Recent Advances in IPv6 Security

Fernando Gont

FLIP6 - LACNIC 2015
Lima, Peru. May 18-22, 2015

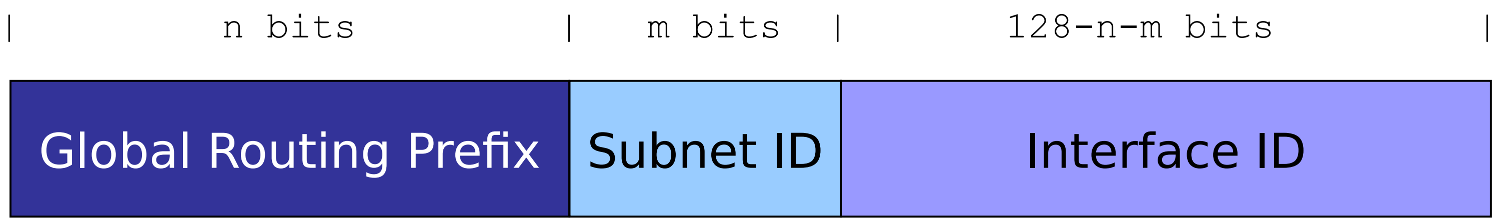
About...

- 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

Brief overview

IPv6 Global Unicast Addresses



- A number of possibilities for generating the Interface ID:
  - Embed the MAC address (traditional SLAAC)
  - Embed the IPv4 address (e.g. 2001:db8::192.168.1.1)
  - Low-byte (e.g. 2001:db8::1, 2001:db8::2, etc.)
  - Wordy (e.g. 2001:db8::dead:beef)
  - According to a transition/co-existence technology (6to4, etc.)

IPv6 Addressing

Overview of Security/Privacy Implications

Security 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

IPv6 Addressing
Mitigation of Security/Privacy Issues

Temporary Addresses (RFC4941)

- RFC 4941: privacy/temporary addresses
  - Random IIDs that change over time
  - Generated **in addition** to traditional SLAAC addresses
  - Traditional addresses used for server-like communications, temporary addresses for client-like communications
- Operational problems:
  - Difficult to manage!
- Security problems:
  - They do not fully replace the traditional SLAAC addresses (hende host-tracking is **only partially mitigated**)
  - They **do not** mitigate host-scanning attacks

SLAAC stable-privacy (RFC7217)

- Generate Interface IDs as:

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

- Where:
  - F() is a PRF (e.g., a hash function)
  - Prefix is the SLAAC or link-local prefix
  - Net_Iface is some interface identifier
  - Network_ID could be e.g. the SSID of a wireless network
  - Counter is used to resolve collissions
  - Secret_Key is unknown to the attacker (and randomly generated by default)

SLAAC stable-privacy (RFC7217) (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”
- A Linux implementation has been committed to Linux 4.0

DHCPv6's draft-ietf-dhc-stable-privacy

- Generate Interface IDs as:

  F(Prefix | Client_DUID | IAID | Counter | secret_key)

- Where:
  - F() is a PRF (e.g., a hash function)
  - Prefix: Represents the managed IPv6 address pool
  - Client_DUID is the Client's DHCPv6 DUID
  - IAID is a unique identifier for this address association
  - Counter is employed to resolve collisions
  - Secret_Key is unknown to the attacker (and randomly generated by default)

DHCPv6's draft-ietf-dhc-stable-privacy (II)

- Allows for multiple DHCPv6 servers to operate within the same subnet
- State about address leases is shared “algorithmically”
  - No need for a new protocol
- Even if the DHCPv6 lease file gets lost/corrupted, addresses will be stable
- dhc wg considering to drop this work (!?).

Other IETF work in this area

- draft-ietf-6man-ipv6-address-generation-privacy
  - Discusses the security implications of IPv6 addressing
- draft-ietf-6man-default-iids
  - Notes that implementations should default to RFC7217

