IPv6 Security

Fernando Gont

SI6 NETWORKS

11st SLO IPv6 Summit
Ljubljana, Slovenia. June 21, 2016

About...

- Security Researcher and Consultant at SI6 Networks
- Published:
  - 20 IETF RFCs (9 on IPv6)
  - 10+ active IETF Internet-Drafts
- Author of the SI6 Networks' IPv6 toolkit
  - http://www.si6networks.com/tools/ipv6toolkit
- I have worked on security assessment of communication protocols for:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- More information at: http://www.gont.com.ar

IPv6 addressing

Security Implications

Sec/Priv Implications of IPv6 Addressing

- **Correlation of network activity over time**
  - 'cause the IID does not change over time
- **Correlation of network activity across networks**
  - 'cause the IID does not change across networks
  - e.g. 2001:db8::**1234:5678:90ab:cdef** vs. fc00:1::**1234:5678:90ab:cdef**
- **Network reconnaissance**
  - 'cause the IIDs are predictable
  - e.g. 2001:db8**::1**, 2001:db8**::2**, etc.
- **Device specific attacks**
  - 'cause the IID leaks out the NIC vendor
  - e.g. 2001:db8::**fad1:11**ff:fec0:fb33 -> Atheros

Auto-configuration address/ID types

	Stable	Temporary
Predictable	IEEE ID-derived	None
Unpredictable	**RFC7217 (new!)**	RFC 4941

- We **used to lack** stable privacy-enhanced IPv6 addresses:
  - Used to replace IEEE ID-derived addresses
  - Pretty much orthogonal to temporary addresses
  - Probably "good enough" in most cases even without RFC 4941

IPv6 addressing

RFC 7217

RFC7217: stable-privacy addresses

- Generate Interface IDs as:

  F(Prefix, Net_Iface, Network_ID, DAD_Count, Secret_Key)

- Where:
  - F(): PRF (e.g., a hash function)
  - Prefix: SLAAC or link-local prefix
  - Net_Iface: some interface identifier
  - Network_ID: e.g. the SSID of a wireless network
  - DAD_Count: initialized to 0, and incremented by 1 upon collisions
  - Secret_Key: unknown to the attacker (and randomly generated by default)

RFC7217: stable-privacy addresses (II)

- As a host moves:
  - Prefix and Network_ID change from one network to another
  - But they remain constant within each network
  - F() varies across networks, but remains constant within each network
- This results in addresses that:
  - Are stable within the same subnet
  - Have different Interface-IDs when moving across networks
  - For the most part, they have “the best of both worlds”

RFC7217: implementation status

- There are at least three different implementations
- Linux kernel v4.0

  http://www.spinics.net/lists/netdev/msg322123.html
- NetworkManager v1.2.0-0.3.20151112gitec4d653.fc24

  https://blogs.gnome.org/lkundrak/2015/12/03/networkmanager-and-privacy-in-the-ipv6-internet/
- dhcpcd 6.4.0

  http://mail-index.netbsd.org/tech-net/2014/06/04/msg004572.html

RFC7217: Demo

- RFC7217 in Fedora

Recent IETF work in this area

- RFC7721
  - Discusses the security implications of IPv6 addressing
- RFC7707
  - The bible of IPv6 network reconnaissance
- RFC7217:
  - Specifies how to generate semantically-opaque addresses

IPv6 addressing

Ongoing work

Address usage advice

- IPv6 can be powerful in terms of the multiple addresses of different types and scopes that are typically configured
- But we are missing guidance on how to employ and use them
- **draft-gont-6man-address-usage-recommendations** provides advice on address usage
- It analyzes address parameters/aspects that affect security/privacy:
  - Scope
  - Stability
  - Usage type

Requirements for non-stable addresses

- RFC4941 requires that temporary addresses be used along stable addresses
- **draft-gont-6man-non-stable-iids**:
  - Updates RFC4941 t allow for temporary addresses only
  - Sets requirements for non-stable addresses:
    - IIDs must be different for each prefix
    - must not be predictable
    - IIDs must be semantically opaque
    - must not embed layer-2 addresses
  - Describes one possible algorithm:
    - Randomize the IID upon network attachment

Address usage advice

- IPv6 can be powerful in terms of the multiple addresses of different types and scopes that are typically configured
- But we are missing guidance on how to employ and use them
- **draft-gont-6man-address-usage-recommendations** provides advice on address usage
- It analyzes address parameters/aspects that affect security/privacy:
  - Scope
  - Stability
  - Usage type

Address usage advice: scope

- A non-global scope may provide “prophylactic” security
- ULA's are one specific case
- For an analysis of ULAs see: draft-ietf-v6ops-ula-usage-considerations

Address usage advice: stability

- The longer an address is employed, the more exposed it becomes:
  - Constant IIDs allow for host-tracking across networks
  - Stable (per network) IIDs allow for activity correlation
  - Temporary addresses allow for activity-correlation limited in time
  - “throw-away” connections would be best as mitigation -- but expensive!
- What to use (and where) is subject of further work
  - For the general case, RFC7217 + RFC4941 is probably best
  - For roaming nodes, “temporary only” might be best

Address usage advice: usage type

- An IPv6 Address may typically be used for:
  - server-like incoming connections
  - client-like outgoing connections
- When offering services:
  - Nodes typically bind() the “wildcard” address
  - They accept incoming connections on any address
  - Thus a node that operates as a client may be scanned for opened ports
- Real world scenario:
  - Debian-derived distributions getting IPv6 port-scanned as a result of employing an NTP server harvesting client addresses
  - See: http://netpatterns.blogspot.be/2016/01/the-rising-sophistication-of-network.html

Address usage advice: usage type (II)

- When employing stable plus temporary addresses, nodes might want to bind() services only to stable addresses
- This is currently difficult:
  - Lack of appropriate APIs
  - Nodes can bind single address, or all addresses, but not a subset
  - Cannot easily bind addresses based on address properties (e.g. stability)

draft-ietf-6man-default-iids

- Specs wise, nothings says you should replace the existing scheme with RFC7217
- It is taking us ages to do it
- Or worse, people keep coming up with really bad ideas
  - (see the next slides)

IPv6 addressing

Related work

MAC address randomization

- Some platforms have started randomizing MAC addresses
  - To prevent tracking at layer-2
  - A good read: http://www.mathyvanhoef.com/2016/03/how-mac-address-randomization-works-on.html
- MAC address randomization and IPv6
  - Some folks argue that if we do MAC address randomization, we can stick to traditional SLAAC
  - **Embedding MAC addresses in the IID (no matter what) is a bad idea**
  - Please see: **draft-gont-predictable-numeric-ids**
- Embedding MAC addresses in the IID
  - Wastes 16 bits of entropy (remember the “0xfffe” thing)
  - Relies on an algorithm we don't control (MAC address randomization)

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com