# IPv6 Secure Neighbor Discovery

Andreas Hunkeler

January 2015

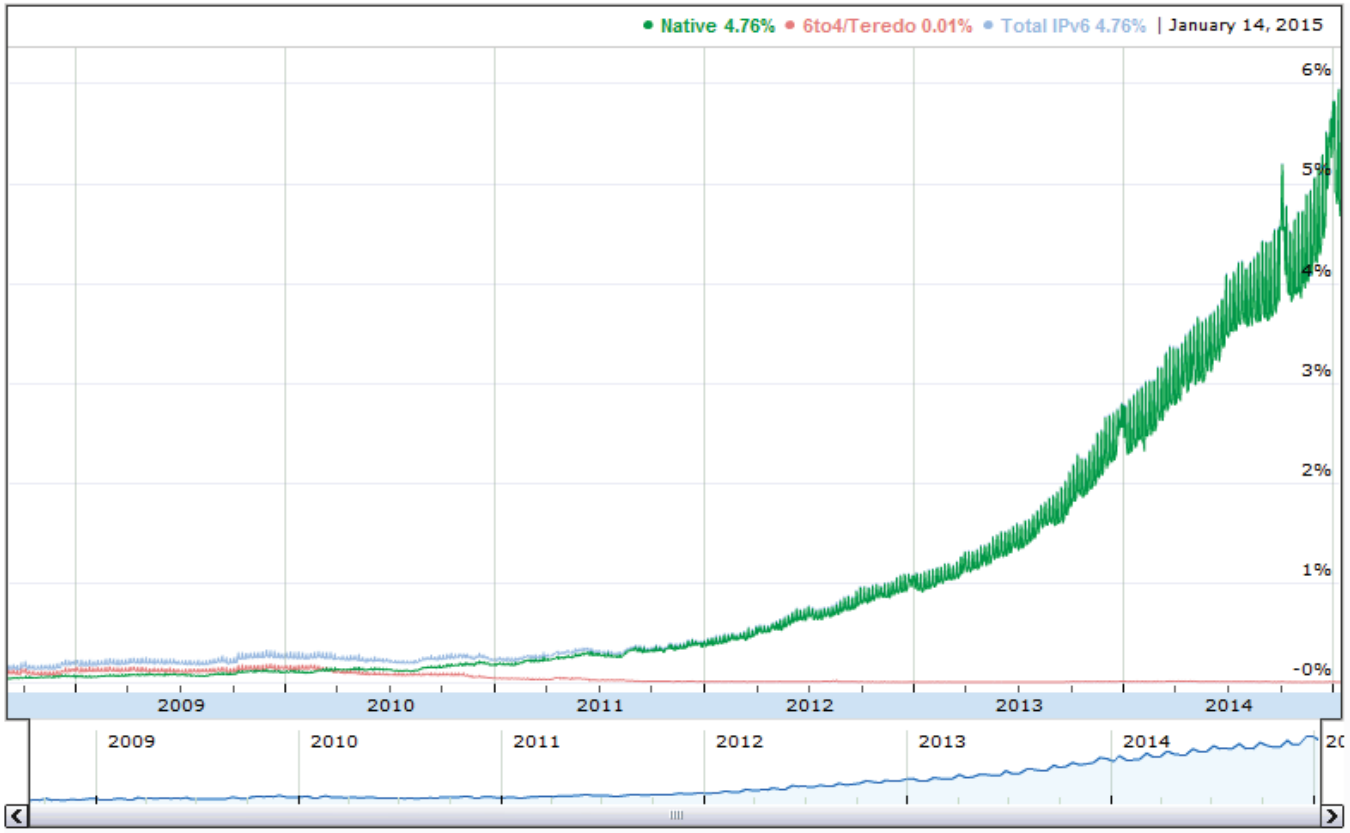
Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

