IPv6 and Security - a love affair?

DENOG 4
Thorsten Dahm
td@google.com

Agenda

Google™

- Sorry, no "what is IPv6" introduction
- Myths and Legends
- Bad news (why the security problems of IPv6 may harm us)
- Often seen problems that make our life harder in Security
- A collection of security problems

- Coffee :-)

Google™

Myths and Legends

Myths and Legends

Google

- Security is built into the protocol
- Increased usage of IPsec
- End-to-end principle will return
  - Firewalls, ACL, Proxy still work with IPv6
- General misunderstanding of security properties in IPv6 is very common
- IPv6 is totally insecure, because NAT66 is missing
- Harming the IPv6 deployment
- A realistic view is essential

- Don't talk about specific vulnerabilities, talk about the protocol itself

Google™

Bad news

The bad news

Google

- Less experience than with IPv4
- Current implementations are ... incomplete
- Key products for security still lack full IPv6 support
- More complexity during the transition phase -> higher security risk
  - 2 internetworking protocols
  - Multiple routing protocols (OSPFv2/v3 & MP-BGP)
  - Tunnels
  - Other technologies, like DS-Lite
- ARP using Ethernet directly, Neighbor Discovery messages can contain extension headers, be fragmented, etc.
- Engineers (Frontline, NOC) not well-trained and prepared

Implications of IPv6 addresses

Google™

- Similar to IPv4, we use in IPv6
  - prefixes (for routing purposes)
  - different address types (unicast, anycast, multicast)
  - different address scopes (link-local, global, etc.)
- Subnet scanning is more difficult (128 bit addresses)
  - not really with EUI-64: Prefix known, OUI known, FF: FE known, 24 bits of MAC address unknown
- Each node uses multiple addresses at any given time
- Global unicast addresses can be generated in different ways
  - EUI-64 format (based on the MAC address)
  - Privacy extensions
  - Manual configuration
  - Specific to a transition/co-existence technology

Google™

Often seen problems

Often seen problems

Google

- Data analysis can be harder
- Filtering of extension headers impossible
- Software & Tools need to be IPv6 aware (2001:ab5::1)
- Automatic tunnel solutions / failover
- Security scan using Neighbor Discovery, mDNS etc. can be intrusive
- Multiple addresses per host
- Privacy extensions

All of the above can make forensics really hard. And operations. And monitoring. And security. And deployment. And [to be continued]

Searching for IPv6 addresses

Google™

- Regular expression for IPv6 addresses (RFC2373):
  (::|(([a-fA-F0-9]{1,4}):){7}([a-fA-F0-9]{1,4}))|(:(:([a-fA-F0-9]{1,4})){1,6})|((([a-fA-F0-9]{1,4}):){1,6}:)|((([a-fA-F0-9]{1,4}):)(:([a-fA-F0-9]{1,4})){1,6})|((([a-fA-F0-9]{1,4}):){2}(:([a-fA-F0-9]{1,4})){1,5})|((([a-fA-F0-9]{1,4}):){3}(:([a-fA-F0-9]{1,4})){1,4})|((([a-fA-F0-9]{1,4}):){4}(:([a-fA-F0-9]{1,4})){1,3})|((([a-fA-F0-9]{1,4}):){5}(:([a-fA-F0-9]{1,4})){1,2}))

- matches (2001:470:b0b4:1:280:c6ff:fef2:9410 | 2001:868:100::3 | 2001:888:144a::a441:888:1002 | ::1 | a:b:: | ::FFFF:1.2.3.4)

Google™

A collection of security problems

Security Problems of IPv6

Google

- Multiple Systems have IPv6 enabled by default
  - Lack of awareness can lead to compromise
  - IPv4-only network can also include partial deployed (and unmaintained) IPv6
- Multiple transition technologies
  - more complexity in the network
  - more potential & hidden vulnerabilities
- "Creative" ways of solving common problems
  - IPv6 Multihoming without NAT (IETF draft)
  - SLAAC & stateless DHCPv6 at the same subnet
  - Dual-stack MPLS (6PE) & IPv6 VPN (6VPE)
  - IPv6 Host to router load sharing (RFC4311)

Security Problems of IPv6

Google

- Attacker can "enable" IPv6 in a local subnet, e.g. by sending ICMPv6 RA
- Set up local tunnel endpoints in a subnet (6to4, Teredo)
- Can be used to evade security controls (e.g. Firewalls) and mask malicious behavior
- Can result in increased and unexpected host exposure

-> Even if you don't use IPv6 yet, you may use it already

If you want a network to be IPv4 only, make sure that this is really the case.

Security Problems of IPv6

Google

- "Ported" ARP spoofing for DoS and MITM (answer every NS, use OVERRIDE flag)
  - SEND (SEcure Neighbor Discovery)
    - Difficult to deploy (requires PKI)
  - Monitor Neighbor Discovery traffic
    - can be trivially evaded
  - Static Neighbor Cache
    - Not really ...
  - Filter packets, restrict to a subnet/local network
    - Not desired and sometimes not possible
- DoS by answering all Duplicate Address Detection packets (mandatory in IPv6)
- Security features similar to DHCP snooping / DAI / arpwatch not available for IPv6 (yet)

Security Problems of IPv6

Google

- Extension Headers can be used for many bad things
  - For example RH0 header
  - Similar to "source-route" feature in IPv4
  - Hosts may support it
  - scapy6: sr1(IPv6(src=me, dst=victim) / IPv6ExtHdrRouting(addresses=[me])/ ICMPv6EchoRequest())

- Possible (MITM) attacks:
  - attract traffic to a specific anycast address (DNS servers, DNS Root servers)
  - 6to4 relay routers (attract traffic to 2002::/16)
  - Teredo relays (attract traffic to 2001:0000::/32)

Security Problems of IPv6

Google™

- Router Advertisements (RA) used in SLAAC allow an attacker to
  - DoS attacks & MITM attacks by forging RA
  - RA-Guard trivial to evade (e.g. fragmented packets & overlapping fragments)
  - Windows 8 still vulnerable to RA Flood DoS
  - For other mitigations like SEND, see previous slide

- IPSec makes IPv6 more secure
  - Support mandatory, not usage!
  - Changed to optional a few weeks ago, not mandatory anymore
  - Has still the same problems as IPSec in IPv4
  - No increased IPSec usage because of IPv6 (yet?)
  - Sniffing traffic of others as easy as with IPv4

Many more issues to consider

Google

- IPv6 fragmentation always done by hosts, never by routers
  - Fragment-ID is predictable (Idle-scan, DoS)
  - Some OS patched now
  - RFC5722 now forbids overlapping fragments
  - draft-ietf-6man-ipv6-atomic-fragments to fix IPv6 atomic fragment handling
- More security features have to be deployed on the host instead the network nodes
- 6man WG @IETF working on multiple drafts to solve problems

Questions?

Thorsten Dahm
td@google.com