
        </xs:simpleType>
     </xs:attribute>
     <xs:attribute name="ext-Justification"
                   type="xs:string" use="optional"/>
    <xs:attribute name="restriction" type="iodef:restriction-type"/>
  </xs:complexType>
<!--Incident Source Information for Result Message-->
<xs:element name="IncidentSource" type="iodef-rid:IncidentSourceType"/>
  <xs:complexType name="IncidentSourceType">
    <xs:sequence>
      <xs:element ref="iodef-rid:SourceFound"/>
      <xs:element ref="iodef:Node" minOccurs="0"
          maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="restriction" type="iodef:restriction-type"/>
  </xs:complexType>
  <xs:element name="SourceFound" type="xs:boolean"/>
<!--
====== Real-Time Inter-network Defense Policy - RIDPolicy ======
======  Definition for RIDPolicy for messaging
 -->
<xs:annotation>
 <xs:documentation>RID Policy used for transport of
     messages</xs:documentation>
</xs:annotation>
<!-- RidPolicy information with setting information listed in RID
     documentation -->
<xs:element name="RIDPolicy" type="iodef-rid:RIDPolicyType"/>
  <xs:complexType name="RIDPolicyType">
    <xs:sequence>
      <xs:element ref="iodef-rid:PolicyRegion" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Node"/>
      <xs:element ref="iodef-rid:TrafficType" maxOccurs="unbounded"/>
```

```
      <xs:element ref="iodef:IncidentID" minOccurs="0"/>
    </xs:sequence>
   <xs:attribute name="MsgType" use="required">
    <xs:simpleType>
```

```
      <xs:restriction base="xs:NMTOKEN">
      <xs:whiteSpace value="collapse"/>
        <xs:enumeration value="TraceRequest"/>
        <xs:enumeration value="RequestAuthorization"/>
        <xs:enumeration value="Result"/>
        <xs:enumeration value="Investigation"/>
        <xs:enumeration value="Report"/>
        <xs:enumeration value="IncidentQuery"/>
        <xs:enumeration value="ext-value"/>
      </xs:restriction>
    </xs:simpleType>
   </xs:attribute>
  <xs:attribute name="ext-MsgType" type="xs:string" use="optional"/>
  <xs:attribute name="MsgDestination" use="required">
    <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
      <xs:whiteSpace value="collapse"/>
        <xs:enumeration value="RIDSystem"/>
        <xs:enumeration value="SourceOfIncident"/>
        <xs:enumeration value="ext-value"/>
      </xs:restriction>
    </xs:simpleType>
   </xs:attribute>
  <xs:attribute name="ext-MsgDestination" type="xs:string"
                use="optional"/>
   </xs:complexType>
  <xs:element name="PolicyRegion">
    <xs:complexType>
     <xs:attribute name="region" use="required">
      <xs:simpleType>
       <xs:restriction base="xs:NMTOKEN">
       <xs:whiteSpace value="collapse"/>
         <xs:enumeration value="ClientToNP"/>
         <xs:enumeration value="NPToClient"/>
         <xs:enumeration value="IntraConsortium"/>
         <xs:enumeration value="PeerToPeer"/>
         <xs:enumeration value="BetweenConsortiums"/>
         <xs:enumeration value="AcrossNationalBoundaries"/>
         <xs:enumeration value="ext-value"/>
       </xs:restriction>
      </xs:simpleType>
     </xs:attribute>
     <xs:attribute name="ext-region"
                   type="xs:string" use="optional"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="TrafficType" default="Attack">
    <xs:complexType>
```

```
     <xs:attribute name="type" use="required">
      <xs:simpleType>
       <xs:restriction base="xs:NMTOKEN">
       <xs:whiteSpace value="collapse"/>
```

```
        <xs:enumeration value="Attack"/>
        <xs:enumeration value="Network"/>
        <xs:enumeration value="Content"/>
        <xs:enumeration value="OfficialBusiness"/>
        <xs:enumeration value="Other"/>
        <xs:enumeration value="ext-value"/>
      </xs:restriction>
     </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="ext-type"
                  type="xs:string" use="optional"/>
   </xs:complexType>
 </xs:element>
</xs:schema>
```

6. Message Transport

The transport specifications is fully defined in a separate document [RFCYYYY]. The specified transport protocols must use encryption to provide an additional level of security, integrity, and authentication through bi-directional certificate usage. Any subsequent transport method defined should take advantage of existing standards for ease of implementation and integration of RID systems. Session encryption for the transport of RID messages is enforced in the transport specification. The privacy and security considerations are addressed fully in RID to protect sensitive portions of documents and provide a method to authenticate the messages. Therefore, RID messages do not rely on the security provided by the transport layer alone. The encryption requirements and considerations for RID are discussed in the Security section of this document.

