Extended Incident Handling Working Group
draft-ietf-inch-rid-08.txt
Expires: February 21, 2007

Kathleen M. Moriarty
MIT Lincoln Laboratory

August 21, 2006

Incident Handling: Real-time Inter-network Defense

Status of this Memo

Abstract

Network security incidents, such as system compromises, worms, viruses, phishing incidents, and denial of service (DoS), typically result in the loss of service, data, and resources both human and system. Network Providers (NPs) 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. This paper outlines a proactive inter-network communication method to facilitate sharing incident handling data and integrate existing tracing mechanisms across NP boundaries to identify the source(s) of an attack. The various methods implemented to detect and trace attacks must be coordinated on the NPs' network as well as provide a communication mechanism across network borders. It is imperative that NPs have quick communication methods defined to enable neighboring NPs to assist in reporting or tracking a security incident across networks. A complete solution integrating incident detection, source identification, reporting and communication capabilities, and methods to stop attack traffic is necessary to attain 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. Introduction

Incident handling involves the detection and identification of the source of an attack, whether it be a system compromise, socially engineered phishing attack, or a denial of service attack. In order to identify the source of an attack, there must be a way to trace the attack traffic iteratively upstream through the network to the source. In cases in which 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.

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

will be represented in an Extensible Markup Language (XML) document and is an extension of the Incident Data Exchange Format (IODEF) model. 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 NPs 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 will take advantage of XML security, 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 will be encapsulated in a SOAP wrapper. The authentication, integrity, and authorization features each layer has to offer will be used to achieve the level of security that is necessary. SOAP is used as a message wrapper to direct messages appropriately, and the SOAP binding will be used with a specific transport protocol with HTTPS set as the mandatory to implement protocol and others are optional such as BEEP, S/MIME, XML SNMP, and others.

1.1 Overview of Attack Types

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.

The CERT Coordination Center published a paper in October 2001 entitled, "Trends in Denial of Service Attack Technology"[19]. The paper outlined the behavior of denial-of-service attacks of both single-source and multiple-source origins. Denial-of-service (DoS) attacks attempt to consume bandwidth, processing power, or system resources for the purposes of denying use by normal users. Bandwidth or processing power-based attacks may use variations on

these packets, such as altering the source address, port numbers, or TCP options.

DoS 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.

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. Recommended Network Provider (NP) 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 and the integration of RID messaging with other components of the network. This system may provide functions such as trend analysis for bandwidth utilization, report communication problems, and trigger a RID trace across the network or communicate with a RID system that can initiate a trace. The RID messaging system may be the same or a system separate from the NMS that communicates with various aspects of the network to coordinate incident response. 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 incident-handling systems to create IODEF documents or RID messages to facilitate security incident handling. IDSs monitor network traffic, analyzing packets to determine if the traffic might be classified as malicious. If an IDS detects malicious traffic, an analyst would determine the validity and severity of the attack traffic and if a trace is necessary. If the analyst determines a trace should be initiated, an IODEF document with RID extensions could be created or the necessary information sent to the RID messaging system in order to create and track the attack traffic. Detection of a security incident is outside the scope of this paper; however, it should be possible to integrate detection methods with RID messaging.

Once a security incident has been identified, the information is put into a RID message to integrate with the NP's single network trace mechanism. RID messaging is intended to be flexible in order to accommodate various trace 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 security team for further investigation. The various technologies used to trace traffic across a network are described in section 3.2.

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 authenticated and encrypted Simple Network Management Protocol (SNMP) or Network Configuration Protocol (NETConf) access to devices over an out-of-band connection or other similar technologies.

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 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. DDoS attacks are also difficult or nearly impossible to trace because of the nature of the attack. Some of the difficulties in tracing these 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 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.

3.1 Tracing a Distributed Attack

Tracing a DDoS attack is a very difficult problem. Since DDoS attacks may involve multiple sources with spoofed addresses, there may only be a small amount of traffic from each of the originating hosts. This makes it difficult to trace back to the sources. The sources may also alternate the type of traffic and the master may vary the sources from within the pool of sources launching the attack. Because of the dynamic nature of the DDos attack, immediate action would need to be taken to have any hope of locating the origin(s) of the attack with a near real-time trace.

In order to identify a DoS attack or DDoS, a client may notify its NP that it is currently under attack. Automated methods might include statistical traffic analysis, which looks for unexpected fluctuations in bandwidth or in the size and types of packets sent between networks, hosts, or an IDS. There is ongoing research in the area of detecting DoS and DDoS, and any effective techniques could be integrated with the tracing techniques described in this paper. Some research approaches include methods that detect backscatter traffic [9], using a data structure for bandwidth attack detection [10], and monitoring congestion through packet retransmission information [11].

Once an attack is suspected, traces would have to quickly identify the various sources of the attack. A generalized approach should be used to trace back connections using packet header information such as the destination IP address and any distinguishing header values of the traffic seen during the attack. The information collected, along with an example packet, would be used in a RID message to communicate incident handling information between NPs.

3.1.1 Tracing Security Incidents

If a trace can identify the sources of a distributed attack, blocking the sources at the NP level close to the attacker could be an immediate action to stop the attack. In the case of a DDoS attack, further information may be obtained from the attacking computers as to the controller of the attack sending the zombies' control information to carry out the attack. A similar example of attack traffic with the possibility of multiple traces required would be one in which an attacker compromised a series of systems and accomplished hiding their source by logging into a string of systems to launch the attack. This additional trace is beyond the scope of this paper, but may use additional tracing mechanisms such as sniffing the network to locate the controllers of the attack.

Finding a faster and more efficient way to trace multiple sources

of an attack is essential to mitigating DDoS attacks. The ability to quickly relay and act upon the trace information gathered is imperative to stopping attack traffic. Tracing multiple attack paths can also cause additional stress on the network and does not

scale well.

A CSIRT report might be generated in the form of an IODEF document and then fed into a RID message or document to facilitate a trace or multiple traces of attack traffic.

3.2 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" [14], and IP Marking [1]. The following sections outline some available solutions for implementing traceback within the confines of a network managed by a single entity. The single network traceback solutions are discussed to determine the information needed to accomplish an inter-network trace where different solutions may be in place.

3.2.1 Trace Approach via Traffic Flow Analysis

Traffic flow analysis is used to monitor individual network traffic streams, such as a single TCP session beginning with the SYN packet and ending with the final FIN ACK in a session. There have been a few efforts to standardize flow analysis for network management, one through the traffic flow management MIB and another through the IP Flow Information eXport (IPFIX) protocol. The "Traffic Flow Management" RFC [RFC2720] was designed to provide management information such as behavior models, capacity planning, network performance, quality of service, and attribution of network usage to system administrators. IPFIX is an IETF standard intended to provide a uniform method of extracting flow information from network devices. There are several competing standardized methods for flow analysis; however, since they differ from each other, it is difficult to generate standardized analysis tools. NetFlow

from Cisco [5] provides similar capabilities to the traffic flow mib, except that it is specific to IP traffic and has already been implemented for traffic management in commercial-off-the-shelf equipment. Although NetFlow was developed by Cisco, it is also an

open standard. The flow analysis in both implementations can monitor with a capture filter on source and destination addresses the number of packets and the count of bytes in each flow, the originating interface of the traffic, and the upstream peer information. The upstream peer information is essential to tracing a spoofed packet back to the true origin.

There are several differences in the implementations and the monitor and capture capabilities of the two flow analysis implementations. NetFlow collects all packets and maintains the following information on packet flows for later analysis:

- Source and destination IP address
- Source and destination TCP/User Datagram Protocol (UDP) ports
- Type of service (ToS)
- Packet and byte counts
- Start and end timestamps
- Input and output interface numbers
- TCP flags and encapsulated protocol (TCP/UDP)
- Routing information (next-hop address, source autonomous system (AS) number, destination AS number, source prefix mask, destination prefix mask)

Based on the information listed above, a spoofed packet can be traced upstream through a network to either identify the true source or the upstream peer. Various flow-based solutions have been developed and implemented for use on a single backbone based on flow analysis, and RID messaging must be able to support existing and future solutions to trace attacks across multiple networks. The AS number listed associated with a source IP address is only valid if the source IP address is valid. The AS number in this case cannot be trusted until the true source has been identified.

