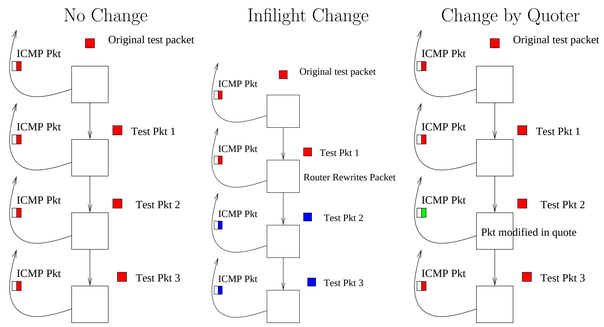
Analysis of ICMP Quotations

David Malone and Matthew Luckie
Hamilton Institute, NUI Maynooth and WAND Group, University of Waikato.

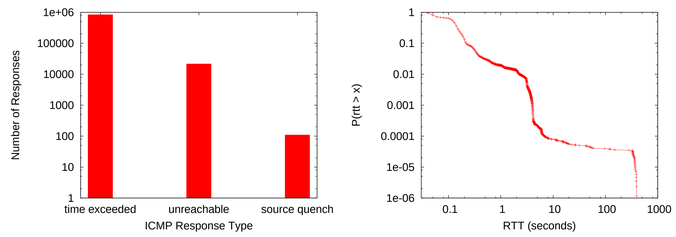
ICMP Quotations

- RFC 792: ICMP error messages quote packet causing error.
- Allows ICMP errors to be directed to correct higher layer instance.
- IP header and at least next eight bytes to be quoted.
- Interested in when the quote does not match what was sent.
- Should be able to see expected changes (TTL, DSCP, ECN).
- May be able to see NAT, packet scrubbing.



Data Set

- `tcptraceroute` to 84393 web servers used in Medina2004.
- Probe each hop once with TCP SYN to port 80.
- Probe had TCP ECE and CWR set, IP DSCP/ECN set to 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.



Matching Responses to Probes

- Want to match responses to probes.
- Want to also allow possible modification.
- Use heuristic designed based on observed data.
  1. Keep list of 25 most recent probes and most recent probe with each IP-ID.
  2. If quoted IP-ID matches IP-ID or byte-swapped IP-ID in 25 most recent, then match.
  3. Otherwise IP-ID substantially altered or response delayed.
  4. Select probe from 25 most recent and matching/byte-swapped IP-ID meeting most of:
     - matching destination IP,
     - matching source port,
     - matching sequence number,
     - no previous matching response,
     - in last 1200 sent.
  5. If at least one of IP-ID, destination IP, source port or sequence number agree, then match.
- Unusual matches manually inspected and appeared genuine.
- Some probes had a long RTTs: 56 over 10s, 34 over 100s, 30 over 300s.

Classification of Changes

Modification Classification

- Some modifications change single field showing no relation to other changes. Classify as zeroed, byte-swapped, incremented or changed.
- Some modifications change set of fields coherently. E.g. insert TCP MSS option = increase IP length, increase TCP HL, add option, recalculate checksums. Classify as single change.
- Some modifications overwrite series of consecutive fields. Classify as clobbering of fields.

Spacial Classification

- A modification seen at one hop but not the next, is classed as *quoter* modification.
- A modification observed at adjacent hops with valid IP or TCP checksum, is classed as *in-flight* modification.
- A modification observed at a hop with no responses from adjacent hops is classed as *edge* modification.

Observability of Changes

- Most quoters (87.60%) quote 28 bytes, the minimum in RFC 792.
- Some quoters (8.60%) quote 40 bytes, the size of the probe.
- Some quoters (2.14%) quote 140 bytes, using ICMP MPLS extensions.
- Therefore, at least 10.7% of quoters quote complete IP and TCP headers.
- Some quoters do strange things (e.g. CERT VU#471084 quoting 60 bytes).

Observed Modifications

Modifications to IP/TCP by quoter

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

```
2b4f4b2055534552010000007920736574 2c206d +OK USER....y set, m
5041535320726963010000000d0a6e6e65637469 PASS ric....  nnecti
000000000000a3fd00c467d345484c4f2074786d ..........g.EHLO txm
474554202f6988392bcf86c2696c644f7665726c GET /i.9+...ildOverl
00000000000005368696c6c792d5368616c6c797c ......Shilly-Shally|
45534d54502053756e2c2030                  ESMTP Sun, 0
6564205065726d616e656e74                  ed Permanent
0a4167653a20313333360d0a                   Age:  1336
0a5365742d436f6f6b69653a                   Set-Cookie:
6374696f6e223e3c623e4d61                  ction"><b>Ma
```

Modifications of Note

IP Header

- 1533 quoters made in-flight modification to DSCP/ECN.
- Some clear DSCP value, some clear both DSCP and ECN.
- Some evidence of consistent DSCP value being 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.