XML security functions such as digital signature [RFC3275] and encryption [3] provide a standards-based method to encrypt and digitally sign RID messages. RID messages specify system use and privacy guidelines through the RIDPolicy class. Public key infrastructure (PKI) provides the base for authentication and authorization, encryption, and digital signatures to establish trust relationships between members of a RID consortium or a peering consortium.

XML security functions such as the digital signature [RFC3275] and encryption [3] can be used within the contents of the message for privacy and security in cases for which certain elements must remain encrypted or signed as they traverse the path of a trace. For example, the digital signature on a TraceRequest can be used to verify the identity of the trace originator. The use of the XML security features in RID messaging is in accordance with the specifications for the IODEF model; however, the use requirements may differ since RID also incorporates communication of security incident information.

6.1 Message Delivery Protocol - Integrity and Authentication

The RID protocol must be able to guarantee delivery and meet the necessary security requirements of a state-of-the-art protocol. In order to guarantee delivery, TCP should be considered as the underlying protocol within the current network standard practices.

Security considerations must include the integrity, authentication, privacy, and authorization of the messages sent between RID communication or IHS systems. The communication between RID systems must be authenticated and encrypted to ensure the integrity

of the messages and the RID systems involved in the trace. Another concern that needs to be addressed is authentication for a request that traverses multiple networks. In this scenario, systems in the path of the multi-hop TraceRequest need to authorize a trace from

not only their neighbor network, but also from the initiating RID system as discussed in section 6.3. Several methods can be used to ensure integrity and privacy of the communication.

The transport mechanism selected (HTTPS, BEEP, etc.) may be agreed upon by a consortium using RID messaging to ensure consistency among the peers. Consortiums may vary their selected transport mechanisms and thus must decide upon a mutual protocol to use for transport when communicating with peers in a neighboring consortium using RID. RID systems MUST implement and deploy HTTPS and optionally support other protocols such as BEEP. RID, the XML security functions, and transport protocols must properly integrate with a public key infrastructure (PKI) managed by the consortium or one managed by a trusted entity. For the Internet, an example of an existing effort that could be leveraged to provide the supporting PKI could be the American Registry for Internet Numbers (ARIN) and Regional Internet Registry's (RIR) PKI hierarchy. Consortiums are discussed in the security and privacy sections.

6.2 Transport Communication

Out-of-band communications dedicated to NP interaction for RID messaging would provide additional security as well as guaranteed bandwidth during a denial-of-service attack. For example, an out-of-band channel may consist of logical paths defined over the existing network. Out-of-band communications may not be possible between all network providers, but should be considered to protect the network management systems used for RID messaging. Methods to protect the data transport may also be provided through session encryption.

In order to address the integrity and authenticity of messages, transport encryption MUST be used to secure the traffic sent between RID systems. Systems with predefined relationships for RID would include those who peer within a consortium with agreed-upon appropriate use regulations and for peering consortiums. Trust relationships may also be defined through a bridged or hierarchical PKI in which both peers belong.

Systems used to send authenticated RID messages between networks MUST use a secured system and interface to connect to a border Network's RID systems. Each connection to a RID system must meet the security requirements agreed upon through the consortium regulations, peering, or SLAs. The RID system must only listen for and send RID messages on the designated port, which also must be over an encrypted tunnel meeting the minimum requirement of algorithms and key lengths established by the consortium, peering,

or SLA. The selected cryptographic algorithms for symmetric encryption, digital signatures, and hash functions must meet minimum security levels of the times. The encryption strength must adhere to import and export regulations of the involved countries

for data exchange.

