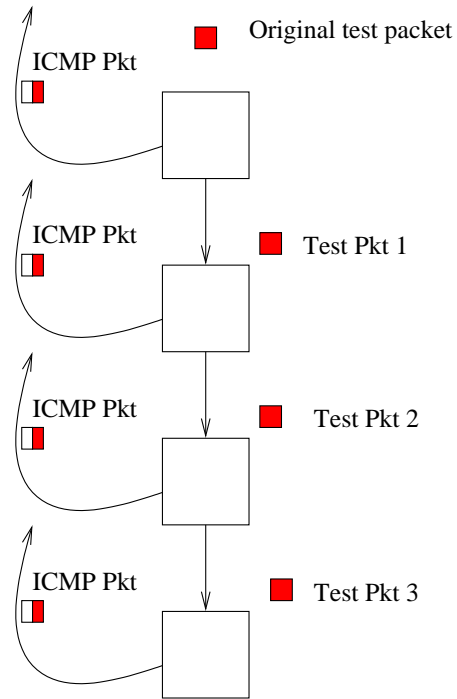# Crazy Traceroute Project

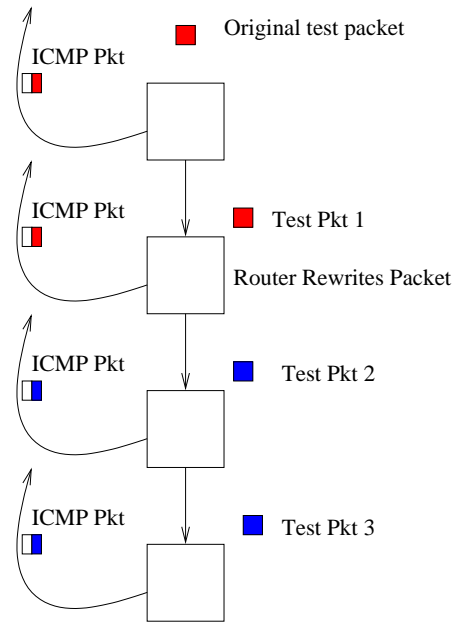## David Malone and Matthew Luckie

11 December 2007

Idea

- RFC 792: ICMP error messages quote packet.

- Allows ICMP errors to be directed to upper layer.

- IP header and at least next eight bytes to be quoted.

- Interested in when the quote does not match what was sent.

- Should see expected changes (TTL, DSCP, ECN).

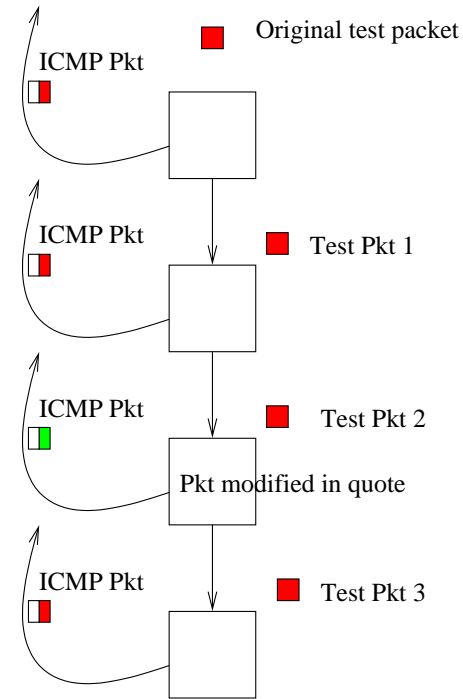- May be able to see NAT, packet scrubbing.

