ETSI GR IP6 031 V1.1.1 (2020-11)

IPv6 Security, Cybersecurity, Blockchain

Disclaimer

The present document has been produced and approved by the IPv6 Integration (IP6) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/IP6-0031

Keywords
blockchain, cybersecurity, internet, IPv6, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) IPv6 Integration (IP6).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document gives the outline of deployment of IPv6 security, Cybersecurity, Blockchain an DatablockMatrix.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] "Are you sharing the same IP address as a criminal? Law enforcement call for the end of carrier grade NAT (CGN) to increase accountability online", October 2017.

NOTE: Available at https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online.

[i.2] IETF draft-chakrabarti-nordmark-6man-efficient-nd: "IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks", February 2015.

[i.3] IETF draft-ietf-dhc-sedhcpv6: "Secure DHCPv6", February 2017.

[i.4] IETF draft-ietf-opsec-ipv6-eh-filtering: "Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers", July 2018.

[i.5] IETF draft-ietf-v6ops-ula-usage-considerations: "Considerations For Using Unique Local Addresses", March 2017.

[i.6] IETF draft-kampanakis-6man-ipv6-eh-parsing: "Implementation Guidelines for parsing IPv6 Extension Headers", August 2014.

[i.7] IETF draft-thubert-savi-ra-throttler: "Throttling RAs on constrained interfaces", June 2012.

[i.8] IETF RFC 1918 (February 1996): "Address Allocation for Private Internets".

[i.9] IETF RFC 2131 (March 1997): "Dynamic Host Configuration Protocol".

[i.10] IETF RFC 2460 (December 1998): "Internet Protocol, Version 6 (IPv6)Specification".

NOTE: Obsoleted by IETF RFC 8200.

[i.11] IETF RFC 2529 (March 1999): "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels".

[i.12] IETF RFC 2740 (December 1999): "OSPF for IPv6".

[i.13] IETF RFC 2784 (March 2000): "Generic Routing Encapsulation (GRE)".

[i.14] IETF RFC 2827 (May 2000): "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing".

[i.15] IETF RFC 2866 (June 2000): "RADIUS Accounting".

[i.16] IETF RFC 3756 (May 2004): "IPv6 Neighbor Discovery (ND) Trust Models and Threats".

[i.17] IETF RFC 3924 (October 2004): "Cisco Architecture for Lawful Intercept in IP Networks".

[i.18] IETF RFC 3971 (March 2005): "SEcure Neighbor Discovery (SEND)".

[i.19] IETF RFC 3972 (March 2005): "Cryptographically Generated Addresses (CGA)".

[i.20] IETF RFC 4193 (October 2005): "Unique Local IPv6 Unicast Addresses".

[i.21] IETF RFC 4293 (April 2006): "Management Information Base for the Internet Protocol (IP)".

[i.22] IETF RFC 4301 (December 2005): "Security Architecture for the Internet Protocol".

[i.23] IETF RFC 4302 (December 2005): "IP Authentication Header".

[i.24] IETF RFC 4303 (December 2005): "IP Encapsulating Security Payload (ESP)".

[i.25] IETF RFC 4364 (February 2006): "BGP/MPLS IP Virtual Private Networks (VPNs)".

[i.26] IETF RFC 4381 (February 2006): "Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)".

[i.27] IETF RFC 4443 (March 2006): "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification".

[i.28] IETF RFC 4649 (August 2006): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option".

[i.29] IETF RFC 4659 (September 2006): "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN".

[i.30] IETF RFC 4798 (February 2007): "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)".

[i.31] IETF RFC 4861 (September 2007): "Neighbor Discovery for IP version 6 (IPv6)".

[i.32] IETF RFC 4864 (May 2007): "Local Network Protection for IPv6".

[i.33] IETF RFC 4890 (May 2007): "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[i.34] IETF RFC 4941 (September 2007): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[i.35] IETF RFC 5340 (July 2008): "OSPF for IPv6".

[i.36] IETF RFC 5635 (August 2009): "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)".

[i.37] IETF RFC 5952 (August 2010): "A Recommendation for IPv6 Address Text Representation".

[i.38] IETF RFC 6092 (January 2011): "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service".

[i.39] IETF RFC 6104 (February 2011): "Rogue IPv6 Router Advertisement Problem Statement".

[i.40] IETF RFC 6105 (February 2011): "IPv6 Router Advertisement Guard".

[i.41] IETF RFC 6146 (April 2011): "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers".

[i.42] IETF RFC 6147 (April 2011): "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers".

[i.43] IETF RFC 6164 (April 2011): "Using 127-Bit IPv6 Prefixes on Inter-Router Links".

[i.44] IETF RFC 6169 (April 2011): "Security Concerns with IP Tunneling".

[i.45] IETF RFC 6192 (March 2011): "Protecting the Router Control Plane".

[i.46] IETF RFC 6221 (May 2011): "Lightweight DHCPv6 Relay Agent".

[i.47] IETF RFC 6241 (June 2011): "Network Configuration Protocol (NETCONF)".

[i.48] IETF RFC 6264 (June 2011): "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition".

[i.49] IETF RFC 6269 (June 2011): "Issues with IP Address Sharing".

[i.50] IETF RFC 6302 (June 2011): "Logging Recommendations for Internet-Facing Servers".

[i.51] IETF RFC 6324 (August 2011): "Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations".

[i.52] IETF RFC 6333 (August 2011): "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion".

[i.53] IETF RFC 6459 (January 2012): "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)".

[i.54] IETF RFC 6564 (April 2012): "A Uniform Format for IPv6 Extension Headers".

[i.55] IETF RFC 6583 (March 2012): "Operational Neighbor Discovery Problems".

[i.56] IETF RFC 6598 (April 2012): "IANA-Reserved IPv4 Prefix for Shared Address Space".

[i.57] IETF RFC 6620 (May 2012): "FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses".

[i.58] IETF RFC 6666 (August 2012): "A Discard Prefix for IPv6".

[i.59] IETF RFC 6762 (February 2013): "Multicast DNS".

[i.60] IETF RFC 6763 (February 2013): "DNS-Based Service Discovery".

[i.61] IETF RFC 6810 (January 2013): "The Resource Public Key Infrastructure (RPKI) to Router Protocol".

[i.62] IETF RFC 6939 (May 2013): "Client Link-Layer Address Option in DHCPv6".

[i.63] IETF RFC 6980 (August 2013): "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery".

[i.64] IETF RFC 7011 (September 2013): "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information".

[i.65] IETF RFC 7012 (September 2013): "Information Model for IP Flow Information Export (IPFIX)".

[i.66] IETF RFC 7039 (October 2013): "Source Address Validation Improvement (SAVI) Framework".

[i.67] IETF RFC 7045 (December 2013): "Transmission and Processing of IPv6 Extension Headers".

[i.68] IETF RFC 7050 (November 2013): "Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis".

[i.69] IETF RFC 7084 (November 2013): "Basic Requirements for IPv6 Customer Edge Routers".

NOTE: Obsoletes IETF RFC 6204.

[i.70] IETF RFC 7112 (January 2014): "Implications of Oversized IPv6 Header Chains".

[i.71] IETF RFC 7113 (February 2014): "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)".

[i.72] IETF RFC 7166 (March 2014): "Supporting Authentication Trailer for OSPFv3".

NOTE: Obsoletes IETF RFC 6506.

[i.73] IETF RFC 7381 (October 2014): "Enterprise IPv6 Deployment Guidelines".

[i.74] IETF RFC 7404 (November 2014): "Using Only Link-LocalAddressing inside an IPv6 Network".

[i.75] IETF RFC 7422 (December 2014): "Deterministic Address Mapping to Reduce Logging in Carrier-Grade NAT Deployments".

[i.76] IETF RFC 7513 (May 2015): "Source Address Validation Improvement (SAVI) Solution for DHCP".

[i.77] IETF RFC 7597 (July 2015): "Mapping of Address and Port with Encapsulation (MAP-E)".

[i.78] IETF RFC 7599 (July 2015): "Mapping of Address and Port using Translation (MAP-T)".

[i.79] IETF RFC 7610 (August 2015): "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers".