6.3 Authentication of RID Protocol

In order to ensure the authenticity of the RID messages, a message authentication scheme is used to secure the protocol. XML security functions, utilized in RID requires a trust center such as a PKI for the distribution of credentials to provide the necessary level of security for this protocol. Layered transport protocols also utilize encryption and rely on a trust center. Public key certificate pairs issued by a trusted Certificate Authority (CA) MAY be used to provide the necessary level of authentication and encryption for the RID protocol. The CA used for RID messaging must be trusted by all involved parties and may take advantage of similar efforts, such as the Internet2 federated PKI or the ARIN/RIR effort to provide PKI to network providers. The PKI infrastructure used for authentication would also provide the necessary certificates needed for encryption via either Transport Layer Security (TLS) used in the HTTPS protocol, BEEP profile, or Secure MIME (S/MIME).

The use of pre-shared keys may be considered for authentication. If this option is selected, the following standard MUST be followed: Pre-Shared Key Ciphersuites for Transport Layer Security [RFC4279].

Hosts receiving a RID message MUST be able to verify that the sender of the request is valid and trusted. Using digital signatures on a hash of the RID message with an X.509 version 3 certificate issued by a trusted party MUST be used to authenticate the request. The X.509 version 3 specifications as well as the digital signature specifications and path validation standards set forth in [RFC5280] and [RFC3379] MUST be followed in order to interoperate with a PKI designed for similar purposes. The IODEF specification must be followed for digital signatures to provide the authentication and integrity aspects required for secure messaging between network providers. The use of digital signatures in RID XML messages MUST follow the World Wide Web Consortium (W3C) recommendations for signature syntax and processing when either the XML encryption [3] or digital signature [5], [RFC3275] is used within a document. Transport specifications are detailed in a separate document.

An optional extension to the authentication scheme would be to incorporate the use of attribute certificates to provide authorization capabilities as described in [RFC3281]. This may be useful as messages are sent from network peers to determine authorization levels based on the attribute information in the

certificate, which could be used to determine priority of a trace request. The attribute information might be used to determine if a request should be processed automatically or if human intervention is required.

6.3.1 Multi-hop TraceRequest Authentication

Bilateral trust relations between network providers ensure the authenticity of requests for TraceRequests from immediate peers in the web of networks formed to provide the traceback capability. A network provider several hops into the path of the RID trace must trust the information from its and the previous trust relationships in the downstream path. For practical reasons, the NPs may want to prioritize incident handling events based upon the immediate peer for a trace request, the originator, and the listed confidence rating for the incident. In order to provide a higher assurance level of the authenticity of the TraceRequest, the originating RID system is included in the TraceRequest along with contact information and the information of all RID systems in the path the trace has taken. This information is provided through the IODEF EventData class nesting the list of systems and contacts involved in a trace, while setting the category attribute to infrastructure.

A second measure must be taken to ensure the identity of the originating RID system. The originating RID system MUST include a digital signature in the TraceRequest sent to all systems in the upstream path. The digital signature from the RID system is performed on the RecordItem class of the IODEF following the XML digital signature specifications from W3C [5] using a detached signature. The signature MUST be passed to all parties that receive a TraceRequest, and each party MUST be able to perform full path validation on the digital signature. Full path validation verifies the chaining relationship to a trusted root and also performs certificate revocation check. In order to accommodate that requirement, the IP packet in the RecordItem data MUST remain unchanged as a request is passed along between providers and is the only element for which the signature is applied. If additional packets are included in the document at upstream peers, the initial packet MUST still remain with the detached signature. The subsequent packets may be signed by the peer adding the incident information for the investigation. A second benefit to this requirement is that the integrity of the filter used is ensured as it is passed to subsequent NPs in the upstream trace of the packet. The trusted PKI also provides the keys used to digitally sign the RecordItem class for TraceRequests to meet the requirement of authenticating the original request. Any host in the path of the trace should be able to verify the digital signature using the trusted PKI.