3.2.2 Trace Approach via Hash-Based IP Traceback

BBN implemented a traceback solution that collects hashes of IP packets across the network. The Hash-Based IP Traceback was designed specifically to trace attack traffic and achieve the following objectives:

- Trace attacks after specific flows of the attack have completed
- Reduce storage requirements needed to save traceable packet data
- Provide a secure method to store packet captures on the Internet

Hash-based IP traceback is another solution to provide the ability to trace attack traffic. By capturing all packets across the network and saving hash values for the IP header information that

does not get altered as it traverses the network, attacks can be traced after the fact. Since hashes of IP header information are stored instead of the actual header information, privacy concerns are no longer an issue as might be the case with packet

captures across the Internet. If a system used to store the packet captures was compromised, the data could not be used to identify which entities are "talking" to each other on the Internet.

BBN also considered how traces could be performed across a single network, for example an NP's backbone. The solution divides the network up into regions, each with its own collection station. The trace might be initiated at a particular collection station where data for a specific router is stored. When the collection station traces through its database for the matches of particular hashes of IP packets, it follows the trace through the network equipment for its own region. The collection station then determines which bordering region was the next upstream source of the attack, and the trace is continued at the next collection agent. The trace continues until the source is identified or a neighboring network is identified as the upstream source of the attack. The upstream network must then be notified in some way in order to continue the trace. The upstream network will require the IP packet information in order to continue the trace. The upstream provider will want to look at its network and resources and decide if it would like to initiate a trace across its network. A limited number of packets can be stored based on resources and network traffic loads. RID is a possible solution for communicating the upstream TraceRequest between bordering networks.

3.2.3 IP Marking

The technique of IP Marking can be used more efficiently than iterative trace mechanisms to trace attacks in which the source address has been spoofed. This technique has been proposed specifically in terms of tracing DoS attacks across a network. All information is correlated at the end node or the target where the packets received would have been marked probabilistically along the path of the traffic. This method requires that routers and other infrastructure equipment have the ability to mark packets so that the path they took can be derived at the destination address for the packets. Since all packets are not marked, depending on the IP Marking scheme used, a number of similar packets would have to be sent from a single source in order for it to be identified. IP Marking alone may not be a complete answer for tracing traffic, since an attacker could switch methods to send very little data from any one host used in a DDoS attack, thus making it unlikely that enough packets will be marked to find the source of each stream. Integrating IP Marking with other techniques may be the best answer to ensure the efficiency and robustness of the system as a whole.

There are several ways in which the IP Marking approach may be useful in integrating with RID. IP Marking may be used to gather information about the path of the trace up to and including

identifying the actual source. A peer closer to the source might be identified if the IP Marking technique were not able to fully reconstruct the path of the trace. In this instance, the trace information could be sent to the closest point identified in the path from the IP Marking technique, thus shortening the length of time required to trace the traffic through the network. If a source was identified, a RID Investigation Request might be used in order to trigger a specific action to take place close to the source to mitigate or stop the effects of the attack.

3.2.4 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 will be 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. Note: Previously, the packet data was contained in a RID class called IPPacket. The IODEF data model was extended in August 2005 to accomodate a packet of type hexidecimal.

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 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

Expediting the communication between NPs 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 security incident response team. 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 network management systems used on the NP's backbone 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 system 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 trace functions. This could be a function of a central organization operating as a computer response team 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 that agree to participate in the RID communication protocol with an agreed-upon policy and communication protocol facilitating the secure transport of RID XML documents. Transport for RID messages will be specified in a separate document.

The first method described prevents the need to permit access to other network's equipment through the use of a standard messaging mechanism to enable RID or NMSs to communicate trace 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 traces through smaller NPs. The 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 a trace. The first method enables the individual NPs to involve their network operations staff to authorize the continuance of a trace 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, out-of-band or protected channels, would be direct communication links 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 will be 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 NMS 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. Real-time Inter-network Defense (RID) provides the framework necessary for communication between networks involved in the traceback and mitigation of a security incident. Several message types described in section 4.3 are necessary to facilitate a trace across multiple networks. The message types include the Report, IncidentQuery, TraceRequest, TraceAuthorization, 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 TraceAuthorization and Result messages are used to communicate the status and result of a trace. 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.

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 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 may cause adverse effects on a network. If the confidence rating is low, it may not be in the Network Provider'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.

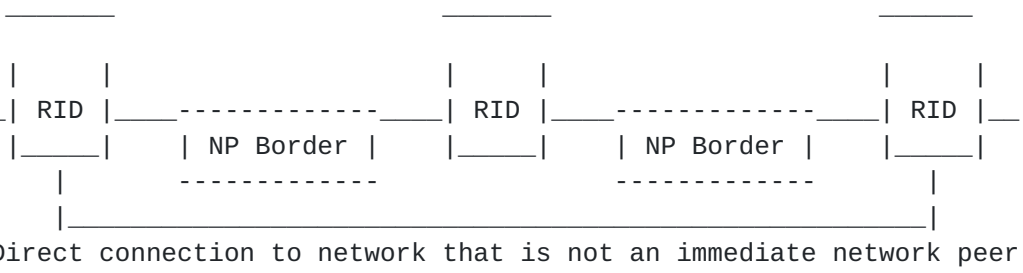


Figure 2: Mesh Peer Topology

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. 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 in a SOAP wrapper. Each RID message type, along with an example, is described in the following sections.

4.3.1 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.

2. TraceAuthorization. This message is sent to the initiating RID system from each of the upstream NPs' RID systems to provide information on the trace 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.

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.

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 is also presented in the SOAP header to facilitate the communication of security incident data to trace, investigate, query, or report information security incident information. The details of the SOAP wrapper are discussed in the SOAP document for transport communications.

4.3.2 RID Data Types

RID is derived from the IODEF data model and inherits all of the data types defined in the IODEF model.

4.3.3 IODEF-Document

The IODEF model will be followed as specified in RFCXXXX for each of the RID message types. (The RFC number will replace the XXXX when a number has been assigned for the document.) The RID schema is used to define an XML envelope for IODEF documents to facilitate RID communications. Each message type varies slightly in format and purpose; hence, the requirements vary and will be 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 defined in section 4.4. The IODEF model MUST be fully implemented to ensure proper parsing of all RID messages.

Please see RFCxxxx for specific information on the IODEF-Document requirements. (The RFC number will be defined when the document becomes an RFC.)

4.3.4 IODEF-RID Schema

There are four classes included in the RID extension required to facilitate RID communications. The NPPath class is used to list out the path a trace has taken at the RID system or NP level; the

TraceStatus 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 in the SOAP header for transport. 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:

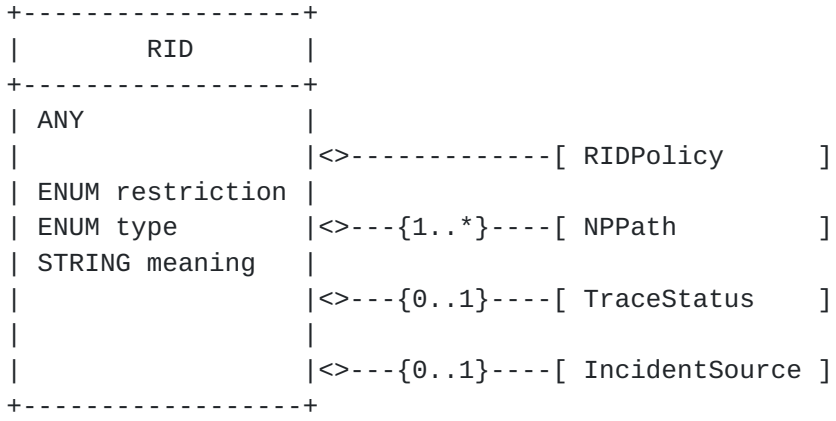


Figure 3: The RID Schema

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

RIDPolicy
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.

