Inter-provider Coordination for Real-Time Tracebacks

Kathleen M. Moriarty

MIT Lincoln Laboratory

2 June 2003

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

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

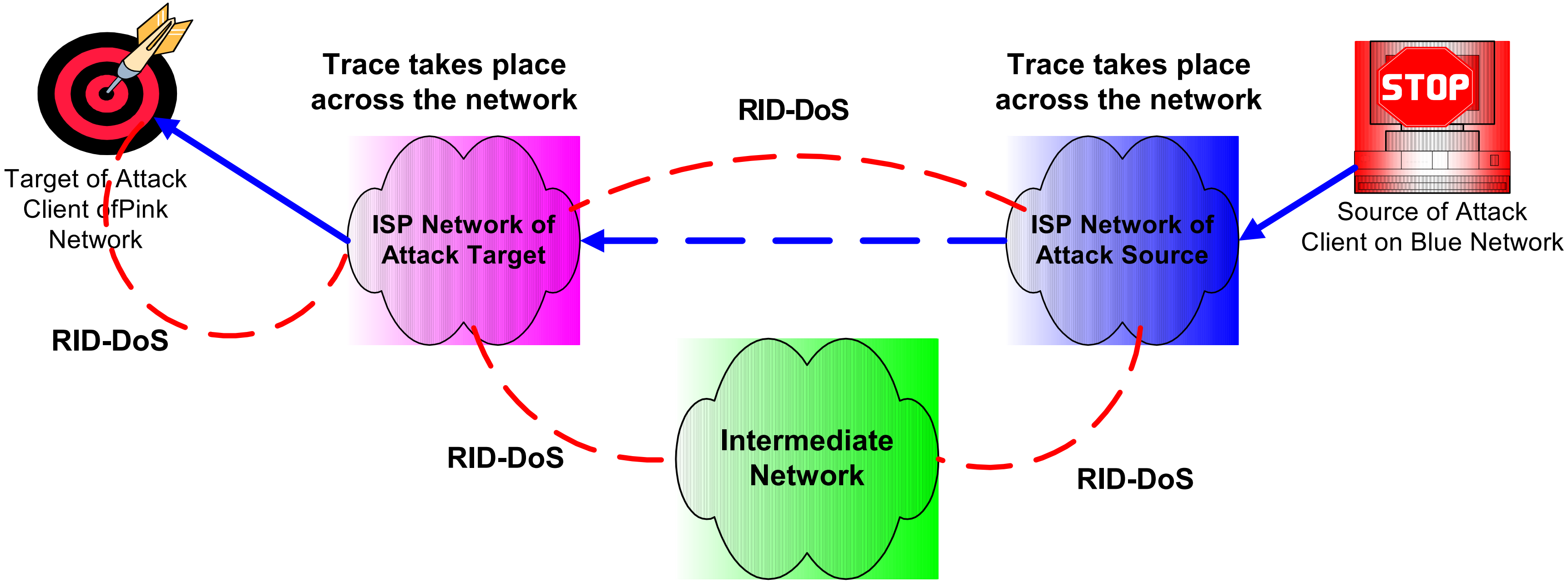
Real-time Inter-network Defense (RID)

- Proposed Internet Draft Standard to provide framework for ISPs to communicate and trace attacks to source
- Standardization of inter-provider coordination by leveraging existing relationships between operators
- Use existing standards to facilitate acceptance by router and Network Management System vendors
- Integration of existing tracing mechanisms across network borders
- Address need for policy on communication issues to coordinate traces between networks
- Small scale implementation using email for transport

Goals

- Real time method to mitigate effects of DoS or DDoS attack
- Capability to continue traces through upstream networks
  - Addresses inter-Network communication issues
    - Social
    - Technical
  - 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-DoS


Trace takes place across the network
RID-DoS
Trace takes place across the network
STOP
Target of Attack Client ofPink Network
ISP Network of Attack Target
ISP Network of Attack Source
Source of Attack Client on Blue Network
RID-DoS
Intermediate Network
RID-DoS
RID-DoS

