Internet Engineering Task Force (IETF)
Request for Comments: 6545
Obsoletes: 6045
Category: Standards Track
ISSN: 2070-1721

K. Moriarty
EMC

April 2012

Real-time Inter-network Defense (RID)

Abstract

Security incidents, such as system compromises, worms, viruses, phishing incidents, and denial of service, typically result in the loss of service, data, and resources both human and system. Service providers and Computer Security Incident Response Teams need to be equipped and ready to assist in communicating and tracing security incidents with tools and procedures in place before the occurrence of an attack. Real-time Inter-network Defense (RID) outlines a proactive inter-network communication method to facilitate sharing incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident-handling solution. Combining these capabilities in a communication system provides a way to achieve higher security levels on networks. Policy guidelines for handling incidents are recommended and can be agreed upon by a consortium using the security recommendations and considerations. This document obsoletes RFC 6045.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6545.

Table of Contents

1. Introduction

Organizations require help from other parties to identify incidents, mitigate malicious activity targeting their computing resources, and to gain insight into potential threats through the sharing of information. This coordination might entail working with a service provider (SP) to filter attack traffic, working with an SP to resolve a configuration issue that is unintentionally causing problems, contacting a remote site to take down a bot network, or sharing watch-lists of known malicious IP addresses in a consortium. The term "SP" is to be interpreted as any type of service provider or Computer Security Incident Response Team (CSIRT) that may be involved in RID communications.

Incident handling involves the detection, reporting, identification, and mitigation of an incident, whether it be a benign configuration issue, IT incident, an infraction to a service level agreement (SLA), system compromise, socially engineered phishing attack, or a denial-of-service (DoS) attack, etc. When an incident is detected, the response may include simply filing a report, notification to the source of the incident, a request to an SP for resolution/mitigation,

or a request to locate the source. One of the more difficult cases is that in which the source of an attack is unknown, requiring the ability to trace the attack traffic iteratively upstream through the network for the possibility of any further actions to take place. In cases when accurate records of an active session between the target or victim system and the source or attacking system are available, the source is easy to identify.

Real-time inter-network defense (RID) outlines a proactive inter-network communication method to facilitate sharing incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution. RID provides a secure method to communicate incident information, enabling the exchange of Incident Object Description and Exchange Format (IODEF) [RFC5070] Extensible Markup Language (XML) documents. RID considers security, policy, and privacy issues related to the exchange of potentially sensitive information, enabling SPs or organizations the options to make appropriate decisions according to their policies. RID includes provisions for confidentiality, integrity, and authentication.

The data in RID messages is represented in an XML [XML1.0] document using the IODEF and RID. By following this model, integration with other aspects for incident handling is simplified. 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 incident or attack at hand. RID is intended to provide a method to communicate the relevant information between CSIRTs while being compatible with a variety of existing and possible future detection-tracing and response approaches. Incidents may be extended to include Information Technology (IT) incidents, where RID enables the communication between or within providers for non-security IT incidents.

Security and privacy considerations are of high concern since potentially sensitive information may be passed through RID messages. RID messaging takes advantage of XML security, privacy, and policy information set in the RID schema. The RID schema defines communication-specific metadata to support the communication of IODEF documents for exchanging or tracing information regarding incidents. RID messages are encapsulated for transport, which is defined in a separate document [RFC6546]. The authentication, integrity, and authorization features that RID and RID transport offer are used to achieve a necessary level of security.

Coordinating with other CSIRTs is not strictly a technical problem. There are numerous procedural, trust, and legal considerations that might prevent an organization from sharing information. RID provides

information and options that can be used by organizations who must then apply their own policies for sharing information. Organizations must develop policies and procedures for the use of the RID protocol and IODEF.

1.1. Changes from RFC 6045

This document contains the following changes with respect to its predecessor [RFC6045]:

- This document is Standards Track, while [RFC6045] was published as Informational.
- This document obsoletes [RFC6045] and moves it to Historic status.
- This document refers to the updated RID transport specification [RFC6546], where appropriate.
- Edits reflected in this updated version of RID are primarily improvements to the informational descriptions. The descriptions have been updated to clarify that IODEF and RID can be used for all types of incidents and are not limited to network security incidents. The language has been updated to change the focus from attacks to incidents, where appropriate. The term "network provider" has been replaced with the more generic term of "service provider". Several introductory informational sections have been removed as they are not necessary for the implementation of the protocol. The sections include:
  - 1.3. Attack Types and RID Messaging,
  - 2. RID Integration with Network Provider Technologies,
  - 3.1. Integrating Trace Approaches, and
  - 3.2. Superset of Packet Information for Traces.
- An option for a star topology has been included in an informational section to meet current use-case requirements of those who provide reports on incident information.
- The schema version was incremented. The schema has changed to include IODEF [RFC5070] enveloped in RID in the RIDPolicy class using the new ReportSchema class, to include one verified erratum, to include additional enumerations in the Justification attribute, to remove the AcrossNationalBoundaries region enumeration, to add the DataWithHandlingRequirements enumeration in TrafficTypes, and to change the name of the RequestAuthorization MsgType to

Acknowledgement. Additional text has been provided to clarify definitions of enumerated values for some attributes. The RequestAuthorization name was replaced with Acknowledgement to more accurately represent the function of that message type. Text was clarified to note the possible use of this message in response to Query and Report messages. The attributes were fixed in the schema to add 'lang' at the RID class level for language support.

- The TraceRequest and Investigation messages have been collapsed into a single message with the requirement to set the MsgType according to the functionality required for automation. The message descriptions were identical with the exception of the MsgType, which remains an exception depending on the desired function. Since both of the enumerations for MsgType are each a Request, 'Investigation' is now 'InvestigationRequest'. Content may vary within the IODEF document for the type of Request specified.

- The IncidentQuery message description name and MsgType enumeration value in the schema have been changed to the more generic name of 'Query'.

- Guidance has been improved to ensure consistent implementations and use of XML encryption to provide confidentiality based on data markers, specifically the iodef:restriction attribute in the IODEF and IODEF-RID schemas. The attribute may also be present in IODEF extension schemas, where the guidance also applies. Additional guidance and restrictions have been added for XML requirements.

- All of the normative text from the Security Considerations section has been moved to a new section, Security Requirements.

- The order in which the RID schema is presented in Section 5 has been changed to match the order in the IODEF-RID schema.

- Additional text has been provided to explain the content and interactions between entities in the examples.

- Additional references have been provided to improve interoperability with stricter guidance on the use of XML digital signatures and encryption.

1.2. Normative and Informative

Sections 1, 2, 3, and 12 provide helpful background information and considerations. RID systems participating in a consortium are REQUIRED to fully implement Sections 4, 5, 6, 7, 8, 9, 10, and 11 to prevent interoperability concerns.

1.3. Terminology

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

2. Characteristics of Incidents

An incident may be defined as a benign configuration issue, IT incident, an infraction to a service level agreement (SLA), system compromise, a worm or Trojan infection, or a single- or multiple-source denial-of-service attack. 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. Incident tracing can be used to identify the source(s) of an attack in order to halt or mitigate the undesired behavior or to correct an identified issue. RID messages can be communicated between entities to report or investigate any type of incident and allow for actions to be taken when the source of the incident or a point closer to the source is known or has been identified. Methods to accomplish mitigation may include remediation of a configuration issue, filtering or rate-limiting the traffic close to the source, or taking the host or network offline. Care must also be taken to ensure that the systems involved in the RID communications are not abused and to use proper analysis in determining if attack traffic is, in fact, attack traffic at each SP involved in the investigation.

Investigating 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 the difficult task of locating the true origin for the administrators. Attackers use many techniques, which can vary between individuals or even organized groups of attackers. Through analysis, the techniques may be grouped into indicators of compromise to be shared via IODEF and RID, further assisting with the improvement of detection capabilities. Security incidents, including distributed denial-of-service (DDoS) attacks, can be difficult or nearly impossible to trace because of the nature of the attack. Some of the difficulties in investigating attacks include the following:

- the incident or attack originates from multiple sources;

- the incident may leverage social-engineering techniques or other methods to gain access to resources and intellectual property using what appears to be legitimate access methods such as outbound web sessions from user systems;

- 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;

- 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 SP or HTTP requests sent to an organization connected to the Internet;

- the attack may utilize varying types of packets including TCP, UDP, ICMP, or other IP protocols;

- the attack may be from "zombies" or large botnets, which then require additional searches to locate a controlling server as the true origin of the attack;

- the attack may use a very small number of packets from any particular source, thus making a trace after the fact nearly impossible;

- the indicators of a compromise may be difficult to detect.

If the source(s) of an incident cannot be determined from IP address information, it may be possible to trace the traffic based on characteristics of the incident such as tracing the increased bandwidth utilization or the type of packets seen by the client. In the case of packets with spoofed source addresses, it is not a trivial task to identify the source of an attack.

IODEF, any extensions to IODEF, and RID can be used to detail an incident, characteristics of the incident (as it evolves), the incident history, and communications of the incident to facilitate the resolution and reporting of the incident.

3. Communication between CSIRTs and Service Providers

Expediting the communication between CSIRTs and SPs is essential when responding to a security-related incident, which may cross network access points between service providers. As a result of the urgency involved in this inter-service-provider security incident communication, there must be an effective system in place to facilitate the interaction. This communication policy or method 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, email may not be received in a timely fashion or be acted upon with the same urgency as a phone call or other communication mechanism like RID.

A technical solution to trace traffic across a single SP may include homegrown or commercial systems for which RID messaging must accommodate the input requirements. The incident-handling system used on the SP's backbone by the CSIRT to coordinate the trace across the single network requires a method to accept, process, and relay RID messages 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 service provider maintains its own system capable of communicating via RID and integrates with a management station used for monitoring and analysis. An alternative for providers lacking sufficient resources may be to have a neutral third party with access to the provider's network resources who could be used to perform the incident-handling functions. This could be a function of a central organization operating as a CSIRT for countries as a whole or within a consortium that may be able to provide centralized resources.

Consortiums could consist of a federation or a group of service providers or CSIRTs that agrees to participate in the RID communication protocol with an agreed-upon policy and communication protocol facilitating the secure transport of IODEF-RID XML documents. Transport for RID messages is specified in [RFC6546].

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

The network used for the communication should consist of out-of-band or protected channels (direct communication links) or encrypted channels dedicated to the transport of RID messages. The communication links would be direct connections (virtual or physical) between peers who have agreed-upon use and abuse policies through 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 or is based on regions and logical groups. 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 arbiter. 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 provider may be negotiated in a contract as part of a value-added service or through a service level agreement (SLA). Further discussion is beyond the scope of this document and may be more appropriately handled in 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, CERT Coordination Center (CERT/CC), Global Information Assurance Certification (GIAC), and the U.S. Federal Bureau of Investigations (FBI) or other assisting government organization in the country of the investigation.

3.1. Inter-Service-Provider RID Messaging

RID provides a protocol and format that ensures interoperability between vendors for the implementation of an incident messaging mechanism. The messages should meet several requirements in order to be meaningful as they traverse multiple networks. RID provides the framework necessary for communication between networks involved in the incident handling, possible traceback, and mitigation of a security incident. Several message types described in Section 4.2 are necessary to facilitate the handling of a security incident. The message types include the Report, Query, Request, Acknowledgement, and Result 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.

A Query message is used to request information on a particular incident. A Request message with options set to 'TraceRequest' is used when the source of the traffic may have been spoofed. In that case, each SP in the upstream path who receives this Request will issue a trace across the network to determine the upstream source of the traffic. The Acknowledgement and Result messages are used to communicate the status and result of a Request. The Request message with options set to 'InvestigationRequest' may be sent to any party assisting in an incident investigation. The InvestigationRequest leverages the bilateral relationships or a consortium's interconnections 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 an InvestigationRequest. A Request message (set to 'TraceRequest' or 'InvestigationRequest') sent between RID systems to stop traffic at the source through a bordering network requires 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 (ASN) [RFC1930] or Network Information Center (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 Request with MsgType set to 'TraceRequest' that contains 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. This identifier 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 established through 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 or 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 Requirements section, along with other requirements that must be agreed upon by participating entities.

RID requests must be legitimate incidents and not used for purposes such as sabotage or censorship. An example of such abuse of the system includes 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 enables a network manager to assess the available resources before continuing a Request message set to 'InvestigationRequest' or 'TraceRequest'. If the Confidence rating (provided in IODEF) is low, it may not be in the provider's best interest to continue the Request with options set to 'InvestigationRequest' or 'TraceRequest'. The Confidence ratings must adhere to the specifications for selecting the percentage used to avoid abuse of the system. Requests must be issued by authorized individuals from the initiating CSIRT, set forth in policy guidelines established through peering or a SLA.

3.2. RID Communication Topology

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

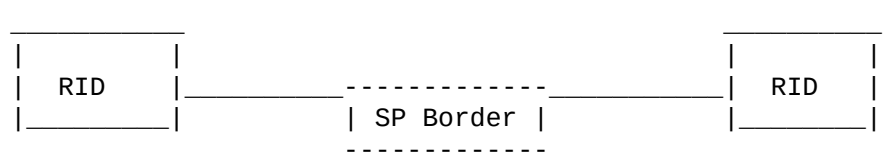

Figure 1: Direct Peer Topology

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 looks like the above diagram; however, there may be an extensive number of interconnections 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 if direct communication between SPs is not possible. An example is illustrated below.

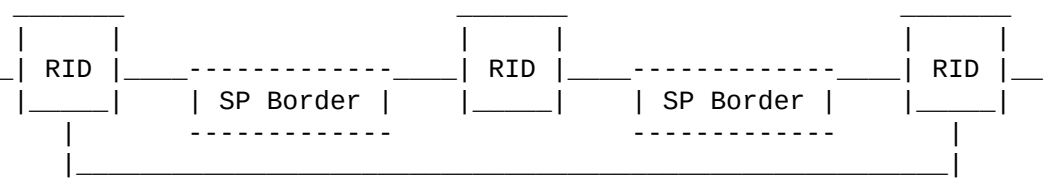

Figure 2: Mesh Peer Topology

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 decreasing the time in which the true source was identified. As a result, many networks would have utilized unnecessary resources for a Request that may have also been unnecessary.

A star topology may be desirable in instances where a peer may be a provider of incident information. This requires trust relationships to be established between the provider of information and each of the consumers of that information. Examples may include country-level CSIRTs or service providers distributing incident information to organizations.

4. Message Formats

4.1. RID Data Types

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

4.1.1. Boolean

A boolean value is represented by the BOOLEAN data type.

The BOOLEAN data type is implemented as "xs:boolean" [XMLschema] in the schema. Note that there are two lexical representations for boolean in [XMLschema]: '1' or 'true' for TRUE and '0' or 'false' or FALSE.

