ICMP attacks against TCP

draft-ietf-tcpm-icmp-attacks-01.txt

Fernando Gont (UTN/FRH)

67th IETF Meeting, San Diego, California, USA
November 5-10, 2006

Overview

- Document discusses a number of attacks that can be performed against TCP by means of ICMP. Namely:
  - Spoof ICMP “hard errors” to reset TCP connections
  - Spoof ICMP Source Quench to slow-down TCP connections
  - Spoof ICMP “frag needed and DF set” to illegitimately reduce the assumed Path-MTU for a given connection.
- Well-known issues, but no documented counter-measures
- Deployment level:
  - Nowadays virtually all implementations implement most of the counter-measures described in the draft.
  - A number of the counter-measures had been widely deployed formore than ten years, in most popular implementations.
- Document was adopted as WG item at the 64th IETF Meeting (Vancouver, BC, Canada), for the **Informational** path

Counter-measures (I)

- Check the TCP SEQ embedded in the ICMP payload
  - This does not really address the reset attack (we'd be back in "in-window" attacks)
  - However, it still requires more packets on the side of the attacker, and improves TCP's robustness to spurious ICMP error messages
  - Does not violate existing requirements
- ICMP hard errors -> soft errors (if the connection is in a synchronized state)
  - This does not violate existing requirements (reaction to hard errors is stated as a SHOULD for all messages but one, which is stated ambiguosly as a SHOULD/MUST)

Counter-measures (II)

- Ignore ICMP Source Quench messages meant for TCP connections
  - This does violate a MUST in RFC 1122
  - However, it is generally accepted that this requirement should be updated
- Honor ICMP “frag needed” only if there’s no progress on the connection
  - Does not seem to violate any existing requirement
  - In the case of IPsec-protected connections, it may be the only thing you can do
  - If you think about it, it is in line with PLPMTUD: there must be a segment loss for the PMTUD to be reduced

Document path

- At IETF 64 (Vancouver, BC, Canada) the WG decided to adopt the document as a WG item, for the Informational path
- Since then, the question has been raised about whether that is the right path for the document. Among other things,
  - we are addressing the TCP-based attacks as standards track, but the (simpler) ICMP-based ones as Informational
  - the fixes have been widely implemented
  - two of the fixes (reset attack, PMTUD attack) do not violate existing requirements
  - the other one (ICMP Source Quench) does violate existing requirements. However, it is widely accepted

Moving forward

- Before continuing tweaking the document, we should decide which path we want to aim at, and how.
- A propsal on a way forward resulted from a long chat with the TCPM WG co-chairs

Proposal (I)

- Split the current document in:
  - A std track document in tsvwg, discussing validation of ICMP error messages (TCP SEQ, reaction depending on connection-state, etc.) for all transport protocols. Make the corresponding changes to the specs
  - A BCP/std track PMTUD–specific document. Discuss it either at PMTUD WG, or TCPM WG, or TSV WG. Get feedback from the PMTUD WG folks.
- Encourage port randomization at TSV WG (document has already been submitted!)

Proposal (II)

- Submit a general document at TSV WG
- Have a std track document at TCPM WG, which references the general doc in TSV WG
- Other transport protocols are free to follow the advice (or not) given in the general doc

Proposal (III)

- Stay at the Informational path
- Make the document more neutral, to “just document what many implementations are doing”
- This might save time
- ICMP-based connection-reset issues, etc., will remain open.
- We probably don’t want this

Moving Forward….

Any comments/questions?

Hums?