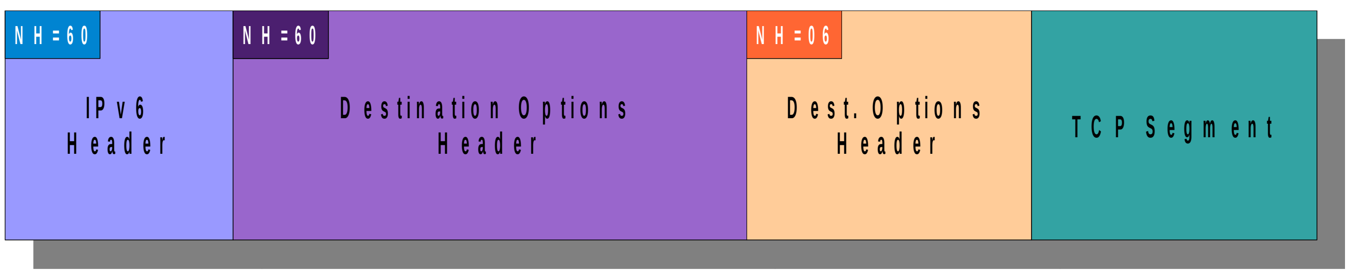
IPv6 Extension Headers

IPv6 Extension Headers

Overview

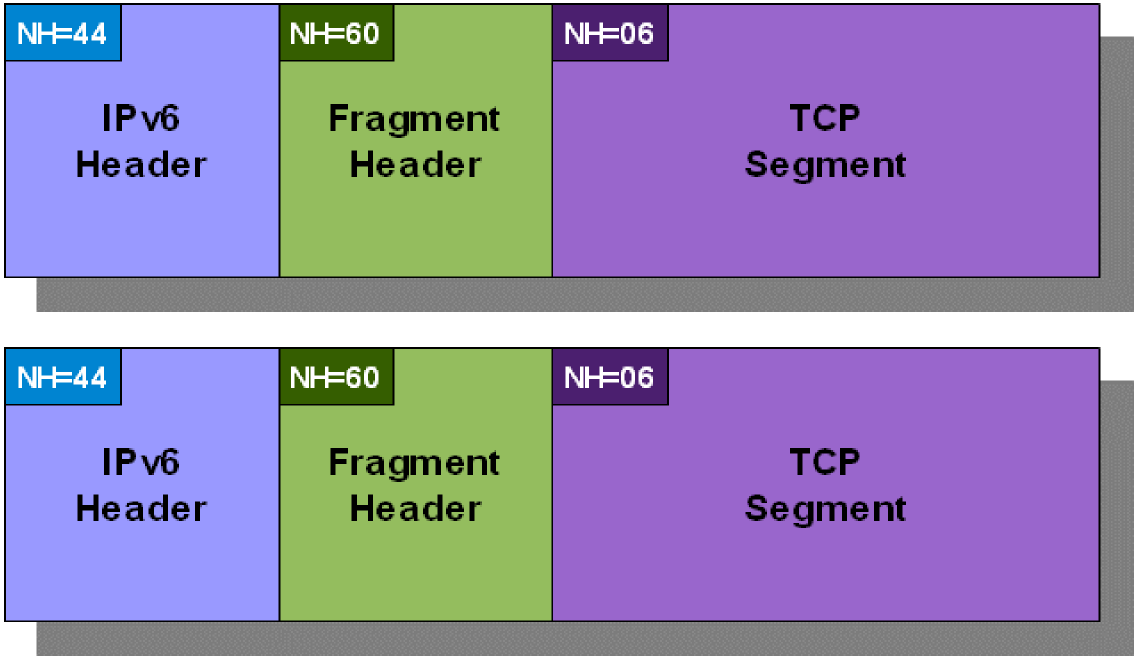
IPv6 Extension Headers

- Fixed-length base header
- Options conveyed in different types of Extension Headers
- Extension Headers organized as a daisy-chain structure



IPv6 Fragmentation

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

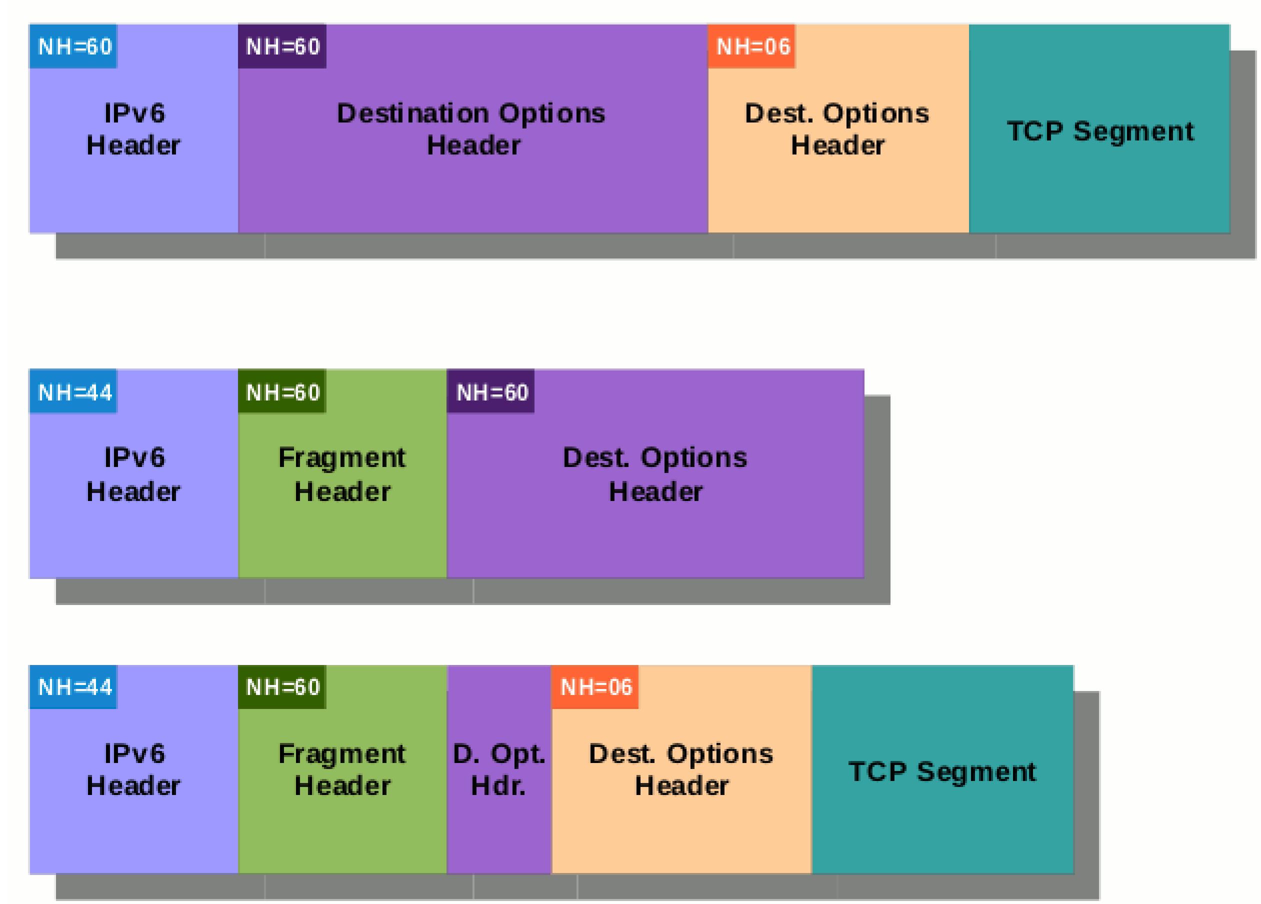


IPv6 Extension Headers

Reality

Finding Upper-layer information

- Finding upper-layer information is painful (if at all possible)