NPPath
One or many. The contact information for the NPs involved in a trace, which includes information on the actual RID or NMS systems involved in the trace. The schema will not enforce the requirement of one entry to enable parsing to work propery in the SOAP header to support transport.

TraceStatus
Zero or One. This is used only in Trace 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.

4.3.4.1 NPPath Class

The NPPath information is represented in the aggregate RID class.

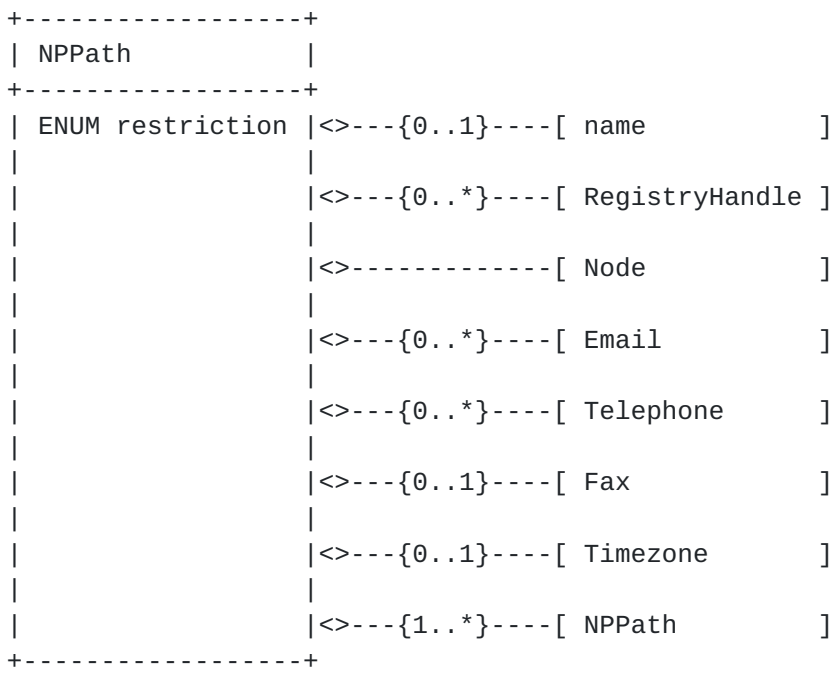


Figure 4: The NPPath Class

The aggregate classes that constitute the NPPath class are as follows:

name
: Zero or one. NAME. The name of the contact. The contact may either be an organization or a person. The type attribute dictates the semantics (organization or person).

RegistryHandle
: Zero or many. The handle name in a registry. Care must be taken to ensure that a handle is meaningful to the recipient. Intra-organizational handles are of not much use for extra-organizational communication. The base definition is from IODEF section 3.7.1.

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

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

Email

Zero or many. EMAIL. The email address of the contact formatted according to IODEF section 2.2.13.

Telephone
Zero or many. PHONE. The telephone number of the contact formatted according to documentation in section 5.21 of RFC2256.

Fax
Zero or one. PHONE. The facsimile telephone number of the contact formatted according to documentation in section 5.21 of RFC2256.

Timezone
Zero or one. STRING. The timezone in which the contact resides.

NPPath
One or many. Recursive definition of NPPath, allowing for grouping of data. This is necessary in order to provide the complete list of systems communicating in the RID Trace, Investigation, or Report messages. The first NPPath definition is used for the originating host and NP information; the second listing is for the first NP that receives a request or message. All subsequent entries are used to list the information for each RID system for the NPs involved.

4.3.4.2 TraceStatus Class

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

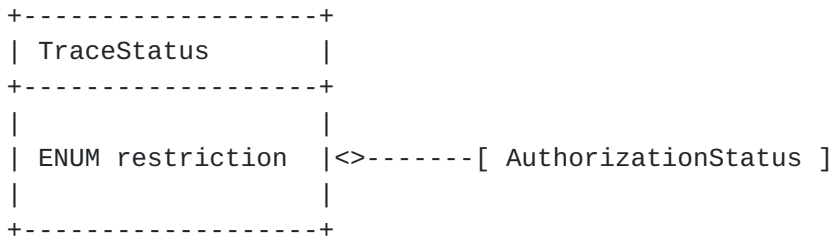


Figure 5: The TraceStatus Class

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

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

Approved. The trace was approved and will begin in the current NP.
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

TraceAuthorization 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.

Pending. Awaiting approval and a time-out period has been reached which resulted in this pending status and TraceAuthorization message being generated.

4.3.4.3 IncidentSource Class

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

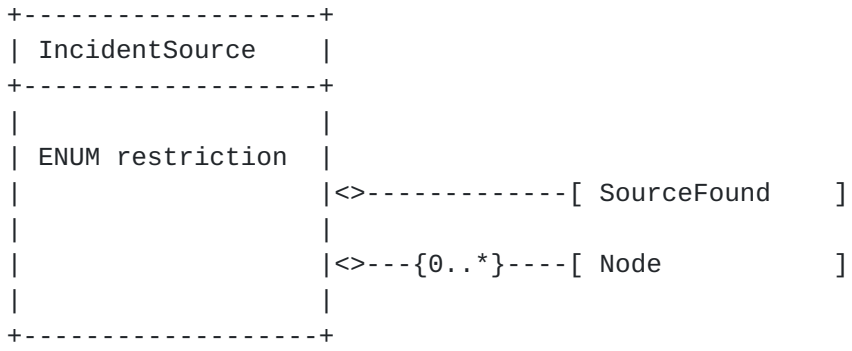


Figure 6: The IncidentSource Class

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 will be 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.

4.3.4.4 RIDPolicy

The RIDPolicy class facilitates the delivery of RID messages and is also referenced in the SOAP header.

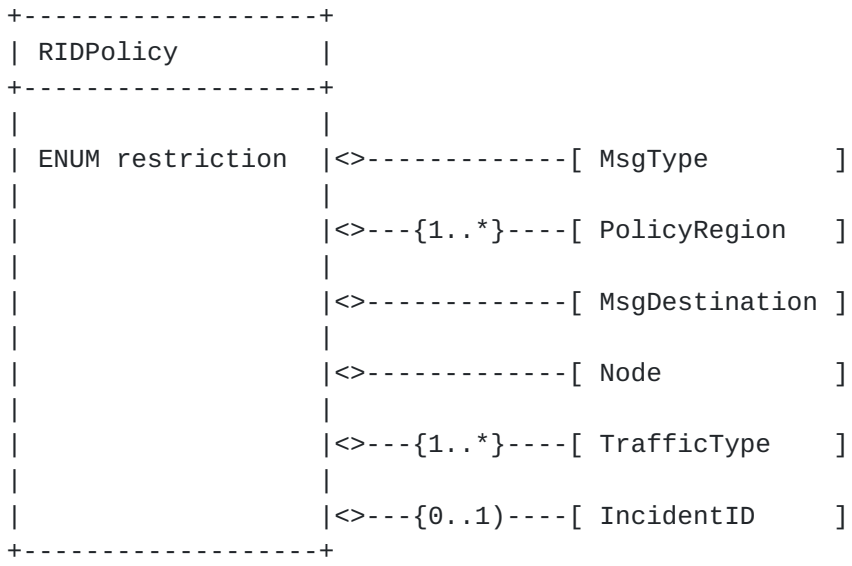


Figure 7: The RIDPolicy Class

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

MsgType
One. Required. STRING. 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.

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.

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

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.

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 network provider

closest to the source of the valid traffic that some event occurred, which may be a security-related incident.

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.

IncidentQuery. This message is used to request information from a trusted RID system about an incident or incident type.

MsgDestination

One. Required. STRING. The destination of the RID message will also appear in the NPPath class, but may be encrypted in some cases. 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.

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

SourceOfIncident. The address listed in the Node element of the RIDPolicy class is the incident source. The IP address will be 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.

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.

PolicyRegion

One or many. Required. STRING. The listed values are used to determine what policy area may require consideration before a trace can be approved. The PolicyRegion may include multiple selections from the list in order to fit all possible policy

considerations when crossing regions, consortiums, or networks.