4.2. RID Message Types

The five RID message types described below MUST be implemented. RID messages uses both the IODEF [RFC5070] and RID document, which MUST be encapsulated for transport as specified in [RFC6546]. The messages are generated and received on designated systems for RID communications. Each RID message type, along with an example, is described in the following sections. The IODEF-RID schema is introduced in Section 5 to support the described RID message types.

1. Request. This message type is used when a request ('InvestigationRequest' or 'TraceRequest') is needed. The purpose of the Request message (set to 'InvestigationRequest') is to leverage the existing peer relationships in order to notify the SP closest to the source of the valid traffic of a security-related incident for any necessary actions to be taken. The Request (set to 'TraceRequest') is used when the traffic has to be traced iteratively through networks to find the source by setting the MsgType to 'TraceRequest'. The 'InvestigationRequest' MsgType is used for all other Request messages.

2. Acknowledgement. This message is sent to the initiating RID system from each of the upstream provider's RID systems to provide information on the status of a Request. The Acknowledgement is also used to provide a reason why a Request, Report, or Query was not accepted.

3. Result. The Result message is used to provide a final report and the notification of actions taken for a Request. This message is sent to the initiating CSIRT through the network of RID systems in the path of the trace as notification that the source of the attack was located.

4. 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, sharing incident information, statistics and trending information, etc.

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

When an application receives a RID message, it must be able to determine the type of message and parse it accordingly. The message type is specified in the RIDPolicy class. The RIDPolicy class may

also be used by the transport protocol to facilitate the communication of security incident data to trace, investigate, query, or report information regarding security incidents.

5. IODEF-RID Schema

There are three classes included in the RID extension required to facilitate RID communications. The RequestStatus class is used to indicate the approval status of a Request message; 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-upon policies and specifies the type of communication message being used.

The RID schema defines communication-specific metadata to support the exchange of incident information in an IODEF document. 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 and RID messages include both the RID and IODEF documents, the RID message acts as an envelope in that policy and security defined at the RID message layer are applied to both documents. One reason for maintaining separate schemas is for flexibility, where the RIDPolicy class can be easily extracted for use in the RID message and by the transport protocol.

The security requirements of sending incident information between entities include the use of encryption. The RIDPolicy information is not required to be encrypted, so separating out this data from the IODEF XML document removes the need for decrypting and parsing the IODEF 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 security requirements and policy guidelines are discussed in Section 9. The policy is defined between RID peers and within or between consortiums. RIDPolicy is meant to be a tool to facilitate the defined policies. This MUST be used in accordance with policy set between clients, peers, consortiums, and/or regions. Security, privacy, and confidentiality MUST be considered as specified in this document.

The RID schema is defined as follows:

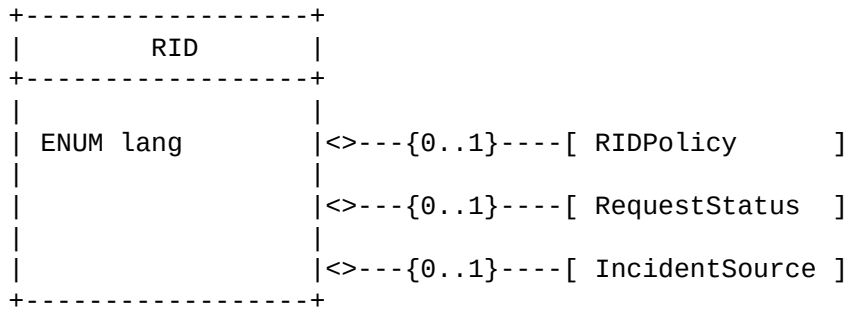

Figure 3: The RID Schema

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

RIDPolicy

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

RequestStatus

Zero or One. The RequestStatus class is used only in Acknowledgement messages. The message reports back to the CSIRT or SP in the Acknowledgement message to provide status on a Request or if an error or problem occurs with the receipt or processing of a Report, Query, or Result message.

IncidentSource

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

Each of the three listed classes may be the only class included in the RID class, hence the option for zero or one. In some cases, RIDPolicy MAY be the only class in the RID definition when used by the transport protocol [RFC6546], as that information should be as small as possible and may not be encrypted. The RequestStatus message MUST be able to stand alone without the need for an IODEF document to facilitate the communication, limiting the data transported to the required elements per [RFC6546].

The RID class has one attribute:

lang

One. REQUIRED. ENUM. A valid language code per [RFC5646] constrained by the definition of "xs:language" inherited from [XML1.0].

5.1. RIDPolicy Class

The RIDPolicy class facilitates the delivery of RID messages and is also referenced for transport in the transport document [RFC6546]. The RIDPolicy Class includes the ability to embed an IODEF document or XML documents that conform to schemas other than IODEF in the ReportSchema element.

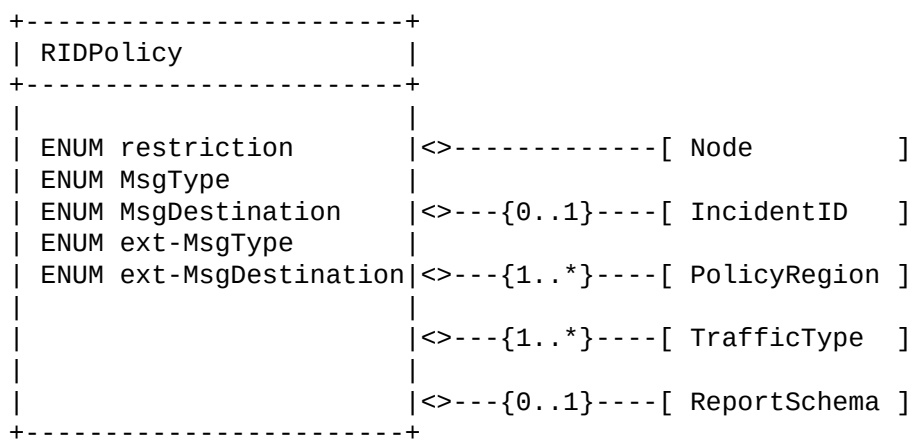

Figure 4: The RIDPolicy Class

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

Node

One. The Node class is used to identify a host or network device, in this case to identify the system communicating RID messages, and the usage is determined by the MsgDestination attribute. The base definition of this class is reused from the IODEF specification [RFC5070], Section 3.16. See Section 11 of this document for Internationalization considerations.

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 include botnets, polymorphic attacks, DDoS attacks, multiple hops of compromised systems found during an investigation, etc.

PolicyRegion

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

region

One or many. REQUIRED. ENUM. The attribute region is used to identify the expected sharing range of the incident information. The region may be within a region or defined by existing relationships such as those of a consortium or a client to a service provider.

1. ClientToSP. A client initiated the request to their service provider (SP). A client may be an individual, enterprise, or other type of entity (government, commercial, education, etc.). An SP may be a network, telecommunications, infrastructure, or other type of SP where a client-to-vendor relationship has been established. The client-to-vendor relationship will typically have established contracts or agreements to define expectations and trust relationships.

2. SPToClient. An SP initiated a RID request or report to a client. A client may be an individual, enterprise, or other type of entity (government, commercial, education, etc.). An SP may be a network, telecommunications, infrastructure, or other type of SP where a client-to-vendor relationship has been established. The client-to-vendor relationship will typically have established contracts or agreements to define expectations and trust relationships.

3. IntraConsortium. Incident information that should have no restrictions within the boundaries of a consortium with the agreed-upon use and abuse guidelines. A consortium is a well-defined group with established members and trust relationships specific to sharing within that group. A consortium would typically define the types of data that can be shared in advance, define the expectations on protecting that data, as well as have established contractual agreements. Examples of consortiums may include industry-focused sharing communities (financial, government, research and education, etc.) or cross industry sharing communities (for instance, organizations within local proximity that form a sharing group).

4. PeerToPeer. Incident information 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. PeerToPeer communications may involve any two individuals or entities that decide to share information directly with each other.

5. BetweenConsortiums. Incident information that should have no restrictions between consortiums that have established agreed-upon use and abuse guidelines. BetweenConsortiums is used when two consortiums (as defined in IntraConsortium above) share data. The types of data that can be shared BetweenConsortiums should be identified in their agreements and contracts along with expectations on how that data should be handled and protected.

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

TrafficType

One or many. REQUIRED. The values for the attribute "type" are meant to assist in determining if a trace is appropriate for the SP 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 that most accurately describes the traffic type.

type

One or many. REQUIRED. ENUM. The attribute type is used to identify the type of information included in the RID message or the type of incident.

1. Attack. This option SHOULD only be selected if the traffic is related to an information security incident or attack. The type of attack MUST also be listed in more detail in the IODEF Method and Impact classes for further clarification to assist in determining if the trace can be continued ([RFC5070], Sections 3.9 and 3.10.1).

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

3. Content. This category MUST be used only in the case in which the request is related to the content and regional restrictions on accessing that type of content exist. This is not malicious traffic but may be used for determining what sources or destinations accessed certain materials available on the Internet, including, but not limited to, news, technology, or inappropriate content.

4. DataWithHandlingRequirements. This option is used when data shared may have additional restrictions for handling, protection, and processing based on the type of data and where it resides. Regulatory or legal restrictions may be imposed on specific types of data that could vary based on the location, region or nation, of the data or where it originated. The IODEF document, as well as any extensions, included with the RID message should indicate the specific restrictions to be considered. The use of this enumeration flag is not legally binding.

5. AudienceRestriction. This option is used to indicate that the message contains data that should be viewed by a restricted audience. This setting should not be used for normal incidents or reporting as it could slow response times. The content may be a business-relevant notification or request. This option MAY be used by a business partner to report or request assistance if an incident has affected a supply chain. This option may also be used if the content is relevant to regulatory obligations, legal (eDiscovery), or other use cases that require management attention.

6. Other. If this option is selected, a description of the traffic type MUST be provided so that policy decisions can be made to continue or stop the investigation. The information should be provided in the IODEF message in the Expectation class or in the History class using a HistoryItem log. This may also be used for incident types other than information-security-related incidents.

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

ReportSchema

Zero or One. The ReportSchema class is used by the message types that require the full IODEF schema to be included in the RID envelope. Alternate schemas may be included if approved by the Designated Reviewer and registered by IANA for use with RID.

The RIDPolicy class has five attributes:

restriction

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

MsgType

One. REQUIRED. ENUM. The type of RID message sent. The five types of messages are described in Section 4.2 and can be noted as one of the six selections below, where a Request is set to either 'InvestigationRequest' or 'TraceRequest'.

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

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

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

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

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

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

Additionally, there is an extension attribute to add new enumerated values:

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

MsgDestination

One. REQUIRED. ENUM. The destination required at this level may either be the RID messaging system intended to receive the request, or, in the case of a Request with MsgType set to 'InvestigationRequest', the source of the incident. In the case of an InvestigationRequest, the RID system that can help stop or mitigate the traffic may not be known, and the message may have to traverse RID messaging systems by following the routing path to the RID system closest to the source of the attack traffic. The Node element lists either the RID system or the IP address of the source, and the meaning of the value in the Node element is determined by the MsgDestination element.

1. RIDSystem. The IP address of the next upstream system accepting RID communications is REQUIRED and is listed in the Node element of the RIDPolicy class. If NodeName element of the Node class is used, it contains a DNS domain name. The originating RID system is required to check that this domain name resolves to the IP address to which the RID message is sent. This check may be performed in advance of sending the message and the result saved for future use with additional RID messages.

2. SourceOfIncident. The Address element of the Node element contains the IP address of the incident source, and the NodeName element of the Node class is not used. The IP address is REQUIRED when this option is selected. The IP address is used to determine the path of systems accepting RID communications that will be used to find the closest RID system to the source of an attack in which the IP address used by the source is believed to be valid and a Request message with MsgDestination set to 'InvestigationRequest' is used. This is not to be confused with the IncidentSource class, as the defined value here is from an initial Request ('InvestigationRequest' or 'TraceRequest'), not the source used in a Result message.

3. ext-value. An escape value used to extend this attribute. All extensions shall specify the contents and meaning of the Node element of RIDPolicy. See IODEF [RFC5070], Section 5.1, on extensibility. If the NodeName element of the Node class is used by an extension, NodeName may contain an Internationalized Domain Name (IDN); see Section 11 for applicable requirements. All extensions SHOULD use an IP address in the Address element of the Node class as the primary means of Node identification.

MsgType-ext

OPTIONAL. STRING. A means by which to extend the MsgType attribute. See IODEF [RFC5070], Section 5.1.

MsgDestination-ext

OPTIONAL. STRING. A means by which to extend the MsgDestination attribute. See IODEF [RFC5070], Section 5.1

5.1.1. ReportSchema

The ReportSchema class is an aggregate class in the RIDPolicy class. The IODEF schema is the approved schema for inclusion in RID messages via the ReportSchema class.

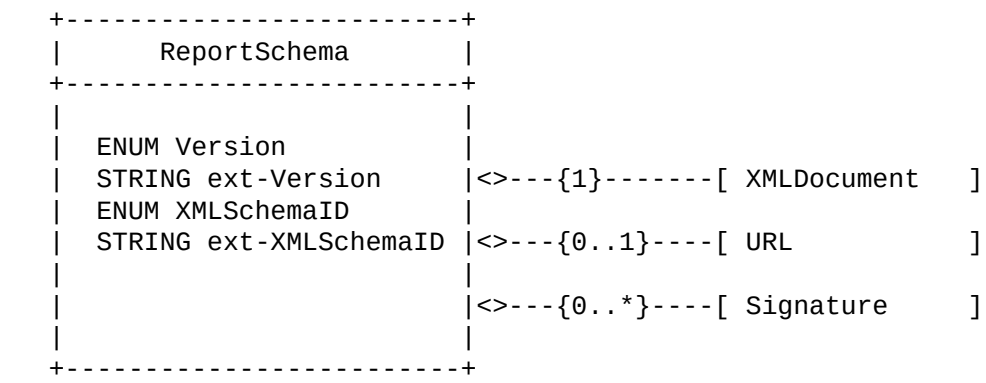

Figure 5: The ReportSchema Class

The elements that constitute the ReportSchema class are as follows:

XMLDocument

One. The XMLDocument is a complete XML document defined by the iodef:ExtensionType class. This class follows the guidelines in [RFC5070], Section 5, where the data type is set to 'xml' and meaning is set to 'xml' to include an XML document.

URL

Zero or One. URL. A reference to the XML schema of the XML document included. The URL data type is defined in [RFC5070], Section 2.15, as "xs:anyURI" in the schema. The schemaLocation for IODEF is already included in the RID schema, so this is not necessary to include a URL for IODEF documents. The list of registered schemas for inclusion will be maintained by IANA.

Signature

Zero to many. The Signature uses the iodef:ExtensionType class to enable this element to contain a detached or enveloped signature. This class follows the guidelines in [RFC5070] Section 5 where the data type is set to 'xml' and meaning is set to 'xml' to include an XML document. This element is used to encapsulate the detached signature based on the iodef: RecordItem class within the IODEF document to verify the originator of the message or to include the enveloped signature. If other schemas are used instead of IODEF, they MUST provide guidance on what class to use if a detached signature is provided for this purpose.