[i.80] IETF RFC 7707 (March 2016): "Network Reconnaissance in IPv6 Networks".

NOTE: Obsoletes IETF RFC 5157.

[i.81] IETF RFC 7721 (March 2016): "Security and Privacy Considerations for IPv6 Address Generation Mechanisms".

[i.82] IETF RFC 7872 (June 2016): "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World".

[i.83] IETF RFC 7915 (June 2016): "IP/ICMP Translation Algorithm".

NOTE: Obsoletes IETF RFC 6145.

[i.84] IETF RFC 7934 (July 2016): "Host Address Availability Recommendations".

[i.85] IETF RFC 8064 (February 2017): "Recommendation on Stable IPv6 Interface Identifiers".

[i.86] IETF RFC 8190 (June 2017): "Updates to the Special-Purpose IP Address Registries".

[i.87] IETF RFC 8273 (December 2017):"Unique IPv6 Prefix per Host".

[i.88] "Mapping the Great Void - Smarter scanning for IPv6".

NOTE: Available at http://www.caida.org/workshops/isma/1202/slides/aims1202_rbarnes.pdf.

[i.89] IETF RFC 8200 (July 2017): "Internet Protocol, Version 6 (IPv6) Specification".

NOTE: Obsoletes IETF RFC 2460.

[i.90] IETF RFC 8415 (November 2018): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

NOTE: Obsoletes IETF RFC 3315.

[i.91] IEEE 802.1X™-2020: "IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control".

NOTE: Available at https://standards.ieee.org/standard/802_1X-2020.html.

[i.92] Kuhn, D. R. (2018): "A data structure for integrity protection with erasure capability. NIST Cybersecurity Whitepaper".

[i.93] Kuhn, R., Yaga, D., & Voas, J. (2019): "Rethinking distributed ledger technology". IEEE Computer, 52(2), 68-72.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AAAA	Authentication, Authorization, Accounting and Auditing
ACL	Access Control List
AFTR	Address Family Translation Router
AH	Authentication Header
AS	Autonomous System
ASIC	Application-Specific Integrated Circuit
AXFR	Authoritative Transfer
BGP	Border Gateway Protocol
CaaS	Cybersecurity as a Service
CAM	Content Addressable Memory
CE	Customer Equipment
CERT	Community Emergency Response Team
CERT	Computer Emergency Response Team Finland
CGA	CryptographicaIIy Generated Address
CGN	Carrier-Grade NAT
CMDB	Configuration Management Data Base
CPE	Customer Premise Equipment
CPU	Central Processing Unit
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DLT	Distributed Ledger Technology
DNS	Domain Name Service
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Services
DS-Lite	Dual Stack Lite
DUID	DHCP Unique ID
ESP	Encapsulating Security Payload
EU	European Union
EUI	Extended Unique Identifier
FQDN	Fully Qualified Domain Name
GDPR	European Union General Data Protection Regulation
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
HMAC	Hash-based Message Authentication Code
IANA	The Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IID	Interface Identifier
IP	Internet Protocol
IPAM	IP Address Management

IPfix	IP Flow Information Export
IPS	International Protective Service
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISAC	Information sharing group
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LSN	Large Scale NAT
MAC	Media Access Control
MAP	Mapping of Address and Port
MAP-E	Mapping of Address and Port with Encapsulation
MAP-T	Mapping of Address and Port with Translation
MD5	Message Digest Algorithm Five
MIB	Management Information Base
MITM	Man-In-The-Middle
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NCSA	National Communications Security Authority Finland
NCSC-FI	The National Cyber Security Centre Finland
ND	Neighbor Discovery
NDP	Neighbor Discovery Protocol
NESA	National Emergency Supply Agency
NETCONF	Network Configuration Protocol (NETCONF)
NOC	Network Operation Centre
NRA	National Regulatory Authority
NTP	Network Time Protocol
OECD	Organization for Economic Cooperation and Development
OS	Operating System
OSPF	Open Shortest Path First
PA	Provider Aggregatable
PE	Provider Equipment
PGW	PDN GateWay
PI	Provider Independent
PMTUD	Path MTU Detection
PPP	Point to Point Protocol
PT	Protocol Translator
RA	Router Advertisement
RADB	Routing Arbiter Database
RADIUS	Remote Authentication Dial In User Service
REC	Recommendation
RP	Router Processor
RSA	Rivest-Shamir-Adleman
RTBH	Remote Triggered Black Hole
SAINT	Systemic Analyser In Network Threats
SAVI	Source Address Validation Improvements
SeND	SEcure Neighbor Discovery
SLAAC	Stateless Address Auto Configuration
SNMP	Simple Network Management Protocol
SP	Service Provider
SSH	SecureShell
SWIFT	Society for the Worldwide Interbank Financial Telecommunication
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Type Length Value
TTL	Time To Live
TV	Television

UDP	User Datagram Protocol
ULA	Unique Local Address
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WPA	Wi-Fi Protected Address

4 Generic IPv6 Security Considerations

4.1 Addressing Architecture

4.1.1 Introduction

IPv6 address allocations and overall architecture are an important part of securing IPv6. Initial designs, even if intended to be temporary, tend to last much longer than expected. Although initially IPv6 was thought to make renumbering easy, in practice, it may be extremely difficult to renumber without a good IP Addresses Management (IPAM) system.

Once an address allocation has been assigned, there should be some thought given to an overall address allocation plan. With the abundance of address space available, an address allocation may be structured around services along with geographic locations, which then can be a basis for more structured security policies to permit or deny services between geographic regions.

A common question is whether companies should use Provider Independent (PI) vs. Provider Aggregatable (PA) space (IETF RFC 7381 [i.73]), but from a security perspective there is little difference. However, one aspect to keep in mind is who has administrative ownership of the address space and who is technically responsible if/when there is a need to enforce restrictions on routability of the space due to malicious criminal activity. Using PA space exposes the organization to a renumbering of the complete network including security policies (based on ACL), audit system, etc., in short a complex task which could lead to some temporary security risk if done for a large network and without automation; hence, for large networks, PI space should be preferred even if it comes with additional complexities (for example BGP routing) and duties (adding a route6 object in the Regional Internet Registry database).

In IETF RFC 7934 [i.84], it is recommended that IPv6 network deployments provide multiple IPv6 addresses from each prefix to general-purpose hosts and it specifically does not recommend to limit a host to only one IPv6 address per prefix. It also recommends that the network give the host the ability to use new addresses without requiring explicit requests (for example by using SLAAC).

4.1.2 Statically Configured Addresses

When considering how to assign statically configured addresses it is necessary to take into consideration the effectiveness of perimeter security in a given environment. There is a trade-off between ease of operation (where some portions of the IPv6 address could be easily recognizable for operational debugging and troubleshooting) versus the risk of trivial scanning used for reconnaissance. SCANNING [i.88] shows that there are scientifically based mechanisms that make scanning for IPv6 reachable nodes more realizable than expected; see also IETF RFC 7707 [i.80]. The use of well-known (such as ff02::1 for all link-local nodes) or the use of commonly repeated addresses could make it easy to figure out which devices are name servers, routers or other critical devices; even a simple trace route will expose most of the routers on a path. There are many scanning techniques and more to come possible, hence, operators should never rely on the 'impossible to find because my address is random' paradigm.

While in some environments obfuscating addresses could be considered an added benefit; it does not preclude that perimeter rules are actively enforced and that statically configured addresses follow some logical allocation scheme for ease of operation (as simplicity always helps security). Typical deployments will have a mix of static and non-static addresses.

4.1.3 Use of ULAs

Unique Local Addresses (ULAs) (IETF RFC 4193 [i.20]) are intended for scenarios where systems are not globally reachable, despite formally having global scope. ULA looks similar to IETF RFC 1918 [i.8] addresses but have different use cases. One use of ULA is described in IETF RFC 4864 [i.32] and some considerations on using ULA are described in IETF draft-ietf-v6ops-ula-usage-considerations [i.5].

4.1.4 Point-to-Point Links

IETF RFC 6164 [i.43] in section 5.1 documents the reasons why to use a /127 for inter-router point-to-point links; notably, a /127 prevents the ping-pong attack between routers not implementing correctly IETF RFC 4443 [i.27] and also prevents a DoS attack on the neighbor cache.