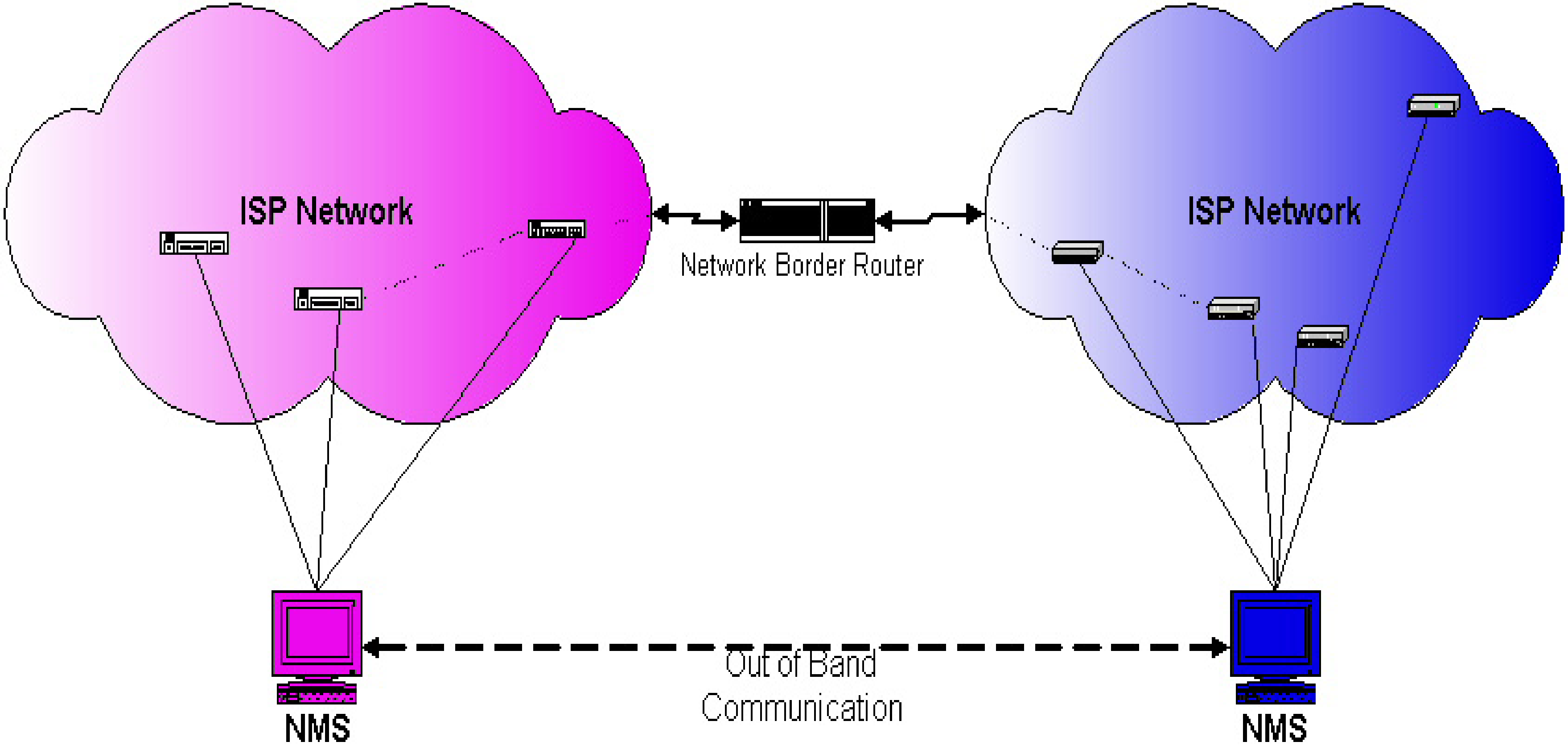
Trace Mechanism

- ISPs and researchers have been working on trace solutions since the beginning of the DoS attacks in the 90s
- Difficult problem to solve
  - Network resources limited, especially during attack
    - Network equipment resources close to capacity
    - Promiscuous listening devices as an alternative
  - Privacy issues and concerns must be addressed
    - Tracing Internet traffic
    - Saving data of established Internet connections
  - Potentially thousands of hosts involved in an attack
    - Small streams of traffic from a particular host
    - Multiple types of traffic
    - Source addresses may be spoofed
- Possible solutions across a single network
  - Network flow analysis
  - Hash-based IP Traceback
  - ICMP Traceback

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

Inter-Network Communication



Communication Between Networks

- Establish trusted communications with border networks
  - Established through peering relationships
  - Legal issues addressed in ISP peering agreement
  - May be a value added service to clients
  - Contact information for peers established as peering points are enabled (ASNs)
- Messaging and Communication methods must be secure
  - Consider an out of band network linking these systems between ISPs
    - Link Layer connections to prevent access from Internet
    - IPSec tunnels established between border network management systems
  - Authentication of request
  - Privacy considerations
- Trusted NMS systems must be secure at each ISP
  - Physical Access Control, Authorization, Access Controls, Authentication
- Must ensure the RID-DoS messages reach their destination
- Must not cause a Denial of Service
  - Ability to approve/disapprove and queue a trace request