ClientToNP. An enterprise network initiated the request.
NPToClient. An NP passed a RID request to a client or an

enterprise attached network to the NP based on the service level agreements.

Inter-Consortium. A trace that should have no restrictions within the boundaries of a consortium with the agreed-upon use and abuse guidelines.

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.

Between-Consortiums. A trace that should have no restrictions between consortiums that have established agreed-upon use and abuse guidelines.

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.

TrafficType

One or many. Required. STRING. The listed values 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.

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. (IODEF sections 3.10 and 3.11)

Network. This option MUST only be selected when the trace is related to NP network traffic or routing issues.

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.

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.

Other. If this option is selected, a description of the trace 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.

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.

4.4 RID Documents Defined by Message Type Derived from IODEF

This section includes the mandatory IODEF information used in all RID messages. Since RID is a wrapper for an IODEF document, the full IODEF specifications MUST be implemented, and the following section identifies the IODEF fields that must be filled in when a RID message or document is generated. Other fields may optionally be filled in to provide further information to an incident handler and thus must be implemented for proper parsing of a RID message wrapping an IODEF document. This section will reference the IODEF model and the sections of the IODEF RFC where each IODEF class can be located.

IODEF Schema Classes

Incident Class (IODEF 3.2)
Purpose: The Purpose will be set according to the purpose of the message type, for instance, incident handling or statistics.
Restriction: Sender can select from the IODEF specifications for this value and fill in as appropriate.
IncidentID (IODEF 3.3)
GUID: Name of CSIRT or NP that created the document.
AlternativeID (IODEF 3.4)
This incident ID is one set by another CSIRT that is tracking the same or a similar incident. This value should not be set in the initial request, but may be set in a request passed forward by an NP in the path of a trace, investigation, or report.

RelatedActivity Class (IODEF 3.5)
This class is optional if an AlternateID is specified.
AdditionalData Class (IODEF 3.6)
This class is optional and may be used if an extended schema is necessary to describe the incident.
Contact: Mandatory for RID (IODEF 3.7)
The required aggregate classes for the contact class in RID

messages include Name, RegistryHandle (IODEF 3.7.1), Email, Telephone. The attributes in the contact class are required in the IODEF document and thus are required in RID messages and include Restriction, Role, and Type.

StartTime: Mandatory for RID (IODEF 3.8.1)
EndTime: Optional for RID, incident may still be in process in which no end time can be listed (IODEF 3.8.2).
DetectTime: Mandatory for RID (IODEF 3.8.3)
ReportTime: Mandatory for RID (IODEF 3.8.4)
EventData: Required for RID (IODEF 3.12)
Much of the EventData Class is a duplicate for the aggregate IncidentData class and the proper uses of this class are defined in the IODEF RFC. The EventData contains the Expectation class to ensure any action requested is associted back to the proper EventData.
Expectation: Mandatory for RID (IODEF 3.13)
The StartTime and EndTime, as well as the accuracy required, can be used to determine the type of trace that would be used on a network with multiple choices. StartTime and EndTime to stop the trace would indicate if a fast or slower and more accurate method should be used for each TraceRequest.
The following attributes are required in RID messages:
Priority and Category. The category attribute is used to place a request for a specific action to be taken close to the source.
Note: Although category is required in a request, the NP closest to the source of the attack decides upon the ultimate response.
Method: Techniques used in attack - Mandatory for RID to determine the type of traffic for RIDPolicy informatio) (IODEF 3.9)
Assessment: Characterization of the impact - Mandatory for RID, (reference IODEF section 3.10)
Impact aggregate class (IODEF 3.10) MUST be used along with the Confidence class (IODEF 3.10.4) in the Assessment Class. The other impact classes are optional and may depend on the Incident type to determine if the additional classes are appropriate.
History: Required for upstream trace requests, investigations, and report messages but not for original request. (IODEF 3.11) The HistoryItem element specifies the actions taken to stop or mitigate the effects of a security incident through the atype attribute. It may also be used to further describe actions taken along the NP Path of a trace as well as to describe the incident handling in a report message.
Flow Class: Optional for RID (IODEF 3.14)
System class: (IODEF 3.15)
The System class is required and the information listed in this class can be automatically entered into this class from the packet used in the incident trace by the RID implementation. Information must be reviewed by the submitter and the additional required classes and attributes filled in for proper processing

of a request. The system class MUST be used to list the source and the target or intermediate system(s) and MUST note if the system was spoofed through the use of the Node class (IODEF 3.16). A separate instance of the System class (and Node Class)

is used for each type of system listed in the document. The spoof section MUST be used in the System EventData Class of all RID messages and is set to the value of spoofed for all TraceRequests that require an actual trace of network traffic. In an Investigation request, the source is believed to be valid. All other classes of the System Class are optional as in the IODEF document.

Node Class and Service class are embedded within other listed classes or the IODEF definitions are reused in the RID specification (IODEF 3.16 and 3.17).

Record Class: Optional for RID (IODEF 3.19)

Required for messages types that must include a sample packet. The RecordItem Class (IODEF 3.19.2) allows for various packet types to be included in an IODEF document. This replaced the need for the IPPacket class in RID and must be used to represent packet data for incident handling.

RID Schema Classes: RID messages require that the NP Path and the RecordItem (including an example packet) class are used to provide adequate information for an upstream peer to perform a trace. The information contained in the NPPath and RecordItem classes must remain and be maintained in each type of RID message document. The TraceStatus class is used in the TraceAuthorization message only since its purpose is to let the downstream NP know if the trace was approved and will begin in the next upstream network. The RIDPolicy class is used in routing RID messages and providing policy information between participating RID hosts.

- NPPath (Original Request should contain originator plus the next peer in the upstream request, the host that is receiving the request)
- TraceStatus (Approval status for the trace in the current network)
- IncidentSource (Source information for Result message)
- RIDPolicy (Policy information to support RID communications)

Restriction

Optional. The IODEF restriction should be used in addition to the RID privacy and security guidelines since this is optional on the part of the receiving end of an IODEF message and is not enforced.

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 NPPath 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 will be provided through:

RID Information:
RIDPolicy
RID message type, IncidentID, and destination policy information
Path information of RID systems used in the trace
NPPath in RID schema

IODEF Information:
Time Stamps (DectectTime, 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.
Event, Record, and RecordItem Classes to include example packets and other information related to the incident.
[Free-form text area for any additional information on justification for Investigation message request, IODEF IncidentData Description]

W3C standards for Encryption and Digital Signatures:
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.

4.4.2 TraceAuthorization Message

Description: This message is sent to the initiating RID system from

the next upstream NP's RID system to provide information on the trace status in the current network.

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

RID Information:
RIDPolicy
RID message type, IncidentID, and destination policy information
Status of TraceRequest
TraceStatus class in RID schema
Path information of RID systems used in the trace
NPPath class in RID schema
The last NP listed is the NP sending this TraceAuthorization message. All previous NPs listed in the NPPath must be retained.

IODEF Information:
Time Stamps (DectectTime, 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 information
Event, Record, and RecordItem Classes to include example packets and other information related to the incident [optional].
[Additional free-form text information on the attack, Description in History Class]

W3C standards for Encryption and Digital Signatures:
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.

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.

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

RID Information:
RIDPolicy
RID message type, IncidentID, and destination policy information
Path information of RID systems used in the trace
NPPath class in RID schema
The last NP listed is the NP, which located the source of the traffic (the NP sending the Result message)
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 (DectectTime, 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 noes any other background information.
Event, Record, and RecordItem Classes to include example packets and other information related to the incident [optional]
[Free-form text area for any additional information on the identified source of the attack traffic, IODEF Description, Incident Class.]

W3C Encryption and Digital Signature standards:
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 will be provided through:

RID Information:
RID Policy
    RID message type, IncidentID, and destination policy information
Path information of RID systems used in the trace
    NPPath class in RID schema

IODEF Information:
Time Stamps (DectectTime, 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.
Event, Record, and RecordItem Classes to include example packets and other information related to the incident.
[Free-form text area for any additional information on justification for Investigation message request, IODEF Description.]

