On the generation of TCP timestamps
(draft-gont-tcpm-tcp-timestamps)

Fernando Gont
on behalf of
UK CPNI

73rd IETF meeting, November 16-21, 2008
Minneapolis, MN, USA
Overview

- RFC1323 describes the generation of TCP timestamps
- It states that they must be monotonically-increasing for a given connection.
- However, it does not require timestamps to be monotonically-increasing across TCP connections (protection against stale segments from previous connections is provided by the TIME-WAIT state and the quiet-time concept).
- However, timestamps that are monotonically-increasing across TCP connections can be useful:
  - They allow the implementation of heuristics for handling incoming connection request when there’s a previous incarnation of the same connection in the TIME-WAIT state.
  - This is similar to what BSD-derived implementations have done with TCP ISNs, but probably works better than the TCP SEQ hack.
So... what is this document about?

- It describes an algorithm for selecting TCP timestamps such that:
  - The TCP timestamps are monotonically-increasing across TCP connections
  - The chances of an off-path attacker for guessing the TCP timestamps used for future connections are reduced
- It describes the heuristics that can be implemented based on the TCP timestamps when processing incoming connection requests.
- This already ships with Linux
Moving forward

Should we adopt this document as a wg item?