In the case in which an enterprise network using RID sends a TraceRequest to its provider, the signature from the enterprise network must be included in the initial request. The NP may

generate a new request to send upstream to members of the NP consortium to continue the trace. If the original request is sent, the originating NP, acting on behalf of the enterprise network under attack, must also digitally sign, with an enveloped

signature, the full IODEF document to assure the authenticity of the TraceRequest. An NP that offers RID as a service may be using its own PKI to secure RID communications between its RID system and the attached enterprise networks. NPs participating in the trace must be able to determine the authenticity of RID requests.

6.4 Consortiums and Public Key Infrastructures

Consortiums of NPs are an ideal way to establish a communication web of trust for RID messaging. The consortium could provide centralized resources, such as a PKI, and established guidelines for use of the RID protocol. The consortium would also assist in establishing trust relationships between the participating NPs to achieve the necessary level of cooperation and experience-sharing among the consortium entities. This may be established through PKI certificate policy [RFC3647] reviews to determine the appropriate trust levels between organizations or entities. The consortium may also be used for other purposes to better facilitate communication among NPs in a common area (Internet, region, government, education, private networks, etc.).

Using a PKI to distribute certificates used by RID systems provides an already established method to link trust relationships between NPs of consortiums that would peer with NPs belonging to a separate consortium. In other words, consortiums could peer with other consortiums to enable communication of RID messages between the participating NPs. The PKI along with Memorandums of Agreement could be used to link border directories to share public key information in a bridge, hierarchy, or a single cross-certification relationship.

Consortiums also need to establish guidelines for each participating NP to adhere to. The RECOMMENDED guidelines include:

- Physical and logical practices to protect RID systems;
- Network and application layer protection for RID systems and communications;
- Proper use guidelines for RID systems, messages, and requests; and
- A PKI to provide authentication, integrity, and privacy.

The functions described for a consortium's role would parallel that of a PKI federation. The PKI federations that currently exist are responsible for establishing security guidelines and PKI trust models. The trust models are used to support applications to share information using trusted methods and protocols.

PKI can also provide the same level of security for communication

between an end entity (enterprise, educational, government customer network) and the NP. The PKI may be a subordinate CA or in the CA hierarchy from the NP's consortium to establish the trust relationships necessary as the request is made to other connected

networks.

6.5 Privacy Concerns and System Use Guidelines

Privacy issues raise many concerns when information sharing is required to achieve the goal of stopping or mitigating the effects of a security incident. The RIDPolicy class is used to automate the enforcement of the privacy concerns listed within this document. The privacy and system use concerns that MUST be addressed in the RID system and other integrated components include the following:

Network Provider Concerns:

- o Privacy of data monitored and/or stored on IDS for attack detection.
- o Privacy of data monitored and stored on systems used to trace traffic across a single network.

Customer attached networks participating in RID with NP:

- O Customer networks may include enterprise, educational, government or other attached network to an NP participating in RID and MUST be made fully aware of the security and privacy considerations for using RID.
- O Customers MUST know the security and privacy considerations in place by their NP and the consortium of which the NP is a member.
- O Customers MUST understand that their data can and will be sent to other NPs in order to complete a trace unless an agreement stating otherwise is made in the service level agreements between the customer and NP.

Parties Involved in the Attack:

- o Privacy of the identity of a host involved in an attack.
- o Privacy of information such as the source and destination used for communication purposes over the monitored or RID connected network(s).
- o Protection of data from being viewed by intermediate parties in the path of a Investigation request MUST be considered.

Consortium Considerations:

- o System use restricted to security incident handling within the local region's definitions of appropriate traffic for the network monitored and linked via RID in a single consortium also abiding by the consortiums use guidelines.
- o System use prohibiting the consortiums participating NPs from inappropriately tracing non-attack traffic to locate sources or

mitigate traffic unlawfully within the jurisdiction or region.

Intra-consortium Considerations:

- o System use between peering consortiums MUST also adhere to any government communication regulations that apply between those two regions, such as encryption export and import restrictions.
- o System use between consortiums MUST NOT request traffic traces and actions beyond the scope intended and permitted by law or intra-consortium agreements.