W3C Encryption and Digital Signature standards:
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 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

IODEF Information:
Time Stamps (DectectTime, 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].

[Free-form text area for any additional information on
incident, IODEF IncidentData Description.]

W3C Encryption and Digital Signature standards:

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 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 NPPath 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 is required for an IncidentQuery message and will be provided through:

RID Information:
RID Policy
RID message type, IncidentID, and destination Policy information
IODEF Information [optional]:
Time Stamps (DectectTime, 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].

[Free-form text area for any additional information on
justification for IncidentQuery, IODEF IncidentData
Description.]

W3C Encryption and Digital Signature standards:
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.

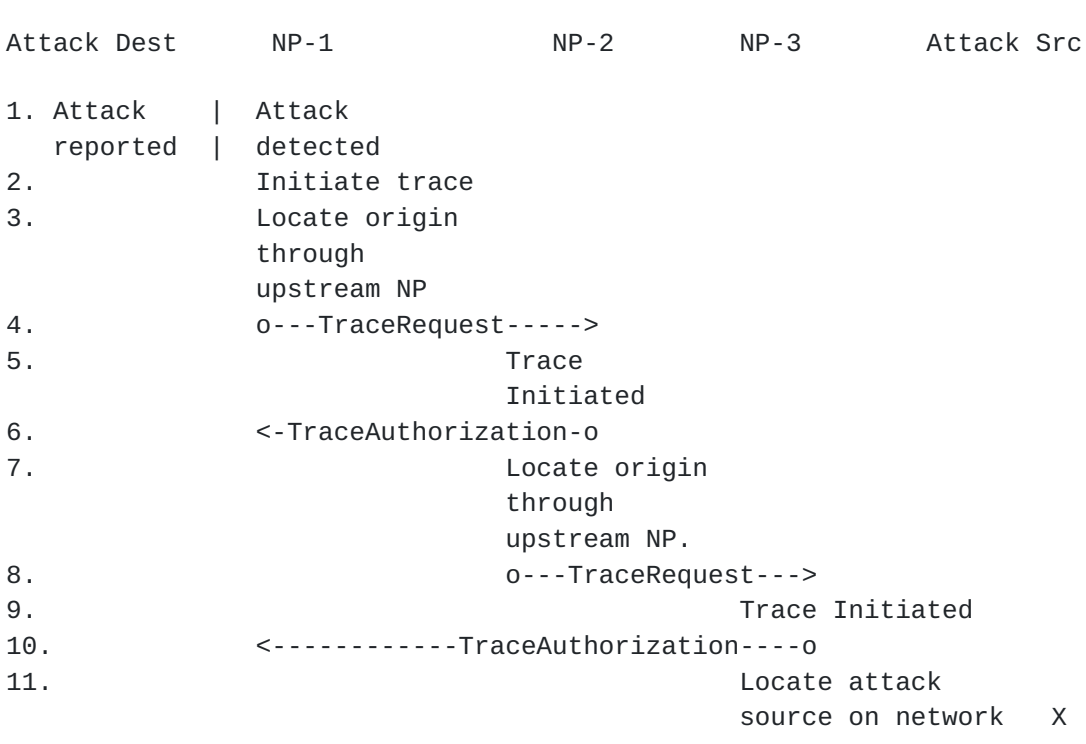
The proper response to the IncidentQuery message is a Report message. Multiple reports may be returned for a single query if an incident type is requested. In this case, the transport would notify the sending system of the expected number of replies for proper handling. The Confidence rating may be used in the Incident Query 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.

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.



12. <------------Result----------------o

Figure 8: TraceRequest Communication Flow

The NP that detected the attack initiates the trace. The attack is traced to the source or the next upstream NP. This process continues until the trace identifies the source of the attack. Any Trace Authorization and Result messages must pass through all RID systems in the path back to the trace initiator because of the secure connections established between RID systems of bordering networks. The involved systems in the path for Trace Authorization and Result messages would then have the ability to see and acknowledge the trace status before sending the messages back along the RID communication path to the originating RID system.

Before a trace can be initialized, the originating RID system must check an internal database to determine if a trace to the same IP address or network address has occurred within a specified period of time, no less than 1 day. The trace may have been initiated by the same RID system or this RID system may have been in the path of the trace. The previous filter must be maintained for a minimum of one week in order to retrieve the filter for comparison before initiating a TraceRequest or allowing a trace continuance to occur. If the network administrator justifies a similar trace, a note might be added to the Description element of the document to provide an additional confidence indication to the upstream NPs in the path of the trace.

A single-network trace may be constrained using factors determined by the associated NP's network trace system in the path of the trace. The trace system may either trace a packet in real time or search through stored packet data for evidence that the packet had traversed the network. In the case of a real-time trace, the traffic needs to be active on the network for the trace to be successful or the trace will cease. A message is sent to indicate the status, that the trace cannot continue, to the originating RID system through the consortium's trust relationships formed by the RID systems in the path of the trace. The packet trace may also be limited due to the lack of storage space on networks for saving traffic data. A TraceAuthorization message is sent, in this case as well, to provide the path information up to the point at which the trace could no longer be continued to the originator of the trace through the RID systems in the path of the trace. This information could also be used to block or mitigate the traffic at the participating NP closest to the source.

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 and NPPath classes. 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>
            <iodef-rid:MsgType>TraceRequest</iodef-rid:MsgType>
            <iodef-rid:PolicyRegion>Inter-Consortium
            </iodef-rid:PolicyRegion>
            <iodef-rid:MsgDestination>RIDSystem
            </iodef-rid:MsgDestination>
               <iodef:Node>
                  <iodef:Address category="ipv4-addr">172.20.1.2
                  </iodef:Address>
               </iodef:Node>
            <iodef-rid:TrafficType>Attack</iodef-rid:TrafficType>
            <iodef:IncidentID
             name="CERT-FOR-OUR-DOMAIN">CERT-FOR-OUR-DOMAIN#207-1
            </iodef:IncidentID>
           <iodef-rid:NPPath>
            <iodef:Name>CSIRT-FOR-OUR-DOMAIN</iodef:Name>
            <iodef:RegistryHandle>CSIRT123</iodef:RegistryHandle>
            <iodef:Email>csirt-for-our-domain@ourdomain</iodef:Email>
            <iodef:Node>
               <iodef:Address category="ipv4-addr">172.17.1.2
               </iodef:Address>
            </iodef:Node>
         </iodef-rid:NPPath>
         <iodef-rid:NPPath>
            <iodef:Name>CSIRT-FOR-UPSTREAM-NP</iodef:Name>
            <iodef:RegistryHandle>CSIRT345</iodef:RegistryHandle>
            <iodef:Email>csirt-for-upstream-np@ourdomain</iodef:Email>
            <iodef:Node>
               <iodef:Address category="ipv4-addr">172.20.1.2
               </iodef:Address>
            </iodef:Node>
         </iodef-rid:NPPath>
   </iodef-rid:RID>

    <IODEF-Document version="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:IncidentData>
            <iodef:Description>Host involved in DOS attack
            </iodef:Description>
            <iodef:StartTime>2004-02-02T22:19:24+00:00
            </iodef:StartTime>
            <iodef:DetectTime>2004-02-02T22:49:24+00:00
```

```
            </iodef:DetectTime>
            <iodef:ReportTime>2004-02-02T23:20:24+00:00
            </iodef:ReportTime>
            <iodef:Assessment>
```