Processing the IPv6 header chain

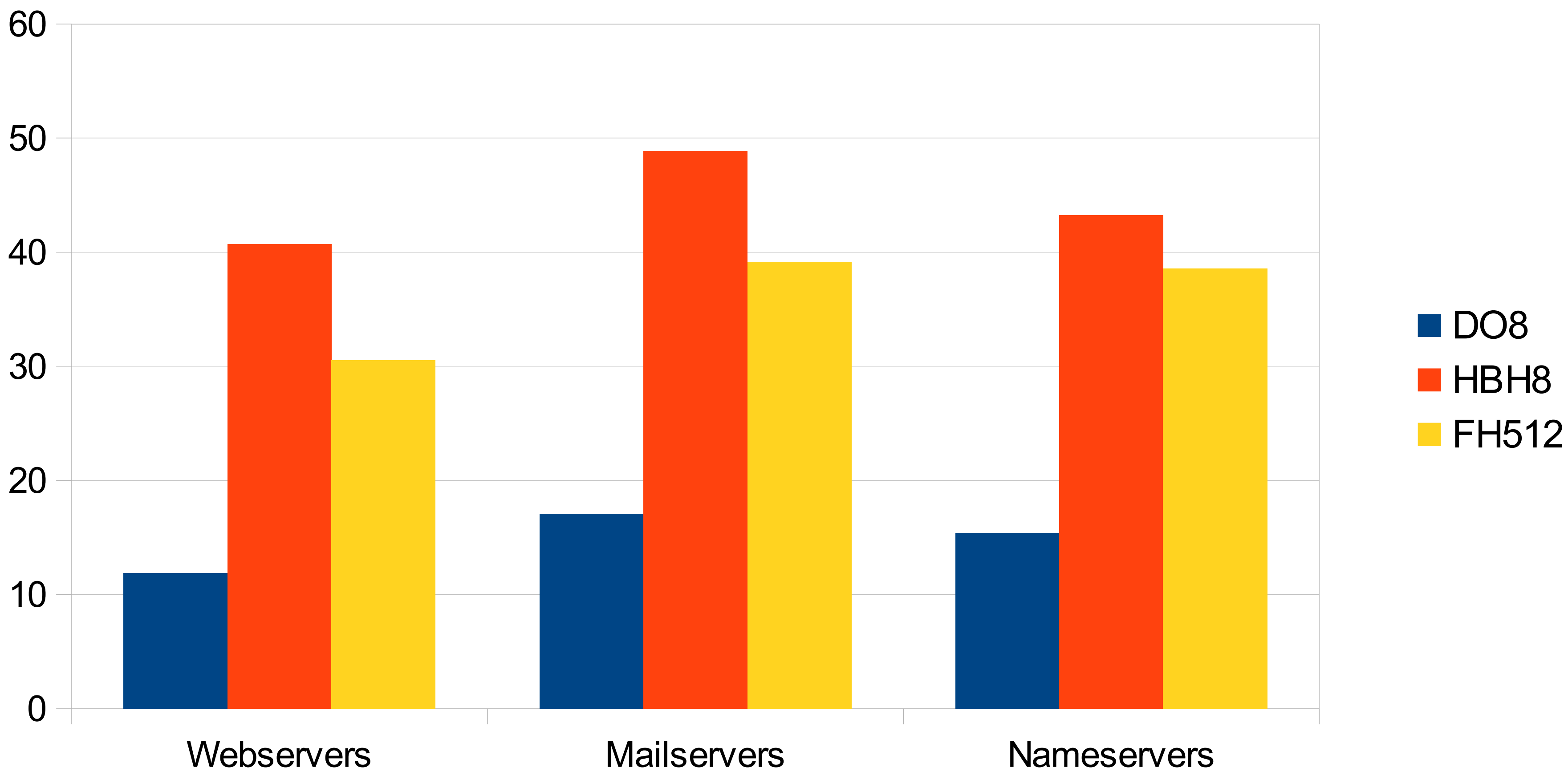
- Processing the IPv6 header chain is expensive
  - May be CPU-intensive
  - Some implementations can inspect only up to 128 bytes (or even some smaller number)
- IPv6 fragmentation deemed as insecure
  - DoS vector
  - Evasion
  - Buggy implementations

