CPNI
Centre for the Protection of National Infrastructure

Security Assessment of the Internet Protocol version 4
(draft-gont-opsec-ip-security)

Fernando Gont

on behalf of

UK CPNI

73rd IETF meeting, November 16-21, 2008

Minneapolis, MN, USA

Problem statement

- There is no single document that discusses the security implications of the IPv4 protocol and the possile mitigation approaches
- As a result,
  - It becomes really hard to produce a resilent IPv4 implementation from the RFCs
  - New implementations of IPv4 re-implement bugs/vulnerabilities that had already been found in older stacks
  - Sometimes new protocols re-implement mechanism that had already been found to have negative security implications

Document overview (I)

- In 2005, 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, discuss counter-measures where necessary, and also research what real implementations were doing.
- Some of the 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 IPv4 mechanisms (e.g., fragment reassembly)
- The result was a 60-page document, with 95+ references to relevant specifications, papers, etc.

Document overview (II)

- draft-gont-opsec-ipsecurity is CPNI's effort to take the results of tat project to the IETF.
- Document revision history:
  - -00: initial version, posted on August 2008.
  - -01: Simply fixes boiler-plate issues.
- While the current version is -01, it has already been thoroughly reviewed by a number of people, and has resulted in a 70-page document.

Moving forward

Should this document be adopted as a wg item?