- o System use between consortiums MUST respect national boundary issues and limit requests to appropriate system use and not to achieve their own agenda to limit or restrict traffic that is otherwise permitted within the country in which the peering consortium resides.

The security and privacy considerations listed above are for the consortiums, NPs, and Enterprises to agree upon. The agreed upon policies may be facilitated through use of the RIDPolicy class. Some privacy considerations are addressed through the RID guidelines for encryption and digital signatures as described in section 7.

RID is useful in determining the true source of a packet that traverses multiple networks or to communicate security incidents and automate the response. The information obtained from the trace may determine the identity of the source host or the network provider used by the source of the traffic. It should be noted that the trace mechanism used across a single-network provider may also raise privacy concerns for the clients of the network. Methods that may raise concern include those, which involve storing packets for some length of time in order to trace packets after the fact. Monitoring networks for intrusions and for tracing capabilities also raises concerns for potentially sensitive valid traffic that may be traversing the monitored network. IDS and single-network tracing is outside of the scope of this document, but the concern should be noted and addressed within the use guidelines of the network. Some IDS and single-network trace mechanisms attempt to properly address these issues. RID is designed to provide the information needed by any single-network trace mechanism. The provider's choice of a single trace mechanism depends on resources, existing solutions, and local legislation. Privacy concerns in regard to the single-network trace must be dealt with at the client-to-NP level and are out of scope for RID messaging.

The identity of the true source of an attack packet being traced through RID could be sensitive. The true identity listed in a Result message can be protected through the use of encryption [3] enveloping the IODEF document and RID Result information, using the public encryption key of the originating NP. Alternatively, the action taken may be listed without the identity being revealed to

the originating NP. The ultimate goal of the RID communication system is to stop or mitigate attack traffic, not to ensure the identity of the attack traffic is known to involved parties. The NP that identifies the source should deal directly with the

involved parties and proper authorities in order to determine the guidelines for the release of such information, if it is regarded as sensitive. In some situations, systems used in attacks are compromised by an unknown source and, in turn, are used to attack other systems. In that situation, the reputation of a business or organization may be at stake, and the action taken may be the only additional information reported in the Result message to the originating system. If the security incident is a minor incident, such as a zombie system used in part of a large-scale DDoS attack, ensuring the system is taken off the network until it has been fixed may be sufficient. The decision is left to the system users and consortiums to determine appropriate data to be shared given that the goal of the specification is to provide the appropriate technical options to remain compliant. The textual descriptions should include details of the incident in order to protect the reputation of the unknowing attacker and prevent the need for additional investigation. Local, state, or national laws may dictate the appropriate reporting action for specific security incidents.

Privacy becomes an issue whenever sensitive data traverses a network. For example, if an attack occurred between a specific source and destination, then every network provider in the path of the trace would become aware that the cyber attack occurred. In a targeted attack, it may not be desirable for the information that two nation states are battling a cyber war to become general knowledge to all intermediate parties. However, it is important to allow the traces to take place in order to halt the activity since the health of the networks in the path could also be at stake during the attack. This provides a second argument for allowing the Result message to only include an action taken and not the identity of the offending host. In the case of an Investigation request, where the originating NP is aware of the NP that will receive the request for processing, the free-form text areas of the document could be encrypted [3] using the public key of the destination NP to ensure that no other NP in the path can read the contents The encryption would be accomplished through the W3C [3] specification for encrypting an element.

In some situations, all network traffic of a nation may be granted through a single network provider. In that situation, options must support sending Result messages from a downstream peer of that network provider. That option provides an additional level of abstraction to hide the identity and the NP of the identified source of the traffic. Legal action may override this technical decision after the trace has taken place, but that is out of the technical scope of this document.

Privacy concerns when using an Investigation request to request action close to the source of valid attack traffic needs to be considered. Although the intermediate NPs may relay the request if there is no direct trust relationship to the closest NP to the

source, the intermediate NPs do not require the ability to see the contents of the packet or the text description field(s) in the request. This message type does not require any action by the intermediate RID systems, except to relay the packet to the next NP in the path. Therefore, the contents of the request may be encrypted for the destination system. The intermediate NPs would only need to know how to direct the request to the manager of the AS number in which the source IP address belongs.