```
            <iodef:Impact severity="low" completion="failed"
             type="dos"></iodef:Impact>
          </iodef:Assessment>
          <iodef:Contact role="creator" role="irt"
           type="organization">
            <iodef:ContactName>CSIRT-FOR-OUR-DOMAIN
            </iodef:ContactName>
            <iodef:Email>csirt-for-our-domain@ourdomain
            </iodef:Email>
          </iodef:Contact>
          <iodef:Contact role="tech" type="organization">
            <iodef:ContactName>Constituency-contact for 10.1.1.2
            </iodef:ContactName>
            <iodef:Email>Constituency-contact@10.1.1.2</iodef:Email>
          </iodef:Contact>
          <iodef:History>
            <iodef:HistoryItem type="notification">
              <iodef:IncidentID
               name="CSIRT-FOR-OUR-DOMAIN">CSIRT-FOR-OUR-DOMAIN#207-1
      </iodef:IncidentID>CERT-FOR-OUR-DOMAIN
              <iodef:Description>Notification sent to next upstream
               NP closer to 10.1.1.2</iodef:Description>
              <iodef:DateTime>2001-09-14T08:19:01+00:00
              </iodef:DateTime>
            </iodef:HistoryItem>
          </iodef:History>
          <iodef:EventData>
            <iodef:System category="source">
              <iodef:Service>
                <iodef:Port>38765</iodef:Port>
              </iodef:Service>
              <iodef:Node>
                <iodef:Address category="ipv4-addr">10.1.1.2
                </iodef:Address>
              </iodef:Node>
            </iodef:System>
            <iodef:System category="target">
              <iodef:Service>
                <iodef:Port>80</iodef:Port>
              </iodef:Service>
                <iodef:Node>
               <iodef:Address category="ipv4-addr">192.168.1.2
               </iodef:Address>
                </iodef:Node>
            </iodef:System>
            <iodef:Expectation priority="high"
                   iodef:atype="rate-limit-host">
              <iodef:Description>Rate limit traffic close to
```

```
                source</iodef:Description>
            </iodef:Expectation>
            <iodef:Record>
            <iodef:RecordData>
```

```
                <iodef:RecordItem dtype="ipv4-packet">450000522ad
                 90000ff06c41fc0a801020a010102976d0050103e020810d
                 94a1350021000ad6700005468616e6b20796f7520666f722
                 06361726566756c6c792072656164696e672074686973205
                 246432e0a
                </iodef:RecordItem>
                <iodef:Description>The IPv4 packet included
                     was used in the described attack
                </iodef:Description>
              </iodef:RecordData>
            </iodef:Record>
          </iodef:EventData>
        </iodef:IncidentData>
      </iodef:Incident>
   </iodef:IODEF-Document>

    <-- Digital Signature applied to the RecordItem class using the
        XML Digital Signature W3C Recommendations.               -->

<?xml version="1.0" encoding="UTF-8"?><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
             6361726566756c6c792072656164696e6720746869732052
             46432e0a
    </iodef:RecordItem>
  </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>
    -->
```

4.5.2 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.

```
  Attack Dest      NP-1              NP-2        Attack Src

  1. Attack    |  Attack
     reported  |  detected
  2.              Determine source
                  of security incident
  3.              o---Investigation---->
  4.                              Research
                                  incident and
                                  determine appropriate
                                  actions to take
  5.              <-------Result-------o
```

Figure 9: Investigation Communication Flow

4.5.2.1 Example Investigation Request

The following example will only include 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>
         <iodef-rid:MsgType>Investigation</iodef-rid:MsgType>
         <iodef-rid:PolicyRegion>PeertoPeer
         </iodef-rid:PolicyRegion>
         <iodef-rid:MsgDestination>SourceOfIncident
         </iodef-rid:MsgDestination>
            <iodef:Node>
               <iodef:Address category="ipv4-addr">172.25.1.33
               </iodef:Address>
            </iodef:Node>
         <iodef-rid:TrafficType>Attack</iodef-rid:TrafficType>
         <iodef:IncidentID
          name="CERT-FOR-OUR-DOMAIN">CERT-FOR-OUR-DOMAIN#208-1
         </iodef:IncidentID>
       </iodef-rid:RIDPolicy>
         <iodef-rid:NPPath>
         <iodef:Name>CSIRT-FOR-OUR-DOMAIN</iodef:Name>
         <iodef:RegistryHandle>CSIRT123</iodef:RegistryHandle>
         <iodef:Email>csirt-for-our-domain@ourdomain</iodef:Email>
         <iodef:Node>
            <iodef:Address category="ipv4-addr">172.17.1.2
            </iodef:Address>
         </iodef:Node>
       </iodef-rid:NPPath>
       <iodef-rid:NPPath>
         <iodef:Name>CSIRT-FOR-UPSTREAM-NP</iodef:Name>
         <iodef:RegistryHandle>CSIRT345</iodef:RegistryHandle>
         <iodef:Email>csirt-for-upstream-np@ourdomain</iodef:Email>
         <iodef:Node>
            <iodef:Address category="ipv4-addr">172.20.1.2
            </iodef:Address>
         </iodef:Node>
       </iodef-rid:NPPath>
     </iodef-rid:RID>
<-- IODEF and XML digital signature follow -->
```

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 10: 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.

4.5.3.1 Report Example

The following example will only include 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>
    <iodef-rid:MsgType>Report</iodef-rid:MsgType>
    <iodef-rid:PolicyRegion>PeertoPeer
    </iodef-rid:PolicyRegion>
    <iodef-rid:MsgDestination>RIDSystem
    </iodef-rid:MsgDestination>
       <iodef:Node>
          <iodef:Address category="ipv4-addr">172.17.1.2
          </iodef:Address>
       </iodef:Node>
    <iodef-rid:TrafficType>Attack</iodef-rid:TrafficType>
    <iodef:IncidentID
     name="CERT-FOR-OUR-DOMAIN">CERT-FOR-OUR-DOMAIN#209-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
   <iodef-rid:NPPath>
```

```
            <iodef:Name>CSIRT-FOR-OUR-DOMAIN</iodef:Name>
            <iodef:RegistryHandle>CSIRT123</iodef:RegistryHandle>
            <iodef:Email>csirt-for-our-domain@ourdomain</iodef:Email>
```

```
            <iodef:Node>
               <iodef:Address category="ipv4-addr">172.20.1.2
               </iodef:Address>
            </iodef:Node>
          </iodef-rid:NPPath>
          <iodef-rid:NPPath>
            <iodef:Name>CSIRT-FOR-REQUESTING-NP</iodef:Name>
            <iodef:RegistryHandle>CSIRT345</iodef:RegistryHandle>
            <iodef:Email>csirt-for-requesting-np@ourdomain
            </iodef:Email>
            <iodef:Node>
               <iodef:Address category="ipv4-addr">172.17.1.2
               </iodef:Address>
            </iodef:Node>
          </iodef-rid:NPPath>
        </iodef-rid:RID>
<-- IODEF and XML digital signature follow -->
```

4.5.4 IncidentQuery Communication Flow

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

```
   NP-1                          NP-2
1. Generate a request for
   information on a specific
   incident number or incident type
2.             o---IncidentQuery--->
3.                              Verify policy information
                                and determine if matches exist
                                for requested information
4.             <-------Report------o
5.  Associate report to request
    by incident number or type
    and file report(s).
```

Figure 11: 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.

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 will remain

null and the IP packet data will not be included in the IODEF RecordItem class and the other incident information will be 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-1.0"
        xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
        <iodef-rid:RIDPolicy>
         <iodef-rid:MsgType>IncidentQuery</iodef-rid:MsgType>
         <iodef-rid:PolicyRegion>PeertoPeer
         </iodef-rid:PolicyRegion>
         <iodef-rid:MsgDestination>RIDSystem
         </iodef-rid:MsgDestination>
            <iodef:Node>
               <iodef:Address category="ipv4-addr">172.20.1.2
               </iodef:Address>
            </iodef:Node>
         <iodef-rid:TrafficType>Attack</iodef-rid:TrafficType>
         <iodef:IncidentID
          name="CERT-FOR-OUR-DOMAIN">CERT-FOR-OUR-DOMAIN#210-1
         </iodef:IncidentID>
       </iodef-rid:RIDPolicy>
        <iodef-rid:NPPath>
         <iodef:Name>CSIRT-FOR-OUR-DOMAIN</iodef:Name>
         <iodef:RegistryHandle>CSIRT123</iodef:RegistryHandle>
         <iodef:Email>csirt-for-our-domain@ourdomain</iodef:Email>
         <iodef:Node>
            <iodef:Address category="ipv4-addr">172.17.1.2
            </iodef:Address>
         </iodef:Node>
       </iodef-rid:NPPath>
       <iodef-rid:NPPath>
         <iodef:Name>CSIRT-FOR-UPSTREAM-NP</iodef:Name>
         <iodef:RegistryHandle>CSIRT345</iodef:RegistryHandle>
         <iodef:Email>csirt-for-upstream-np@ourdomain</iodef:Email>
         <iodef:Node>
            <iodef:Address category="ipv4-addr">172.20.1.2
            </iodef:Address>
         </iodef:Node>
       </iodef-rid:NPPath>
 </iodef-rid:RID>
```