The ReportSchema class has four attributes:

Version

OPTIONAL. One. The Version attribute is the version number of the specified XML schema. That schema must be an approved version of IODEF or a schema registered with IANA for use with RID. The IANA registry for managing schemas other than IODEF is specified in Section 12.

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

ext-Version

OPTIONAL. One. The ext-Version attribute is the version number of the included XML schema. This attribute is used if a schema other than IODEF or an IANA-registered schema that has been added to the enumerated list for Version is included.

XMLSchemaID

OPTIONAL. One. The XMLSchemaID attribute is the identifier, the defined namespace [XMLNames], of the XML schema of the XML document included. The XMLSchemaID and Version specify the format of the XMLDocument element. The only permitted values, include the namespace for IODEF [RFC5070], "urn:ietf:params:xml:ns:iodef-1.0", any future IETF-approved versions of IODEF, and any namespace included in the IANA-managed list of registered schemas for use with RID. The IANA registry for managing schemas other than IODEF is specified in Section 12.

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

ext-XMLSchemaID

OPTIONAL. One. The ext-XMLSchemaID attribute is the identifier (defined namespace) of the XML schema of the XML document included. The ext-XMLSchemaID and ext-Version specify the format of the XMLDocument element and are used if the included schema is not IODEF version 1.0 or an IANA-registered schema that has been added to the enumerated list for XMLSchemaID.

5.2. RequestStatus

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

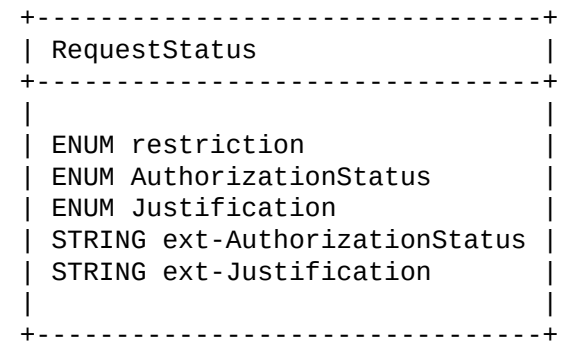

Figure 6: The RequestStatus Class

The RequestStatus class has five attributes:

restriction

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

AuthorizationStatus

One. REQUIRED. ENUM. The listed values are used to provide a response to the requesting CSIRT of the status of a Request, Report, or Query.

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

2. Denied. The trace was denied in the current SP. The next closest SP can use this message to filter traffic from the upstream SP using the example packet to help mitigate the effects of the attack as close to the source as possible. The Acknowledgement message must be passed back to the originator and a Result message must be used from the closest SP to the source in order to indicate actions taken in the IODEF History class.

3. Pending. Awaiting approval; a timeout period has been reached, which resulted in this Pending status and Acknowledgement message being generated.

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

Justification

OPTIONAL. ENUM. Provides a reason for a Denied or Pending message.

1. SystemResource. A resource issue exists on the systems that would be involved in the request.

2. Authentication. The enveloped digital signature [RFC3275] failed to validate.

3. AuthenticationOrigin. The detached digital signature for the original requestor on the RecordItem entry failed to validate.

4. Encryption. The recipient was unable to decrypt the request, report, or query.

5. UnrecognizedFormat. The format of the provided document was unrecognized.

6. CannotProcess. The document could not be processed. Reasons may include legal or policy decisions. Resolution may require communication outside of this protocol to resolve legal or policy issues. No further messages SHOULD be sent until resolved.

7. Other. There were other reasons this request could not be processed.

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

AuthorizationStatus-ext

OPTIONAL. STRING. A means by which to extend the AuthorizationStatus attribute. See IODEF [RFC5070], Section 5.1.

Justification-ext

OPTIONAL. STRING. A means by which to extend the Justification attribute. See IODEF [RFC5070], Section 5.1.

5.3. IncidentSource

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

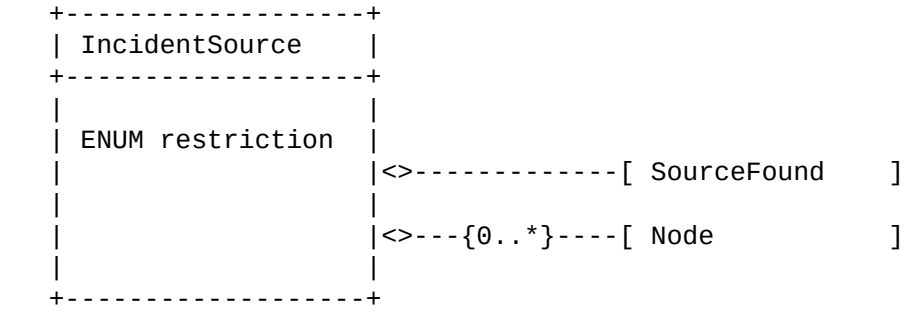

Figure 7: The IncidentSource Class

The elements that constitute the IncidentSource class follow:

SourceFound

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

True. Source of incident was identified.

False. Source of incident was not identified.

Node

Zero or many. The Node class is used to identify a system identified as part of an incident. If this element is used, the Address element of the Node element MUST contain the IP address of the system. If the NodeName element of the Node class is used, it contains a DNS domain name that has been checked to ensure that it resolved to that IP address when the check was performed. See Section 11 of this document for internationalization considerations for NodeName. The base definition of this class from the IODEF ([RFC5070], Section 3.16) can be expanded to include other identifiers.

The IncidentSource class has one attribute:

restriction

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

5.4. RID Name Spaces

The RID schema declares a namespace of "urn:ietf:params:xml:ns:iodef-rid-2.0" and registers it per [RFC3688]. Each IODEF-RID document MUST use the "iodef-rid-2.0" namespace in the top-level element RID-Document. It can be referenced as follows:

```
<RID-Document version="2.0" lang="en-US"
   xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-2.0"
   xmlns:xsi="http://www.w3c.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:ietf:params:xml:ns:iodef-rid-2.0.xsd">
```

5.5. Encoding

RID documents MUST begin with an XML declaration and MUST specify the XML version used; also, the use of UTF-8 encoding is REQUIRED ([RFC3470], Section 4.4). RID conforms to all XML data encoding conventions and constraints.

The XML declaration with no character encoding will read as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
```

The following characters have special meaning in XML and MUST be escaped with their entity reference equivalent: "&", "<", ">", "\"" (double quotation mark), and "'" (apostrophe). These entity references are "&", "<", ">", """, and "'", respectively.

5.6. Including IODEF or Other XML Documents

In order to support the changing activity of CSIRTS, the RID schema can include an IODEF or other data model. The IODEF is also extensible, enabling the schemas to evolve along with the needs of CSIRTs. This section discusses how to include the IODEF XML document or other XML documents to leverage the security and trust

relationships established through the use of RID. These techniques are designed so that adding new data will not require a change to the RID schema. This approach also supports the exchange of private XML documents relevant only to a closed consortium. XML documents can be included through the ReportSchema class in the RIDPolicy class. The XMLDocument attribute is set to 'xml' to allow for the inclusion of full IODEF or other XML documents. The following guidelines MUST be followed:

1. The included schema MUST define a separate namespace, such as the declared namespace for IODEF of "urn:ietf:params:xml:ns:iodef-1.0".

2. When a parser encounters an included XML document it does not understand, the included document MUST be ignored (and not processed), but the remainder of the document MUST be processed. Parsers will be able to identify the XML documents for which they have no processing logic through the namespace declaration. Parsers that encounter an unrecognized element in a namespace that they do support SHOULD reject the document as a syntax error.

3. Implementations SHOULD NOT download schemas at runtime due to the security implications, and included documents MUST NOT be required to provide a resolvable location of their schema.

The examples included in Section 7 demonstrate how an IODEF document is included. The included schema of IODEF is represented in ReportSchema as follows:

```
Version: "1.0"

XMLSchemaID: "urn:ietf:params:xml:ns:iodef-1.0"

URL: "http://www.iana.org/assignments/xml-registry/schema/
iodef-1.0.xsd"
```

The URL is optionally included for IODEF since it is already in the RID schema, and the schemaLocation is defined.

5.6.1. Including XML Documents in RID

XML schemas may be registered for inclusion in a RID message. This may include schemas other than IODEF or updated versions of IODEF. The registered IANA information for additional schemas MUST include the specification name, version, specification Uniform Resource Identifier (URI), and namespace. The following provides an example of the necessary information for additional schemas beyond IODEF.

Example Name (XXXX)