# IPv6 Adoption

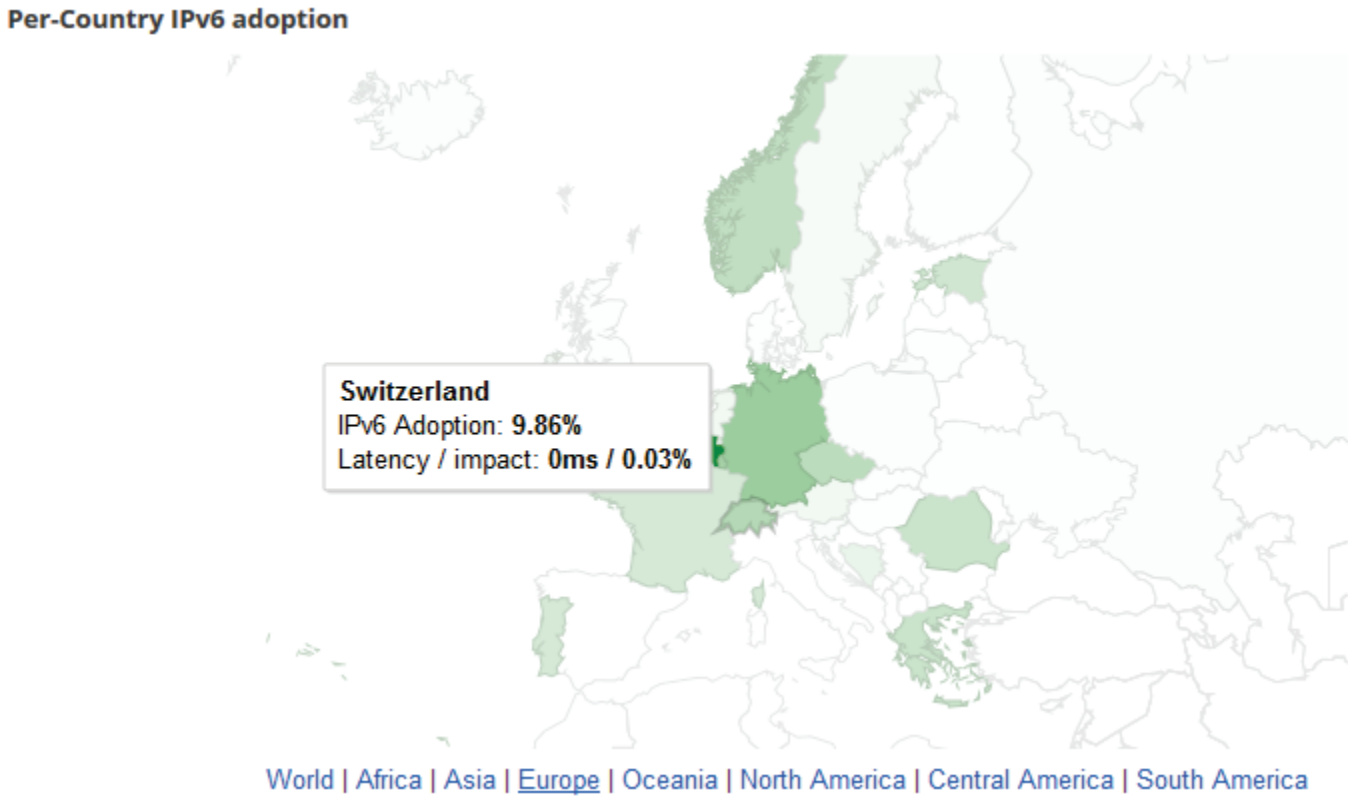
**IPv6 Adoption**

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.




