RID-DoS:
Real-time Inter-network Defense Against Denial of Service Attacks

Kathleen M. Moriarty

MIT Lincoln Laboratory

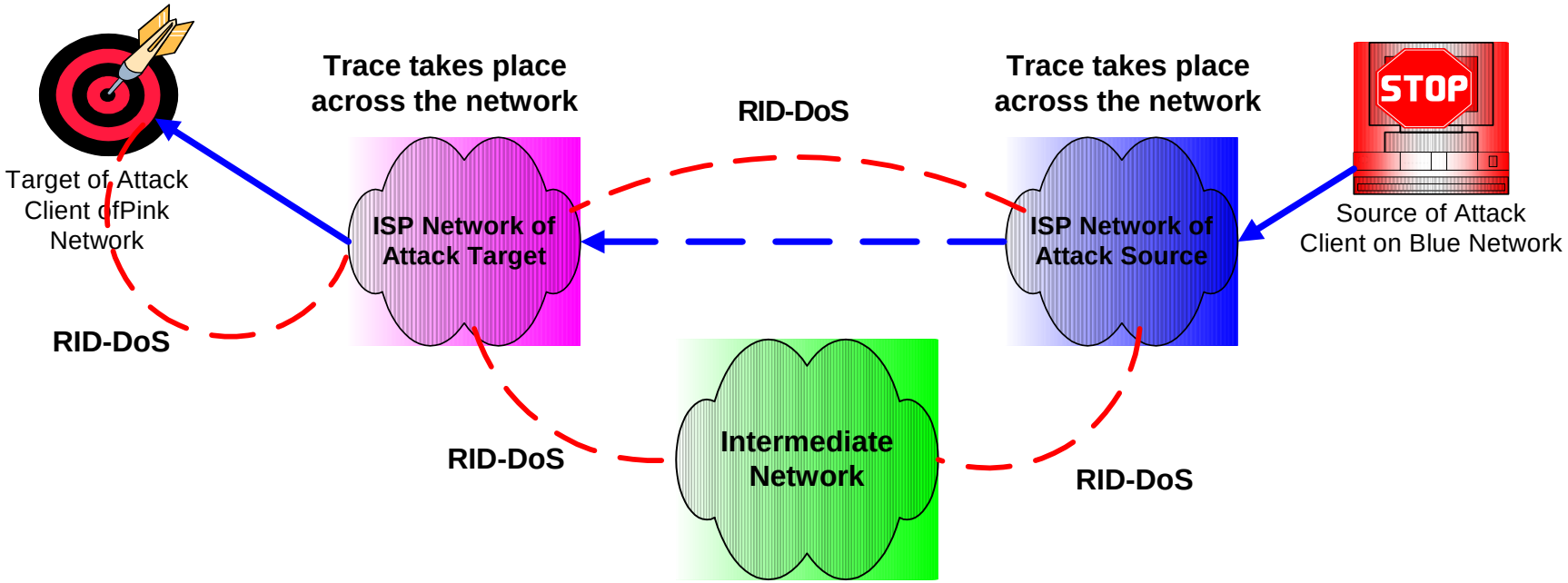
22 October 2002

This work was sponsored by the Air Force Contract number F19628-00-C-002.

RID Goals

- Real time method to mitigate effects of network attacks
- Establish communication mechanism for network peers
  - ISPs, Education, Government, etc.
- Capability to continue traces through upstream networks
  - Addresses inter-Network communication issues
  - Respect network boundaries
  - Integrate existing trace implementations
  - Ability to trace attack back to valid/spoofed source address
- Use existing infrastructure for attack detection and trace
  - Network statistics used to detect variations in traffic types
  - Compensate for network events to reduce false positives
  - Backbone outage or network event
  - Flexible - Integrate new detection and single network trace methods

Communication via RID



Parameters for Trace Approaches

- Many solutions require IP header information as parameters to trace request
- Time range of attack
- RID-DoS would need to incorporate the following parameters for Flow analysis or filter approaches
  - Non-changing fields of IP header
  - IP protocol
  - IP source address and port
  - IP destination address and port
  - TCP flags
  - Packet size
  - Start and stop time traffic detected
- Hash based IP Traceback also requires 1st 8 bytes of the packet payload
- PATH information for each hop (network) in the trace
  - AS Number, IP of NMS
- Action Taken
  - Additional fields required

RID Notification / Attack Mitigation

- Proposal provides Inter-ISP communication to support continued trace to attack source
- RID messages are text
  - Parsed at receiving host
  - Trace continuance must be authorized
  - Trace continuance may be automated based on confidence rating
- Four Message Types
  - Request, Status, Source Found, Relay
- Notification of the status of the trace is sent back to the originator of the trace as it traverses multiple networks
  - Must be passed through each NMS in path
- Notification sent to trace originator upon completion
  - Source of attack found
  - Action taken included in communication
    - Blocked at source assists in mitigating or stopping the DoS or DDoS attack
    - Notify client and other traffic blocking mechanisms included in options

Message Type 1 – Trace Request

Message Type 1

Time Stamp

Incident Identifier = ASN + Incident number + Instance

Confidence rating of detected Denial of Service attack (0-100)

Level	Meaning
1	Low probability detected attack occurred
100	Attack detected with 100 percent confidence rating

Filter used to trace incident across meters in the network – IP Header Information

Number of NMS in the path listed in message

Path information of Network Management Systems used in the trace

- Autonomous System Number and NMS IP address of Next Network
- Autonomous System Number and NMS IP address Current Network
- ...
- Autonomous System Number and NMS IP address of Originating Network

Summary

- Uses existing network infrastructure
  - NMS to relay RID Messages to request trace continuance
- RID messaging incorporates a communication mechanism in order to trace traffic across network boundaries
- Expand entries in several fields
- Extension to accommodate additional parameters
- http://www.ietf.org/internet-drafts/draft-moriarty-ddos-rid-05.txt