Security Implications of Predictable Fragment Identification Values
(draft-gont-6man-predictable-fragment-id)

Fernando Gont

on behalf of

UK CPNI

IETF 83

Paris, France. March 25-30, 2012

Generation of Fragment IDs

- At any given time, the tuple (Src. Addr., Dst. Addr., Frag ID) must be unique
- Page 19 of RFC 2460 notes that:

  “*it is assumed that the requirement can be met by maintaining the Identification value as a simple, 32-bit, "wrap-around" counter, incremented each time a packet must be fragmented. It is an implementation choice whether to maintain a single counter for the node or multiple counters, e.g., one for each of the node's possible source addresses, or one for each active (source address, destination address) combination*”

What did real implementations do?

Operating System	Algorithm
Windows Vista/Seven	Global Counter (init. to 0)
Linux	Global counter (init. to 0)
Solaris	Per-dest. counter (init. to 0)
OpenBSD	Randomized Frag ID
Juniper	Randomized Frag ID

Sec. Implications of Predictable Frag. IDs

- We already know most of them from the IPv4 world
- They allow an attacker to:
  - determine the packet rate at which a given system is transmitting information,
  - perform stealth port scans to a third-party,
  - uncover the rules of a number of firewalls,
  - count the number of systems behind a middle-box, or,
  - perform a Denial of Service (DoS) attack

draft-gont-6man-predictable-fragment-id

- Formally requires that the Frag ID is not easily guessable by off-path attackers
- Proposes a number of algorithms to achieve that goal
  - One RECOMMENDED algorithm, and a number of OPTIONAL (alternative) algorithms
  - But we may simply discuss their pros and cons, and let the implementations decide for themselves

Response to this I-D

- A number of OSes have produced patches:
  - Linux
  - OpenSolaris
  - Other OSes are following
- This is good news!

Moving forward

- Adopt this document as a 6man wg item?

Feedback?

Fernando Gont

fgont@si6networks.com