# Defending Against Sequence Number Attacks

## (draft-gont-tcpm-rfc1948bis-00.txt)

**Fernando Gont (UTN/FRH)**

**Steven Bellovin (Columbia U.)**

80th IETF meeting, Prague, Czech Republic
March 27-April 1, 2011

# Introduction

- The current standard algorithm for genearting Initial Sequence Numbers (ISNs) produces sequences that are trivially predicable by off-path attackers
- The security implications of predictable TCP sequence numbers have been known for a long time (e.g., Morris paper in 1985)
- RFC 1948 [Bellovin, 1996] proposed an algorithm for selecting ISNs such that they are not easily predictable by off-path attackers

# RFC 1948

- Proposed to generate ISNs with:

  ISN = M + F(localhost, localport, remotehost, remoteport)
- Where M is a timer, and F is suggested to be a cryptographic hash function such as MD5
- This expression leads to monotonically-increasing ISNs that are unpredictable by off-path attackers
- RFC 1948 was published as an **Informational** RFC
- It has been widely implemented and deployed

# draft-gont-tcpm-rfc1948bis

- New document aims at Standards Track (rather than Informational):

  *TCP SHOULD generate its Initial Sequence Numbers with the expression:*
  *ISN = M + F(localip, localport, remoteip, remoteport)*
- The discussion of address-based trust relationship attacks IN rfc 1948 was updated to reflect current attack scenarios, and moved to an Appendix.
- Documentation of an old BSD bug was also moved to an Appendix
- In version -00 of the document, the recommended hash algorithm had been changed to SHA-256 [FIPS-SHS]
  - This had been motivated by non-technical reasons
  - Based on later discussions on the mailing-list, we will switch back to MD5 in the next revision

# Moving Forward

- This is TCP maintenance work, that is within the charter of the TCPM WG
- So far, the document has received some support on the mailing-list (e.g., William Simpson and Richard Scheffenegger)
- Should TCPM adopt this as a WG item?