Survey of Security Hardening Methods for Transmission Control Protocol (TCP) Implementations
(draft-ietf-tcpm-tcp-security)

Fernando Gont
on behalf of
UK CPNI

IETF 83
Paris, France. March 25-30, 2012

Overview

- More than 100 vulnerabilities discovered in TCP implementations over the years:
  - Some based on implementation bugs
  - Others based on the protocol issues
- Sometimes, implementations “fixed” things the wrong way
- draft-ietf-tcpm-tcp-security aims at:
  - helping TCP implementers avoid issues that have hit other implementations in the past
  - documenting what some implementations have done to mitigate those issues

Overview (II)

- Progress was stalled last year (my fault!)
- Some folks have showed concerns about a single document updating many specs (fair enough)
- Others have expressed concerns about the document repeating stuff from other documents (fair enough)
- Document size didn't make reviewing it very attractive, either

Moving forward

- We have changed the track of draft-ietf-tcpm-tcp-security from Std Track to Informational
- The document has been largely edited
  - Lots of text replaced with pointers to relevant documents
  - Other pieces extracted into stand-alone documents
  - Still lots of edits to do on draft-ietf-tcpm-tcp-security
- But hopefully it is clear we're heading in a different direction

Moving forward (II)

- draft-ietf-tcpm-tcp-security still being edited
  - Goal is to have it “done” before the next IETF
- Two stand-alone documents already published:
  - draft-gont-tcpm-tcp-mirrored-endpoints
  - draft-gont-tcpm-tcp-seccomp-prec
- By extracting Std Track parts into stand-alone documents:
  - Its easier to review and decide what to do with them
  - We continue improving draft-ietf-tcpm-tcp-security

Moving forward (III)

- We need volunteers to review these two small documents
  - Are they worth pursuing?
  - Are them a bad idea we should drop?
  - Either way we can move on to the next topic
- In parallel, I'll get draft-ietf-tcpm-tcp-security in good shape for review before the next IETF

Comments?

Fernando Gont

fgont@si6networks.com