Traces must be legitimate security-related incidents and not used for purposes such as sabotage or censorship. An example of such abuse of the system would include a request to block or rate-limit legitimate traffic to prevent information from being shared between users on the Internet (restricting access to online versions of papers) or restricting access from a competitor's product in order to sabotage a business.

Intra-consortium RID communications raise additional issues especially when the peering consortiums reside in different regions or nations. TraceRequests and requested actions to mitigate traffic must adhere to the appropriate use guidelines and yet prevent abuse of the system. First, the peering consortiums MUST identify the types of traffic that can be traced between the borders of the participating NPs of each consortium. The traffic traced should be limited to security incident-related traffic. Second, the traces permitted within one consortium if passed to a peering consortium may infringe upon the peering consortium's freedom of information laws. An example would be a consortium in one country permitting a trace of traffic containing objectionable material, outlawed within that country. The RID trace may be a valid use of the system within the confines of that country's network border; however, it may not be permitted to continue across network boundaries where such content is permitted under law. By continuing the trace in another country's network, the trace and response could have the effect of improperly restricting access to data. A continued trace into a second country may break the laws and regulations of that nation. Any such traces MUST cease at the country's border.

The privacy concerns listed in this section address issues among the trusted parties involved in a trace within an NP, a RID consortium, and peering RID consortiums. Data used for RID communications must also be protected from parties that are not trusted. This protection is provided through the authentication and encryption of documents as they traverse the path of trusted servers. Each RID system MUST perform a bi-directional authentication when sending a RID message and use the public encryption key of the upstream or downstream peer to send a message

or document over the network. This means that the document is decrypted and re-encrypted at each RID system either via TLS over BEEP or HTTP. The RID messages may be decrypted at each RID system in order to properly process the request or relay the information.

Today's processing power is more than sufficient to handle the minimal burden of encrypting and decrypting relatively small typical RID messages.

7. Security Considerations

Communication between NPs' RID systems must be protected. RID has many security considerations built into the design of the protocol, several of which are decribed in sub-sections of 6 in addition to this section. For a complete view of security, considerations must include the availability, confidentiality, and integrity concerns for the transport, storage, and exchange of information.

When considering the transport of RID messages, an out-of-band network, either logical or physical, would prevent outside attacks against RID communication. An out-of-band connection would be ideal, but not necessarily practical. Authenticated encrypted tunnels between RID systems MUST be used to provide confidentiality, integrity, authenticity, and privacy for the data. Trust relationships are based on consortiums and established trust relationships of PKI cross certifications of consortiums. By using RIDPolicy information, TLS, and the XML security features of encryption [3] and digital signatures [RFC3275],[5], RID takes advantage of existing security standards. The standards provide clear methods to ensure messages are secure, authenticated, authorized, meet policy and privacy guidelines, and maintain integrity.

As specified in the relevant sections of this document, the XML digital signature [RFC3275] and XML encryption [3] are used in the following cases:

XML Digital Signature

- Originator of the Trace or Investigation Request MUST use a detached signature to sign at least one of the original IP packets included in the RecordItem class data to provide authentication to all upstream participants in the trace of the origin. All IP packets provided by the originator may be signed and additional packets added by upstream peers in the trace may be signed by the peer adding the data, while maintaining the IP packet and detached signature from the original requestor. This signature MUST be passed to all recipients of the TraceRequest.
- For all message types, the full IODEF/RID document MUST be Signed using an enveloped signature by the sending peer to provide authentication and integrity to the receiving RID system.

XML Encryption

- The IODEF/RID document may be encrypted to provide an extra layer of security between peers so that the message is not only encrypted for the transport, but also while stored. This

behavior would be agreed upon between peers or a consortium, or determined on a per message basis based on security requirements. It should be noted, there are cases for transport where the RIDPolicy class MUST be presented in clear

text as detailed in the transport document [RFCYYYY].