Some environments are also using link-local addressing for point-to-point links. While this practice could further reduce the attack surface against infrastructure devices, the operational disadvantages need also to be carefully considered; see also IETF RFC 7404 [i.74].

4.1.5 Temporary Addresses - Privacy Extensions for SLAAC

Historically Stateless Address Auto Configuration (SLAAC) relied on an automatically generated64 bit interface identifier (IID) based on the EUI-64 MAC address, which together with the /64 prefix makes up the globally unique IPv6 address. The EUI-64 address is generated from the 48-bit stable MAC address.

Randomly generating an interface ID, as described in IETF RFC 4941 [i.34], is part of SLAAC with so-called privacy extension addresses and used to address some privacy concerns. Privacy extension addresses a.k.a. temporary addresses may help to mitigate the correlation of activities of a node within the same network, and may also somehow reduce the attack exposure window.

Using IETF RFC 4941 [i.34] privacy extension addresses prevents the operator from building host specific access control lists (ACLs).

IETF RFC 8064 [i.85] specifies another way to generate while still keeping the same IID for each network prefix; this allows SLAAC nodes to always have the same stable IPv6 address on a specific network while having different IPv6 address on different networks.

As IETF RFC 4941 [i.34] privacy extension addresses could also be used to obfuscate some malevolent activities (whether on purpose or not), specific user attribution/accountability procedures should be put in place as described in clause 4.6.

In some extreme use cases where user accountability is more important than user privacy, network operators may consider disabling SLAAC and rely only on DHCPv6; but not all operating systems support DHCPv6 so some hosts will not get any IPv6 connectivity. Disabling SLAAC and privacy extensions addresses can be done for most OS and for non-hacker users by sending RA messages with a hint to get addresses via DHCPv6 by setting the M-bit but also disabling SLAAC by resetting all A-bits in all prefix information options. Hackers will find a way to bypass this mechanism if not enforced at the switch/ router level.

However, in scenarios where anonymity is a strong desire (protecting user privacy is more important than user attribution), privacy extension addresses should be used. When IETF RFC 8064 [i.85] is available, the stable privacy address is probably a good balance between privacy (among multiple networks) and security/user attribution (within a network).

4.1.6 Privacy Consideration of Addresses

The reader can learn more about privacy considerations for IPv6addresses in IETF RFC 7721 [i.81].

4.1.7 DHCP/DNS Considerations

Many environments use DHCPv6 to allocate addresses to ensure audit-ability and traceability (but see clause 4.6.2.5). A main security concern is the ability to detect and counteract against rogue DHCP servers (clause 4.3.3).

While there are no fundamental differences with IPv4 and IPv6security concerns about DNS, there are specific consideration in DNS64 (IETF RFC 6147 [i.42]) environments that need to be understood. Specifically, the interactions and potential to interference with DNSSEC implementation need to be understood - these are pointed out in detail in clause 4.7.3.2.

4.1.8 Using a /64 per host

An interesting approach is using a /64 per host as proposed in IETF RFC 8273 [i.87]. This allows an easier user attribution (typically based on the host MAC address) as its /64 prefix is stable even if applications, containers within the host can change of IPv6 address within this /64.

4.2 Extension Headers

4.2.1 Overview

The extension headers are an important difference between IPv4 and IPv6. The packet structure does make a big difference. The IANA has closed the existing empty "Next Header Types" registry to new entries and is redirecting its users to a new "IPv6 Extension Header Types" registry per IETF RFC 7045 [i.67].

They have also become a very controversial topic since forwarding nodes that discard packets containing extension headers are known to cause connectivity failures and deployment problems (IETF RFC 7872 [i.82]).Understanding the role of varying extension headers is important and this clause enumerates the ones that need careful consideration.

A clarification on how intermediate nodes should handle existing packets with extension headers and any extension headers that are defined in the future is found in IETF RFC 7045 [i.67]. The uniform TLV format is used for defining future extension headers is described in IETF RFC 6564 [i.54].

Since there is no indication in the packet whether the Next Protocol field points to an extension header or to a transport header, this may confuse some filtering rules.

There is work in progress at the IETF about filtering rules for those extension headers:

- IETF draft-ietf-opsec-ipv6-eh-filtering [i.4] for transit routers.

4.2.2 Order and Repetition of Extension Headers

While IETF RFC 8200 [i.89] recommends the order and the maximum repetition of extension headers, there are still IPv6 implementations at the time of writing the present document which support a non-recommended order of headers (such as ESP before routing) or an illegal repetition of headers (such as multiple routing headers). The same applies for options contained in the extension headers (see IETF draft-kampanakis-6man-ipv6-eh-parsing [i.6]). In some cases, it has led to nodes crashing when receiving or forwarding wrongly formatted packets.

A firewall or any edge device should be used to enforce the recommended order and number of occurrences of extension headers.

4.2.3 Hop-by-Hop Options Header

The hop-by-hop options header, when present in an IPv6 packet, forces all nodes in the path to inspect this header in the original IPv6 specification (IETF RFC 2460 [i.10]). This was of course a large avenue for a denial of service as most if not all routers cannot process this kind of packets in hardware but have to 'punt' this packet for software processing. Clause 4.3 of IETF RFC 8200 [i.89], is more sensible to this respect as the processing of hop-by-hop options header by intermediate routers is optional.

4.2.4 Fragment Header

The fragment header is used by the source (and only the source) when it has to fragment packets. IETF RFC 7112 [i.70] and section 4.5 of IETF RFC 8200 [i.89] explain why it is important to firewall and security devices should drop first fragments that do not contain the entire ipv6 header chain (including the transport-layer header); destination nodes should discard first fragments that do not contain the entire ipv6 header chain (including the transport-layer header).

Else, stateless filtering could be bypassed by a hostile party. IETF RFC 6980 [i.63] applies a stricter rule to NDP by enforcing the drop of fragmented NDP packets. IETF RFC 7113 [i.71] describes how RA-guard function described in IETF RFC 6105 [i.40] should behave in presence of fragmented RA packets.

4.2.5 IP Security Extension Header

The IPsec (IETF RFC 4301 [i.22]) extension headers (AH (IETF RFC 4302 [i.23]) and ESP (IETF RFC 4303 [i.24]) are required if IPsec is to be utilized for network level security functionality.

4.3 Link-Layer Security

4.3.1 ND/RA Rate Limiting

IPv6 relies heavily on the Neighbor Discovery protocol (NDP) (IETF RFC 4861 [i.31]) to perform a variety of link operations such as discovering other nodes on the link, resolving their link-layer addresses, and finding routers on the link. If not secured, NDP is vulnerable to various attacks such as router/neighbor message spoofing, redirect attacks, Duplicate Address Detection (DAD) DoS attacks, etc. many of these security threats to NDP have been documented in IPv6 ND Trust Models and Threats (IETF RFC 3756 [i.16]) and in IETF RFC 6583 [i.55].

Neighbor Discovery (ND) can be vulnerable to Denial of Service (DoS) attacks in which a router is forced to perform address resolution for a large number of unassigned addresses. Possible side effects of this attack preclude new devices from joining the network or even worse rendering the last hop router ineffective due to high CPU usage. Easy mitigative steps include rate limiting Neighbor Solicitations, restricting the amount of state reserved for unresolved solicitations, and clever cache/timer management.

IETF RFC 6583 [i.55] discusses the potential for DoS in detail and suggests implementation improvements and operational mitigation techniques that may be used to mitigate or alleviate the impact of such attacks. Here are some feasible mitigation options that can be employed by network operators today:

- Ingress filtering of unused addresses by ACL, route filtering, longer than /64 prefix; these require static configuration of the addresses.
- Tuning of NDP process (where supported).
- Using /127 on point-to-point link per (IETF RFC 6164 [i.43]).

Additionally, IPv6 ND uses multicast extensively for signalling messages on the local link to avoid broadcast messages for on-the-wire efficiency. However, this has some side effects on Wi-Fi networks, especially a negative impact on battery life of smart phones and other battery-operated devices that are connected to such networks. The following drafts are actively discussing methods to rate limit RAs and other ND messages on Wi-Fi networks in order to address this issue:

- IETF draft-thubert-savi-ra-throttler [i.7].
- IETF draft-chakrabarti-nordmark-6man-efficient-nd [i.2].