IPv6 EHs in the Real World

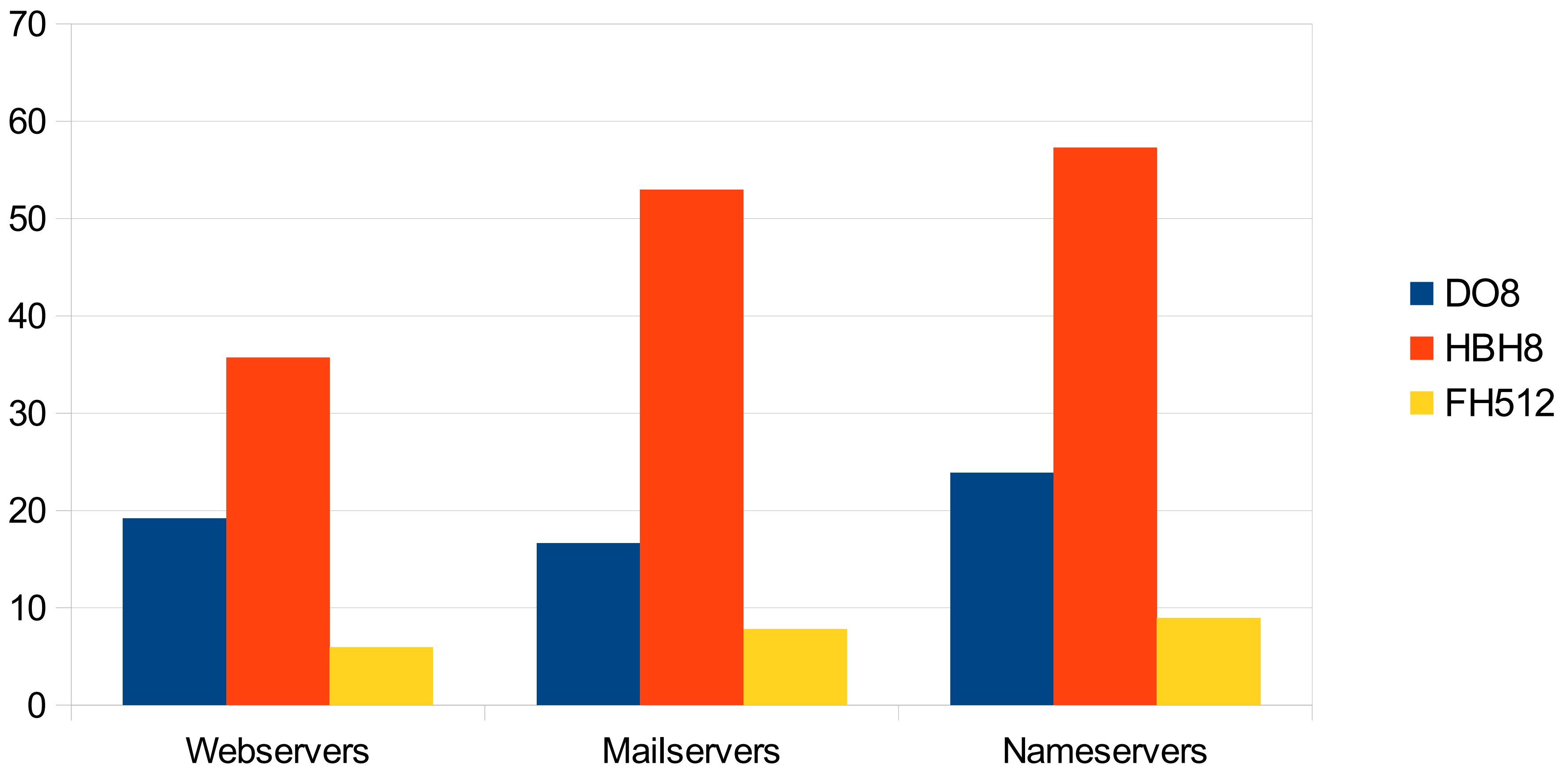
- Many operators allegedly filter them, as a result of:
  - Perceived issues with IPv6 Fragmentation and EH
  - Almost no current dependence on them
- But there was no real data..
- So we measured the IPv6 Internet ourselves:

  draft-ietf-v6ops-ipv6-ehs-in-real-world

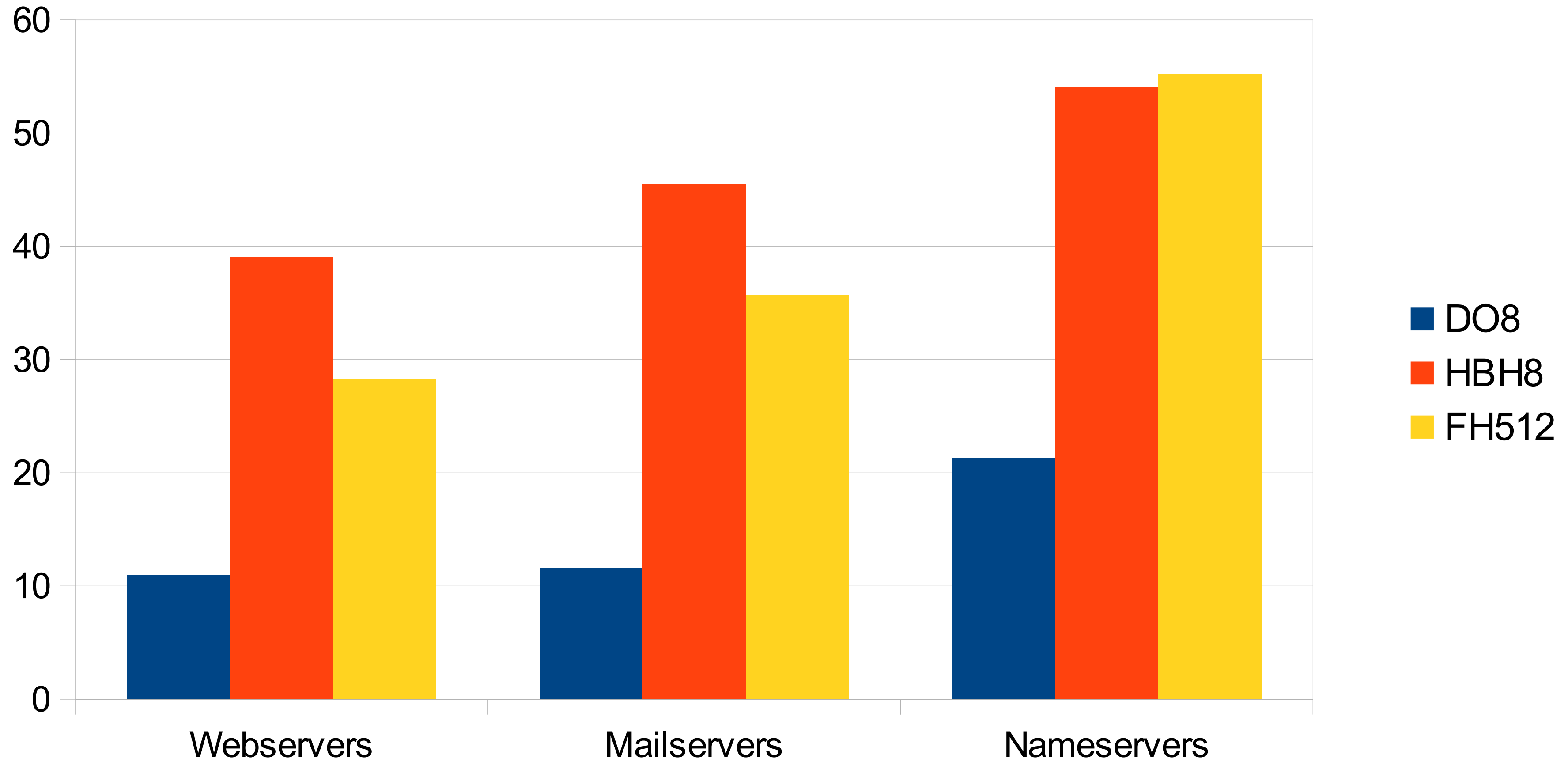
WIPv6LD dataset: Packet Drop rate



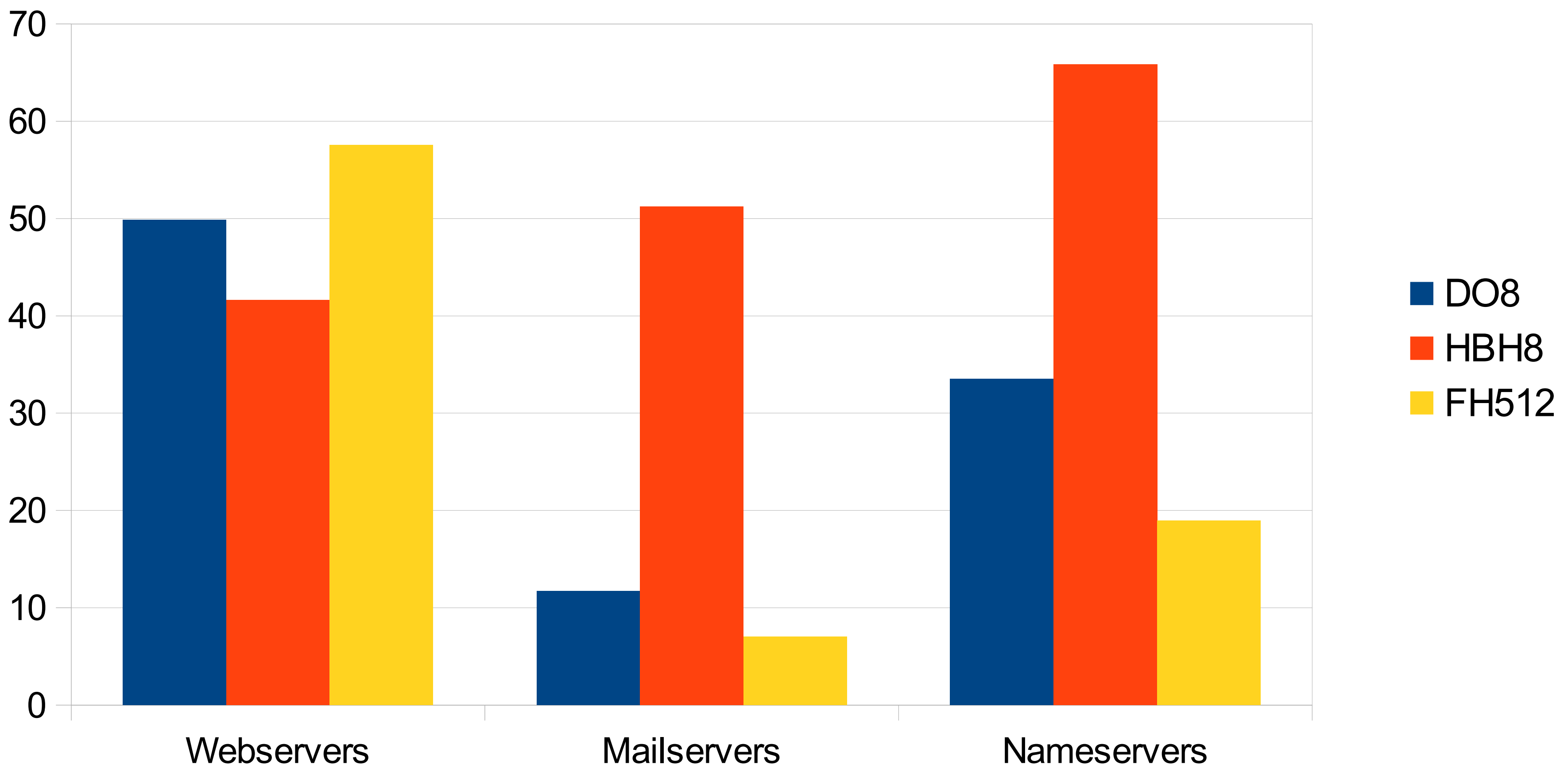
WIPv6LD dataset: Drops by diff. AS



Alexa dataset: Packet Drop rate



Alexa dataset: Drops by diff. AS



So... what does this all mean?

