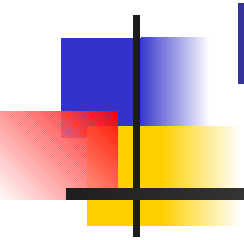


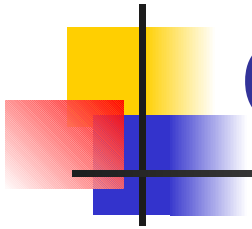
ICMP attacks against TCP

Fernando Gont (UTN/FRH)

(presented by Pekka Savola)

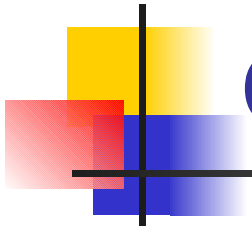
IETF 62, Minneapolis, MN, USA

March 10, 2005



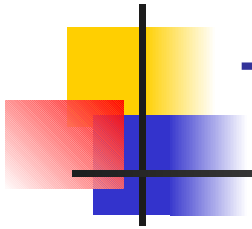
Overview

- ICMP can be used to perform blind connection-reset and blind throughput-reduction attacks against TCP
- The current IETF specs do not recommend any checks on the received ICMP messages
- This makes ICMP attacks the most trivial attacks that can be performed against TCP



General counter-measures

- TCP sequence number checking
- Port randomization
- Packet-filtering based on the payload of the ICMP message
- TCP acknowledgement number checking
- IPsec authentication

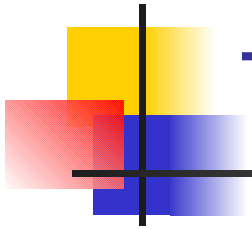


TCP SEQ checking deployment

The TCP SEQ cheking has been implemented by, at least:

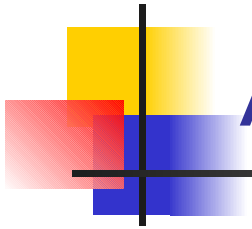
- Linux
- FreeBSD
- OpenBSD

The author is aware most vendors are implementing the TCP SEQ checking as their basic counter-measure against ICMP attacks



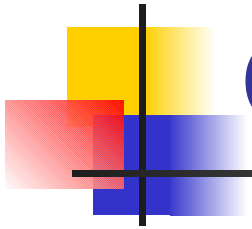
Things that can still go wrong

- The general counter-measures provide an acceptable level of protection for many scenarios
- However, an attacker could still guess all the values that are required to perform the attacks (including the TCP SEQ)



Attack-specific counter-measures

- Treat ICMP “hard errors” as “soft errors” (for connections in any of the synchronized states)
- Ignore ICMP Source Quench messages
- Divide PMTUD into two stages (“Initial PMTUD”, and “PMTU Update”). In the “Update PMTU” stage, delay the reaction on ICMP PTB until the corresponding segment timeouts



Current deployment

Change in the reaction to “hard errors”:

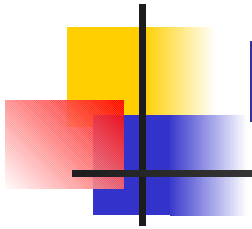
- Linux (for years)
- {Free, Net, Open}BSD (for years)

Ignoring ICMP Source Quench:

- Linux

PMTUD fix:

- Not implemented, yet

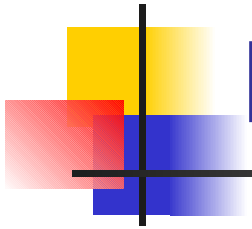


Issues raised

- Should we do something about these attacks?

  (There seems to be consensus on the mailing-list to do something about it)

- Move the discussion to TSVWG?
  - DCCP is affected by these attacks
  - UDP is affected by these attacks
  - SCTP checks the verification tag



Next steps

- Take as WG document?
- Move the discussion to TSVWG?
  - Interesting to discuss how these attacks affect other transport protocols
  - However, this may delay a TCP-specific fix