4.3.2 RA/NA Filtering

Router Advertisement spoofing is a well-known attack vector and has been extensively documented. The presence of rogue RAs, either intentional or malicious, can cause partial or complete failure of operation of hosts on an IPv6 link. For example, a host can select an incorrect router address which can be used as a Man-In-The-Middle (MITM) attack or can assume wrong prefixes to be used for Stateless Address Auto Configuration (SLAAC). IETF RFC 6104 [i.39] summarizes the scenarios in which rogue RAs may be observed and presents a list of possible solutions to the problem. IETF RFC 6105 [i.40] (RA-Guard) describes a solution framework for the rogue RA problem where network segments are designed around switching devices that are capable of identifying invalid RAs and blocking them before the attack packets actually reach the target nodes.

However, several evasion techniques that circumvent the protection provided by RA-Guard have surfaced. A key challenge to this mitigation technique is introduced by IPv6 fragmentation. An attacker can conceal the attack by fragmenting his packets into multiple fragments such that the switching device that is responsible for blocking invalid RAs cannot find all the necessary information to perform packet filtering in the same packet. IETF RFC 7113 [i.71] describes such evasion techniques, and provides advice to RA-Guard implementers such that the aforementioned evasion vectors can be eliminated.

Given that the IPv6 Fragmentation Header can be leveraged to circumvent current implementations of RA-Guard, IETF RFC 6980 [i.63] updates IETF RFC 4861 [i.31] such that use of the IPv6 Fragmentation Header is forbidden in all Neighbor Discovery messages except "Certification Path Advertisement", thus allowing for simple and effective measures to counter Neighbor Discovery attacks.

The Source Address Validation Improvements (SAVI) working group has worked on other ways to mitigate the effects of such attacks. IETF RFC 7513 [i.76] would help in creating bindings between a DHCPv4 (IETF RFC 2131 [i.9])/DHCPv6 (IETF RFC 8415 [i.90]) assigned source IP address and a binding anchor (IETF RFC 7039 [i.66]) on a SAVI device. Also, IETF RFC 6620 [i.57] describes how to glean similar bindings when DHCP is not used. The bindings can be used to filter packets generated on the local link with forged source IP address.

It is still recommended that RA-Guard and SAVI be employed as a first line of defense against common attack vectors including misconfigured hosts. This line of defense is fully effective when weird fragments are dropped by routers and switches as described in clause 4.2.4. The generated log should also be analysed to act on violations.

4.3.3 Securing DHCP

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (IETF RFC 8415 [i.90]) enables DHCP servers to pass configuration parameters such as IPv6 network addresses and other configuration information to IPv6 nodes. DHCP plays an important role in any large network by providing robust stateful configuration and auto registration of DNS Host Names.

The two most common threats to DHCP clients come from malicious (a.k.a. rogue) or unintentionally misconfigured DHCP servers. A malicious DHCP server is established with the intent of providing incorrect configuration information to the client to cause a denial of service attack or mount a man in the middle attack while unintentionally, a misconfigured DHCP server can have the same impact. Additional threats against DHCP are discussed in the security considerations section of IETF RFC 8415 [i.90].

IETF RFC 7610 [i.79], DHCPv6-Shield, specifies a mechanism for protecting connected DHCPv6 clients against rogue DHCPv6 servers. This mechanism is based on DHCPv6 packet-filtering at the layer-2 device; the administrator specifies the interfaces connected to DHCPv6 servers. Of course, extension headers could be leveraged to bypass DHCPv6-Shield unless IETF RFC 7112 [i.70] is enforced. Another way to secure DHCPv6 would be to use the secure DHCPv6 protocol which is currently work in progress per (IETF draft-ietf-dhc-sedhcpv6 [i.3]), but, with no real deployment known by the authors of the present document. It is recommended to use DHCP-shield and to analyse the log generated by this security feature.

4.3.4 3GPP Link-Layer Security

The 3GPP link is a point-to-point like link that has no link-layer address. This implies there can only be an end host (the mobile hand-set) and the first-hop router (i.e. a GPRS Gateway Support Node (GGSN) or a Packet Gateway (PGW)) on that link. The GGSN/PGW never configures a non link-local address on the link using the advertised /64 prefix on it. There is no need for an address resolution on the 3GPP link, since there are no link-layer addresses. Furthermore, the GGSN/PGW assigns a prefix that is unique within each 3GPP link that uses IPv6 stateless address auto configuration. This avoids the necessity to perform DAD at the network level for every address built by the mobile host. The GGSN/PGW always provides an IID to the cellular host for the purpose of configuring the link-local address and ensures the uniqueness of the IID on the link (i.e. no collisions between its own link-local address and the mobile host's one).

The 3GPP link model itself mitigates most of the known NDP-related Denial-of-Service attacks. In practice, the GGSN/PGW only needs to route all traffic to the mobile host that falls under the prefix assigned to it. As there is also a single host on the 3GPP link, there is no need to defend that IPv6 address.

See section 5 of IETF RFC 6459 [i.53] for a more detailed discussion on the 3GPP link model, NDP on it and the address configuration detail.

4.3.5 SeND and CGA

SEcureNeighbor Discovery (SeND), as described in IETF RFC 3971 [i.18], is a mechanism that was designed to secure ND messages. This approach involves the use of new NDP options to carry public key-based signatures. Cryptographically Generated Addresses (CGA), as described in IETF RFC 3972 [i.19], are used to ensure that the sender of a Neighbor Discovery message is the actual "owner" of the claimed IPv6 address. A new NDP option, the CGA option, was introduced and is used to carry the public key and associated parameters. Another NDP option, the RSA Signature option, is used to protect all messages relating to neighbor and Router discovery.

SeND protects against:

- Neighbor Solicitation/Advertisement Spoofing.
- Neighbor Unreachability Detection Failure.
- Duplicate Address Detection DoS Attack.
- Router Solicitation and Advertisement Attacks.
- Replay Attacks.
- Neighbor Discovery DoS Attacks.

SeND does NOT:

- Protect statically configured addresses.
- Protect addresses configured using fixed identifiers (i.e. EUI-64).
- Provide confidentiality for NDP communications.
- Compensate for an unsecured link - SEND does not require that the addresses on the link and Neighbor Advertisements correspond.

However, at this time and after many years after their specifications, CGA and SeND do not have wide support from generic operating systems; hence, their usefulness is limited and should not be relied upon.

4.4 Control Plane Security

4.4.1 Overview

IETF RFC 6192 [i.45] defines the router control plane. This definition is repeated here for the reader's convenience.

Modern router architecture design maintains a strict separation of forwarding and router control plane hardware and software. The router control plane supports routing and management functions. It is generally described as the router architecture hardware and software components for handling packets destined to the device itself as well as building and sending packets originated locally on the device. The forwarding plane is typically described as the router architecture hardware and software components responsible for receiving a packet on an incoming interface, performing a lookup to identify the packet's IP next hop and determine the best outgoing interface towards the destination, and forwarding the packet out through the appropriate outgoing interface.

While the forwarding plane is usually implemented in high-speed hardware, the control plane is implemented by a generic processor (named router processor RP) and cannot process packets at a high rate. Hence, this processor can be attacked by flooding its input queue with more packets than it can process. The control plane processor is then unable to process valid control packets and the router can lose OSPF or BGP adjacencies which can cause a severe network disruption.

The mitigation technique is:

- to drop non-legit control packet before they are queued to the RP (this can be done by a forwarding plane ACL); and

- to rate limit the remaining packets to a rate that the RP can sustain. Protocol specific protection should also be done (for example, a spoofed OSPFv3 packet could trigger the execution of the Dijkstra algorithm, therefore the number of Dijkstra execution should be also rate limited).

This clause will consider several classes of control packets:

- Control protocols: routing protocols: such as OSPFv3, BGP and by extension Neighbor Discovery and ICMP.
- Management protocols: SSH, SNMP, IPfix, etc.
- Packet exceptions: which are normal data packets which require a specific processing such as generating a packet-too-big ICMP message or having the hop-by-hop options header.

