Recent IPv6 Security Standardization Efforts

Fernando Gont

SI6 NETWORKS

UK IPv6 Council Security Workshop

London, UK. July 12, 2017

Part I: Protocol Issues

IPv6 Addressing

Security & Privacy Analysis

- **RFC 7721:** “Security and Privacy Considerations for IPv6 Address Generation Mechanisms”
- **RFC 7707:** “Network Reconnaissance in IPv6 Networks”

Mitigation of Security & Privacy Issues

- **RFC 7217:** "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)"
- **RFC 8064:** "Recommendation on Stable IPv6 Interface Identifiers"

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

- Known implementations:
  - Linux kernel v4.0
  - NetworkManager v1.2.0-0.3.20151112gitec4d653.fc24
  - dhcpcd 6.4.0
- OSes known to already ship with RFC7217:
  - Mac OS Sierra
  - Fedora

RFC7217 in Fedora (I)

- Node connects to Network #1

```
[root@localhost fgont]# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fc00:1::e17:cbfb:392d:a9dc  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::267c:28dc:2598:78ff  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c2:e3:95  txqueuelen 1000  (Ethernet)
        RX packets 50893  bytes 45348708 (43.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20968  bytes 1283359 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost fgont]#
```

RFC7217 in Fedora (II)

- Node connects to Network #2

```
[root@localhost fgont]# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fc00:2::48a0:c116:8a8:ec56  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::267c:28dc:2598:78ff  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c2:e3:95  txqueuelen 1000  (Ethernet)
        RX packets 50894  bytes 45348818 (43.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20994  bytes 1287393 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost fgont]#
```

RFC7217 in Fedora (III)

- Node connects (back again) to Network #1

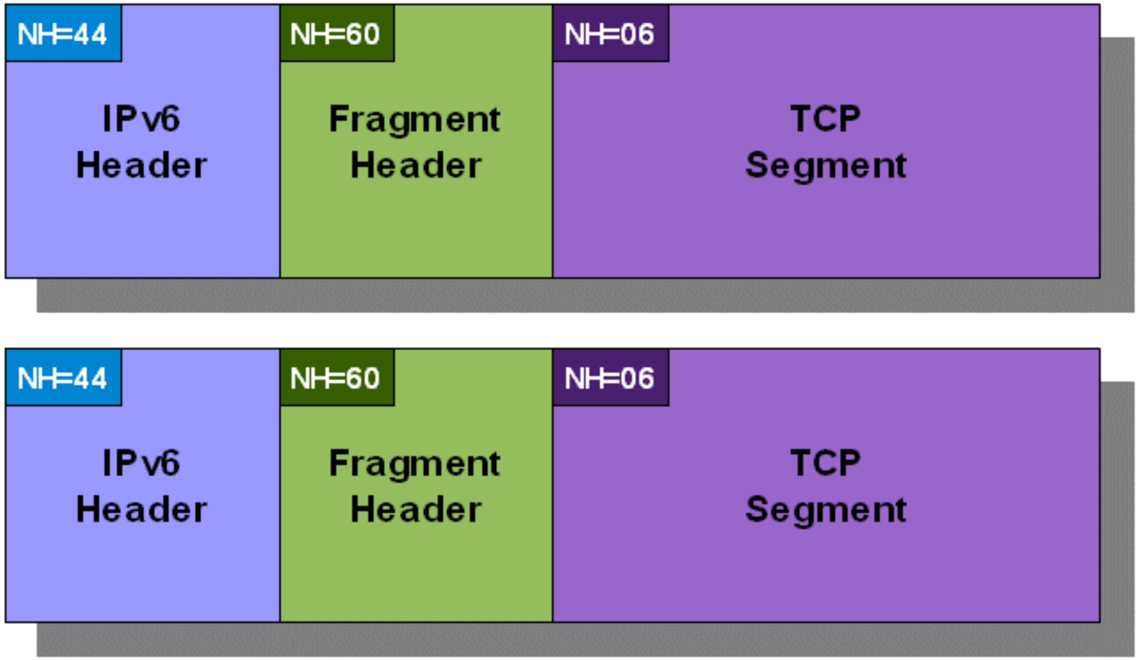
```
[root@localhost fgont]# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fc00:1::e17:cbfb:392d:a9dc  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::267c:28dc:2598:78ff  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c2:e3:95  txqueuelen 1000  (Ethernet)
        RX packets 50893  bytes 45348708 (43.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20968  bytes 1283359 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost fgont]# 
```