**http://www.google.com/intl/en/ipv6/statistics.html**

# IPv6 Adoption Switzerland




**http://www.google.com/intl/en/ipv6/statistics.html**

# What the talk is about…

➔ IPv6 will be used more widely in the future

➔ ARP spoofing is well-known

Therefore, these slides cover:

- What is the IPv6 Neighbor Discovery (ND) protocol
- Intro to IPv6 Secure Neighbor Discovery (SeND)
- Problems and challenges with SeND
- Existing implementations

# Neighbor Discovery Protocol (NDP)

Same as ARP in IPv4 but with extended functionality

## Neighbor Discovery messages

- Neighbor Solicitation (NS)

  NS resolves the neighbor node's IPv6 address to its MAC address and verifies that the node is still reachable
- Neighbor Advertisement (NA)

  The node that receives an NS message sends back an NA message with its own MAC address
- Router Solicitation (RS)

  IPv6 host sends RS to discover the default router and learn network information, such as prefixes and Domain Name Server (DNS) addresses
- Router Advertisement (RA)

  Router that receives an RS message sends back an RA message (solicited RA) and IPv6 routers send RA periodically (unsolicited multicast RA) with e.g. prefix
- Redirect

  Used by routers to inform hosts of a better first hop for a destination

# Neighbor Discovery Protocol (NDP)

➔ Part of the Internet Control Message Protocol for IPv6 (ICMPv6)

Some of the key functionalities:

- discovering nodes on the same broadcast domain
- SLAAC (IPv6 stateless address auto-configuration)
- determining link-layer addresses
- detecting duplicate addresses (DAD)
- finding routers
- crucial role in mobile IPv6 (MIPv6)

# NDP Problems…

All hosts trust each other

All hosts trust routers

All routers trust hosts…➔ like ARP

IPv6 neighbor discovery is vulnerable to

- Spoofing
- Denial-of-service
  (flood_advertise6, flood_router6, dos-new-ip6)
- Replay
- Redirect (parasite6)
- Rogue router attacks (fake_router6)
- Privacy issues with auto generated addresses

# Existing mitigations

Router Advertisement Guard (RA Guard)

- RA guards monitors and detects RA
- Only protects an interface from a rogue RA, not traffic from NA and NS badness

Privacy Extensions for Stateless Address Autoconfiguration in IPv6 described in RFC4941

- Interface Identifier (IID) which changes over time
- Doesn't protect against spoofing

Use monitoring tools like NDPMon or Ramond

- Passive detection tools

Cisco First Hop Security (FHS)