4.4.2 Control Protocols

This class includes OSPFv3, BGP, NDP and ICMP.

An ingress ACL to be applied on all the router interfaces SHOULD be configured such as:

- drop OSPFv3 (identified by Next-Header being 89) and RIPng (identified by UDP port 521) packets from a non link-local address;
- allow BGP (identified by TCP port 179) packets from all BGP neighbors and drop the others;
- allow all ICMP packets (transit and to the router interfaces).

NOTE: Dropping OSPFv3 packets which are authenticated by IPsec could be impossible on some routers whose ACL are unable to parse the IPsec ESP or AH extension headers. Rate limiting of the valid packets SHOULD be done. The exact configuration obviously depends on the power of the Route Processor.

4.4.3 Management Protocols

This class includes:

- SSH;
- SNMP;
- syslog;
- NTP;
- etc.

An Ingress ACL to be applied on all the router interfaces is supposed to be configured such as:

- Drop packets destined to the routers except those belonging to protocols which are used (for example, permit TCP 22 and drop all when only SSH is used).
- Drop packets where the source does not match the security policy, for example if SSH connections should only be originated from the NOC, then the ACL should permit TCP port 22 packets only from the NOC prefix.

Rate limiting of the valid packets is supposed to be done. The exact configuration obviously depends on the power of the Route Processor.

4.4.4 Packet Exceptions

This class covers multiple cases where a data plane packet is punted to the route processor because it requires specific processing:

- generation of an ICMP packet-too-big message when a data plane packet cannot be forwarded because it is too large;

- generation of an ICMP hop-limit-expired message when a data plane packet cannot be forwarded because its hop-limit field has reached 0;
- generation of an ICMP destination-unreachable message when a data plane packet cannot be forwarded for any reason;
- processing of the hop-by-hop options header, new implementations follow section 4.3 of IETF RFC 8200 [i.89] where this processing is optional; or
- more specific to some router implementation: an oversized extension header chain which cannot be processed by the hardware and force the packet to be punted to the generic router CPU.

On some routers, not everything can be done by the specialized data plane hardware which requires some packets to be 'punted' to the generic RP. This could include for example the processing of a long extension header chain in order to apply an ACL based on layer 4 information. IETF RFC 6980 [i.63] and more generally IETF RFC 7112 [i.70] highlights the security implications of oversized extension header chains on routers and updates the original IPv6 specifications, (IETF RFC 2460 [i.10]), such that the first fragment of a packet is required to contain the entire IPv6 header chain. Those changes are incorporated in the IPv6 standard (IETF RFC 8200 [i.89]).

An ingress ACL cannot help to mitigate a control plane attack using those packet exceptions. The only protection for the RP is to limit the rate of those packet exceptions forwarded to the RP, this means that some data plane packets will be dropped without any ICMP messages back to the source which may cause Path MTU holes.

In addition to limiting the rate of data plane packets queued to the RP, it is also important to limit the generation rate of ICMP messages both the save the RP but also to prevent an amplification attack using the router as a reflector.

4.5 Routing Security

4.5.1 Authenticating Neighbors/Peers

A basic element of routing is the process of forming adjacencies, neighbor, or peering relationships with other routers. From a security perspective, it is very important to establish such relationships only with routers and/or administrative domains that one trusts. A traditional approach has been to use MD5 HMAC, which allows routers to authenticate each other prior to establishing a routing relationship.

OSPFv3 can rely on IPsec to fulfil the authentication function. However, it should be noted that IPsec support is not standard on all routing platforms. In some cases, this requires specialized hardware that offloads crypto over to dedicated ASICs or enhanced software images (both of which often come with added financial cost) to provide such functionality. An added detail is to determine whether OSPFv3 IPsec implementations use AH or ESP-Null for integrity protection. In early implementations all OSPFv3 IPsec configurations relied on AH since the details were not specified in IETF RFC 5340 [i.35] or IETF RFC 2740 [i.12] that was obsoleted by the former.

IETF RFC 7166 [i.72] changes OSPFv3's reliance on IPsec by appending an authentication trailer to the end of the OSPFv3 packets; it does not specifically authenticate the specific originator of an OSPFv3 packet; rather, it allows a router to confirm that the packet has indeed been issued by a router that had access to the shared authentication key.

With all authentication mechanisms, operators should confirm that implementations can support re-keying mechanisms that do not cause outages. There have been instances where any re-keying cause outages and therefore the tradeoffs between utilizing this functionality need to be weighed against the protection it provides.

4.5.2 Securing Routing Updates Between Peers

IPv6 initially mandated the provisioning of IPsec capability in all nodes. Theoretically it is possible, and recommended, that communication between two IPv6 nodes, including routers exchanging routing information be encrypted using IPsec. In practice however, deploying IPsec is not always feasible given hardware and software limitations of various platforms deployed, as described in clause 4.5.1.

4.5.3 Route Filtering

Route filtering policies will be different depending on whether they pertain to edge route filtering vs. internal route filtering. At a minimum, IPv6 routing policy as it pertains to routing between different administrative domains should aim to maintain parity with IPv4 from a policy perspective e.g.:

- Filter internal-use, non-globally routable IPv6 addresses at the perimeter.
- Discard packets from and to bogon and reserved space (see IETF RFC 8190 [i.86]).
- Configure ingress route filters that validate route origin, prefix ownership, etc., through the use of various routing databases, e.g. RADB. There is additional work being done in this area to formally validate the origin ASs of BGP announcements in IETF RFC 6810 [i.61].

4.6 Logging/Monitoring

4.6.1 Overview

In order to perform forensic research in case of any security incident or to detect abnormal behaviours, network operators should log multiple pieces of information.

This includes:

- logs of all applications when available (for example web servers);
- use of IP Flow Information Export (IETF RFC 7011 [i.64]) also known as IPfix;
- use of SNMP MIB (IETF RFC 4293 [i.21]);
- use of the Neighbor cache;
- use of stateful DHCPv6 (IETF RFC 8415 [i.90]) lease cache, especially when a relay agent (IETF RFC 6221 [i.46]) in layer-2 switches is used;
- use of Source Address Validation Improvement (SAVI) (IETF RFC 7039 [i.66]) events, especially the binding of an IPv6 address to a MAC address and a specific switch or router interface;
- use of RADIUS (IETF RFC 2866 [i.15]) for accounting records.

Please note that there are privacy issues related to how those logs are collected, kept and safely discarded. Operators are urged to check their country legislation.

All those pieces of information will be used for:

- Forensic (clause 4.6.3.1) investigations such as who did what and when?
- Correlation (clause 4.6.3.3): which IP addresses were used by a specific node (assuming the use of privacy extensions addresses (IETF RFC 4941 [i.34])?
- Inventory (clause 4.6.3.2): which IPv6 nodes are on my network?
- Abnormal behaviour detection (clause 4.6.3.4): unusual traffic patterns are often the symptoms of an abnormal behaviour which is in turn a potential attack (denial of services, network scan, a node being part of a botnet, etc.).

4.6.2 Data Sources

4.6.2.1 Logs of Applications

Those logs are usually text files where the remote IPv6 address is stored in all characters (not binary). This can complicate the processing since one IPv6 address, 2001:db8::1 can be written in multiple ways such as:

- 2001:DB8::1 (in uppercase);
- 2001:0db8::0001 (with leading 0); and
- many other ways including the reverse DNS mapping into a FQDN (which should not be trusted).

IETF RFC 5952 [i.37] explains this problem in detail and recommends the use of a single canonical format (in short use lower case and suppress leading 0). This memo recommends the use of canonical format (IETF RFC 5952 [i.37]) for IPv6 addresses in all possible cases. If the existing application cannot log under the canonical format, then this memo recommends the use an external program in order to canonicalize all IPv6 addresses.