5. RID Schema Definition

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSPY v2004 rel. 3 U (http://www.xmlspy.com) by
     Kathleen M Moriarty (MIT Lincoln Laboratory) -->
<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"/>
<!-- ************************************************************
*********************************************************************
*** Incident Object Description and Exchange Format XML Schema    ***
***               Version 08,   August 2006                       ***
*********************************************************************
***  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"/>
<-- NPPath must be included in every RID message but is set to
    monOccurs 0 for the purpose of proper parsing of the SOAP
    header.  NPPath is needed for the proper flow and response
    of RID messages-->
      <xs:element ref="iodef-rid:NPPath" minOccurs="0"
          maxOccurs="unbounded"/>
      <xs:element ref="iodef-rid:TraceStatus"/>
```

```
      <xs:element ref="iodef-rid:IncidentSource" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="meaning" type="xs:string"/>
  </xs:complexType>
```

```
<!--Path of the RID trace includes information on each NP
        involved in the upstream trace-->
<xs:element name="NPPath" type="iodef-rid:NPPathType"/>
  <xs:complexType name="NPPathType">
    <xs:sequence>
      <xs:element ref="iodef:ContactName" minOccurs="0"/>
      <xs:element ref="iodef:RegistryHandle" minOccurs="0"
          maxOccurs="unbounded"/>
      <xs:element ref="iodef:Email" minOccurs="0"
          maxOccurs="unbounded"/>
      <xs:element ref="iodef:Telephone" minOccurs="0"
          maxOccurs="unbounded"/>
      <xs:element ref="iodef:Fax" minOccurs="0"/>
      <xs:element ref="iodef:TimeZone" minOccurs="0"/>
      <xs:element ref="iodef-rid:NPPath" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="restriction" type="xs:NMTOKEN"/>
    <xs:attribute name="NPPath" type="xs:NMTOKEN" use="required"/>
  </xs:complexType>
  <xs:element name="TimeZone"/>
<!--Used in Trace Authorization Message for RID-->
<xs:element name="TraceStatus" type="iodef-rid:TraceStatusType"/>
  <xs:complexType name="TraceStatusType">
    <xs:sequence>
      <xs:element name="AuthorizationStatus" default="Approved">
        <xs:simpleType>
          <xs:restriction base="xs:string">
          <xs:whiteSpace value="collapse"/>
            <xs:enumeration value="Approved"/>
            <xs:enumeration value="Denied"/>
            <xs:enumeration value="Pending"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
    <xs:attribute name="restriction" type="xs:NMTOKEN"/>
  </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:complexType>
  <xs:element name="SourceFound" type="xs:boolean"/>
<!--
```

```
====== Real-Time Inter-network Defense Policy - RIDPolicy ======
====  Suggested definition for RIDPolicy for messaging
 -->
<xs:annotation>
```

```
 <xs:documentation>RID Policy used in SOAP header 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:MsgType"/>
      <xs:element ref="iodef-rid:PolicyRegion" maxOccurs="unbounded"/>
      <xs:element ref="iodef-rid:MsgDestination"/>
      <xs:element ref="iodef:Node"/>
      <xs:element ref="iodef-rid:TrafficType" maxOccurs="unbounded"/>
      <xs:element ref="iodef:IncidentID"/>
    </xs:sequence>
  </xs:complexType>
  <xs:element name="MsgType" default="Report">
    <xs:simpleType>
      <xs:restriction base="xs:string">
      <xs:whiteSpace value="collapse"/>
        <xs:enumeration value="TraceRequest"/>
        <xs:enumeration value="TraceAuthorization"/>
        <xs:enumeration value="Result"/>
        <xs:enumeration value="Investigation"/>
        <xs:enumeration value="Report"/>
        <xs:enumeration value="IncidentQuery"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="MsgDestination" default="RIDSystem">
    <xs:simpleType>
      <xs:restriction base="xs:string">
      <xs:whiteSpace value="collapse"/>
        <xs:enumeration value="RIDSystem"/>
        <xs:enumeration value="SourceOfIncident"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="PolicyRegion">
    <xs:simpleType>
      <xs:restriction base="xs:string">
      <xs:whiteSpace value="collapse"/>
        <xs:enumeration value="ClientToNP"/>
        <xs:enumeration value="NPToClient"/>
        <xs:enumeration value="InterConsortium"/>
        <xs:enumeration value="PeerToPeer"/>
        <xs:enumeration value="BetweenConsortiums"/>
        <xs:enumeration value="AcrossNationalBoundaries"/>
```