```
Schema Name:   XXXX_1.1
Version:       1.1
Namespace:     <registered namespace>
Specification URI:  http://www.example.com/XXXX
```

The version attribute of the ReportSchema class is populated with the approved versions of IODEF or any additional schemas registered by IANA; see Section 12.

The XMLSchemaID of the ReportSchema class is populated with the namespace of the included schema. The attribute enumeration values include the namespace for IODEF and any schema registered by IANA; see Section 12.

The URL element of the ReportSchema class is populated with the Specification URI value of the included schema.

6. RID Messages

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

Note: The implementation of RID may automate the ability to fill in the content required for each message type from packet input, incident data, situational awareness information, or default values such as those used in the EventData class.

6.1. Request

Description: This message type is used to request assistance in a computer security investigation. The investigation request may be directed to another party that can assist with forensics and continue the investigation (the incident may have originated on the SP network to which the Request was sent), or it may be directed to an SP to trace the traffic from an unknown source. The Request message with MsgType set to 'InvestigationRequest' may leverage the existing bilateral peer relationships in order to notify the SP closest to the source of the valid traffic that some event occurred, which may be a

security-related incident. A Request message with the MsgType set to 'TraceRequest' may be sent to an upstream peer to trace back through the network to locate the source of malicious traffic. The following information is REQUIRED for Request messages and is provided through the following data structures:

RID Information:

RIDPolicy

RID message type, IncidentID, and destination policy information

IODEF Information:

Timestamps (DetectTime, StartTime, EndTime, ReportTime).

Incident Identifier (Incident class, IncidentID).

Confidence rating of security incident (Impact and Confidence class).

System class is used to list both the Source and Destination.

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

Path information of nested RID systems, beginning with the request originator used in the trace using IODEF EventData with category set to 'infrastructure'.

Event, Record, and RecordItem classes to include example packets and other information related to the incident. Note: Event information included here requires a second instance of EventData in addition to that used to convey SP path contact information.

Standards for encryption and digital signatures [RFC3275] [XMLsig] [XMLencrypt]:

Digital signature from initiating CSIRT or provider system sending the RID message, passed to all systems receiving the Request using a detached XML digital signature on a RecordItem entry, placed in an instance of the Signature element.

Digital signature of sending CSIRT or SP for authenticity of the RID message, from the CSIRT or provider creating this message using an enveloped XML digital signature on the IODEF document, placed in an instance of the Signature element.

XML encryption as required by policy, agreements, and data markers.

Security requirements include the ability to encrypt [XMLencrypt] the contents of the Request message using the public key of the destination RID system. The incident number increases whether the Request message has the MsgDestination set to 'InvestigationRequest' or 'TraceRequest' in order to ensure uniqueness within the system. The relaying peers also append their Autonomous System (AS) or RID system information using the path information as the Request message was relayed through SPs. This enables the response (Result message) to utilize the same path and trust relationships for the return message, indicating any actions taken. The request is recorded in the state tables of both the initiating and destination SP RID systems. The destination SP is responsible for any actions taken as a result of the request in adherence to any service level agreements or policies. The SP MUST confirm that 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 MsgDestination of RIDPolicy set to 'SourceOfIncident'. Note: Any intermediate parties in a TraceRequest MUST be able to view RIDPolicy information of responding message types in order to properly direct RID messages.

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 enables the administrators to determine if the exact trace already passed through a single network. The Incident Identifier must also be used to identify multiple Requests from a single incident. If a single Request results in divergent paths of Requests, a separate instance number MUST be used under the same IncidentID. The IncidentID instance number of IODEF can be used to correlate related incident data that is part of a larger incident.

6.2. Acknowledgement

Description: The Acknowledgement is also used to provide a status to any message type and to provide a Justification if the message could not be processed for any reason. This message is sent to the initiating RID system from the next upstream provider's application or system designated for accepting RID communications to provide information on the request status in the current SP.

The following information is REQUIRED for Acknowledgement messages and is provided through the following data structures:

RID Information:

RIDPolicy

RID message type, IncidentID, and destination policy information

RequestStatus class:

Status of Request

Standards for encryption and digital signatures [RFC3275], [XMLsig], [XMLencrypt]:

Digital signature of responding CSIRT or provider for authenticity of Trace Status Message, from the CSIRT or provider creating this message using an enveloped XML digital signature.

XML encryption as required by policy, agreements, and data markers.

A message is sent back to the initiating CSIRT or provider's system; it accepts RID communications 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 CSIRT or provider's RID system. The Pending status is automatically generated after a 2-minute timeout without system-predefined or administrator action to approve or disapprove the trace continuance. If a Request is denied, the originator and sending peer (if they are not the same) MUST both receive the message. This provides the sending peer with the option to take action to stop or mitigate the traffic as close to the source as possible.

6.3. Result

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 is provided through the IncidentSource class. The Result information MUST go back to the originating RID system that began the investigation or trace. A provider may use any number of incident-handling data sources to ascertain the true source of an attack. All of the possible information sources may or may not be readily tied into the RID communications system.

The following information is REQUIRED for Result messages and will be provided through the following data structures:

RID Information:

RIDPolicy

RID message type, IncidentID, and destination policy information

Incident Source

The IncidentSource class of the RID schema is used to note if a source was identified and provide the source address(es) or other Node information.

IODEF Information:

Timestamps (DetectTime, StartTime, EndTime, ReportTime).

Incident Identifier (Incident class, IncidentID).

Trace number is used for multiple traces of a single incident; it MUST be included if the response is specific to an instance of an incident.

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 in RID an upstream Request set to 'TraceRequest'.

History class "atype" attribute is used to note any actions taken.

History class also notes any other background information including notes about the Confidence level or rating of the result information.

Path information of nested RID systems, beginning with the request originator used in the trace using IODEF EventData with category set to 'infrastructure'. The last SP listed is the SP that located the source of the traffic (the provider sending the Result message).

Event, Record, and RecordItem classes to include example packets and other information related to the incident (optional). Note: Event information included here requires a second instance of EventData in addition to that used to convey SP path contact information.

Standards for encryption and digital signatures [RFC3275], [XMLsig], [XMLencrypt]:

Digital signature of source CSIRT or provider for authenticity of Result message, from the CSIRT or provider creating this message using an enveloped XML digital signature.

XML encryption as required by policy, agreements, and data markers.

A message is sent back to the initiating CSIRT or provider's RID system to notify the 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 SP to act upon the discovery of the source of a trace should be included. The SP 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 and block all Internet access until the host has taken the appropriate action to resolve any security issues. The SP may be limited in their options for filtering due to agreements or other restrictions resulting in less comprehensive filters, such as rate-limiting the ingress traffic as close to the source as possible.

Security and privacy requirements discussed in Section 9 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 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 Request is made.

6.4. Report

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 the following data structures:

RID Information:

RIDPolicy RID message type, IncidentID, and destination policy information

The following data is RECOMMENDED if available and can be provided through the following data structures:

IODEF Information:

Timestamps (DetectTime, StartTime, EndTime, ReportTime).

Incident Identifier (Incident class, IncidentID).

Trace number is used for multiple traces of a single incident; it MUST be included if the Report is specific to an instance of an incident.

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 are used to include example packets and other information related to the incident (optional).

Standards for encryption and digital signatures [RFC3275], [XMLsig], [XMLencrypt]:

Digital signature from initiating RID system, passed to all systems receiving the report using an enveloped XML digital signature, placed in an instance of the Signature element.

XML encryption as required by policy, agreements, and data markers.

Security requirements include the ability to encrypt [XMLencrypt] the contents of the Report message 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 to respond to a Query, and data sensitivity must be considered in both cases. The SP path information is not necessary for this message, as it will be communicated directly between two trusted RID systems.

6.5. Query

Description: The Query 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 Query, the return report may be automated; otherwise, analyst intervention may be required.

The following information is REQUIRED for a Query message and is provided through the following data structures:

- RID Information:
  - RIDPolicy
    - RID message type, IncidentID, and destination policy information
- IODEF Information (optional):
  - Timestamps (DetectTime, StartTime, EndTime, ReportTime).
  - Incident Identifier (Incident class, IncidentID).
    - Trace number is used for multiple traces of a single incident; it MUST be included if the Query is an instance of an incident.
  - 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 are used to include example packets and other information related to the incident (optional).

Standards for encryption and digital signatures [RFC3275], [XMLsig], [XMLencrypt]:

Digital signature from the CSIRT or SP initiating the RID message, passed to all systems receiving the Query using an enveloped XML digital signature, placed in an instance of the Signature element.

XML encryption as required by policy, agreements, and data markers.

The proper response to the Query message is a Report message. Multiple incidents may be returned for a single query if an incident type is requested. In this case, the receiving system sends an IODEF document containing multiple incidents or all instances of an incident. The system sending the reply may preset a limit to the number of documents returned in one report. The recommended limit is 5, to prevent the documents from becoming too large. Other transfer methods may be better suited than RID for large transfers of data. The Confidence rating may be used in the 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 Query is intended to gather data about a specific type of incident.

7. RID Communication Exchanges

The following section outlines the communication flows for RID and also provides examples of messages.

The possible set of message exchanges include:

- Request: Asynchronous Request for assistance and/or action to be taken, MAY involve multiple systems and iterative Requests

  MsgType set to 'InvestigationRequest' or 'TraceRequest'

  Possible responses:

  + Acknowledgement (OPTIONAL for InvestigationRequest)

  + Result (REQUIRED unless Acknowledgement was set to 'no')

  + Report (OPTIONAL; zero or more; Report can be sent unsolicited)

- Query: Synchronous request for information

  MsgType set to 'Query'

  Possible responses:

  + Acknowledgement (OPTIONAL if yes; REQUIRED if no Report will be sent)

  + Report (REQUIRED unless Acknowledgement was set to 'no')

- Report: Asynchronous information report; may be pushed to systems or may be a response to a Query

  MsgType set to 'Report'

  Possible responses:

  + Acknowledgement (OPTIONAL)

Processing considerations for the IODEF document and any IODEF included elements or attributes MUST follow the guidelines specified in [RFC5070], Section 4. [RFC3023] and [RFC3470] specify requirements and best practices for the use of XML in IETF application protocols. RID and IODEF documents MUST be well-formed (see [RFC3470], Section 4.1) and MUST be validated against the appropriate schema. Internal or external DTD subsets are prohibited in RID; see [RFC3023], Section 3.

Comments can be ignored by conform ant processors for RID or IODEF documents (see [RFC3470], Section 4.6) and are included below for informational purposes only. The first example demonstrates the use of a detached digital signature. Subsequent examples do not include the detached signature required for some message types. The signature is applied after the message is created as demonstrated in the first example.

Note: For each example listed below, [RFC5735] addresses were used. Assume that each IP address listed is actually a separate network range held by different SPs. Addresses were used from /27 network ranges.

7.1. Upstream Trace Communication Flow

The diagram below outlines the RID Request communication flow for a TraceRequest between RID systems on different networks tracing an attack. The Request message with MsgDestination set to

'TraceRequest' is represented in the diagram by "TraceRequest". SP-1, SP-2, and SP-3 represent service providers that are involved in the example trace communication flow.

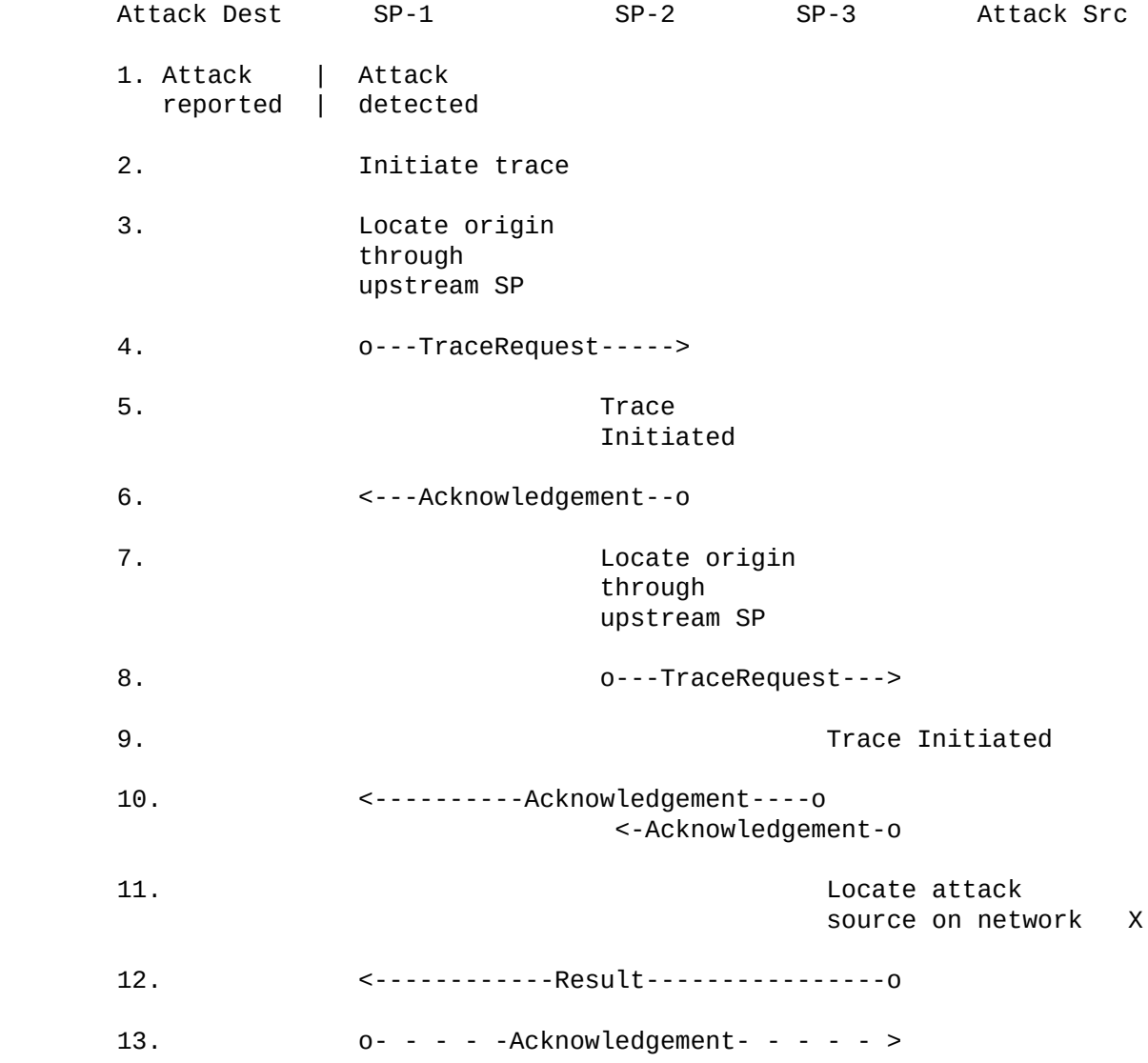

Figure 8: TraceRequest Communication Flow

Before a trace is initiated, the RID system should verify that an instance of the trace or a similar request is not active. The traces may be resource intensive; therefore, providers need to be able to detect potential abuse of the system or unintentional resource

drains. Information such as the Source and Destination Information, associated packets, and the incident may be desirable to maintain for a period of time determined by administrators.

The communication flow demonstrates that an Acknowledgement message is sent to both the downstream peer and the original requestor. If a Request in a traceback is denied, the downstream peer has the option to take an action and respond with a Result message. The originator of the request may follow up with the downstream peer of the SP involved using a Request with the MsgType set to 'InvestigationRequest' to ensure that an action is taken if no response is received. Nothing precludes the originator of the request from initiating a new Request with the MsgType set to 'TraceRequest' thereby bypassing the SP that denied the request, if a trace is needed beyond that point. Another option may be for the initiator to send an 'InvestigationRequest' to an SP upstream of the SP that denied the request. This action assumes enough information was gathered to discern the true source of the attack traffic from the incident-handling information.

The proper response to a TraceRequest is an Acknowledgement message. The Acknowledgement message lets the requestor know if the trace will continue through the next upstream network. If there is a problem with the request, such as a failure to validate the digital signature or decrypt the request, an Acknowledgement message MUST be sent to the requestor and the downstream peer (if they are not one and the same) providing the reason why the message could not be processed. Assuming that the trace continued, additional TraceRequests with the response of an Acknowledgement message would occur, thereby passing the request upstream in the path to the source of the traffic related to the incident. Once a source is found, a Result message is sent to the originator of the trace, as determined by the SP path information provided through the document instance of EventData, where contact is set to 'infrastructure'. The SP path information is also used when sending the Acknowledgement messages to the first entry (the trace originator) and the last nested entry (the downstream peer). The Result message is encrypted [XMLencrypt] for the originator providing information about the incident source and any actions taken. If the originator fails to decrypt or authenticate the Result message, an Acknowledgement message is sent in response; otherwise, no return message is sent. The final Acknowledgement to the Result message is depicted as optional in the diagram above. If an Acknowledgement message is sent with the RequestStatus set to Denied, a downstream peer receiving this message may choose to take action to stop or mitigate the traffic at that point in the network, as close to the source as possible. If the downstream peer chooses this option, it would send a Result message to the trace originator.

7.1.1. RID TraceRequest Example

The example listed is of a Request message with MsgDestination set to 'TraceRequest' based on the incident report example from the IODEF document. The RID classes were included as appropriate for a Request message of this type using the RIDPolicy class. The example given is that of a CSIRT reporting a DoS attack in progress to the upstream SP. The request asks the next SP to continue the trace and have the traffic mitigated closer to the source of the traffic. The example Request message is the first step of a TraceRequest as depicted in the previous diagram, where 'Attack Dest' is represented by 192.0.2.67 (and SP-1). The 'Attack Src' is later identified in the Result message example as 192.0.2.37 and initially as tracing closer to 192.0.2.35. SP-1 is identified in the Request as CSIRT-FOR-OUR-DOMAIN, and SP-2 is identified in the RID document for the Request as the 'RIDSystem' in 'MsgDestination' as 192.0.2.3 using the Node class. SP-3 is later used in the Result message and the administrator is identified as 'Admin-contact@10.1.1.2' as they searched for 192.0.2.35; the administrator may be different than the constituency contact (an additional Request with MsgDestination set to 'TraceRequest' occurred between SP-2 to SP-3 that is not included). SP-3 is the service provider for 192.0.2.32/27 and was able to take the action to rate-limit their traffic. The SP-1, SP-2, and SP-3 information would be replaced with the appropriate (and valid) email and other contact information in real usages. The Node class enables multiple methods to identify a system, such as a fully qualified domain name or the IP address to be provided for the SP. Any mapping of existing relationships from the SP Node information to the name, contact, digital signature verification information and other identifying or trust information is provided at the application layer to support end users of the incident management system. A packet is provided in this example to enable any traces to be performed by SP-2 and SP-3 to perform traces to the attack source before taking the requested action to 'rate-limit' the traffic. The subnet of 192.0.2.0 uses a 27-bit mask in the examples below.

In the following example, use of [XMLsig] to generate digital signatures follows the guidance of [XMLsig] 1.0. Version 1.1 of [XMLsig] supports additional digest algorithms. Reference [RFC4051] for URIs intended for use with XML digital signatures, encryption, and canonicalization. SHA-1 SHOULD NOT be used; see [RFC6194] for further details.

Note: Due to the limit of 72 characters per line, some line breaks were added in the examples and schemas in this document.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<iodef-rid:RID lang="en-US"
 xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-2.0"
 xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:iodef-rid-2.0">
 <iodef-rid:RIDPolicy MsgDestination="RIDSystem" MsgType="TraceRequest">
   <iodef-rid:PolicyRegion region="IntraConsortium"/>
     <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.3</iodef:Address>
     </iodef:Node>
     <iodef-rid:TrafficType type="Attack"/>
     <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
            CERT-FOR-OUR-DOMAIN#207-1
     </iodef:IncidentID>
     <!-- IODEF-Document included in RID -->
     <iodef-rid:ReportSchema Version="1.0">
      <iodef-rid:XMLDocument dtype="xml" meaning="xml">
       <IODEF-Document lang="en">
        <iodef:Incident purpose="traceback" restriction="need-to-know">
          <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
                          CERT-FOR-OUR-DOMAIN#207-1
          </iodef:IncidentID>
          <iodef:DetectTime>2004-02-02T22:49:24+00:00</iodef:DetectTime>
          <iodef:StartTime>2004-02-02T22:19:24+00:00</iodef:StartTime>
          <iodef:ReportTime>2004-02-02T23:20:24+00:00</iodef:ReportTime>
          <iodef:Description>
                          Host involved in DoS attack
          </iodef:Description>
          <iodef:Assessment>
            <iodef:Impact completion="failed" severity="low"
                         type="dos"/>
          </iodef:Assessment>
          <iodef:Contact role="creator" type="organization">
            <iodef:ContactName>Constituency-contact for 192.0.2.35
            </iodef:ContactName>
            <iodef:Email>Constituency-contact@192.0.2.35</iodef:Email>
          </iodef:Contact>
          <iodef:EventData>
            <iodef:Flow>
              <iodef:System category="source">
                <iodef:Node>
                  <iodef:Address category="ipv4-addr">192.0.2.35
                  </iodef:Address>
                </iodef:Node>
                <iodef:Service ip_protocol="6">
                  <iodef:Port>38765</iodef:Port>
                </iodef:Service>
```

```
            </iodef:System>
            <iodef:System category="target">
              <iodef:Node>
                <iodef:Address category="ipv4-addr">192.0.2.67
                </iodef:Address>
              </iodef:Node>
              <iodef:Service ip_protocol="6">
                <iodef:Port>80</iodef:Port>
              </iodef:Service>
            </iodef:System>
          </iodef:Flow>
          <iodef:Expectation action="rate-limit-host" severity="high">
            <iodef:Description>
                   Rate-limit traffic close to source
          </iodef:Description>
        </iodef:Expectation>
        <iodef:Record>
          <iodef:RecordData>
            <iodef:Description>
             The IPv4 packet included was used in the described attack
            </iodef:Description>
            <iodef:RecordItem dtype="ipv4-packet">450000522ad9
              0000ff06c41fc0a801020a010102976d0050103e020810d9
              4a1350021000ad6700005468616e6b20796f7520666f7220
              6361726566756c6c7920726164696e6720746869732052
              46432e0a
            </iodef:RecordItem>
           </iodef:RecordData>
          </iodef:Record>
         </iodef:EventData>
         <iodef:History>
           <iodef:HistoryItem action="rate-limit-host">
             <iodef:DateTime>
                    2001-09-14T08:19:01+00:00
             </iodef:DateTime>
             <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
                    CSIRT-FOR-OUR-DOMAIN#207-1
             </iodef:IncidentID>
             <iodef:Description>
            Notification sent to next upstream SP closer to 192.0.2.35
             </iodef:Description>
            </iodef:HistoryItem>
           </iodef:History>
          </iodef:Incident>
        </IODEF-Document>
      </iodef-rid:XMLDocument>
    <!-- End of IODEF-Document included in RID -->
    <!-- Start of detached XML signature included in RID -->
```

```
       <iodef-rid:Signature dtype="xml" meaning="xml">
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"
                   Id="dsig-123456">
        <SignedInfo>
<CanonicalizationMethod
  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<SignatureMethod
  Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <Reference URI="">
    <Transforms>
     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     <Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
     <XPath xmlns="http://www.w3.org/2002/06/xmldsig-filter2"
       xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
       xmlns:dsig-trans="http://www.w3.org/2002/06/xmldsig-filter2"
       Filter="intersect">
       //dsig:Signature[@Id = 'dsig-123456']/
       ancestor::iodef-rid:ReportSchema/
       iodef-rid:XMLDocument/IODEF-Document[1]/iodef:Incident[1]/
       iodef:EventData[1]/iodef:Record[1]/iodef:RecordData[1]/
       iodef:RecordItem[1]</XPath></Transform></Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <DigestValue>
       NQuIhPjdZuZJnPi/hW62dwJT1dR+vqcZV8mpemCVN5g=
    </DigestValue>
   </Reference></SignedInfo>
   <SignatureValue>
lnq/ePQ4AVpxCR0ifCp9sMsW0r/AdT3C2GR/zaN1V+hZ/NApOygUjMzTCQnx+RvGPNkO/RVq
BEIDgZQUEnQZn/uSbmr0tQ6xpBfaxF1DCosLgiZy+2jFzpXrwoN/jHNgtxR/9QLW9mZ+I7V6
LEEJ73Kut+d0naTGHlyi64ab2PqsVuRXQ4pXUKbhMkhzeTIqvFLK93KGfsIMd6Cb+n2u/ABy
Lkc+gflJYUWVP4DxkQ4cyex6hM6RYTRUSr7jVD9K4d8KFP2g85i69YLtSu01W1Np0afpJ4a9
MK0E7ISMNRmC8wIklCAsSXiBRqyaEwaSy/clybI0vCTPqGOYh3/SZg==
   </SignatureValue>
   <KeyInfo>
    <KeyValue>
      <RSAKeyValue>
       <Modulus>
z8adrX9m0S8OxIxN+fui33wiz4ZYgb4xPbR9MS5pOp1A8kVpH5Ew3N6O3/dMs2a4diIxyGLV
h0r86QXWH/W6T2IC2ny+hi+jWRwXrvgTY3ZAFgePvz2OdRhVN/cUbOto4Pa4I2mVZWW+/Q0F
n7YpqPBDDxlGq/xyFPuYq/4y7Y+Ah+vHO2ZSaiQjbj8F38XrGhwlcbFVyK8AmxK3z0zWwX86
uMEqVCjW6s6j2KAWdbAjEpgZHlJY87i/DqnFgxfmdg3oru+YeiEPVRY8hyQpYbtgryveZOHT
gnCHmS/53U9jSS0cyb/ADuj1upfyNoOiMMgQr7Olhc5pTvuWAl4Fnw==</Modulus>
       <Exponent>AQAB</Exponent>
      </RSAKeyValue>
      </KeyValue>
    </KeyInfo>
   </Signature>
  </iodef-rid:Signature>
```

```
  <!-- End of detached XML signature included in RID -->
      </iodef-rid:ReportSchema>
   </iodef-rid:RIDPolicy>
</iodef-rid:RID>
```