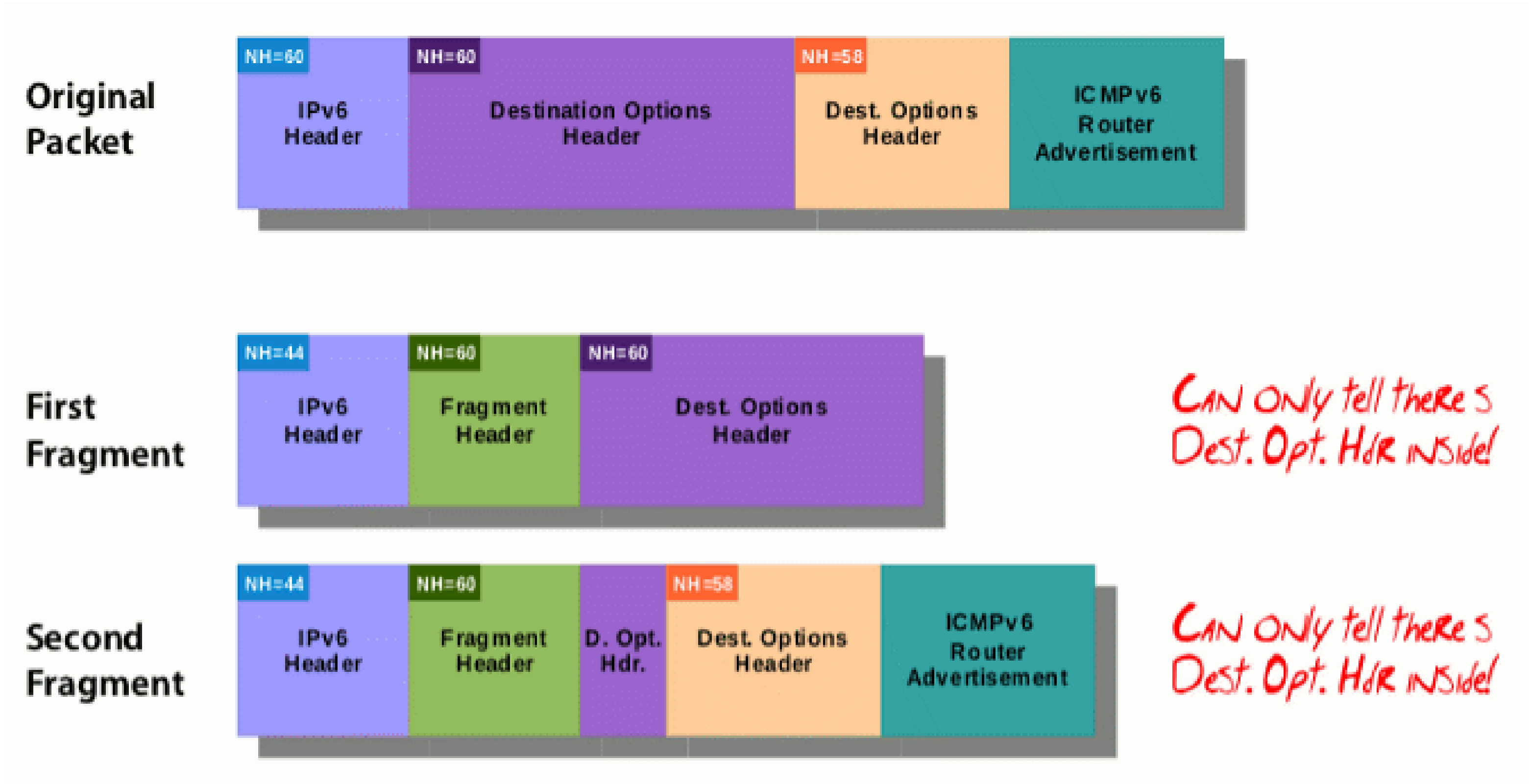
- Good luck with getting IPv6 EHs working in the public Internet!
  - They are widely dropped
- IPv6 EHs “not that cool” for evasion, either
  - Chances are that you will not even hit your target