- Cisco's solution for mitigating IPv6 attacks

# SeND (Secure Neighbor Discovery)

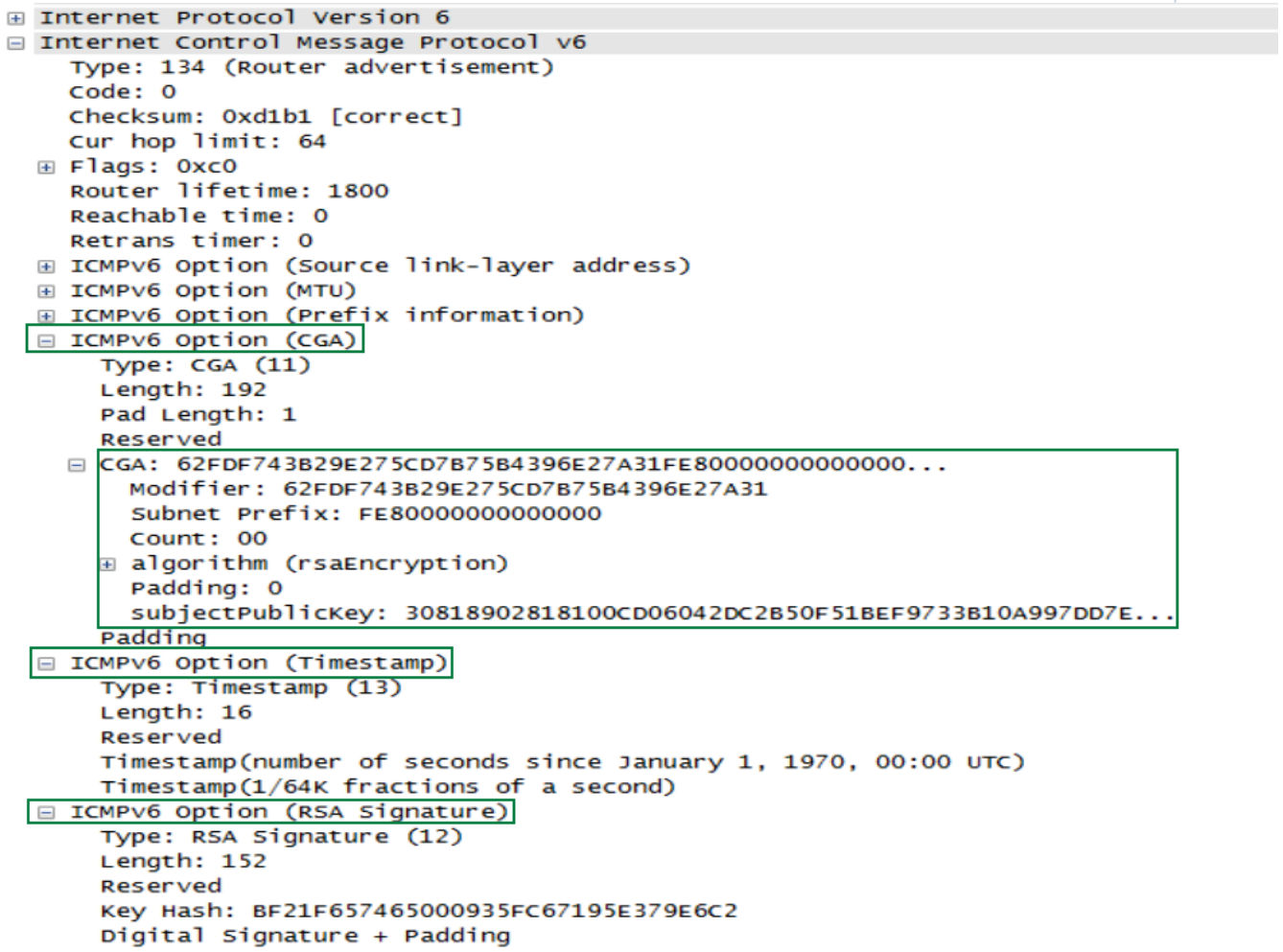
SeND offers three additional features to NDP

- Address ownership proof
- Message protection
- Router authorization mechanism

SeND uses cryptographically generated addresses (CGA,CGA++) to prevent address stealing. The node's IPv6 address is bound to its public key. Each node must generate or obtain a public/private RSA pair before it can claim an address.

SeND includes a nonce in the solicitation message (request) and requires advertisements (response) to include this nonce.

