ICMP Traceback Messages

Steven M. Bellovin

smb@research.att.com

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

Goals

- Trace of packets coming at you.
- Primary motive: trace back denial of service attacks.
- Other uses: path characterization; asymmetric route detection; incoming traffic matrix.
- Product of informal research group; members include Steven M. Bellovin, Matt Blaze, Bill Cheswick, Cory Cohen, Jon David, Jim Duncan, Jim Ellis, Paul Ferguson, John Ioannidis, Marcus Leech, Perry Metzger, Robert Stone, Vern Paxson, Ed Vielmetti, Wietse Venema.

What is the Problem?

- Many denial of service attacks (i.e., SYN floods, Trinoo) use forged source addresses.
- How do you track down the source?
- Assumption: it only really matters if a *lot* of traffic is heading your way.

Basic Scheme

- With low probability (about $1/20,000$), routers should send an ICMP Traceback message to the destination, along with the triggering packet.
- Traceback packets contain forward and backwards router links, the traced packet, and an authentication field.
- TTL always set to 255 by sending system, thus providing distance to recipient.

Link Field Contents

- Fields always in ”forward order”, even on backwards links.
- Subfields:
  - Interface name.
  - Source/dest IP addresses (if available) for this hop.
  - Linking blob, preferably formed from source/dest MAC addresses.

Operation

- End system (or outboard monitor) collects ITRACE packets.
- Optionally, select only those for “interesting” packets.
- Link fields used to match up routers along the path. (For distributed DoS attacks, this will likely be a tree structure.)
- Eventually points back to (or near) originating system.

Authentication

- Must guard against attacker sending spoofed ITRACE packets.
- Ideal would be per-message digital signature, but that's too expensive today.
- Choices are null authentication, cleartext random strings, and HMACs.

Null Authentication

- Do we really need authentication?
- The TTL definition provides an unspoofable minimum distance measure.
- Is that good enough? It certainly determines a path, with corruption at some point beyond the end.

Cleartext Random String

- Include per-output interface authenticator string in each packet.
- Strings last for several minutes.
- Possible version: <interfacename, NTP time>, digitally signed.
- Traceback packets would also include digitally-signed list of last several strings.
- Hard for attacker to spoof, since to eavesdrop they would need to be closer to you than the emitting router.

HMAC

- Short-lived secret used to generate HMAC of traceback packet.
- After the secret has expired, digitally-signed, timestamped copy is added to list of previous secrets.
- In other words, you need to see two ITRACE packets from each router, separated by several minutes.

PKI Issues

- How does the recipient validate the signature? That is, who has the right to sign a message from a given router?
- Ideally, need PKI based on assigned IP addresses. (Also need global addresses for all routers. . .)
- Until then, each ISP needs its own ITRACE PKI, with a published root certificate.

Related Work

- Packet-marking by Savage *et al* — encodes path information in packet's IP ID field. See their paper for details: http://www.cs.washington.edu/homes/savage/traceback.html
- IDIP (Intrusion Detection and Isolation Protocol), by Schnackenberg *et al*: ftp://ftp.tislabs.com/pub/IDIP/DISCEX_IDR-Infrastructure.pdf

Major Open Issues

- Does this help enough with enough DoS attacks to be worthwhile?
- Will ISPs permit a mechanism that exposes so much of their network structure?
- Are there privacy implications?
- What authentication mechanism is best?
- What should the PKI look like?