IPv6 Security @ ETH Netsec

ETH zürich ungleich

Nico Schottelius

<2020-10-01 Thu 16:15>

About Nico Schottelius

- Former Netsec student
- Regular speaker at network conferences
- CEO of ungleich glarus ag and ungleich GmbH
- IPv6-first data centre "Data Center Light" in Glarus

IPv6 overview

- 128 Bit address space
  - 340.282.366.920.938.463.463.374.607.431.768.211.456 IP addresses
  - 340 undecillion, 282 decillion, 366 nonillion, 920 octillion, 938 septillion, 463 sextillion, 463 quintillion, 374 quadrillion, 607 trillion, 431 billion, 768 million, 211 thousand and 456
- Typical network sizes:
  - /32 per ISP
  - /48 per location (65.536 networks per ISP)
  - /64 per logical network (65.536 networks per location)
    - Max 2^{64} hosts (18.446.744.073.709.551.616) per network
- Typical IPv6 address: 2001:db8:cafe:7ea::42

IPv6 addresses

- Link Local: fe80::/10 (typically: fe80::/64)
  - Every IPv6 host has this
- GUA (global unique address)
  - Globally reachable
  - The "normal" IPv6 address
- ULA (unique local address)
  - For local deployments
  - Can be NAT'ed to GUA

How to get IPv6 addresses

- Router advertisements (RFC4861)
  - Stateless protocol
  - Multicasts network prefixes
    - Remember: there is no broadcast in IPv6
  - Nodes assign themselves
- DHCPv6 (RFC8415)
  - Additional to RAs
  - Flag set in RA
  - Additional options like boot filename
  - Stateful addresses supported
- Default: router advertisements
- Fun article about RA & DHCPv6
  - `https://teamarin.net/2018/06/25/common-mistake-dhcpv6/`

DAD DoS

- Nodes assign themself an IPv6 address
- Nodes use DAD (duplicate address detection, RFC3484, RFC4429)
- Simplified:
  - "Has somebody this IPv6 address?"
  - (no answer)
  - Great, I take it
- Easy Denial of Service (DoS) attack
  - Answer "Yes I have" to every DAD request

IPv6 Shadow networks

What if you had IPv6, but you did not know about it?

- If a network is not configured for IPv6
- However some nodes are IPv6 enabled
- The network administrator is not aware of this
- IPv6 traffic passes in and out without being subject to firewall rules

IPv6 connectivity anywhere

- Can we bring IPv6 connectivity into any network?
  - Generally speaking: yes
- Tunnel services and protocols (Teredo, HE.net, IPv6VPN.ch)
  - Transport IPv6 via IPv4
- Teredo (automatic IPv6 assignment + tunneling)
  - Was enabled by default in Windows
  - Is blocked in ETH Zurich networks
  - See RFC 4380 - quite impressive protocol!

Rogue Router 1: Injecting IPv6 addresses

- Assume there is no local IPv6 router
- What if we setup any computer as an IPv6 router?
  - All IPv6 capable hosts automatically assign themself an IPv6 address
  - We have become a man in the middle (MITM)
- Combination with IPv6 tunnels
  - Completely bypasses IPv4 firewalls
  - Globally reachable addresses for everyone

Rogue Router 2: overriding advertisements

- What if there is already a local IPv6 router?
- Router advertisements have a priority field
- Setup a higher priority router
  - Again all IPv6 capable hosts automatically assign themself an IPv6 address
  - Again we have become a man in the middle (MITM)

Preventing Rogue Route Advertisements

- What can we do against rogue route advertisements?
  - Filter appropriate RA messages in the network
  - Filter DHCPv6 messages in the network
- Needs to be done at all places
  - Switches usually distribute RAs
  - Network segment might be hijacked
- Very similar problem to rogue IPv4 DHCP servers

Preventing IPv6 connectivity

- How can we prevent a host to access the IPv6 Internet?
- As long as there is outgoing traffic with a related incoming traffic allowed: We cannot prevent it
- Any bi-directional communication can be used as a tunnel
- Popular examples:
  - Wireguard VPN: use any remote UDP port (f.i. 53)
  - Corkscrew: tunneling traffic through HTTP proxies
  - iodine: DNS/ICMP tunneling (only needs DNS/ICMP traffic)
  - Teredo
- Alternative
  - Whitelisting of trusted protocols, ports - often irrealistic