For example, this Perl script can be used:

```
#!/usr/bin/perl -w
use strict ;
use warnings ;
use Socket ;
use Socket6 ;

my (@words, $word, $binary_address) ;

   ## go through the file one line at a time
   while (my $line = <STDIN>) {
     chomp $line;
     foreach my $word (split /[\s+]/, $line) {
       $binary_address = inet_pton AF_INET6, $word ;
       if ($binary_address) {
         print inet_ntop AF_INET6, $binary_address ;
       } else {
print $word ;
       }
       print " " ;
     }
print "\n" ;
   }
```

4.6.2.2 IP Flow Information Export by IPv6 Routers

IPfix (IETF RFC 7012 [i.65]) defines some data elements that are useful for security:

- in section 5.4 (IP Header fields): nextHeaderIPv6 and sourceIPv6Address;
- in section 5.6 (Sub-IP fields) sourceMacAddress.

Moreover, IPfix is very efficient in terms of data handling and transport. It can also aggregate flows by a key such as sourceMacAddress in order to have aggregated data associated with a specific sourceMacAddress. This memo recommends the use of IPfix and aggregation on nextHeaderIPv6, sourceIPv6Address and sourceMacAddress.

4.6.2.3 SNMP MIB by IPv6 Routers

IETF RFC 4293 [i.21] defines a Management Information Base (MIB) for the two address families of IP. This memo recommends the use of:

- ipIfStatsTable table which collects traffic counters per interface;
- ipNetToPhysicalTable table which is the content of the Neighbor cache, i.e. the mapping between IPv6 and data-link layer addresses.

4.6.2.4 Neighbor Cache of IPv6 Routers

The neighbor cache of routers contains all mappings between IPv6 addresses and data-link layer addresses. It is usually available by two means:

- the SNMP MIB (clause 4.6.2.3) as explained above;
- using NETCONF (IETF RFC 6241 [i.47]) to collect the state of the neighbor cache;
- also, by connecting over a secure management channel (such as SSH) and explicitly requesting a neighbor cache dump via the Command Line Interface or any other monitoring mechanism.

The neighbor cache is highly dynamic as mappings are added when a new IPv6 address appears on the network (could be quite often with privacy extension addresses (IETF RFC 4941 [i.34]) or when they are removed when the state goes from UNREACH to removed (the default time for a removal per Neighbor Unreachability Detection (IETF RFC 4861 [i.31]) algorithm is 38 seconds for a typical user host).

This is an important source of information because it is trivial (on a switch not using the SAVI [i.66] algorithm) to defeat the mapping between data-link layer address and IPv6 address. The previous statement can be rephrased as below:

- having access to the current and past content of the neighbor cache has a paramount value for forensic and audit trail.

Using the approach of one /64 per host (clause 4.1.8) replaces the neighbor cache dumps by a mere caching of the allocated /64 prefix when combined with strict enforcement rule on the router and switches to prevent IPv6 spoofing.

4.6.2.5 Stateful DHCPv6 Lease

In some networks, IPv6 addresses are managed by stateful DHCPv6 server (IETF RFC 8415 [i.90]) that leases IPv6 addresses to clients. It is indeed quite similar to DHCP for IPv4 so it can be tempting to use this DHCP lease file to discover the mapping between IPv6 addresses and data-link layer addresses as it was usually done in the IPv4 era. It is not so easy in the IPv6 era because not all nodes will use DHCPv6 (there are nodes which can only do stateless auto configuration) but also because DHCPv6 clients are identified not by their hardware-client address as in IPv4 but by a DHCP Unique ID (DUID) which can have several formats: some being the data-link layer address, some being data-link layer address pretended with time information or even an opaque number which is useless for operation security. Moreover, when the DUID is based on the data-link address, this address can be of any interface of the client (such as the wireless interface while the client actually uses its wired interface to connect to the network).

If a lightweight DHCP relay agent (IETF RFC 6221 [i.46]) is used in the layer-2 switches, then the DHCP server also receives the Interface-ID information which could be save in order to identify the interface of the switches which received a specific leased IPv6 address. Also, if a 'normal' (not lightweight) relay agent adds the data-link layer address in the option for Relay Agent Remote-ID (IETF RFC 4649 [i.28] or IETF RFC 6939 [i.62]), then the DHCPv6 server can keep track of the data-link and leased IPv6 addresses.

In short, the DHCPv6 lease file is less interesting than in the IPv4 era. DHCPv6 servers that keep the relayed data-link layer address in addition to the DUID in the lease file do not suffer from this limitation.

The mapping between data-link layer address and the IPv6 address can be secured by using switches implementing the SAVI (IETF RFC 7513 [i.76]) algorithms. Of course, this also requires that data-link layer address is protected by using layer-2 mechanism such as (IEEE 802.1X [i.91]).

4.6.2.6 RADIUS Accounting Log

For interfaces where the user is authenticated via a RADIUS (IETF RFC 2866 [i.15]) server, and if RADIUS accounting is enabled, then the RADIUS server receives accounting Acct-Status-Type records at the start and at the end of the connection which include all IPv6 (and IPv4) addresses used by the user. This technique can be used notably for Wi-Fi networks with Wi-Fi Protected Address (WPA) or any other IEEE 802.1X [i.91] wired interface on an Ethernet switch.

4.6.2.7 Other Data Sources

There are other data sources that can be kept exactly as in the IPv4 network:

- historical mapping of IPv6 addresses to users of remote access VPN;
- historical mapping of MAC address to switch interface in a wired network.

4.6.3 Use of Collected Data

4.6.3.1 Forensic and User Accountability

The forensic use case is when the network operator needs locate an IPv6 address that was present in the network at a certain time or is still currently in the network.

The source of information can be, in decreasing order, neighbor cache, DHCP lease file. Then, the procedure is:

1) based on the IPv6 prefix of the IPv6 address find the router(s) which is(are) used to reach this prefix (assuming that anti-spoofing mechanisms are used);
2) based on this limited set of routers, on the incident time and onIPv6 address to retrieve the data-link address from live neighbor cache, from the historical data of the neighbor cache or from SAVI events;
3) based on the incident time and on the IPv6 address, retrieve the data-link address from the DHCP lease file (clause 4.6.2.5);
4) based on the data-link layer address, look-up on which switch interface was this data-link layer address. In the case of wireless LAN, the RADIUS log should have the mapping between user identification and the MAC address. If a Configuration Management Data Base (CMDB) is used, the mappings between the data-link layer address and a switch port.

At the end of the process, the interface the host originating malicious activity or the username which was abused for malicious activity has been determined.

4.6.3.2 Inventory

IETF RFC 7707 [i.80] is about the difficulties for an attacker to scan an IPv6 network due to the vast number of IPv6 addresses per link (and why in some case it can still be done). While the huge addressing space can sometime be perceived as a 'protection', it also makes the inventory task difficult in an IPv6 network while it was trivial to do in an IPv4 network (a simple enumeration of all IPv4 addresses, followed by a ping and a TCP/UDP port scan). Getting an inventory of all connected devices is of prime importance for a secure operation of a network.

There are many ways to do an inventory of an IPv6 network.

The first technique is to use the IPfix information and extract the list of all IPv6 source addresses to find all IPv6 nodes that sent packets through a router. This is very efficient but alas will not discover silent node that never transmitted such packets.

The second way is again to use the collected neighbor cache content to find all IPv6 addresses in the cache. This process will also discover all link-local addresses. See clause 4.6.2.4.

Another way works only for local network, it consists in sending an ICMP ECHO_REQUEST to the link-local multicast address ff02::1 which is all IPv6 nodes on the network. All nodes should reply to this ECHO_REQUEST per IETF RFC 4443 [i.27].

Other techniques involve obtaining data from DNS, parsing log files, leveraging service discovery such as mDNS IETF RFC 6762 [i.59] and IETF RFC 6763 [i.60].

Enumerating DNS zones, especially looking at reverse DNS records and CNAMES, is another common method employed by various tools. As already motioned in IETF RFC 7707 [i.80], this allows an attacker to prune the IPv6 reverse DNS tree, and hence enumerate it in a feasible time. Furthermore, authoritative servers that allow zone transfers (AXFR) may be a further information source.

4.6.3.3 Correlation

In an IPv4 network, it is easy to correlate multiple logs, for example to find events related to a specific IPv4 address. A simpleUnix grep command was enough to scan through multiple text-based files and extract all lines relevant to a specific IPv4 address.