7.1.2. Acknowledgement Message Example

The example Acknowledgement message is in response to the Request message listed above. The SP that received the request is responding to approve the trace continuance in their network.

```
<iodef-rid:RID lang="en"
               xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-2.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="Acknowledgement"
                       MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="IntraConsortium"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.67</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#207-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
  <iodef-rid:RequestStatus AuthorizationStatus="Approved"/>
</iodef-rid:RID>
```

7.1.3. Result Message Example

The example Result message is in response to the Request listed above. This message type only comes after an Acknowledgement within the Request flow of messages where a TraceRequest is in progress. It may be a direct response to a Request with the MsgType set to 'InvestigationRequest'. This message provides information about the source of the attack and the actions taken to mitigate the traffic. The Result message is typically the last message in a Request flow; however, an Acknowledgement MAY follow if there are any issues receiving or processing the Result.

```
<iodef-rid:RID lang="en"
               xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-2.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="Result"
                       MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="IntraConsortium"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.67</iodef:Address>
```

```
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#207-1
    </iodef:IncidentID>
<!-- IODEF-Document included in RID -->
    <iodef-rid:ReportSchema Version="1.0">
     <iodef-rid:XMLDocument dtype="xml" meaning="xml">
      <iodef:IODEF-Document lang="en">
      <iodef:Incident restriction="need-to-know" purpose="traceback">
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#207-1
        </iodef:IncidentID>
      <iodef:DetectTime>2004-02-02T22:49:24+00:00</iodef:DetectTime>
      <iodef:StartTime>2004-02-02T22:19:24+00:00</iodef:StartTime>
      <iodef:ReportTime>2004-02-02T23:20:24+00:00</iodef:ReportTime>
      <iodef:Description>Host involved in DoS attack</iodef:Description>
      <iodef:Assessment>
        <iodef:Impact severity="low" completion="failed"
                      type="dos"/>
      </iodef:Assessment>
      <iodef:Contact role="creator" type="organization">
        <iodef:ContactName>Constituency-contact for 192.0.2.35
        </iodef:ContactName>
        <iodef:Email>Constituency-contact@192.0.2.35</iodef:Email>
      </iodef:Contact>
      <iodef:EventData>
        <iodef:Contact role="admin" type="organization">
          <iodef:ContactName>Admin-contact for 192.0.2.35
          </iodef:ContactName>
          <iodef:Email>Admin-contact@10.1.1.2</iodef:Email>
        </iodef:Contact>
        <iodef:Flow>
          <iodef:System category="intermediate">
            <iodef:Node>
              <iodef:Address category="ipv4-addr">192.0.2.35
              </iodef:Address>
            </iodef:Node>
          </iodef:System>
        </iodef:Flow>
        <iodef:EventData>
          <iodef:Contact role="admin" type="organization">
            <iodef:ContactName>Admin-contact for 192.0.2.3
            </iodef:ContactName>
            <iodef:Email>Admin-contact@192.0.2.3</iodef:Email>
          </iodef:Contact>
          <iodef:Flow>
            <iodef:System category="intermediate">
```

```
            <iodef:Node>
              <iodef:Address category="ipv4-addr">192.0.2.3
              </iodef:Address>
            </iodef:Node>
          </iodef:System>
        </iodef:Flow>
      </iodef:EventData>
    </iodef:EventData>
    <iodef:EventData>
      <iodef:Flow>
        <iodef:System category="source">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.35
            </iodef:Address>
          </iodef:Node>
          <iodef:Service ip_protocol="6">
            <iodef:Port>38765</iodef:Port>
          </iodef:Service>
        </iodef:System>
        <iodef:System category="target">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.67
            </iodef:Address>
          </iodef:Node>
          <iodef:Service ip_protocol="6">
            <iodef:Port>80</iodef:Port>
          </iodef:Service>
        </iodef:System>
      </iodef:Flow>
      <iodef:Expectation severity="high" action="rate-limit-host">
        <iodef:Description>
          Rate-limit traffic close to source
        </iodef:Description>
      </iodef:Expectation>
      <iodef:Record>
        <iodef:RecordData>
          <iodef:Description>
            The IPv4 packet included was used in the described attack
          </iodef:Description>
          <iodef:RecordItem dtype="ipv4-packet">450000522ad9
          0000ff06c41fc0a801020a010102976d0050103e020810d9
          4a1350021000ad6700005468616e6b20796f7520666f7220
          6361726566756c6c792072656164696e6720746869732052
          46432e0a
          </iodef:RecordItem>
        </iodef:RecordData>
      </iodef:Record>
    </iodef:EventData>
```

```
      <iodef:History>
        <iodef:HistoryItem action="rate-limit-host">
          <iodef:DateTime>2004-02-02T22:53:01+00:00</iodef:DateTime>
          <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
            CSIRT-FOR-OUR-DOMAIN#207-1
          </iodef:IncidentID>
          <iodef:Description>
            Notification sent to next upstream SP closer to 192.0.2.35
          </iodef:Description>
        </iodef:HistoryItem>
        <iodef:HistoryItem action="rate-limit-host">
          <iodef:DateTime>2004-02-02T23:07:21+00:00</iodef:DateTime>
          <iodef:IncidentID name="CSIRT-FOR-SP3">
            CSIRT-FOR-SP3#3291-1
          </iodef:IncidentID>
          <iodef:Description>
            Host rate-limited for 24 hours
            </iodef:Description>
          </iodef:HistoryItem>
        </iodef:History>
      </iodef:Incident>
      </iodef:IODEF-Document>
     </iodef-rid:XMLDocument>
<!-- End of IODEF-Document included in RID -->
   </iodef-rid:ReportSchema>
  </iodef-rid:RIDPolicy>
  <iodef-rid:IncidentSource>
    <iodef-rid:SourceFound>true</iodef-rid:SourceFound>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.37</iodef:Address>
    </iodef:Node>
  </iodef-rid:IncidentSource>
</iodef-rid:RID>
```

7.2. Investigation Request Communication Flow

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

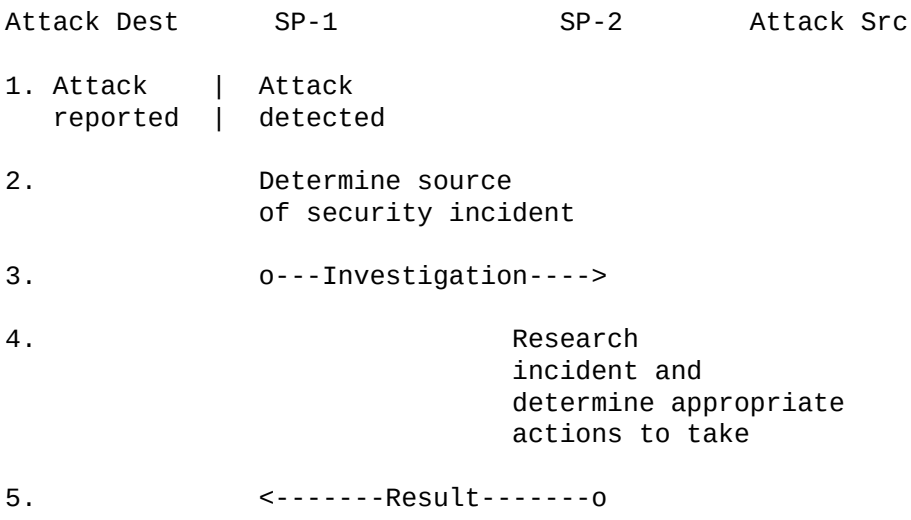

Figure 9: Investigation Request Communication Flow

7.2.1. Investigation Request Example

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

This flow does not include a Result message because the request is denied as shown in the Acknowledgement response.

SP-1 is represented by CERT-FOR-OUR-DOMAIN and 192.0.2.67. SP-2 is identified by 192,0.2.98. In this example, SP-2 is the service provider for systems on the 192.0.2.32/27 subnet. The contact for the host 192.0.2.35 is known at the start of the request as 'Constituency-contact@10.1.1.2'.

```
<iodef-rid:RID lang="en"
               xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-2.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="InvestigationRequest"
                       MsgDestination="SourceOfIncident">
    <iodef-rid:PolicyRegion region="PeerToPeer"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.98</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
```

```
      <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
        CERT-FOR-OUR-DOMAIN#208-1
      </iodef:IncidentID>
  <!-- IODEF-Document included in RID -->
      <iodef-rid:ReportSchema Version="1.0">
       <iodef-rid:XMLDocument dtype="xml" meaning="xml">
    <iodef:IODEF-Document lang="en">
    <iodef:Incident restriction="need-to-know" purpose="other">
      <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
        CERT-FOR-OUR-DOMAIN#208-1
      </iodef:IncidentID>
      <iodef:DetectTime>2004-02-05T08:13:33+00:00</iodef:DetectTime>
      <iodef:StartTime>2004-02-05T08:13:31+00:00</iodef:StartTime>
      <iodef:EndTime>2004-02-05T08:13:33+00:00</iodef:EndTime>
      <iodef:ReportTime>2004-02-05T08:13:35+00:00</iodef:ReportTime>
      <iodef:Description>Host involved in DoS attack</iodef:Description>
      <iodef:Assessment>
        <iodef:Impact severity="low" completion="failed" type="recon"/>
      </iodef:Assessment>
      <iodef:Contact role="creator" type="organization">
        <iodef:ContactName>Constituency-contact for 192.0.2.35
        </iodef:ContactName>
        <iodef:Email>Constituency-contact@10.1.1.2</iodef:Email>
      </iodef:Contact>
      <iodef:EventData>
        <iodef:Flow>
          <iodef:System category="source">
            <iodef:Node>
              <iodef:Address category="ipv4-addr">192.0.2.35
              </iodef:Address>
            </iodef:Node>
            <iodef:Service ip_protocol="6">
              <iodef:Port>41421</iodef:Port>
            </iodef:Service>
          </iodef:System>
          <iodef:System category="target">
            <iodef:Node>
              <iodef:Address category="ipv4-addr">192.0.2.67
              </iodef:Address>
            </iodef:Node>
            <iodef:Service ip_protocol="6">
              <iodef:Port>80</iodef:Port>
            </iodef:Service>
          </iodef:System>
        </iodef:Flow>
        <iodef:Expectation severity="high" action="investigate">
          <iodef:Description>
            Investigate whether source has been compromised
```

```
          </iodef:Description>
        </iodef:Expectation>
      </iodef:EventData>
      <iodef:History>
        <iodef:HistoryItem action="block-host">
          <iodef:DateTime>2004-02-05T08:19:01+00:00</iodef:DateTime>
          <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
            CSIRT-FOR-OUR-DOMAIN#208-1
          </iodef:IncidentID>
          <iodef:Description>
            Investigation request sent to SP for 192.0.2.35
          </iodef:Description>
        </iodef:HistoryItem>
      </iodef:History>
    </iodef:Incident>
    </iodef:IODEF-Document>
       </iodef-rid:XMLDocument>
  <!-- End of IODEF-Document included in RID -->
      </iodef-rid:ReportSchema>
    </iodef-rid:RIDPolicy>
  </iodef-rid:RID>
```

