Security Assessment of the IPv6 Flow Label

(draft-gont-6man-flowlabel-security-00)

Fernando Gont
on behalf of
UK CPNI

IETF 79
November 7-12, 2010. Beijing,China.

Summary

- **Document is part of a larger document on IPv6 security being produced by UK CPNI (yet unpublished)**
- **Analyzes the security implications of the Flow Label field**
- **Proposes an algorithm for selecting flow labels**

Security Implications of the Flow Label field

- **Possible (theoretical) DoS vector resulting from Flow Label verification described in RFC 2460**
- **Covert Channels**
- **QoS theft**
- **Information leaking**

Selecting Flow Labels

- **Requirements:**
  - **Flow Labels that are predictable by off-path attackers**
  - **Flow Label collisions are reduced**
- **Proposed algorithm (a la RFC 1948, and compliant with RC 3697):**

Flow Label = counter + hash(Source Address, Destination Address, Secret Key)

Moving forward

- **Comments?**
- **Adopt as wg item?**