In an IPv6 network, this is slightly more difficult because different character strings can express the same IPv6 address. Therefore, the simple Unix grep command cannot be used. Moreover, an IPv6 node can have multiple IPv6 addresses.

In order to do correlation in IPv6-related logs, it is advised to have all logs with canonical IPv6 addresses. Then, the neighbor cache current (or historical) data set can be searched to find the data-link layer address of the IPv6 address. Then, the current and historical neighbor cache data sets can be searched for all IPv6 addresses associated to this data-link layer address: this is the search set. The last step is to search in all log files (containing only IPv6 address in canonical format) for any IPv6 addresses in the search set.

Moreover, IETF RFC 7934 [i.84] recommends to use multiple IPv6 addresses per prefix, so, the correlation can also be done among those multipleIPv6 addresses, for example by discovering in the NDP cache (clause 4.6.2.4) all IPv6 addresses associated with the same MAC address and interface.

4.6.3.4 Abnormal Behaviour Detection

Abnormal behaviours (such as network scanning, spamming, denial of service) can be detected in the same way as in an IPv4 network:

- sudden increase of traffic detected by interface counter (SNMP) or by aggregated traffic from IPfix records (IETF RFC 7012 [i.65]);
- change of traffic pattern (number of connections per second, number of connection per host, etc.) with the use of IPfix (IETF RFC 7012 [i.65]).

4.6.4 Summary

While some data sources (IPfix, MIB, switch CAM tables, logs, etc.) used in IPv4 are also used in the secure operation of an IPv6 network, the DHCPv6 lease file is less reliable and the neighbor cache is of prime importance.

The fact that there are multiple ways to express in a character string the same IPv6 address renders the use of filters mandatory when correlation need to be done.

4.7 Transition/Coexistence Technologies

4.7.1 Dual Stack

Dual stack is often the first deployment choice for network operators. Dual stacking the network offers some advantages over other transition mechanisms. Firstly, the impact on existing IPv4 operations is reduced. Secondly, in the absence of tunnels or address translation, the IPv4 and IPv6 traffics are native (easier to observe and secure) and should have the same network processing (path, quality of service, etc.). Dual stack allows operators to gradually turn IPv4 operations down when IPv6 network is ready for prime time. On the other hand, the operators have to manage two networks with the added complexities.

From an operational security perspective, this now means that operators have twice the exposure. One needs to think about protecting both protocols now. At a minimum, the IPv6 portion of a dual stacked network should maintain parity with IPv4 from a security policy point of view. Typically, the following methods are employed to protect IPv4 networks at the edge:

- ACLs to permit or deny traffic.
- Firewalls with stateful packet inspection.

It is recommended that these ACLs and/or firewalls be additionally configured to protect IPv6 communications. Also, given the end-to- end connectivity that IPv6 provides, it is also recommended that hosts be fortified against threats. General device hardening guidelines are provided in clause 4.8.

For many years, all host operating systems have IPv6 enabled by default, so, it is possible even in an 'IPv4-only' network to attack layer-2 adjacent victims over IPv6 link-local address or over a global IPv6 address is rogue RA or rogue DHCPv6 addresses are provided by an attacker.

4.7.2 Transition Mechanisms

4.7.2.1 Security issues

There are many tunnels used for specific use cases. Except when protected by IPsec (IETF RFC 4301 [i.22]), all those tunnels have a couple of security issues (most of them because they are tunnels and are described in IETF RFC 6169 [i.44]:

- tunnel injection: a malevolent person knowing a few pieces of information (for example the tunnel endpoints and the used protocol) can forge a packet which looks like a legit and valid encapsulated packet that will gladly be accepted by the destination tunnel endpoint, this is a specific case of spoofing;
- traffic interception: no confidentiality is provided by the tunnel protocols (without the use of IPsec), therefore anybody on the tunnel path can intercept the traffic and have access to the clear-text IPv6 packet; combined with the absence of authentication, a man in the middle attack can also be mounted;
- service theft: as there is no authorization, even a non authorized user can use a tunnel relay for free (this is a specific case of tunnel injection);
- reflection attack: another specific use case of tunnel injection where the attacker injects packets with an IPv4 destination address not matching the IPv6 address causing the first tunnel endpoint to re-encapsulate the packet to the destination. Hence, the final IPv4 destination will not see the original IPv4 address but only one IPv4 address of the relay router;
- bypassing security policy: if a firewall or an IPS is on the path of the tunnel, then it will probably neither inspect nor detect a malevolent IPv6 traffic contained in the tunnel.

To mitigate the bypassing of security policies, it is recommended to block all default configuration tunnels by denying all IPv4 traffic matching:

- IP protocol 41: this will block ISATAP, 6to4, 6rd as well as 6in4 (clause 4.7.2.2) tunnels;
- IP protocol 47: this will block GRE tunnels;
- UDP protocol 3544: this will block the default encapsulation of Teredo tunnels.

Ingress filtering (IETF RFC 2827 [i.14]) should also be applied on all tunnel endpoints if applicable to prevent IPv6 address spoofing.

As several of the tunnel techniques share the same encapsulation(i.e. IPv4 protocol 41) and embed the IPv4 address in the IPv6 address, there are a set of well-known looping attacks described in IETF RFC 6324 [i.51], this IETF RFC also proposes mitigation techniques.

4.7.2.2 Site-to-Site Static Tunnels

Site-to-site static tunnels are described in IETF RFC 2529 [i.11] and in GRE (IETF RFC 2784 [i.13]). As the IPv4 endpoints are statically configured and are not dynamic they are slightly more secure (bi-directional service theft is mostly impossible) but traffic interception and tunnel injection are still possible. Therefore, the use of IPsec (IETF RFC 4301) [i.22] in transport mode and protecting the encapsulated IPv4 packets is recommended for those tunnels. Alternatively, IPsec in tunnel mode can be used to transport IPv6 traffic over a non-trusted IPv4 network.

4.7.2.3 6PE and 6VPE

Organizations using MPLS in their core can also use 6PE (IETF RFC 4798 [i.30]) and 6VPE (IETF RFC 4659 [i.29]) to enable IPv6 access over MPLS. As 6PE and 6VPE are really similar to BGP/MPLS IP VPN described in IETF RFC 4364 [i.25], the security of these networks is also similar to the one described in IETF RFC 4381 [i.26]. It relies on:

- Address space, routing and traffic separation with the help of VRF (only applicable to 6VPE).
- Hiding the IPv4 core, hence removing all attacks against P-routers.
- Securing the routing protocol between CE and PE, in the case of 6PE and 6VPE, link-local addresses (see IETF RFC 7404 [i.74]) can be used and as these addresses cannot be reached from outside of the link, the security of 6PE and 6VPE is even higher than the IPv4 BGP/MPLS IP VPN.

4.7.2.4 Mapping of Address and Port

With the encapsulation and translation versions of mapping of Address and Port MAP-E (IETF RFC 7597 [i.77]) and MAP-T (IETF RFC 7599 [i.78]), the access network is purely an IPv6 network and MAP protocols are used to give IPv4 hosts on the subscriber network, access to IPv4 hosts on the Internet. The subscriber router does stateful operations in order to map all internal IPv4 addresses and layer-4 ports to the IPv4 address and the set of layer-4 ports received through MAP configuration process. The SP equipment always does stateless operations (either decapsulation or stateless translation). Therefore, as opposed to clause 4.7.3.3 there is no state-exhaustion DoS attack against the SP equipment because there is no state and there is no operation caused by a new layer-4 connection (no logging operation).

The SP MAP equipment is required to implement all the security considerations of IETF RFC 7597 [i.77]; notably, ensuring that the mapping of the IPv4 address and port are consistent with the configuration. As MAP has a predictable IPv4 address and port mapping, the audit logs are easier to manage.

4.7.3 Translation Mechanisms

4.7.3.1 Carrier-Grade NAT (CGN)

Carrier-Grade NAT (CGN), also called NAT444 CGN or Large Scale NAT (LSN) or SP NAT is described in IETF RFC 6264 [i.48] and is utilized as an interim measure to prolong the use of IPv4 in a large service provider network until the provider can deploy and effective IPv6 solution. IETF RFC 6598 [i.56] requested a specific IANA allocated /10 IPv4 address block to be used as address space shared by all access networks using CGN. This has been allocated as 100.64.0.0/10.