RID-DoS Notification / Attack Mitigation

- Proposal provides Inter-ISP communication to support continued trace to attack source
- RID-DoS messages are text
  - Parsed at receiving host
  - Trace continuance must be authorized
  - Trace continuance may be automated based on confidence rating
- 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

RID-DoS Traces

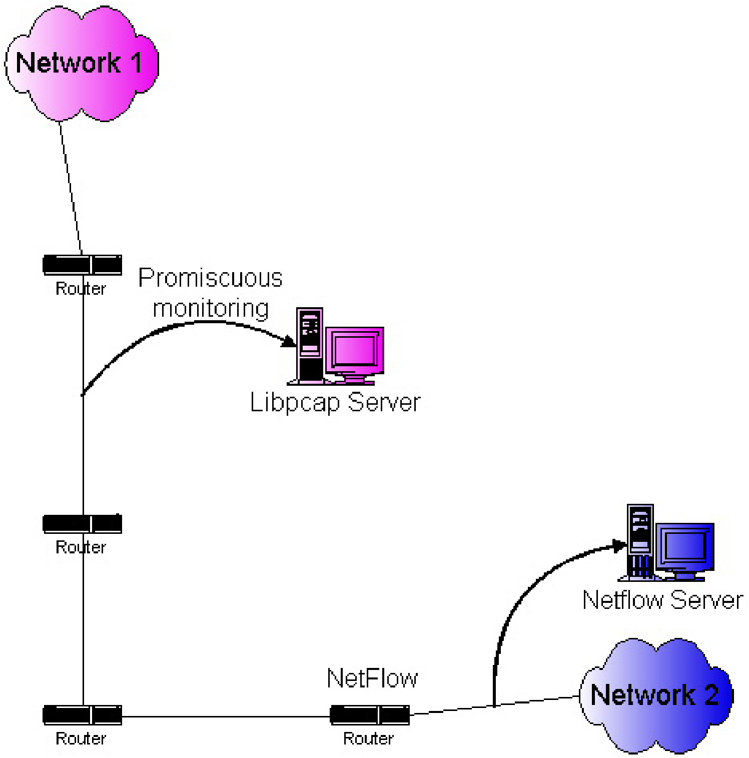
- DDoS Attack
  - Multiple traces initiated
  - Initiating management system must queue requests and limit to a reasonable number of traces
  - Management systems in path can defer traces if large number of requests received
    - Capacity of network and RID-DoS system may determine limit
- Types of attacks
  - Distributed Denial of Service
    - Reflection
    - Fragmented packets
    - Multiple identical packets from various sources
  - Security incident
    - System Compromise

Email Based Test

- Email system implemented for initial testing
  - Test between several systems sending trace requests, trace authorization, and trace completed messages
  - Next step would be to test system across real network boundaries using various trace mechanisms on the respective networks
- Comma delimited email message parsed via perl script
  - Fields used match that of the three message types
  - Contact Information Table for Border Networks, ASN also used
- Encrypt, decrypt, and sign messages
  - S/MIME via PKI, or PGP
  - Digital signatures used in packet implementation can be implemented through S/MIME for simplicity in testing
- Information Exchanged when Establishing Peer Relationship
  - Obtain contact information for peers
- Tracking mechanism used to ensure traces are not duplicated across individual networks

RID Testing

- Two trace types of single network traces used in testing
  - Libpcap data
    - Search on stored data
    - Dynamic implementation of filters to match packet in trace request
  - Netflow
    - Search on stored data
    - Dynamic implementation of filters to match packet in trace request
- Communication via email
  - Located packet using data contained in trace requests
    - Originate Trace Request
  - Send notification messages to originating server
    - Trace Authorization
    - Source Found



Current Issues

- Involves entire Internet community, ISPs internationally
- Additional motivation needed for ISPs to work on solution
- Funding needed for resources
  - People, Equipment, etc.
- Consensus needed from ISPs and vendors on RID-DoS messaging formats and capabilities of trace continuance
  - Support needed in trace management systems used by ISPs
  - Information passed between networks
  - Ability to decide if a trace will continue on your network
- Additional feedback needed on current draft revision
- Have received some input from a few ISPs that would be interested in working on this
- Need more support and feedback – International as well

Summary

- Uses existing network infrastructure, routers and switches, to perform traces
  - Could use promiscuous sniffers as an alternative for monitoring devices
- Various Trace implementations must be considered to carry the appropriate trace information in RID-DoS messages
- RID-DoS messaging used to communicate with systems on border networks to enable inter-network tracing capability
- Social issues need to be addressed
  - Motivation to use system

- http://www.ietf.org/internet-drafts/draft-moriarty-ddos-rid-03.txt