7.2.2. Acknowledgement Message Example

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

```
<iodef-rid:RID lang="en"
               xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-2.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="Acknowledgement"
                       MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="IntraConsortium"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.67</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#208-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
  <iodef-rid:RequestStatus AuthorizationStatus="Denied"
                           Justification="Authentication"/>
</iodef-rid:RID>
```

7.3. Report Communication Flow

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

```
        SP-1                          SP-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 incidents. Incident information may be shared between CSIRTs or other entities 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 hexadecimal packet and incident class information, can be used to compare with existing database entries. The Report message typically does not have a response. If there is a problem with the Report message, such as a failure to validate the digital signature [RFC3275] or decrypt the request, an Acknowledgement message is sent to the requestor. The Acknowledgement message should provide the reason why the message could not be processed.

7.3.1. Report Example

The following example only includes the RID-specific details. This report is an unsolicited Report message that includes an IPv4 packet. The IODEF document and digital signature is similar to the Request example with MsgDestination set to 'TraceRequest'.

This example is a message sent from SP-1, CERT-FOR-OUR-DOMAIN at 192.0.2.67, to SP-2 at 192.0.2.130 for informational purposes on an attack that took place.

```
<iodef-rid:RID lang="en"
               xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-2.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="Report" MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="PeerToPeer"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.130</iodef:Address>
    </iodef:Node>
```

```
      <iodef-rid:TrafficType type="Attack"/>
      <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
        CERT-FOR-OUR-DOMAIN#209-1
      </iodef:IncidentID>
  <!-- IODEF-Document included in RID -->
      <iodef-rid:ReportSchema>
       <iodef-rid:XMLDocument dtype="xml" meaning="xml">
    <iodef:IODEF-Document lang="en">
    <iodef:Incident restriction="need-to-know" purpose="reporting">
      <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
        CERT-FOR-OUR-DOMAIN#209-1
      </iodef:IncidentID>
      <iodef:DetectTime>2004-02-05T10:21:08+00:00</iodef:DetectTime>
      <iodef:StartTime>2004-02-05T10:21:05+00:00</iodef:StartTime>
      <iodef:EndTime>2004-02-05T10:35:00+00:00</iodef:EndTime>
      <iodef:ReportTime>2004-02-05T10:27:38+00:00</iodef:ReportTime>
      <iodef:Description>Host illicitly accessed admin account
      </iodef:Description>
      <iodef:Assessment>
        <iodef:Impact severity="high" completion="succeeded"
                      type="admin"/>
        <iodef:Confidence rating="high"/>
      </iodef:Assessment>
      <iodef:Contact role="creator" type="organization">
        <iodef:ContactName>Constituency-contact for 192.0.2.35
        </iodef:ContactName>
        <iodef:Email>Constituency-contact@10.1.1.2</iodef:Email>
      </iodef:Contact>
      <iodef:EventData>
        <iodef:Flow>
          <iodef:System category="source">
            <iodef:Node>
              <iodef:Address category="ipv4-addr">192.0.2.35
              </iodef:Address>
            </iodef:Node>
            <iodef:Service ip_protocol="6">
              <iodef:Port>32821</iodef:Port>
            </iodef:Service>
          </iodef:System>
          <iodef:System category="target">
            <iodef:Node>
              <iodef:Address category="ipv4-addr">192.0.2.67
              </iodef:Address>
            </iodef:Node>
            <iodef:Service ip_protocol="6">
              <iodef:Port>22</iodef:Port>
            </iodef:Service>
          </iodef:System>
```

```
        </iodef:Flow>
      </iodef:EventData>
      <iodef:History>
        <iodef:HistoryItem action="rate-limit-host">
          <iodef:DateTime>2004-02-05T10:28:00+00:00</iodef:DateTime>
          <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
            CSIRT-FOR-OUR-DOMAIN#209-1
          </iodef:IncidentID>
          <iodef:Description>
            Incident report sent to SP for 192.0.2.35
          </iodef:Description>
        </iodef:HistoryItem>
      </iodef:History>
    </iodef:Incident>
    </iodef:IODEF-Document>
       </iodef-rid:XMLDocument>
  <!-- End of IODEF-Document included in RID -->
    </iodef-rid:ReportSchema>
    </iodef-rid:RIDPolicy>
  </iodef-rid:RID>
```

7.4. Query Communication Flow

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

```
        SP-1                            SP-2

     1. Generate a request for
        information on a specific
        incident number or incident type

     2.             o-------Query------->

     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: Query Communication Flow

The Query message communication receives a response of a Report message. If the Report message is empty, the responding host did not

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

7.4.1. Query Example

The Query request may be received in several formats as a result of the type of query being performed. If the incident number is the only information provided, the IODEF document and IP packet data may not be needed to complete the request. However, if a type of incident is requested, the incident number remains NULL, and the IP packet data will not be included in the IODEF RecordItem class; the other incident information is the main source for comparison. In the case in which an incident number may not be the same between CSIRTs, 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).

This query is sent to 192.0.2.3, inquiring about the incident with the identifier CERT-FOR-OUR-DOMAIN#210-1. The Report will be provided to the requestor identified and verified through the authentication and digital signature information provided in the RID message. An example Report is provided above.

```
<iodef-rid:RID lang="en"
               xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-2.0"
               xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
  <iodef-rid:RIDPolicy MsgType="Query"
                       MsgDestination="RIDSystem">
    <iodef-rid:PolicyRegion region="PeerToPeer"/>
    <iodef:Node>
      <iodef:Address category="ipv4-addr">192.0.2.3</iodef:Address>
    </iodef:Node>
    <iodef-rid:TrafficType type="Attack"/>
    <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
      CERT-FOR-OUR-DOMAIN#210-1
    </iodef:IncidentID>
  </iodef-rid:RIDPolicy>
</iodef-rid:RID>
```

8. RID Schema Definition

```
<?xml version="1.0" encoding="UTF-8"?>
 <xs:schema xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-2.0"
  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-2.0"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
 <xs:import namespace="urn:ietf:params:xml:ns:iodef-1.0"
 schemaLocation="http://www.iana.org/assignments/xml-registry/schema/
 iodef-1.0.xsd"/>
 <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
 schemaLocation="http://www.w3.org/TR/xmldsig-core/
 xmldsig-core-schema.xsd"/>

 <!-- ****************************************************************
 ****************************************************************
 ***  Real-time Inter-network Defense - RID XML Schema             ***
 ***    Namespace - iodef-rid, April 2012                        ***
 ***    The namespace is defined to support transport of IODEF     ***
 ***     documents for exchanging incident information.            ***
 ****************************************************************
 -->
 <!--RID messages act as an envelope for IODEF and RID documents
     to support the exchange of incident information-->
 <!--
 ====== Real-Time Inter-network Defense - RID ======
 ====  Suggested definition for RID messaging ======

  -->

 <xs:annotation>
   <xs:documentation>XML Schema wrapper for IODEF</xs:documentation>
 </xs:annotation>
 <xs:element name="RID" type="iodef-rid:RIDType"/>
   <xs:complexType name="RIDType">
     <xs:sequence>
       <xs:element ref="iodef-rid:RIDPolicy" minOccurs="0"/>
       <xs:element ref="iodef-rid:RequestStatus" minOccurs="0"/>
       <xs:element ref="iodef-rid:IncidentSource" minOccurs="0"/>
     </xs:sequence>
     <xs:attribute name="lang"
                    type="xs:language" use="required"/>
   </xs:complexType>

 <!--Used in Acknowledgement Message for RID-->
```

```
<xs:element name="RequestStatus" type="iodef-rid:RequestStatusType"/>
  <xs:complexType name="RequestStatusType">
     <xs:attribute name="AuthorizationStatus" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
          <xs:whiteSpace value="collapse"/>
            <xs:enumeration value="Approved"/>
            <xs:enumeration value="Denied"/>
            <xs:enumeration value="Pending"/>
            <xs:enumeration value="ext-value"/>
          </xs:restriction>
        </xs:simpleType>
     </xs:attribute>
     <xs:attribute name="ext-AuthorizationStatus"
                   type="xs:string" use="optional"/>
     <xs:attribute name="Justification">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
          <xs:whiteSpace value="collapse"/>
            <xs:enumeration value="SystemResource"/>
            <xs:enumeration value="Authentication"/>
            <xs:enumeration value="AuthenticationOrigin"/>
            <xs:enumeration value="Encryption"/>
            <xs:enumeration value="UnrecognizedFormat"/>
            <xs:enumeration value="CannotProcess"/>
            <xs:enumeration value="Other"/>
            <xs:enumeration value="ext-value"/>
          </xs:restriction>
        </xs:simpleType>
     </xs:attribute>
     <xs:attribute name="ext-Justification"
                   type="xs:string" use="optional"/>
    <xs:attribute name="restriction" type="iodef:restriction-type"/>
  </xs:complexType>

<!--Incident Source Information for Result Message-->

<xs:element name="IncidentSource" type="iodef-rid:IncidentSourceType"/>
  <xs:complexType name="IncidentSourceType">
    <xs:sequence>
      <xs:element ref="iodef-rid:SourceFound"/>
      <xs:element ref="iodef:Node" minOccurs="0"
          maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="restriction" type="iodef:restriction-type"/>
  </xs:complexType>
  <xs:element name="SourceFound" type="xs:boolean"/>
```

```
<!--
====== Real-Time Inter-network Defense Policy - RIDPolicy ======
======  Definition for RIDPolicy for messaging
 -->

<xs:annotation>
 <xs:documentation>RID Policy used for transport of
     messages</xs:documentation>
</xs:annotation>

<!-- RIDPolicy information with setting information listed in RID
     documentation -->

<xs:element name="RIDPolicy" type="iodef-rid:RIDPolicyType"/>
  <xs:complexType name="RIDPolicyType">
    <xs:sequence>
      <xs:element ref="iodef-rid:PolicyRegion" maxOccurs="unbounded"/>
      <xs:element ref="iodef:Node"/>
      <xs:element ref="iodef-rid:TrafficType" maxOccurs="unbounded"/>
      <xs:element ref="iodef:IncidentID" minOccurs="0"/>
      <xs:element ref="iodef-rid:ReportSchema" minOccurs="0"/>
    </xs:sequence>
   <xs:attribute name="MsgType" use="required">
    <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
      <xs:whiteSpace value="collapse"/>
        <xs:enumeration value="TraceRequest"/>
        <xs:enumeration value="Acknowledgement"/>
        <xs:enumeration value="Result"/>
        <xs:enumeration value="InvestigationRequest"/>
        <xs:enumeration value="Report"/>
        <xs:enumeration value="Query"/>
        <xs:enumeration value="ext-value"/>
      </xs:restriction>
    </xs:simpleType>
   </xs:attribute>
  <xs:attribute name="ext-MsgType" type="xs:string" use="optional"/>
  <xs:attribute name="MsgDestination" use="required">
    <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
      <xs:whiteSpace value="collapse"/>
        <xs:enumeration value="RIDSystem"/>
        <xs:enumeration value="SourceOfIncident"/>
        <xs:enumeration value="ext-value"/>
      </xs:restriction>
    </xs:simpleType>
   </xs:attribute>
  <xs:attribute name="ext-MsgDestination" type="xs:string"
```

```
                use="optional"/>
   <xs:attribute name="restriction" type="iodef:restriction-type"/>
    </xs:complexType>
   <xs:element name="PolicyRegion">
     <xs:complexType>
      <xs:attribute name="region" use="required">
       <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
        <xs:whiteSpace value="collapse"/>
          <xs:enumeration value="ClientToSP"/>
          <xs:enumeration value="SPToClient"/>
          <xs:enumeration value="IntraConsortium"/>
          <xs:enumeration value="PeerToPeer"/>
          <xs:enumeration value="BetweenConsortiums"/>
          <xs:enumeration value="ext-value"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:attribute>
      <xs:attribute name="ext-region"
                    type="xs:string" use="optional"/>
     </xs:complexType>
   </xs:element>
   <xs:element name="TrafficType">
     <xs:complexType>
      <xs:attribute name="type" use="required">
       <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
        <xs:whiteSpace value="collapse"/>
          <xs:enumeration value="Attack"/>
          <xs:enumeration value="Network"/>
          <xs:enumeration value="Content"/>
          <xs:enumeration value="DataWithHandlingRequirements"/>
          <xs:enumeration value="AudienceRestriction"/>
          <xs:enumeration value="Other"/>
          <xs:enumeration value="ext-value"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:attribute>
      <xs:attribute name="ext-type"
                    type="xs:string" use="optional"/>
     </xs:complexType>
   </xs:element>
 <!--Used to include an enveloped XML document in RID-->
 <xs:element name="ReportSchema" type="iodef-rid:ReportSchemaType"/>
   <xs:complexType name="ReportSchemaType">
     <xs:sequence>
       <xs:element ref="iodef-rid:XMLDocument" minOccurs="1"
                   maxOccurs="1"/>
```

```
      <xs:element ref="iodef-rid:URL" minOccurs="0"
                  maxOccurs="1"/>
      <xs:element ref="iodef-rid:Signature" minOccurs="0"
                  maxOccurs="unbounded"/>
    </xs:sequence>
     <xs:attribute name="Version" use="optional">
      <xs:simpleType>
       <xs:restriction base="xs:NMTOKEN">
       <xs:whiteSpace value="collapse"/>
         <xs:enumeration value="1.0"/>
              <xs:enumeration value="ext-value"/>
       </xs:restriction>
      </xs:simpleType>
     </xs:attribute>
     <xs:attribute name="ext-Version"
                   type="xs:string" use="optional"/>
     <xs:attribute name="XMLSchemaID" use="optional">
      <xs:simpleType>
       <xs:restriction base="xs:anyURI">
       <xs:whiteSpace value="collapse"/>
         <xs:enumeration value="urn:ietf:params:xml:ns:iodef-1.0"/>
              <xs:enumeration value="ext-value"/>
       </xs:restriction>
      </xs:simpleType>
     </xs:attribute>
     <xs:attribute name="ext-XMLSchemaID"
                   type="xs:string" use="optional"/>
    </xs:complexType>
  <xs:element name="XMLDocument"
              type="iodef:ExtensionType"/>
  <xs:element name="URL"
              type="xs:anyURI"/>
  <xs:element name="Signature"
              type="iodef:ExtensionType"/>
</xs:schema>
```

9. Security Requirements

9.1. XML Digital Signatures and Encryption

RID leverages existing security standards and data markings in RIDPolicy to achieve the required levels of security for the exchange of incident information. The use of standards includes TLS and the XML security features of encryption [XMLencrypt] and digital signatures [RFC3275] [XMLsig]. The standards provide clear methods to ensure that messages are secure, authenticated, and authorized; meet policy and privacy guidelines; and maintain integrity. XML

Signature Best Practices [XMLSigBP] should be referenced by implementers for information on improving security to mitigate attacks.