```
      </xs:restriction>
    </xs:simpleType>

  </xs:element>
```

```
  <xs:element name="TrafficType" default="Attack">
    <xs:simpleType>
      <xs:restriction base="xs:string">
      <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:restriction>
    </xs:simpleType>
  </xs:element>
</xs:schema>
```

6. Message Transport

The transport specifications will be fully defined in a separate document. The specified transport protocols must use encryption to provide an additional level of security, integrity, and authentication through bi-directional certificate usage. SOAP [15] will be used as a wrapper for the RID messages, then a protocol binding will be used for the overlying transport. Any transport method defined will take advantage of existing standards for ease of implementation and integration of RID systems. Session encryption for the transport RID messages will be enforced in the transport specification. The privacy and security considerations are addressed fully in RID and do not rely on the security provided by the transport layer. The encryption requirements and considerations for RID are discussed in the Security section of this document.

XML security functions such as digital signature and encryption 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 and encryption 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 will be 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 NMS 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, S/MIME, 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 support HTTPS and optionally support other protocols such as S/MIME and BEEP. RID, the XML security functions, and transport protocols must properly integrate with a public key infrastructure (PKI) managed by the consortium. 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.

In order to address the integrity and authenticity of messages, transport encryption MUST be used to secure the traffic sent between RID systems with pre-defined trust relationships. Systems with predefined relationships for RID would include those who peer within a consortium with agreed-upon appropriate use regulations and for peering consortiums.

Systems used to send authenticated RID messages between networks MUST use a dedicated and secured 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 interface must only listen for and send RID messages, 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 using a PKI must be inherent to the protocol. SOAP tied together with TLS used with BEEP or HTTP(S) using WS-Security requires a trust center such as a PKI or Kerberos key distribution center for the distribution of

credentials to provide the necessary levels of security for this protocol. Public key certificate pairs issued by a trusted Certificate Authority (CA) will 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. 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).

Hosts receiving a RID message, such as a TraceRequest, for example, 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 can be used to authenticate the request. The X.509 version 3 specifications as well as the digital signature specifications and Certificate Revocation List (CRL) Internet standards set forth in RFC2459 must be followed in order to interoperate with a PKI designed for similar Internet 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 or digital signature is used within a document. Transport specifications will be 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 TraceRequest should be processed automatically or if human intervention is required.

6.4 Authentication Considerations for a Multi-hop TraceRequest

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 peer as to the confidence rating of the attack and the previous trust relationships in the downstream path. 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.

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 [22]. 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 status. 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. 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 used in section 6.3 will also provide the keys used to digitally sign the RecordItem class for TraceRequests to meet the requirement of authenticating the original request. Since the CA is known and trusted by all parties, any host in the path of the trace can verify the digital signature.

In the case in which an enterprise network using RID sends a trace request 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 the message to assure the authenticity of the trace. 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 at the NP level.

6.4.1 Public Key Infrastructures and Consortiums

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. 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 guidelines MUST include

O Physical and logical practices to protect RID systems;
O Network and application layer protection for RID systems and communications;
O Proper use guidelines for RID systems, messages, and requests; and
O 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.

Inter-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 inter-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.

RID is useful in determining the true source of a packet that traverses multiple networks or to communicate security incidents and automate the response.

In order to identify the source and trace multiple networks, the packet header information along with 8 bytes of payload are used in the packet identification. 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-network provide 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 on the fields containing the identity, using the public encryption key for 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 needs to 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 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 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 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 relay the request 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. 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.

Inter-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 have addressed issues of privacy 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 S/MIME or TLS over BEEP or HTTPS. The RID messages must 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. 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 SOAP, RIDPolicy information, Transport Layer Security (TLS), and the XML security features of encryption and digital signatures, 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 and XML encryption are used in the following cases:

XML Digital Signature

- Originator of the Trace or Investigation Request MUST sign the RecordItem class data to provide authentication to all

upstream participants in the trace of the origin. This signature MUST be passed to all recipients of the TraceRequest.

- For all message types, the full RID message MUST be signed by the sending peer to provide authentication and integrity to the

receiving RID system.

XML Encryption

- The entire message 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. The RIDPolicy class will be presented in clear text in the SOAP header.
- 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 the SOAP header 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, the entire message, with the exception of the RIDPolicy information and incident identifier, could be encrypted for the originator of the request. The existence of the Result message for an incident would tell the intermediate parties used in the path of the trace that the incident trace has been completed.

Policies between NPs must be established to provide guidelines for communication. The policy should include communication methods, security, and fall-back procedures. The policy should establish a method to protect communications of RID systems between all bordering NPs. The trust relationships should extend to all bordering NPs to support tracing and stopping attacks throughout the network. A fully meshed communication ability would provide the means for all RID messages to be sent directly to the intended RID system. If a fully meshed communication system is not available, messages may have to traverse multiple systems to reach the intended RID system. Other policy considerations include how the RegistryHandle and RID system IP address should be shared. This should also be coupled with any necessary pre-shared key or certificate (or trusted Security Authority) stored in the RID system for encryption negotiation where PKI is in use.

Note: The contact information and corresponding IP address for a network RID system is shared among cooperating networks via a predefined table. This information may be stored locally in RID systems or a central database accessible on the secured network

used for inter-NP messaging. The repository can also be used as the border directory to other consortiums for sharing public key information necessary to establish and protect communications.

The method of passing a TraceRequest message to subsequent networks eliminates the need for granting access to remote entities to configure network equipment on border networks. Access to network equipment to configure systems for trace continuance remains in the responsibility of the parties who own and manage that equipment. Thus, there is no need to share authentication information with devices outside of the network operation center managing the device. Network administrators, who have the ability to base the decision on the available resources and other factors of their network, maintain control of the continuance of a trace.

8. IANA Considerations

This document uses URNs to describe XML namespaces and XML schemas 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 and denial-of-service attacks 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 a network provider's 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 that may originate on an IDS system wrapped in a RID message. A TraceRequest or Investigation request is communicated to an upstream provider 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. References

[ISO 9594/8] CCITT Rec. X.509 (1994) | ISO/IEC 9594-8:1994, Information Technology - Open Systems Interconnection The Directory: Authentication Framework

[RFC791] "Internet Protocol, DARPA Internet Program, Protocol Specification." Information Sciences Institute, University of Southern California. September 1981.

[RFC1213] "Management Information Base for Network Management of TCP/IP-based Internets: MIB-II." K. McCloghrie and M . Rose. March 1991.

[RFC1215] "A Convention for Defining Traps for use with the SNMP." M. Rose. March 1991.

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

[RFC2246] "The TLS Protocol." T. Dierks and C. Allen. January 1999.

[RFC2256] "A Summary of the X.500(96) User Schema for use with LDAPv3." M. Wahl. December 1997.

[RFC2459] "Internet Public Key Infrastructure: Part I: X.509 Certificate and CRL Profile." R. Housley, W. Ford, W. Polk, and D. Solo. January 1999.

[RFC2527] "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework." S. Chokhani and W. Ford. March 1999.

[RFC2528] "Internet X.509 Public Key Infrastructure: Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates." R. Housley and W. Polk. March 1999.

[RFC2720] "Traffic Flow Measurement: Meter MIB." N. Brownlee. October 1999.

[RFC2722]"Traffic Flow Measurement: Architecture." N. Brownlee, C. Mills, and G. Ruth. October 1999.

[RFC2723] "SRL: A Language for Describing Traffic Flows and Specifying Actions for Flow Groups." N. Brownlee. October 1999.

[RFC2827] "Network Ingress Filtering: Defeating Denial of Service

Attacks Which Employ IP Source Address Spoofing." P. Ferguson and
D. Senie. May 2000.

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

[RFC3821] "An Internet Attribute Certificate Profile for Authorization." S. Farrell and R. Housley. April 2002.

[RFCXXXX] "The Incident Data Exchange Format Data Model and XML Implementation." J. Meijer, R. Danyliw, and Y. Demchenko. August 2006. http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-08.txt

[RFCXXXX] "Requirements for the Format for INcident information Exchange," Y. Demchenko, R. Danyliw, and G. Keeni, June 2006. http://www.ietf.org/internet-drafts/draft-ietf-inch-requirements-08.txt

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

[2] Applied Cryptography: Protocols, Algoritms, and Source Code B.C. Schneier. Second edition. John Wiley & Sons. 1996.

[3] "CenterTrack: An IP Overlay Network for Tracing DoS Floods." R. Stone. 9th Usenix Security Symposium Proceedings. August 2000.

[4] 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

[5] http://www.cisco.com/go/netflow

[6] http://www.info-sec.com/denial/infosece.html-ssi

[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] "Inferring Internet Denial of Service Activity." D. Moore, G. M. Voelker, and S. Savage. Published in Proceedings of the 2001 USENIX Security Symposium.

[10] "MULTOPS: A Data-Structure For Bandwidth Attack Detection." T. M. Gil and M. Poletta. Published in Proceedings of

the 2001 USENIX Security Symposium.

[11] "Network Congestion Monitoring and Detection using the IMI

infrastructure." T. Saitoh, G. Mansfield, and N.Shiratori.
Graduate School of Information Sciences, Tohoku University.

[12] PKCS 5 v2.0 Password-Based Cryptography Standard. RSA Security
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-5/index.html.
March 1999.

[13] PKCS 7 Cryptographic Message Syntax Standard. RSA Security.
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html.
May 1997.

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

[15] Security Architecture for Open Agent Systems. Vrije
Universiteit. Y. Demchenko, B. Overiender, and H. M. Boonstra.
http://carol.science.uva.nl/~demch/worksinprogress/
draft-saas-paper03.pdf

[16] "Security in a Web Services World: A Proposed Architecture
and Roadmap." IBM and Microsoft. April 2002.
http://www-106.ibm.com/developerworks/webservices/library/ws-secmap

[17] SOAP Version 1.2 Part 0: Primer. W3C Recommendation.
http://www.w3c.org/TR/REC-soap12-part0-20030624/. 24 June 2004.

[18] SOAP Version 1.2 Part 1:Messaging Framework. W3C
Recommendation. http://www.w3c.org/TR/REC-soap12-part1-20030624/.
24 June 2004.

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

[20] XML Encryption Syntax and Processing, W3C Recommendation.
T. Imamura, B. Dillaway, and E. Simon. December 2002.

http://www.w3.org/TR/xmlenc-core/

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

[22] 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.

10.1 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: Dr. Robert K. Cunningham, Cynthia D. McLain, Dr. William Streilein, Iljitsch van Beijnum, Steve Bellovin, Yuri Demchenko, Jean-Francois Morfin, Jose Nazaro, Stephen Northcutt, Jeffrey Schiller, Brian Trammell, Roman Danyliw, and Tony Tauber.

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

10.2 Author Information

Kathleen M. Moriarty
MIT Lincoln Laboratory
244 Wood Street
Lexington, MA 02420
Email: Moriarty@ll.mit.edu

rights.

Disclaimer of Validity

Copyright Statement

Sponsor Information

This work was sponsored by the Air Force under Air Force Contract FA8721-05-C-0002.

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