IPv6 Extension Headers

IPv6 Fragmentation

- Conceptually, same as in IPv4
- Implemented with an IPv6 Fragmentation Header



IPv6 Fragmentation Overview

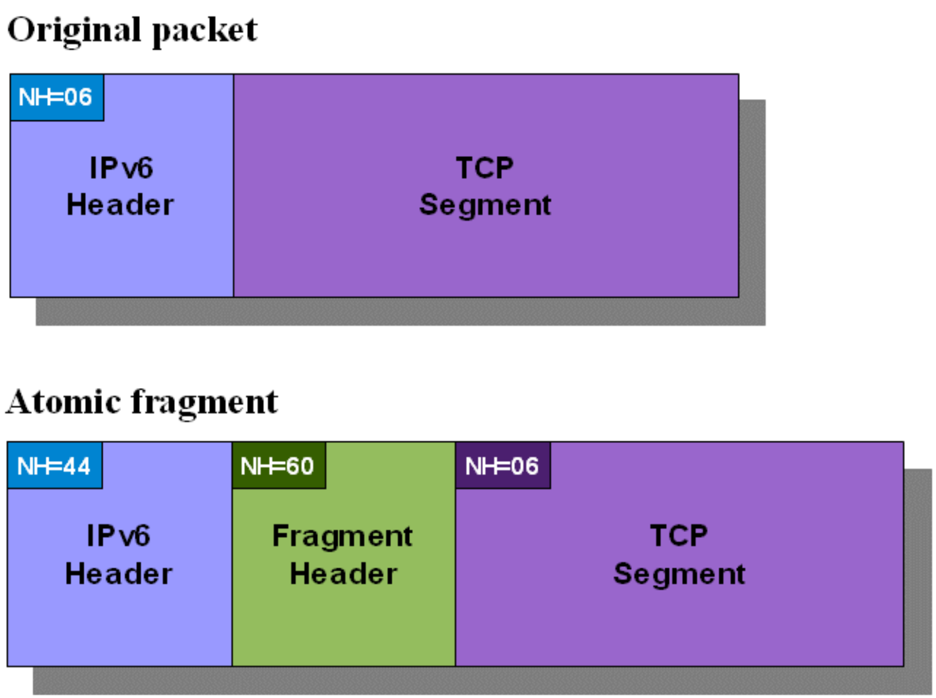
- IPv6 fragmentation performed only by hosts (never by routers)
- Fragmentation support implemented in “Fragmentation Header”

8 bits	8 bits	13 bits	2b	1b
Next Header	Reserved	Fragment Offset	Res	M
Identification				

- Where:
  - Fragment Offset: Position of this fragment with respect to the start of the fragmentable part
  - M: “More Fragments”, as in IPv4
  - “Identification”: Identifies the packet (with Src IP and Dst IP)

Atomic fragments

- Atomic fragments: a complete packet that includes a fragment header (FO: 0, MF: 0)
- (Used to be) generated upon receipt of MTU<1280



Mitigating miscellaneous issues

- **RFC 6980**: *Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*
- **RFC 7739**: *Security Implications of Predictable Fragment Identification Values*
- **RFC 7112**: *Implications of Oversized IPv6 Header Chains*
- **draft-ietf-6man-rfc2460bis**: *Internet Protocol, Version 6 (IPv6) Specification*

Mitigating issues with atomic fragments

- **RFC 8021**: *Generation of IPv6 Atomic Fragments Considered Harmful*
- **RFC 6946**: *Processing of IPv6 "Atomic" Fragments*
- **RFC 7915**: *IP/ICMP Translation Algorithm*
- **draft-ietf-6man-rfc2460bis**: *Internet Protocol, Version 6 (IPv6) Specification*

IPv6 Standardizaton Efforts
Part II: Operational Issues

Operational Security Considerations

- **draft-ietf-opsec-v6**: *Operational Security Considerations for IPv6 Networks*

First-Hop Security

- **RFC 7113**: *Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)*
- **RFC 7610**: *DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers*
- ***RFC 6959**: Source Address Validation Improvement (SAVI) Threat Scope*

IPv6/IPv4 Interaction

- **RFC 7123**: *Security Implications of IPv6 on IPv4 Networks*
- **RFC 7359**: *Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks*

Some conclusions

Some conclusions

- Increased interest and operational experience with IPv6 led to many improvements
- **A lot** has been done in the last 5 years or so!

Questions?

Thank you's

- Veronika McKillop
- Tim Chown
- Andy Butcher
- UK IPv6 Council
- Axians

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

https://www.si6networks.com/community/

www.si6networks.com