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

XML Digital Signature

- The originator of a Request MUST use a detached signature to sign at least one of the original elements contained in the RecordItem class to provide authentication to all upstream participants in the trace or those involved in the investigation. All instances of RecordItem provided by the originator may be individually signed, and additional RecordItem entries by upstream peers in the trace or investigation may be signed by the peer adding the data, while maintaining the original RecordItem entry(s) and detached signature(s) from the original requestor. It is important to note that the data is signed at the RecordItem level. Since multiple RecordItems may exist within an IODEF document and may originate from different sources, the signature is applied at the RecordItem level to enable the use of an XML detached signature. Exclusive canonicalization [XMLCanon] is REQUIRED for the detached signature and not the references, as the XML document generated is then included in the RID message within the Signature element of the ReportSchema class. This signature MUST be passed to all recipients of the Request message.

- If a Request does not include a RecordItem entry, a timestamp MUST be used to ensure there is data to be signed for the multi-hop authentication use case. The DateTime element of the iodef: RecordData class ([RFC5070], Section 3.19.1) is used for this purpose.

- For all message types, the full IODEF-RID document MUST be signed using an enveloped signature by the sending peer to provide authentication and integrity to the receiving RID system. The signature is placed in an instance of the Signature element.

- XML Signature Best Practices [XMLSigBP] guidance SHOULD be followed to prevent or mitigate security risks. Examples include the recommendation to authenticate a signature prior to processing (executing potentially dangerous operations) and the recommendation to limit the use of URIs since they may enable cross-site scripting attacks or access to local information.

- XML Path Language (XPath) 2.0 [XMLPath] MUST be followed to specify the portion of the XML document to be signed. XPath is used to specify a location within an XML document. Best practice recommendations for using XPath [XMLSigBP] SHOULD be referenced to reduce the risk of denial-of-service attacks. The use of XSLT transforms MUST be restricted according to security guidance in [XMLSigBP].

XML Encryption

- The IODEF-RID document MAY be encrypted to provide an extra layer of security between peers so that not only the message is encrypted for transport. This behavior would be agreed upon between peers or a consortium, or determined on a per-message basis, depending on security requirements. It should be noted that there are cases for transport where the RIDPolicy class needs to be presented in clear text, as detailed in the transport document [RFC6546].

- A Request, or any other message type that may be relayed through RID systems before reaching the intended destination as a result of trust relationships, MAY be encrypted specifically 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 as such, RIDPolicy is maintained in clear text.

- The action taken in the Result message may be encrypted using the key of the request originator. In that case, the intermediate parties can view the RIDPolicy information and know the trace has been completed and do not need to see the action. If the use of encryption were limited to sections of the message, the History class information would be encrypted. Otherwise, it is RECOMMENDED to encrypt the entire IODEF-RID document and use an enveloped signature for the originator of the request. The existence of the Result message for an incident would tell any intermediate parties used in the path of the incident investigation that the incident handling has been completed.

- The iodef:restriction attribute sets expectations for the privacy of an incident and is defined in Section 3.2 of RFC 5070. Following the guidance for XML encryption in the Security Requirements section, the iodef:restriction attribute can be set in any of the RID classes to define restrictions and encryption requirements for the exchange of incident information. The restriction options enable encryption capabilities for the

complete exchange of an IODEF document (including any extensions), within specific classes of IODEF, or IODEF extensions, where more limited restrictions are desired. The restriction attribute is contained in each of the RID classes and MUST be used in accordance with confidentiality expectations for either sections of the IODEF document or the complete IODEF document. Consortiums and organizations should consider this guidance when creating exchange policies.

- Expectations based on how restriction is set:

  * If restriction is set to 'private', the class or document MUST be encrypted for the recipient using XML encryption and the public key of the recipient. See Section 9.3 for a discussion on public key infrastructure (PKI) and other security requirements.

  * If restriction is set to 'need-to-know', the class or document MUST be encrypted to ensure only those with need-to-know access can decrypt the data. The document can either be encrypted for each individual for which access is intended or be encrypted with a single group key. The method used SHOULD adhere to any certificate policy and practices agreements between entities for the use of RID. A group key in this instance refers to a single key (symmetric) that is used to encrypt the block of data. The users with need-to-know access privileges may be given access to the shared key via a secure distribution method, for example, providing access to the symmetric key encrypted with each of the user's public keys.

  * If restriction is set to 'public', the class or document MUST be sent in clear text. This setting can be critical if certain sections of a document or an entire document are to be shared without restrictions. This provides flexibility within an incident to share certain information freely where appropriate.

  * If restriction is set to 'default', the information can be shared according to an information disclosure policy pre-arranged by the communicating parties.

- Expectations based on placement of the restriction setting:

  * If restriction is set within one of the RID classes, the restriction applies to the entire IODEF document.

  * If restriction is set within individual IODEF classes, the restriction applies to the specific IODEF class and the children of that class.

The formation of policies is a very important aspect of using a messaging system like RID to exchange potentially sensitive information. Many considerations should be involved for peering parties, and some guidelines to protect the data, systems, and transport are covered in this section. Policies established should provide guidelines for communication methods, security, and fall-back procedures. See Sections 9.4 and 9.5 for additional information on consortiums and PKI considerations.

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

RID provides a method to exchange incident-handling requests and Report messages between entities. Administrators have the ability to base decisions on the available resources and other factors of their network and maintain control of incident investigations within their own network. Thus, RID provides the ability for participating networks to manage their own security controls, leveraging the information listed in RIDPolicy.

RID is used to transfer or exchange XML documents in an IODEF format or using another IANA-registered format. Implementations SHOULD NOT download schemas at runtime due to the security implications, and included documents MUST NOT be required to provide a resolvable location of their schema.

9.2. Message Transport

A transport specification is defined in a separate document [RFC6546]. The specified transport protocols MUST use encryption to provide an additional level of security and integrity, while supporting mutual authentication through bidirectional certificate usage. Any subsequent transport method defined should take advantage of existing standards for ease of implementation and integration of RID systems. Session encryption for the transport of RID messages is enforced in the transport specification. The privacy and security considerations are addressed fully in RID to protect sensitive portions of documents and to provide a method to authenticate the messages. Therefore, RID messages do not rely on the security provided by the transport layer alone. The encryption requirements and considerations for RID messages are discussed in Section 9.1 of this document.

Consortiums may vary their selected transport mechanisms and thus decide upon a mutual protocol to use for transport when communicating with peers in a neighboring consortium using RID. RID systems MUST implement and deploy HTTPS as defined in the transport document [RFC6546] and optionally MAY support other protocols such as the Blocks Extensible Exchange Protocol (BEEP) [RFC3080]. Bindings would need to be defined to enable support for other transport protocols.

Systems used to send authenticated RID messages between networks MUST use a secured system and interface to connect to a border network's RID systems. Each connection to a RID system MUST meet the security requirements agreed upon through the consortium regulations, peering, or SLAs. The RID system MUST listen for and send RID messages on only the designated port, which also MUST be over an encrypted tunnel meeting the minimum requirement of algorithms and key lengths established by the consortium, peering, or SLA. The selected cryptographic algorithms for symmetric encryption, digital signatures, and hash functions MUST meet minimum security levels of the times. The encryption strength MUST adhere to import and export regulations of the involved countries for data exchange.

Out-of-band communications dedicated to SP 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 practical or possible between service providers, but provisions should be considered to protect the incident management systems used for RID messaging. Methods to protect the data transport may also be provided through session encryption.

9.3. Public Key Infrastructure

It is RECOMMENDED that RID, the XML security functions, and transport protocols properly integrate with a PKI managed by the consortium, federate PKIs within a consortium, or use a PKI managed by a trusted third party. Entities MAY use shared keys as an alternate solution, although this may limit the ability to validate certificates and could introduce risk. For the Internet, a few examples of existing efforts that could be leveraged to provide the supporting PKI include the Regional Internet Registry's (RIR's) PKI hierarchy, vendor issued certificates, or approved issuers of Extended Validation (EV) Certificates. Security and privacy considerations related to consortiums are discussed in Sections 9.4 and 9.5.

The use of PKI between entities or by a consortium SHOULD adhere to any applicable certificate policy and practices agreements for the use of RID. [RFC3647] specifies a commonly used format for

certificate policy (CP) and certification practices statements (CPS). Systems with predefined relationships for RID include those who peer directly or through a consortium with agreed-upon appropriate use agreements. The agreements to trust other entities may be based on assurance levels that could be determined by a comparison of the CP, CPS, and/or RID operating procedures. The initial comparison of policies and the ability to audit controls provide a baseline assurance level for entities to form and maintain trust relationships. Trust relationships may also be defined through a bridged or hierarchical PKI in which both peers belong. If shared keys or keys issued from a common CA are used, the verification of controls to determine the assurance level to trust other entities may be limited to the RID policies and operating procedures.

XML security functions utilized in RID require a trust center such as a PKI for the distribution of credentials to provide the necessary level of security for this protocol. Layered transport protocols also utilize encryption and rely on a trust center. Public key certificate pairs issued by a trusted Certification Authority (CA) MAY be used to provide the necessary level of authentication and encryption for the RID protocol. The CA used for RID messaging must be trusted by all involved parties and may take advantage of similar efforts, such as the Internet2 federated PKI or the ARIN/RIR effort to provide a PKI to service providers. The PKI used for authentication also provides the necessary certificates needed for encryption used for the RID transport protocol [RFC6546].

9.3.1. Authentication

Hosts receiving a RID message MUST be able to verify that the sender of the request is valid and trusted. Using digital signatures on a hash of the RID message with an X.509 version 3 certificate issued by a trusted party MUST be used to authenticate the request. The X.509 version 3 specifications as well as the digital signature specifications and path validation standards set forth in [RFC5280] MUST be followed in order to interoperate with a PKI designed for similar purposes. Full path validation verifies the chaining relationship to a trusted root and also performs a certificate revocation check. 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 [XMLencrypt] or digital signature [XMLsig] [RFC3275] is used within a document.

It might be helpful to define an extension to the authentication scheme that uses attribute certificates [RFC5755] in such a way that an application could automatically determine whether human intervention is needed to authorize a request; however, the specification of such an extension is out of scope for this document.

The use of pre-shared keys may be considered for authentication at the transport layer. If this option is selected, the specifications set forth in "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)" [RFC4279] MUST be followed. Transport specifications are detailed in a separate document [RFC6546].

9.3.2. Multi-Hop Request Authentication

The use of multi-hop authentication in a Request is used when a Request is sent to multiple entities or SPs in an iterative manner. Multi-hop authentication is REQUIRED in Requests that involve multiple SPs where Requests are forwarded iteratively through peers. Bilateral trust relationships MAY be used between peers; multi-hop authentication MUST be used for cases where the originator of a message is authenticated several hops into the message flow.

For practical reasons, SPs may want to prioritize incident-handling events based upon the immediate peer for a Request, the originator of a request, and the listed Confidence rating for the incident. In order to provide a higher assurance level of the authenticity of a Request, the originating RID system is included in the Request along with contact information and the information of all RID systems in the path the trace has taken. This information is provided through the IODEF EventData class, which nests the list of systems and contacts involved in a trace, while setting the category attribute to "infrastructure".

To provide multi-hop authentication, the originating RID system MUST include a digital signature in the Request 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 [XMLsig] using a detached signature. The signature MUST be passed to all parties that receive a Request, and each party MUST be able to perform full path validation on the digital signature [RFC5280]. In order to accommodate that requirement, the RecordItem data MUST remain unchanged as a request is passed along between providers and is the only element for which the signature is applied. If additional RecordItems are included in the document at upstream peers, the initial RecordItem entry MUST still remain with the detached signature. The subsequent RecordItem elements may be signed by the peer adding the incident information for the investigation. A second

benefit to this requirement is that the integrity of the filter used is ensured as it is passed to subsequent SPs in the upstream trace of the incident. The trusted PKI also provides the keys used to digitally sign the RecordItem class for a Request to meet the requirement of authenticating the original request. Any host in the path of the trace should be able to verify the digital signature using the trusted PKI.

In the case in which an enterprise using RID sends a Request to its provider, the signature from the enterprise MUST be included in the initial request. The SP may generate a new request to send upstream to members of the SP consortium to continue the investigation. If the original request is sent, the originating SP, acting on behalf of the enterprise network under attack, MUST also digitally sign, with an enveloped signature, the full IODEF document to assure the authenticity of the Request. An SP 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. SPs participating in the trace MUST be able to determine the authenticity of RID requests.

9.4. Consortiums and Public Key Infrastructures

Consortiums are an ideal way to establish a communication web of trust for RID messaging. It should be noted that direct relationships may be ideal for some communications, such as those between a provider of incident information and a subscriber of the incident reports. The consortium could provide centralized resources, such as a PKI, and established guidelines and control requirements for use of RID. The consortium may assist in establishing trust relationships between the participating SPs to achieve the necessary level of cooperation and experience-sharing among the consortium entities. This may be established through PKI certificate policy [RFC3647] reviews to determine the appropriate trust levels between organizations or entities. The consortium may also be used for other purposes to better facilitate communication among SPs 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 consortiums that peer with SPs belonging to a separate consortium. In other words, consortiums could peer with other consortiums to enable communication of RID messages between the participating SPs. The PKI along with Memorandums of Agreement could be used to link border directories to share public key information in a bridge, a hierarchy, or a single cross-certification relationship.

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

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

The functions described for a consortium's role parallel those 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.

A PKI can also provide the same level of security for communication between an end entity (enterprise, educational, or government customer network) and the SP.

9.5. 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 for the system communicating RID messages and other integrated components include the following:

Service Provider Concerns:

- Privacy of data monitored and/or stored on Intrusion Detection Systems (IDSs) for attack detection.
- Privacy of data monitored and stored on systems used to trace traffic across a single network.
- Privacy of incident information stored on incident management systems participating in RID communications.

