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

Fernando Gont
SI6 Networks

IETF 84
Vancouver, Canada. July 29-August 3, 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*"

Sec. Implications of Predictable Frag. IDs

- Most of them known from the IPv4 world
- They allow an attacker to:
  - perform a Denial of Service (DoS) attacks
  - obtain information about the number of packets transmitted by a target node
    - determine the packet rate
    - 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
    - etc.

What did real implementations do?

Operating System	Fragment Identification
FreeBSD 9.0	Randomized
NetBSD 5.1	Randomized
OpenBSD-current	Randomized (based on SKIPJACK)
Linux 3.0.0-15	Predictable (GC init. to 0, incr. by +1)
Linux-current	Unpredictable (PDC init. to random value)
Solaris 10	Predictable (PDC, init. to 0)
Windows 7 Home Prem.	Predictable (GC, init. to 0, incr. by +2)

GC: Global Counter PDC: Per-Destination Counter

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

- Formally requires that the Frag ID is not easily guessable by off-path attackers
- Specifies a number of algorithms that could be employed to achieve that goal
  - Pros and cons are discussed
  - But it is up to the implementation which specific algorithm is employed

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

- Why bother?
  - Because we do not want to repeat IPv4's history with the Frag ID
- Should I care?
  - Yes
  - If not convinced, try these tools (frag6, icmp6): http://www.si6networks.com/tools

Moving forward

- Adopt this document as a 6man wg item?

Feedback?

Fernando Gont

fgont@si6networks.com