Overview

- This document describes how to defend transport protocols against blind attacks through ephemeral port obfuscation.
- It provides an overview of the characteristics of a good ephemeral port selection algorithm.
- It describes a number of approaches for obfuscating ephemeral port numbers.
- It includes a survey of what popular implementations are doing with respect to ephemeral port selection.
This document was born in 2004 to address the problem of blind attacks against transport protocols.

It was adopted in 2007 as a wg item of the TSVWG.

It has been pretty stable during the last few revisions

We have received very thorough feedback from Mark Allman on the last revision (-02)

There has been some discussion on-list that will lead to a number of changes
Changes to be incorporated in the next revision

- The document title will be changed
  - “Port randomization” -> “Defending against blind attacks through ephemeral port obfuscation”

- The comparison of the different algorithms will be backed-up by the results of ongoing work by Mark Allman.

- Some text will be included pointing out that collisions might be avoided by maintaining the TIME-WAIT state also on the client-side.

- RFC 1337 and [Faber et al, 1999], (“The TIME-WAIT state and its effect…”) will be referenced for a discussion of the TIME-WAIT issues.

- A small comment will be included about the TCP SEQ numbers and the TCP timestamps heuristics performed by a number of implementations when processing incoming connection requests.

- A number of clarifications will be incorporated.

- Overall, all this feedback will require small changes to the document.
Moving the document forward

- Our plan is to publish a revision (-03) of this document in the next few weeks that incorporates the aforementioned changes.
- We think that a WGLC should be started when that version is published.
Any comments or questions?