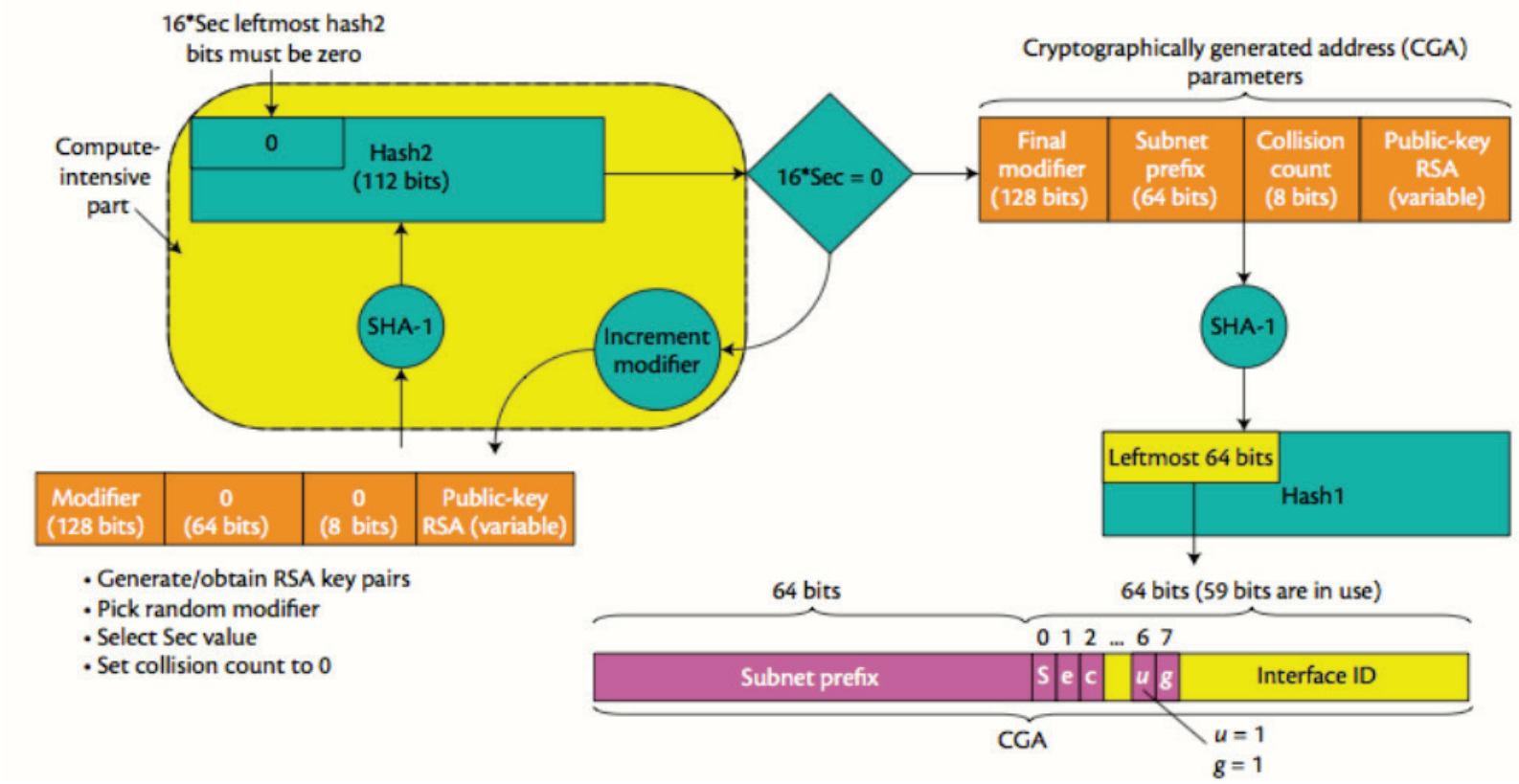
# ICMPv6 Paket




**«IPv6 Secure Neighbor Discovery (SeND) and CGA", Jeremy Duncan**

# Cryptographically Generated Addresses

➔ also called Hash Based Addresses or Key Based Addresses




**"IPv6 Secure Neighbor Discovery", EPFL, C. Musso, S. Boujnah, K. Hajji, Dec 2013**

# SeND (Secure Neighbor Discovery)

SeND uses authorization delegation discovery (ADD) to validate and authorize IPv6 routers to act as default gateways and specifies IPv6 prefixes that a router is authorized to announce on its link

SeND offers two new ICMPv6 messages to identify the router authorization process:

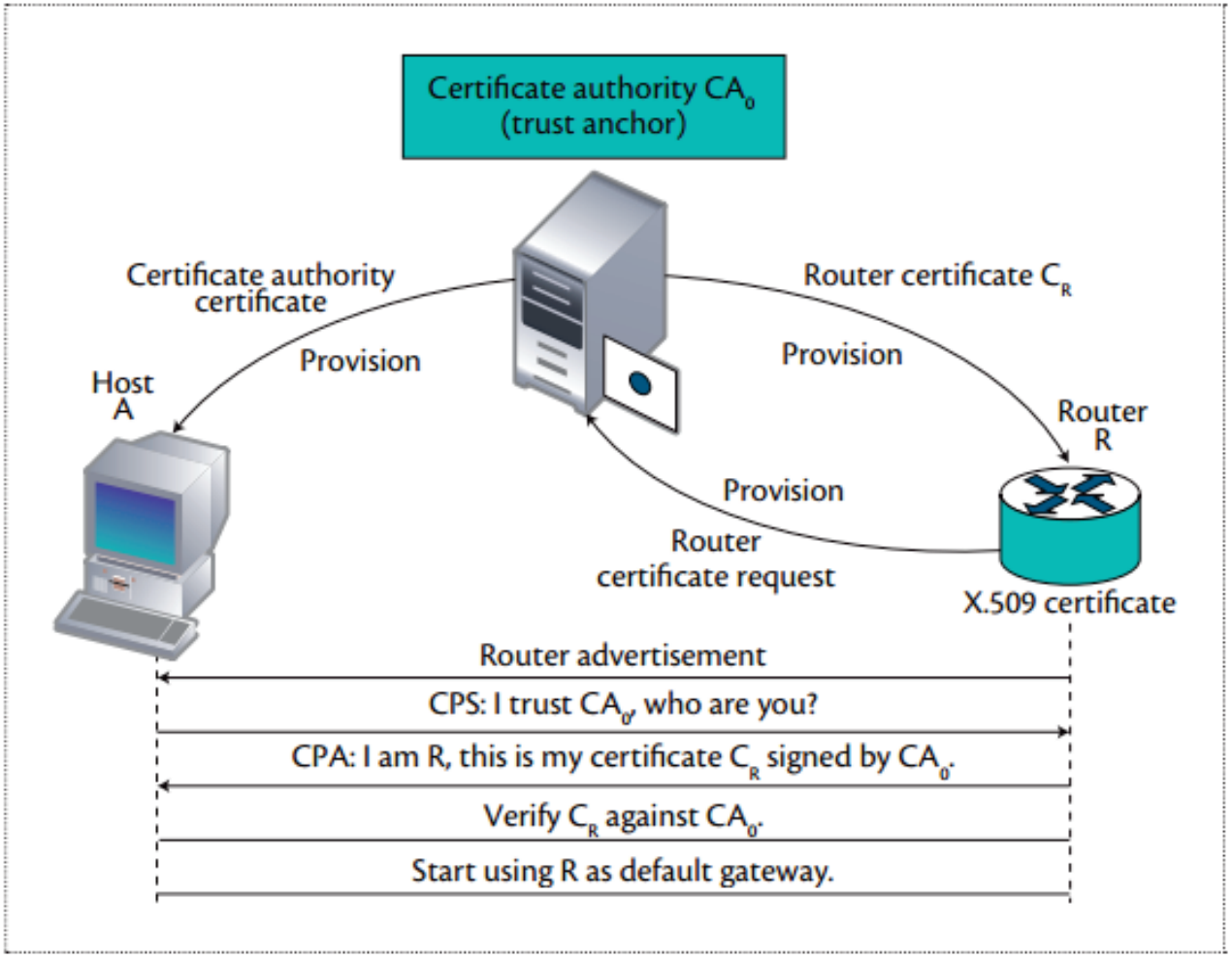
- certificate path solicitation (CPS)

  request a certification path between a router and one of the host's trust anchors

- and certificate path advertisement (CPA)

  sent in reply to the CPS message and contains the router certificate

# SeND: Router authorization process




**"IPv6 Secure Neighbor Discovery", EPFL, C. Musso, S. Boujnah, K. Hajji, Dec 2013**

# SeND RFCs

RFC3971: Secure Neighbor Discovery (SeND)

RFC3972: Cryptographically Generated Addresses (CGAs)

RFC3779: X.509 Extensions for IP Address and AS Identifiers

# Security concerns with SeND

CGA can't provide assurance about the real node's identity

Because CGAs aren't certified, attackers can create new valid addresses from their own public keys and start the communication. For more security, a certificate authority is necessary to validate the keys.