Customer Attached Networks Participating in RID with SP:

- Customer networks may include enterprise, educational, government, or other networks attached to an SP participating in RID. Customers should review data handling policies to understand how

data will be protected by a service provider. This information will enable customers to decide what types of data at what sensitivity level can be shared with service providers. This information could be used at the application layer to establish sharing profiles for entities and groups; see Section 9.6.

- Customers should request information on the security and privacy considerations in place by their SP and the consortium of which the SP is a member. Customers should understand if their data were to be forwarded, how it might be sanitized and how it will be protected. In advance of sharing data with their SP, customers should also understand if limitations can be placed on how it will be used.

- Customers should be aware that their data can and will be sent to other SPs in order to complete a trace unless an agreement stating otherwise is made in the service level agreements between the customer and SP. Customers considering privacy options may limit the use of this feature if they do not want the data forwarded.

Parties Involved in the Attack:

- Privacy of the identity of a host involved in an attack or any indicators of compromise.

- Privacy of information such as the source and destination used for communication purposes over the monitored or RID-connected network(s).

- Protection of data from being viewed by intermediate parties in the path of an Request request should be considered.

Consortium Considerations:

- System use restrictions for security incident handling within the local region’s definitions of appropriate traffic. When participating in a consortium, appropriate use guidelines should be agreed upon and entered into contracts.

- System use prohibiting the consortium’s participating SPs from inappropriately tracing traffic to locate sources or mitigate traffic unlawfully within the jurisdiction or region.

Inter-Consortium Considerations:

- System use between peering consortiums should consider any government communication regulations that apply between those two regions, such as encryption export and import restrictions.

- System use between consortiums SHOULD NOT request traffic traces and actions beyond the scope intended and permitted by law or inter-consortium agreements.

- System use between consortiums should consider national boundary issues and request limits in their appropriate system use agreements. Appropriate use should include restrictions to prevent the use of the protocol for limiting or restricting traffic that is otherwise permitted within the country in which the peering consortium resides.

The security and privacy considerations listed above are for the consortiums, SPs, and enterprises to agree upon. The agreed-upon policies may be facilitated through use of the RIDPolicy class and application-layer options. Some privacy considerations are addressed through the RID guidelines for encryption and digital signatures as described in Section 9.1.

RID is useful in determining the true source of an incident that traverses multiple networks or to communicate security incidents and automate the response. The information obtained from the investigation may determine the identity of the source host or the SP used by the source of the traffic. It should be noted that the trace mechanism used across a single SP may also raise privacy concerns for the clients of the network. Methods that may raise concern include those that 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. IDSs and single-network tracing are outside of the scope of this document, but the concern should be noted and addressed within the use guidelines of the network. Some IDSs 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-SP level and are out of scope for RID messaging.

The identity of the true source of an attack being traced through RID could be sensitive. The true identity listed in a Result message can be protected through the use of encryption [XMLencrypt] enveloping the IODEF document and RID Result information, using the public encryption key of the originating SP. Alternatively, the action taken may be listed without the identity being revealed to the originating SP. The ultimate goal of the RID communication system is to stop or mitigate attack traffic, not to ensure that the identity of the attack traffic is known to involved parties. The SP that

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

Privacy becomes an issue whenever sensitive data traverses a network. For example, if an attack occurred between a specific source and destination, then every SP in the path of the trace becomes aware that the cyber attack occurred. In a targeted attack, it may not be desirable that information about two nation states that are battling a cyber war would 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 a Request or Report, where the originating SP is aware of the SP that will receive the request for processing, the free-form text areas of the document could be encrypted [XMLencrypt] using the public key of the destination SP to ensure that no other SP in the path can read the contents. The encryption is accomplished through the W3C [XMLencrypt] specification for encrypting an element.

In some situations, all network traffic of a nation may be granted through a single SP. In that situation, options must support sending Result messages from a downstream peer of that SP. That option provides an additional level of abstraction to hide the identity and the SP 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 Request message to request action close to the source of valid attack traffic need to be considered. Although the intermediate SPs may relay the request if there is no direct trust relationship to the closest SP to the source, the intermediate SPs 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 SP in the path. Therefore, the contents of the request may be encrypted for the destination system. The intermediate SPs only need to know how to direct the request to the manager of the ASN 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 includes a request to block or rate-limit legitimate traffic to prevent information from being shared between users on the Internet (restricting access to online versions of papers) or restricting access from a competitor's product in order to sabotage a business.

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

The privacy concerns listed in this section address issues among the trusted parties involved in a trace within an SP, 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 and through the local security controls in place for the incident management systems. Each RID system MUST perform a bidirectional 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 via TLS over a transport protocol such as [RFC6546]. The RID messages may be decrypted at each RID system in order to properly process the request or relay the information. Today's processing power is more than sufficient to handle the minimal burden of encrypting and decrypting relatively small typical RID messages.

9.6. Sharing Profiles and Policies

The application layer can be used to establish workflows and rulesets specific to sharing profiles for entities or consortiums. The profiles can leverage sharing agreements to restrict data types or classifications of data that are shared. The level of information or classification of data shared with any entity may be based on protection levels offered by the receiving entity and periodic validation of those controls. The profile may also indicate how far information can be shared according to the entity and data type. The profile may also indicate whether requests to share data from an entity must go directly to that entity.

In some cases, pre-defined sharing profiles will be possible. These include any use case where an agreement is in place in advance of sharing. Examples may be between clients and SPs, entities such as partners, or consortiums. There may be other cases when sharing profiles may not be established in advance, such as an organization dealing with an incident who requires assistance from an entity that it has not worked with before. An organization may want to establish sharing profiles specific to possible user groups to prepare for possible incident scenarios. The user groups could include business partners, industry peers, service providers, experts not part of a service provider, law enforcement, or regulatory reporting bodies.

Workflows to approve transactions may be specific to sharing profiles and data types. Application developers should include capabilities to enable these decision points for users of the system.

Any expectations between entities to preserve the weight and admissibility of evidence should be handled at the policy and agreement level. A sharing profile may include notes or an indicator for approvers in workflows to reflect if such agreements exist.

10. Security Considerations

RID has many security requirements and considerations built into the design of the protocol, several of which are described in the Security Requirements section. For a complete view of security, considerations include the availability, confidentiality, and integrity concerns for the transport, storage, and exchange of information.

Protected tunnels between systems accepting RID communications are used to provide confidentiality, integrity, authenticity, and privacy for the data at the transport layer. Encryption and digital signatures are also used at the IODEF document level through RID options to provide confidentiality, integrity, authenticity, privacy and traceability of the document contents at the application layer. Trust relationships are based on PKI and the comparison/validation of security controls for the incident management systems communicating via RID. Trust levels can be established in cross-certification processes where entities compare PKI policies that include the specific management and handling of an entity's PKI and certificates issued under that policy. [RFC3647] defines an Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework that may be used in the comparison of policies to establish trust levels and agreements between entities, an entity and a consortium, and consortiums. The agreements SHOULD consider key management practices including the ability to perform path validation on certificates [RFC5280], key distribution techniques [RFC2585], and Certificate Authority and Registration Authority management practices.

The agreements between entities SHOULD also include a common understanding of the usage of RID security, policy, and privacy options discussed in both the Security Requirements and Security Considerations sections. The formality, requirements, and complexity of the agreements for the certificate policy, practices, supporting infrastructure, and the use of RID options SHOULD be decided by the entities or consortiums creating those agreements.

11. Internationalization Issues

The Node class identifies a host or network device. This document reuses the definition of Node from the IODEF specification [RFC5070], Section 3.16. However, that document did not clearly specify whether a NodeName could be an Internationalized Domain Name (IDN). RID systems MUST treat the NodeName class as a domain name slot [RFC5890]. RID systems SHOULD support IDNs in the NodeName class. If they do so, the UTF-8 representation of the domain name MUST be used, i.e., all of the domain name's labels MUST be U-labels

expressed in UTF-8 or NR-LDH labels [RFC5890]; A-labels MUST NOT be used. An application communicating via RID can convert between A-labels and U-labels by using the Punycode encoding [RFC3492] for A-labels as described in the protocol specification for Internationalized Domain Names in Applications [RFC5891].

12. IANA Considerations

This document uses URNs to describe XML namespaces and XML schemas [XMLschema] conforming to a registry mechanism described in [RFC3688].

Registration request for the iodef-rid namespace:

URI: urn:ietf:params:xml:ns:iodef-rid-2.0

Registrant Contact: IESG.

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-2.0

Registrant Contact: IESG.

XML: See Section 8, "RID Schema Definition", of this document.

The following registry has been created and is now managed by IANA:

Name of the registry: "XML Schemas Exchanged via RID"

Namespace details: A registry entry for an XML Schema Transferred via RID consists of:

Schema Name: A short string that represents the schema referenced. This value is for reference only in the table. The version of the schema MUST be included in this string to allow for multiple versions of the same specification to be in the registry.

Version: The version of the registered XML schema. The version is a string that SHOULD be formatted as numbers separated by a '.' (period) character.

Namespace: The namespace of the referenced XML schema. This is represented in the RID ReportSchema class in the XMLSchemaID attribute as an enumerated value is represented by a URN or URI.

Specification URI: A URI [RFC3986] from which the registered specification can be obtained. The specification MUST be publicly available from this URI.

Reference: The reference to the document that describes the schema.

Information that must be provided to assign a new value: The above list of information.

Fields to record in the registry: Schema Name, Version, Namespace, Specification URI, Reference

Initial registry contents: See Section 5.6.1.

Allocation Policy: Expert Review [RFC5226] and Specification Required [RFC5226].

The Designated Expert is expected to consult with the MILE (Managed Incident Lightweight Exchange) working group or its successor if any such WG exists (e.g., via email to the working group's mailing list). The Designated Expert is expected to retrieve the XML schema specification from the provided URI in order to check the public availability of the specification and verify the correctness of the URI. An important responsibility of the Designated Expert is to ensure that the XML schema is appropriate for use in RID.

The following registry has been created and is now managed by IANA:

Name of the registry: "RID Enumeration List"

The registry is intended to enable enumeration value additions to attributes in the iodef-rid XML schema.

Fields to record in the registry: Attribute Name, Attribute Value, Description, Reference

Initial registry content: none.

Allocation Policy: Expert Review [RFC5226]

The Designated Expert is expected to consult with the MILE (Managed Incident Lightweight Exchange) working group or its successor if any such WG exists (e.g., via email to the working group's mailing list). The Designated Expert is expected to review the request and validate the appropriateness of the enumeration for the attribute. If a specification is associated with the request, it MUST be reviewed by the Designated Expert.

13. Summary

Security incidents have always been difficult to trace as a result of 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. SPs need policies and automated methods to combat the hacker's efforts. SPs 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 SP resources for each aspect of attack detection, tracing, and source identification and extends the communication capabilities among SPs. The communication is accomplished through the use of flexible IODEF XML-based documents passed between incident-handling systems or RID systems. A Request is communicated to an upstream SP 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 SPs, which is essential for incident handling.

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2585] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", RFC 2585, May 1999.

[RFC3023] Murata, M., St. Laurent, S., and D. Kohn, "XML Media Types", RFC 3023, January 2001.

[RFC3275] Eastlake, D., Reagle, J., and D. Solo, "(Extensible Markup Language) XML-Signature Syntax and Processing", RFC 3275, March 2002.

[RFC3470] Hollenbeck, S., Rose, M., and L. Masinter, "Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols", BCP 70, RFC 3470, January 2003.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, March 2003.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

[RFC4051] Eastlake, D., "Additional XML Security Uniform Resource Identifiers (URIs)", RFC 4051, April 2005.

[RFC4279] Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, December 2007.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5646] Phillips, A. and M. Davis, "Tags for Identifying Languages", BCP 47, RFC 5646, September 2009.

[RFC5755] Farrell, S., Housley, R., and S. Turner, "An Internet Attribute Certificate Profile for Authorization", RFC 5755, January 2010.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, August 2010.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, August 2010.

[RFC6546] Trammell, B., "Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS", RFC 6546, April 2012.

[XML1.0] Bray, T., Maler, E., Paoli, J., Sperberg-McQueen, C., and F. Yergeau, "Extensible Markup Language (XML) 1.0", W3C Recommendation XML 1.0, November 2008, <http://www.w3.org/TR/xml/>.

[XMLCanon] Boyer, J., "Canonical XML 1.0", W3C Recommendation 1.0, December 2001, <http://www.w3.org/TR/xml-c14n>.

[XMLPath] Berglund, A., Boag, S., Chamberlin, D., Fernandez, M., Kay, M., Robie, J., and J. Simeon, "XML Schema Part 1: Structures", W3C Recommendation Second Edition, December 2010, <http://www.w3.org/TR/xpath20/>.

[XMLSigBP] Hirsch, F. and P. Datta, "XML-Signature Best Practices", W3C Recommendation, August 2011, <http://www.w3.org/TR/xmldsig-bestpractices/>.

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

[XMLschema] Thompson, H., Beech, D., Maloney, M., and N. Mendelsohn, "XML Schema Part 1: Structures", W3C Recommendation Second Edition, October 2004, <http://www.w3.org/TR/xmlschema-1/>.

[XMLsig] Bartel, M., Boyer, J., Fox, B., LaMaccia, B., and E. Simon, "XML-Signature Syntax and Processing", W3C Recommendation Second Edition, June 2008, <http://www.w3.org/TR/xmldsig-core/>.

14.2. Informative References

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, March 1996.

[RFC3080] Rose, M., "The Blocks Extensible Exchange Protocol Core", RFC 3080, March 2001.

[RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, November 2003.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC5735] Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses", BCP 153, RFC 5735, January 2010.

[RFC6045] Moriarty, K., "Real-time Inter-network Defense (RID)", RFC 6045, November 2010.

[RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, March 2011.

[XMLNames] Bray, T., Hollander, D., Layman, A., Tobin, R., and H. Thomson, "Namespaces in XML 1.0 (Third Edition)", W3C Recommendation , December 2009, <http://www.w3.org/TR/xml-names/>.

Appendix A. Acknowledgements

Many thanks to colleagues and the Internet community for reviewing and commenting on the document as well as providing recommendations to improve, simplify, and secure the protocol: Steve Bellovin, David Black, Harold Booth, Paul Cichonski, Robert K. Cunningham, Roman Danyliw, Yuri Demchenko, Sandra G. Dykes, Stephen Farrell, Katherine Goodier, Cynthia D. McLain, Thomas Millar, Jean-Francois Morfin, Stephen Northcutt, Damir Rajnovic, Tony Rutkowski, Peter Saint-Andre, Jeffrey Schiller, Robert Sparks, William Streilein, Richard Struse, Tony Tauber, Brian Trammell, Sean Turner, Iljitsch van Beijnum, and David Waltermire.

Author's Address

Kathleen M. Moriarty
EMC Corporation
176 South Street
Hopkinton, MA
United States

EMail: Kathleen.Moriarty@emc.com