IPv6 addresses information leakage

- Self assigned IPv6 addresses can embedd their MAC address
- Variety of algorithms out there nowadays:
  - Embed 48 Bit of mac address + add ff:fe in the middle (EUI-64, RFC4291)
  - Randomly generate IPv6 address, rotate periodically (RFC4941)
  - Generate random, persistent IPv6 address (RFC7217)

IPv6 addresses information leakage (2)

- EUI-64 example
  - MAC address 00:1b:21:bb:68:f0
  - Prefix 2a0a:e5c0:2::/64
  - IPv6 address 2a0a:e5c0:2:0:21b:21ff:febb:68f0/64
- Mac address contain vendor information - allows physical attack:
  - Scan a network for the mac of a specific vendor
  - Count the value of hardware connected
  - Physically approach location, steal targeted hardware

IPv6 address attack: FIB exhaustion

- Need to map IPv6 addresses to mac addresses
  - Linux: ip -6 neigh show
- Default network size: 64 bit
- Mapping for a /64 network: 2^{64} * (128+48) bit = 360.448 PB = 352 Exabyte
- Denial of Service attacks
  - Buffer overrun
  - Overwrite real entries with fake IPv6 addresses
- Counter measures:
  - Port rate limiting
  - Limit of IPv6 addresses per MAC address

IPv6 Address Exhaustion

- IPv6 hosts usually have multiple IPv6 addresses (f.i. link local, GUA)
- How many addresses per host at maximum?
  - Usually software defined
- Attack using rogue router that sends 16 prefixes
  - Uses all available slots
  - Depends on timing, clients might be unable to assign legitimate IPv6 addresses

```
root@line:~# cat /proc/sys/net/ipv6/conf/all/max_addresses
16
```

IPv6 Network scanning

- Brute force scanning a /64 at 1024 addresses/second
  - 2^{54} seconds or more than 23 milion years
- You can try well known IP addresses
  - . . . :1-1000 (first thousand)
  - L33t speak words (cafe, f00d, 7ea, fac3:b00c, . . .)
- IPv4 networks usually 256 to 65536 hosts
  - Easy to scan

IPv6 Networking scanning from inside

- Various interesting multicast groups
- For instance:
  - ff02::1 - all link local nodes
    - Devices reply with their link local address
    - Use the network prefix to find out GUA (global unique address)
  - ff02::2 - all link local routers
  - See RFC3513
- ping6 to either of them to reach all nodes
- Sub second results

Filtering per IP address

- In the IPv4 world stateful / dynamic firewalls filter per IP
- Attacker easily controls /64 up to /48
  - Need 2 Exabyte of storage to store /64 network block list
- Solution: Dynamic approach
  - Filter IP address
  - Then filter /64
  - Then filter /48
  - Then filter Autonomous System (AS)

No fragmentation attacks

- IPv4 packets can be fragmented
  - Routers need to store/re-assemble packets
- IPv6 does not support fragmentation by the network
  - Work is shifted to clients
  - Routers return ICMP6 message "packet too big"
- No memory exhaustion attacks based on fragments in the IPv6 world

IPSEC

- Part of the IPv6 specification (mandatory!)
  - Not implemented by everyone
- Allows authentication and encryption
- High degree of complexity
  - Does not work through NAT(64)
  - Needs NAT traversal
  - Variety of algorithms and implementations
- In theory: good idea
- In practice: abandoned

NAT is not security (NINS)

- NAT (network address translation)
  - Mapping IP address (1:1, 1:n)
  - Mapping addresses and protocol ports (PNAT)
- NAT is not a firewall
  - If table entries are known, access from outside is possible
- Firewalls
  - Have stateless or stateful rules
  - Can block incoming / outgoing traffic
  - Work quite similar for IPv6 and IPv4

THC: THC-IPV6-ATTACK-TOOLKIT

- thcp-ipv6 is an IPv6 test suite
- It contains many examples and real life usable tools
- Do not use without consent of the network administrator
- `https://github.com/vanhauser-thc/thc-ipv6`

Conclusions

- IPv6 is generally speaking not more or less secure than IPv4
- Many attacks similar to the ones from the IPv4 world
- Networks need to be prepared for handling IPv6
  - Avoidance leads to security holes
- Start with IPv6 now - for fun and profit!

More of this

- The IPv6 Chat on `https://ipv6.chat`
  - Informal exchange of IPv6 operators and users
- Interesting IPv6 security related pages
  - `http://www.swissipv6council.ch/sites/default/files/docs/ipv6_security.pdf`
  - `https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml`
  - `https://pacsec.jp/psj05/psj05-vanhauser-en.pdf`