IPv6 Extension Headers

Attacks

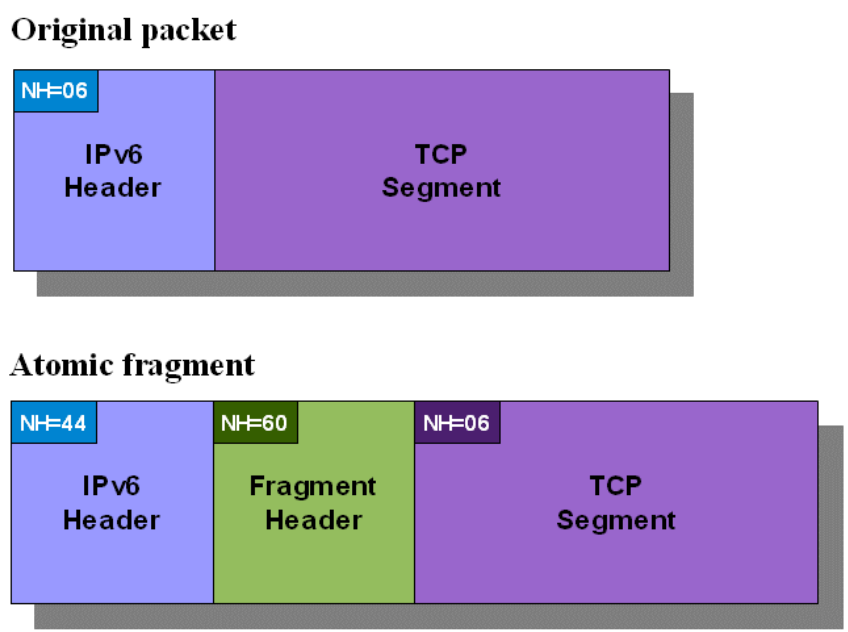
Old/obvious/boring stuff

- e.g. RA-Guard evasion



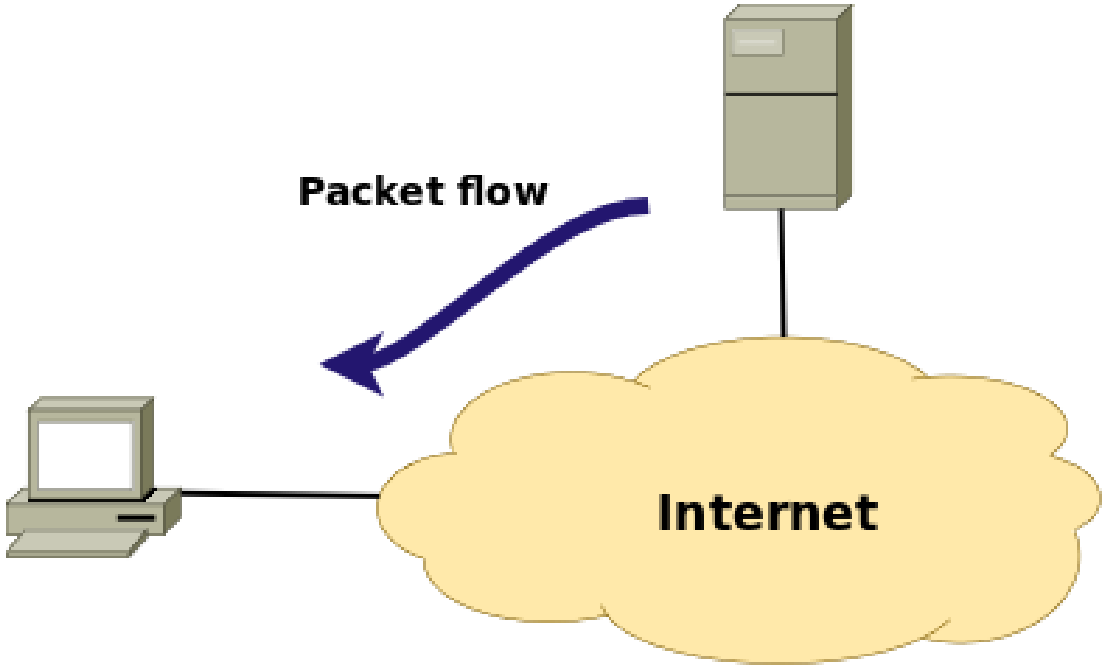
More interesting stuff

- If IPv6 frags are widely dropped...What if we triggered their generation?
  - Send an ICMPv6 PTB with an MTU<1280
  - The node will then generate IPv6 atomic fragments
  - Packets will get dropped



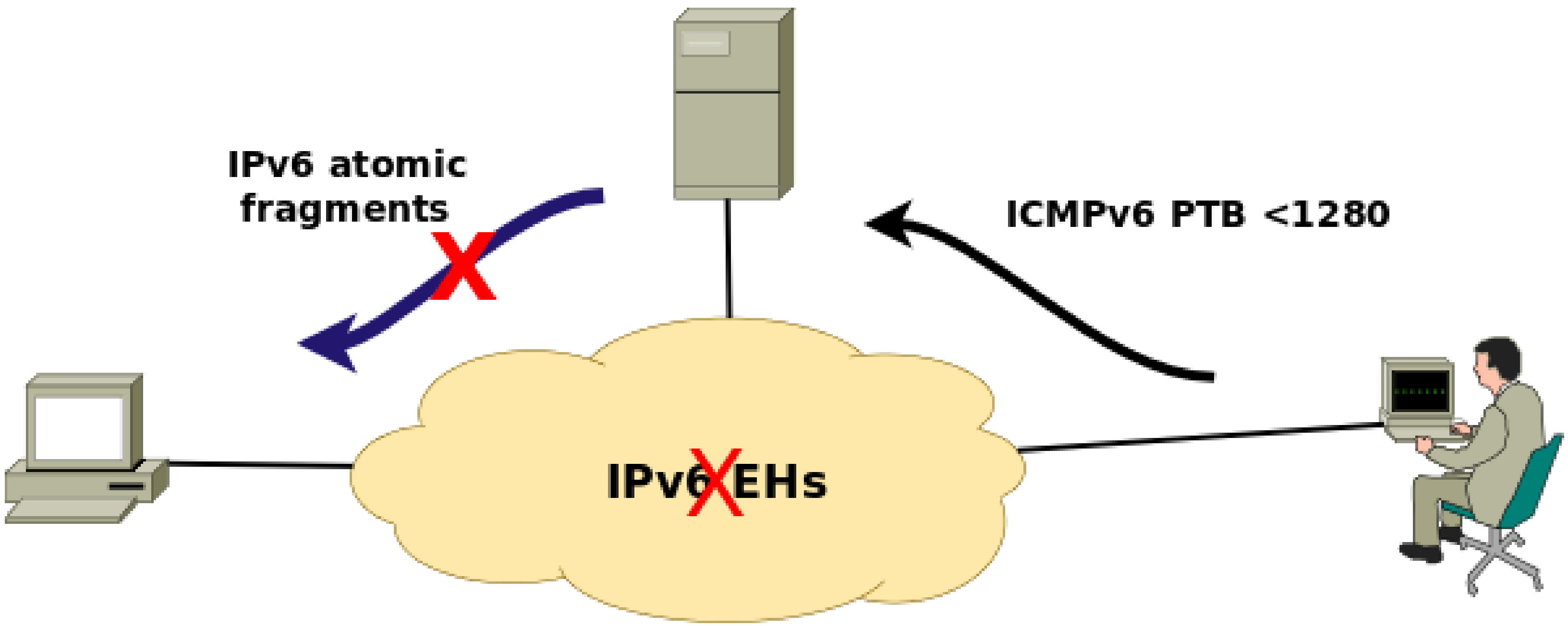
Attack Scenario #1

- Client communicates with a server



Attack Scenario #1 (II)

