# Security Assessment of the Transmission Control Protocol (TCP)

(draft-gont-tcp-security-00.txt)

Presented by

Joel Jaeggli

IETF 74, San Francisco, USA

# Problem statement

- There is no single document that discusses the security implications of TCP and the possible mitigation approaches
- As a result,
  - It becomes really difficult to produce a resilent TCP implementation from the RFCs
  - It becomes really tedious to find documentation about TCP vulnerabilities faced in the past and the best possible mitigations for them
  - New implementations of TCP re-implement bugs/vulnerabilities that had already been found in older stacks

# Document overview

- In 2005, the UK CPNI started a project to change this state of affairs
- The goal of the project was to perform a security assessment of the relevant specifications, and also research what real implementations were doing.
- Some areas that were explored as part of this project:
  - Enforcing checks on each of the header fields
  - Security implications of each of the header fields
  - Security implications of each of the TCP mechanisms (e.g., segment reassembly, congestion control, etc.)
- The result of this project was a 140-page document (with 100+ references to relevant specifications and papers) entitled “Security Assessment of the Transmision Control Protocol (TCP)”, that was released in February 2009.

# Overview of draft-gont-tcp-security

- It's the IETF I-D version of the aforementioned document, and is meant to bringthe results of the UK CPNI project to the IETF
- Similar to the "Security Assessment of the Internet Protocol version 4" (draft-ietf-opsec-internet-security) that is already an opsec wg item…. but about TCP ☺
- While it's the first version (-00) of the I-D, it was thoroughly reviewed by a number of people (see the "Acknowledgements" section of the document).
- The resulting I-D/RFC need not be a verbatim copy of the document released by the UK CPNI, but would reflect wg consensus.

# Moving forward

- Feedback wanted!
- Opsec wg would be a possible venue for discussing this document within the IETF
- Thoughts?