- An Investigation request, or any other message type that may be relayed through RID systems other than the intended destination as a result of trust relationships, may be encrypted for the intended recipient. This may be necessary if the RID network is being used for message transfer, the intermediate parties do not need to have knowledge of the request contents, and a direct communication path does not exist. In that case, the RIDPolicy class is used by intermediate parties and is maintained in clear text.
- The action taken in the Result message may be encrypted using the key of the request originator. In that case, the intermediate parties can view the RIDPolicy information and know the trace has been completed and do not need to see the action. If the use of encryption were limited to sections of the message, the History class information would be encrypted. Otherwise, it is RECOMMENDED to encrypt the entire IODEF/RID document, using an enveloped signature, for the originator of the request. The existence of the Result message for an incident would tell any intermediate parties used in the path of the incident investigation that the incident handling has been completed.

The formation of policies is a very important aspect of using a messaging system like RID to exchange potentially sensitive information. Many considerations should be involved for peering parties and some guidelines to protect the data, systems, and transport are covered in Section 6. Policies established should provide guidelines for communication methods, security, and fall-back procedures.

The security considerations for the storage and exchange of information in RID messaging may include adherance to local, regional, or national regulations in addition to the obligations to protect client information during an investigation. RID Policy is a necessary tool for listing the requirements of messages to provide a method to categorize data elements for proper handling. Controls are also provided for the sending entity to protect messages from third parties through XML encryption.

RID provides a method to exchange incident handling request and Report messages to peer networks. Network administrators, who have the ability to base the decision on the available resources and other factors of their network, maintain control of incident investigations within their own network. Thus, RID provides the ability for participating networks to manage their own security controls, leverging the information listed in RIDPolicy.

8. IANA Considerations

This document uses URNs to describe XML namespaces and XML schemas

[4] conforming to a registry mechanism described in [RFC3688].

Registration request for the iodef-rid namespace:

URI: urn:ietf:params:xml:ns:iodef-rid-1.0

Registrant Contact: See the "Author's Address" section 10.2 of this document.

XML: None. Namespace URIs do not represent an XML specification.

Registration request for the iodef-rid XML schema:

URI: urn:ietf:params:xml:schema:iodef-rid-1.0

Registrant Contact: See the "Author's Address" section 10.2 of this document.

XML: See the "RID Schema Definition" section 5 of this document.

9. Summary

Security incidents have always been difficult to trace as a result of the spoofed sources, resource limitations, and bandwidth utilization problems. Incident response is often slow even when the IP address is known to be valid because of the resources required to notify the responsible party of the attack and then to stop or mitigate the attack traffic. Methods to identify and trace attacks near real time are essential to thwarting attack attempts. Network providers need policies and automated methods to combat the hacker's efforts. NPs need automated monitoring and response capabilities to identify and trace attacks quickly without resource-intensive side effects. Integration with a centralized communication system to coordinate the detection, tracing, and identification of attack sources on a single network is essential. RID provides a way to integrate NP resources for each aspect of attack detection, tracing, and source identification and extends the communication capabilities among network providers. The communication is accomplished through the use of flexible IODEF XML based documents passed between IHS or RID systems. A TraceRequest or Investigation request is communicated to an upstream NP and may result in an upstream trace or in an action to stop or mitigate the attack traffic. The messages are communicated among peers with security inherent to the RID messaging scheme provided through existing standards such as XML encryption and digital signatures. Policy information is carried in the RID message itself through the use of the RIDPolicy. RID provides the timely communication among NPs, which is essential for incident handling.

10. Normative References

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner. March 1997.

[RFC3275] "(Extensible Markup Language) XML-Signature Syntax and Processing", D. Eastlake 3rd, J. Reagle, D. Solo. March 2002.

[RFC5280] "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile." D. Cooper, S. Santesson, S.Farrell, S. Boeyen, R. Housley, W. Polk. May 2008.

[RFC3281] "An Internet Attribute Certificate: Profile for Authorization." S. Farrell, R. Housley. April 2002.

[RFC3379] "Delegated Path Validation and Delegated Path Discovery Protocol Requirements", D. Pinkas, R. Housley. September 2002.