- Attacking client-server communications



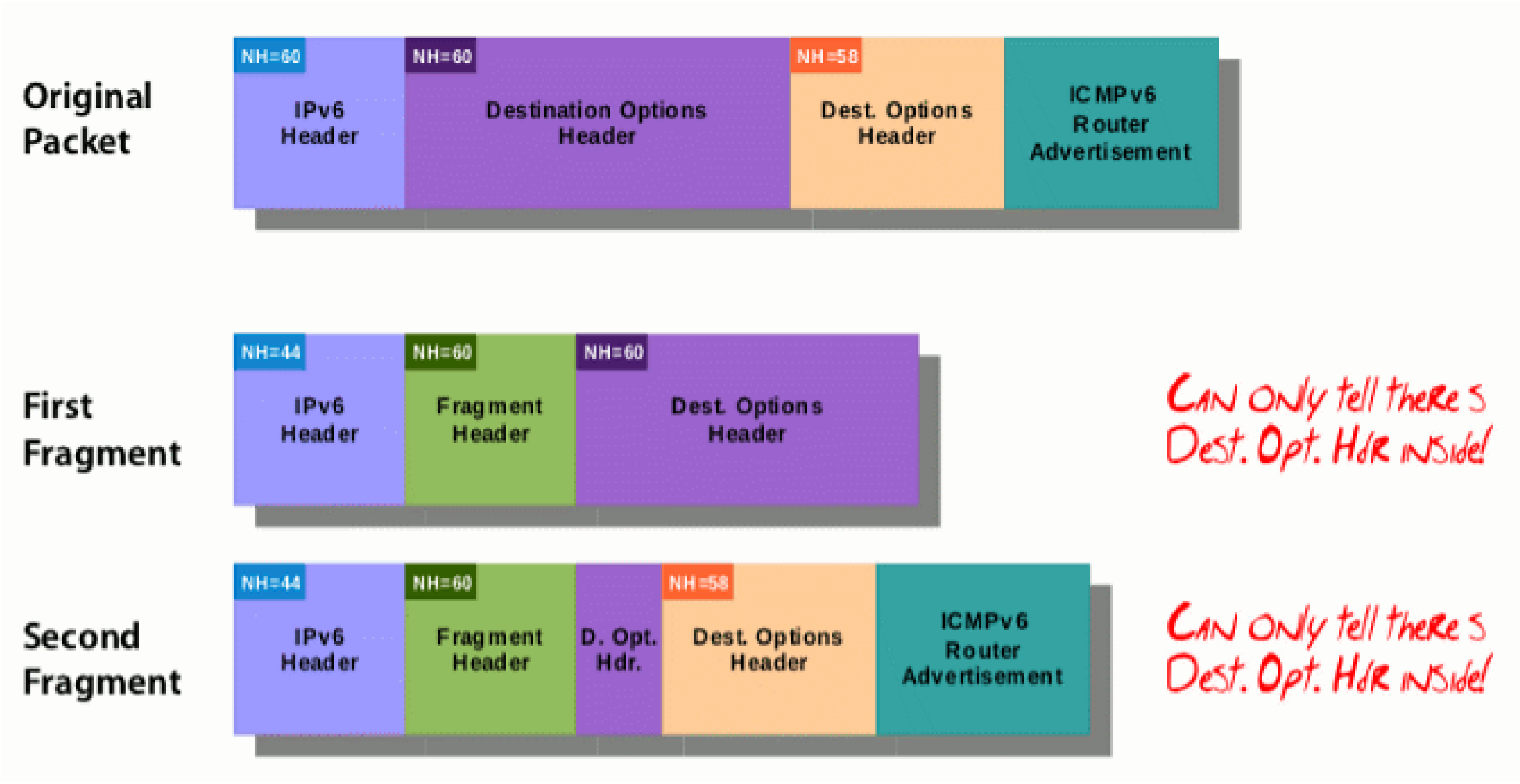
Sample attack scenario: Lovely BGP

- Say:
  - We have two BGP peers
  - They drop IPv6 fragments “for security reasons”
  - But they do process ICMPv6 PTBs
- Attack:
  - Fire an ICMPv6 PTB <1280 (probably one in each direction)
- Outcome:
  - Packets get dropped (despite TCP MD5, IPsec, etc.)
  - Denial of Service

IPv6 Extension Headers
Improvements

Oversized IPv6 Header Chains

- RFC 7112 forbids oversized IPv6 header chains. e.g.:



Fragmentation and Neighbor Discovery

- Fragmentation makes policyng at layer-2 virtually impossible
- RFC 6980 forbids the use of fragmentation with IPv6 ND.

IPv6 atomic fragment generation

- draft-ietf-6man-deprecate-atomfrag-generation
  - “Do not send IPv6 atomic fragments in response to ICMPv6 PTB < 1280”
  - Update SIIT (IPv6/IPv4 translation) such that it does not rely on them

Filtering of IPv6 Extension Headers

- There was no guidance in this area
- We produced draft-ietf-opsec-ipv6-eh-filtering
  - Advice on filtering IPv6 packets that contain IPv6 Extension Headers

Some conclusions

- The IPv6 Internet is the IPv4 Internet of the '90's
- Still lots of stuff to be done in the IPv6 security arena
  - Improve the specs
  - Patch your IPv6 stack
  - Write code that demonstrates new ideas
- **Master IPv6 before it is too late**

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

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

www.si6networks.com