No Change

Original test packet

ICMP Pkt

ICMP Pkt   Test Pkt 1

ICMP Pkt   Test Pkt 2

ICMP Pkt   Test Pkt 3

Infilight Change

Original test packet

ICMP Pkt

ICMP Pkt   Test Pkt 1

Router Rewrites Packet

ICMP Pkt   Test Pkt 2

ICMP Pkt   Test Pkt 3

Change by Quoter

Original test packet

ICMP Pkt

ICMP Pkt   Test Pkt 1

ICMP Pkt   Test Pkt 2

Pkt modified in quote

ICMP Pkt   Test Pkt 3
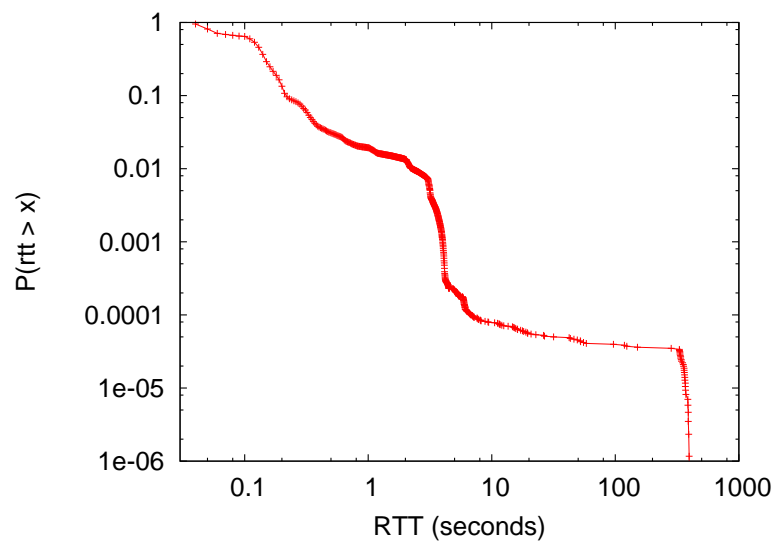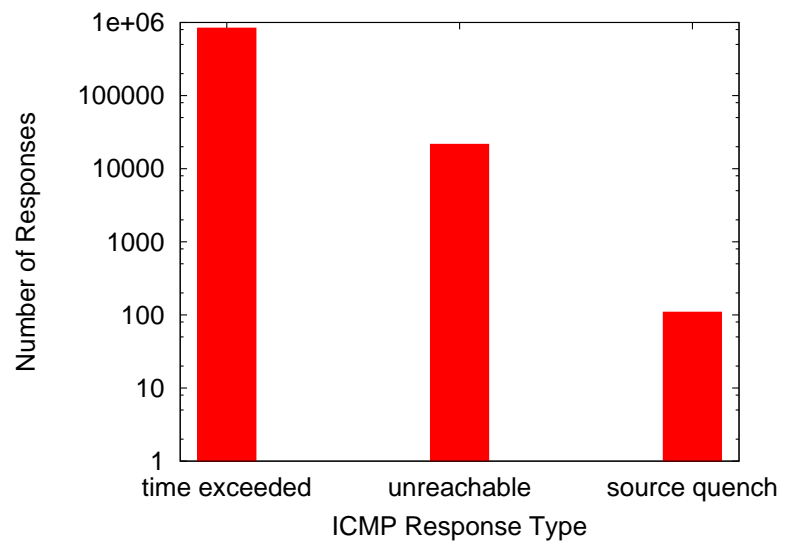
- `tcptraceroute` to 84393 web servers (Medina2004).

- Probe each hop once with TCP SYN to port 80.

- TCP ECE and CWR set, IP DSCP/ECN = 0x0f, DF set.

- Collect TCP SYN and ICMP errors with `tcpdump`.

- Data collected 6–12 May 2005.

- 1190351 probes sent.

- 858090 ICMP responses matched from 53768 unique IPs, 9 unmatched.

Observability of Changes

- Most (87.60%) quote 28 bytes, (min in RFC 792).

- Some (8.60%) quote 40 bytes, the size of the probe.

- Some (2.14%) quote 140 bytes, using ICMP MPLS extensions.

- So, $> 10.7\%$ quote complete IP and TCP headers.

- Some quoters do strange things (e.g. CERT VU#471084 quoting 60 bytes).

Observed Modifications

Modification	In-flight	Quoter	Edge	Total Unique
IPTOS_MOD	1533 (2.9%)	146 (0.3%)	1674 (3.1%)	3030 (5.6%)
IPLEN_SWAP	0 (0.0%)	0 (0.0%)	1 (0.0%)	1 (0.0%)
IPLEN_MOD	0 (0.0%)	174 (0.3%)	322 (0.6%)	480 (0.9%)
IPID_SWAP	0 (0.0%)	29 (0.1%)	469 (0.9%)	494 (0.9%)
IPID_MOD	0 (0.0%)	1 (0.0%)	19 (0.0%)	20 (0.0%)
IPDF_MOD	4 (0.0%)	1 (0.0%)	30 (0.1%)	35 (0.1%)
IPOFF_SWAP	0 (0.0%)	32 (0.1%)	49 (0.1%)	80 (0.2%)
IPDST_MOD	29 (0.1%)	36 (0.1%)	1189 (2.2%)	1248 (2.3%)
TCPSRC_MOD	0 (0.0%)	3 (0.0%)	43 (0.1%)	46 (0.1%)
TCPDST_MOD	1 (0.0%)	2 (0.0%)	129 (0.2%)	132 (0.3%)
TCPSEQ_MOD	1 (0.0%)	0 (0.0%)	12 (0.0%)	13 (0.0%)
TCPACK_MOD	0 (0.0%)	0 (0.0%)	19 (0.0%)	19 (0.0%)
TCPMSS_ADD	4 (0.0%)	0 (0.0%)	19 (0.0%)	23 (0.0%)

Example Clobbers

```
2b4f4b2055534552010000079207365742c206d      +OK USER....y set, m

5041535320726963010000000d0a6e6e65637469      PASS ric....  nnecti

000000000000a3fd00c467d345484c4f2074786d      ..........g.EHLO txm

474554202f6988392bcf86c2696c644f7665726c      GET /i.9+...ildOverl

0000000000005368696c6c792d5368616c6c797c      ......Shilly-Shally|

45534d54502053756e2c2030                      ESMTP Sun, 0

6564205065726d616e656e74                      ed Permanent

0a4167653a20313333360d0a                       Age:  1336

0a5365742d436f6f6b69653a                       Set-Cookie:

6374696f6e223e3c623e4d61                      ction"><b>Ma
```

IP Header

- 1533 made in-flight modification to DSCP/ECN.

- Some clear DSCP value, some clear DSCP and ECN.

- Evidence of consistent DSCP value assigned.

- Small number of in-flight modifications to destination IP, some using RFC 1918 addresses.

- 4 quoters seen clearing DF bit in flight.

- Quoter modification: add IP header length to IP length field, sometimes byte-swapping.

TCP Header

- Many more edge changes.

- 132 quoters showed modifications to destination port.

- Some show signs of port redirection to port 81, 8080.

- 46 quoters showed modifications to source port, less coherent.

- 23 quoters revealed an MSS option added.

- MSS values of 536, 1360 1414, 1436 and 1460 seen.