[RFC3688] "The IETF XML Registry", BCP 81, M. Mealling. January 2004.

[RFC4279] "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", P. Eronen, H. Tschofenig. December 2005.

[RFC5070] "The Incident Object Description Exchange Format." R. Danyliw, J. Meijer, and Y. Demchenko. December 2007.

[RFCYYYY] "Transport of Real-time Inter-network Defense (RID) Messages," K. Moriarty, B. Trammell March 2010. http://tools.ietf.org/html/draft-moriarty-post-inch-rid-transport-02

[1] Extensible Markup Language (XML) 1.0 (Second Edition). W3C Recommendation. T. Bray, E. Maler, J. Paoli, and C. M. Sperberg-McQueen. October 2000. http://www.w3.org/TR/2000/REC-xml-20001006

[2] Namespaces in XML. W3C Recommendation. T.Bray, D. Hollander, A. Layman, R. Tobin. August 2006. http://www.w3.org/TR/REC-xml-names/

[3] XML Encryption Syntax and Processing, W3C Recommendation. T. Imamura, B. Dillaway, and E. Simon. December 2002. http://www.w3.org/TR/xmlenc-core/

[4] XML Schema. E. Van der Vlist. O'Reilly. 2002.

[5] XML-Signature Syntax and Processing. W3C Recommendation. M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon. February

2002. http://www.w3.org/TR/xmldsig-core/#sec-Design.

11. Informative References

[RFC1930] "Guidelines for creation, selection, and registration of an Autonomous System (AS)." J. Hawkinson and T. Bates. March 1996.

[RFC2827] "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing." P. Ferguson and D. Senie. May 2000.

[RFC3330] "Special-Use IPv4 Addresses." IANA. September 2002.

[RFC3647] "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework." S. Chokhani, W. W. Ford, R. Sabett, C. Merrill, S. Wu. November 2003.

[RFC3917] "Requirements for IP Flow Information Export (IPFIX)". J. Quittek, T. Zseby, B. Claise, S. Zander. October 2004.

[6] Advanced and Authenticated Marking Schemes for IP Traceback. D. Song and A. Perrig. IEEE INFOCOM 2001.

[7] "Hash Based IP Traceback." A. Snoren, L. Sanchez, C. Jones, F. Tchakountio, S. Kent, and W. Strayer. SIGCOMM'01. August 2001.

[8] "ICMP Traceback Messages." S. M. Bellovin, M. Leech, and T. Taylor. Internet Draft: http://www.ietf.org/proceedings/03mar/I-D/draft-ietf-itrace-04.txt February 2003.

[9] "Network Congestion Monitoring and Detection using the IMI infrastructure." T. Saitoh, G. Mansfield, and N.Shiratori. Graduate School of Information Sciences, Tohoku University.

[10] "Practical Network support for IP Traceback." S. Savage, D. Wetherall, A. Karlin, and T. Anderson. SIGCOMM'00. August 2000.

[11] "Trends in Denial of Service Attack Technology." K. Houle, G. Weaver, N. Long, and R. Thomas. CERT Coordination Center. October 2001.

12. Acknowledgements

Many thanks to coworkers and the Internet community for reviewing and commenting on the draft as well as providing recommendations to simplify and secure the protocol: Robert K. Cunningham, Ph.D, Cynthia D. McLain, Dr. William Streilein, Iljitsch van Beijnum, Steve Bellovin, Yuri Demchenko, Jean-Francois Morfin, Stephen Northcutt, Jeffrey Schiller, Brian Trammell, Roman Danyliw, Tony Tauber, and Sandra G. Dykes, Ph.D.

Funding for the RFC Editor function is currently provided by the Internet Society.

13. Author Information

Kathleen M. Moriarty
RSA, The Security Division of EMC
174 Middlesex Turnpike
Bedford, MA 01730
Email: Moriarty_Kathleen@EMC.com

Sponsor Information

This work was sponsored by the Air Force under Air Force Contract FA8721-05-C-0002, while working at MIT Lincoln Laboratory.

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