SHA-1 used for hashing and only 59 bits of cryptographic payload (64-bit minus 3-bit for the sec parameter and minus 1-bit for the u/g parameter ➔ see slide 7)

# Operational concerns with SeND

- Works as expected in **IPv6-only networks**
- DoS attacks are possible because of **computational cost** and because of the use of non-CGAs to set DAD collision count to 2 (CGA algorithm might need to be extended to verify the DAD message responses before the increment of the collision count) ➔ every node must support CGA
- If the generation and verification values exceed 0.5 second, DAD would fail because it expects to send and receive two ND messages in less than 1 second, as RFC 4861 indicates.
- Any node trying to verify router authorization must be prepared beforehand with the anchor certificate
- Mobile IPv6 (MIPv6) needs to finish the address generation within hundreds of milliseconds
- Every devices must implement the protocol

# Existing Implementations

Conclusion: Lack of sophisticated implementations, most operating systems support NDP but lack support for SeND

Kernel modifications vs. user-land applications

Linux

- NDprotector. NDprotector (htt://amnesiak.org/NDprotector)
- Easy-SEND
- Native SeND kernel API for BSD (send-0.3)
- ipv6-send-cga, code.google.com/p/ipv6-send-cga)

Windows / Mac

- WinSEND (only Windows, third-party implementation, won the German IPv6 Council Application Award for 2011)
- TrustRouter (only RA)

# Possible Deployment Approach

Using CGA with RAGuard prevents address theft and detects fake RA

- CGA protects the local link from address theft
- and the RAGuard protects the local link from fake RA

# Windows

IPv6 enabled by default

Windows does **not** support SeND (Windows 7, 2008, 2012 and 8)

Window Server 2012 now has NAT64/DNS64 (DirectAccess clients must use IPv6 to connect to the DA server)

Microsoft no longer tests their software with IPv4 ONLY networks

➔ Disabling IPv6 could lead to operational problems

# Other platforms

SeND not supported on

- Mac OS/X
- iOS
- Android
- HP Networking

Juniper JUNOS supports SeND with 9.3+

SeND: IOS 12.4-24(T) +

- Only T and M on ISR routers (not in new ASR)

RA Guard in Cisco IOS Release

Implemented RFC3971 (SeND) & RFC3972 (CGA)

Leverage PKI tooling already available on routers

First-Hop-Security for IPv6 is available

- First phase (Port ACL & RA Guard) available since Summer 2010
- Second phase (NDP & DHCP snooping) available since Summer 2011
- Third phase (Source Guard, Destination Guard) available since Summer 2013

# Cisco – First Hop Security

Port ACL – blocks all ICMPv6 RA from hosts

RAguard lite

- also dropping all RA received on this port, 12.2(33)SXI4 & 12.2(54)SG

RAguard (12.2(50)SY, 15.0(2)SE)

- attach-policy
- device-role host | router

# Facts

IPv4 still in use within enterprise networks

A long way to go for IPv6-only

IPv6 SeND only supported in experimental state

# Conclusion

SeND would allow to prevent the IPv4 style «ARP spoofing» in the IPv6 world (impersonation / address stealing)

SeND would allow to prevent rogue router advertisements (fake router, flooding)

BUT we're currently not able to use it due to the lack of support and productive-ready implementations

# References


- Ed Horley IPv6 Bootcamp presentation, 2014
- «IPv6 Secure ND implementation report on Cisco IOS» by Eric Levy-Abegnoli, IETF 70th, Vancouver
- «Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations", A. AlSa'deh and C. Meinel, Hasso-Plattner- Institut, 2012
- http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-602135.html, «IPv6 First Hop Security», 2010
- http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-2mt/ip6-send.html, «IPv6 Secure Neighbor Discovery», 2012
- «IPv6 Security», Eric Vyncke, Cisco, 2014
- «GUIDELINES FOR THE SECURE DEPLOYMENT OF IPV6», NIST, 2010
- «IPv6 Secure Neighbor Discovery», EPFL, Claire Musso, Syrine Boujnah, Khalil Hajji, Dec 2013
- «Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SeND) of IPv6 NDP Security», Dec 2011, Yvette E. Gelogo, Ronnie D. Caytiles, Byungjoo Park
- «IPv6 Secure Neighbor Discovery (SeND) and CGA», Jeremy Duncan
- «Securing IPv6 Neighbor and Router Discovery», J. Arkko, T. Aura et al.


COMPASS
SECURITY
NETWORK COMPUTING AG