Section 13 of IETF RFC 6269 [i.49] lists some specific security-related issues caused by large scale address sharing. The Security Considerations section of IETF RFC 6598 [i.56] also lists some specific mitigation techniques for potential misuse of shared address space. Some Law Enforcement Agencies have identified CGN as impeding their cyber-crime investigations (for example Europol press release on CGN [i.1]). Many translation techniques (NAT64, DS-lite, etc.) have the same security issues as CGN when one part of the connection is IPv4-only.

IETF RFC 6302 [i.50] has recommendations for Internet-facing servers to also log the source TCP or UDP ports of incoming connections in an attempt to help identify the users behind such a CGN.

IETF RFC 7422 [i.75] suggests the use of deterministic address mapping in order to reduce logging requirements for CGN. The idea is to have an algorithm mapping back and forth the internal subscriber to public ports.

4.7.3.2 NAT64/DNS64

Stateful NAT64 translation (IETF RFC 6146 [i.41]) allows IPv6-only clients to contact IPv4 servers using unicast UDP, TCP, or ICMP. It can be used in conjunction with DNS64 (IETF RFC 6147 [i.42]), a mechanism which synthesizes AAAA records from existing A records. There is also a stateless NAT64 (IETF RFC 7915 [i.83]) which is similar for the security aspects with the added benefit of being stateless, so, less prone to a state exhaustion attack.

The Security Consideration section of IETF RFC 6146 [i.41] and IETF RFC 6147 [i.42] list the comprehensive issues. A specific issue with the use of NAT64 is that it will interfere with most IPsec deployments unless UDP encapsulation is used. DNS64 has an incidence on DNSSEC see section 3.1 of IETF RFC 7050 [i.68].

4.7.3.3 DS-Lite

Dual-Stack Lite (DS-Lite) (IETF RFC 6333 [i.52]) is a transition technique that enables a service provider to share IPv4 addresses among customers by combining two well-known technologies:

- IP in IP (IPv4-in-IPv6); and
- Network Address and Port Translation (NAPT).

Security considerations with respect to DS-Lite mainly revolve around logging data, preventing DoS attacks from rogue devices (as the AFTR function is stateful) and restricting service offered by the AFTR only to registered customers.

Section 11 of IETF RFC 6333 [i.52] describes important security issues associated with this technology.

4.8 General Device Hardening

There are many environments which rely too much on the network infrastructure to disallow malicious traffic to get access to critical hosts. In new IPv6 deployments it has been common to see IPv6 traffic enabled but none of the typical access control mechanisms enabled for IPv6 device access. With the possibility of network device configuration mistakes and the growth of IPv6 in the overall Internet it is important to ensure that all individual devices are hardened against miscreant behaviour.

The following guidelines should be used to ensure appropriate hardening of the host, be it an individual computer or router, firewall, load-balancer, server, device, etc.:

- Restrict access to the device to authorized individuals.
- Monitor and audit access to the device.
- Turn off any unused services on the end node.
- Understand which IPv6 addresses are being used to source traffic and change defaults if necessary.
- Use cryptographically protected protocols for device management if possible (SNMPv3, SSH, TLS, etc.).
- Use host firewall capabilities to control traffic that gets processed by upper layer protocols.
- Use virus scanners to detect malicious programs.

5 Enterprises Specific Security Considerations

5.1 External Security Considerations

The external aspect deals with providing security at the edge or perimeter of the enterprise network where it meets the service providers' network. This is commonly achieved by enforcing a security policy either by implementing dedicated firewalls with stateful packet inspection or a router with ACLs. A common default IPv4 policy on firewalls that could easily be ported to IPv6 is to allow all traffic outbound while only allowing specific traffic, such as established sessions, inbound (see also IETF RFC 6092 [i.38]). Here are a few more things that could enhance the default policy:

- Filter internal-use IPv6 addresses at the perimeter.
- Discard packets from and to bogon and reserved space.
- Accept certain ICMPv6 messages to allow proper operation of ND and PMTUD, see also IETF RFC 4890 [i.33].
- Filter specific extension headers by accepting only the required ones (white list approach) such as ESP, AH (not forgetting the required transport layers: ICMP, TCP, UDP, etc.), where possible at the edge and possibly inside the perimeter; see also IETF draft-ietf-opsec-ipv6-eh-filtering [i.4].

- Filter packets having an illegal IPv6 headers chain at the perimeter (and possible inside as well), see clause 4.2.
- Filter unneeded services at the perimeter.
- Implement anti-spoofing.
- Implement appropriate rate-limiters and control-plane policies.

5.2 Internal Security Considerations

The internal aspect deals with providing security inside the perimeter of the network, including the end host. The most significant concerns here are related to Neighbor Discovery. At the network level, it is recommended that all security considerations discussed in clause 4.3 be reviewed carefully and the recommendations be considered in-depth as well.

Hosts need to be hardened directly through security policy to protect against security threats. The host firewall default capabilities have to be clearly understood, especially 3rd party ones which can have different settings for IPv4 or IPv6 default permit/deny behaviour. In some cases, 3rd party firewalls have no IPv6 support whereas the native firewall installed by default has it. General device hardening guidelines are provided in clause 4.8.

It should also be noted that many hosts still use IPv4 for transport for things like RADIUS, TACACS+, SYSLOG, etc. This will require some extra level of due diligence on the part of the operator.

6 Service Providers Security Considerations

6.1 BGP

The threats and mitigation techniques are identical between IPv4 and IPv6. Broadly speaking they are:

- Authenticating the TCP session.
- TTL security (which becomes hop-limit security in IPv6).
- Prefix Filtering.

These are explained in more detail in clause 4.5.

RTBH (IETF RFC 5635 [i.36]) works identically in IPv4 and IPv6. IANA has allocated 100::/64 as discard prefix (IETF RFC 6666 [i.58]) for the purpose of facilitating IPv6 remote triggered black hole filtering and routing.

6.2 Transition Mechanism

SP will typically use transition mechanisms such as 6rd, 6PE, MAP, DS-Lite which have been analysed in clause 4.7.2.

6.3 Lawful Intercept

The Lawful Intercept requirements are similar for IPv6 and IPv4architectures and will be subject to the laws enforced in varying geographic regions. The local issues with each jurisdiction can make this challenging and both corporate legal and privacy personnel should be involved in discussions pertaining to what information gets logged and what the logging retention policies will be.

The target of interception will usually be a residential subscriber (e.g. his/her PPP session or physical line or CPE MAC address). With the absence of NAT on the CPE, IPv6 has the provision to allow for intercepting the traffic from a single host (a /128 target) rather than the whole set of hosts of a subscriber (which could be a /48, a /60 or /64).

In contrast, in mobile environments, since the 3GPP specifications allocate a /64 per device, it may be sufficient to intercept traffic from the /64 rather than specific /128's (since each time the device powers up it gets a new IID).

A sample architecture which was written for informational purposes is found in IETF RFC 3924 [i.17].

7 Residential Users Security Considerations

The IETF Homenet working group is working on how IPv6 residential network should be done; this obviously includes operational security considerations; but this is still work in progress.

Residential users have usually less experience and knowledge about security or networking. As most of the recent hosts, smart phones, tablets have all IPv6 enabled by default, IPv6 security is important for those users. Even with an IPv4-only ISP, those users can get IPv6 Internet access with the help of Teredo tunnels. Several peer-to-peer programs (notably BitTorrent) support IPv6 and those programs can initiate a Teredo tunnel through the IPv4 residential gateway, with the consequence of making the internal host reachable from any IPv6 host on the Internet. It is therefore recommended that all host security products (personal firewall, etc.) are configured with a dual-stack security policy.

If the Residential Gateway has IPv6 connectivity, IETF RFC 7084 [i.69] defines the requirements of an IPv6 CPE and does not take position on the debate of default IPv6 security policy as defined in IETF RFC 6092 [i.38]:

- outbound only: allowing all internally initiated connections and block all externally initiated ones, which is a common default security policy enforced by IPv4 Residential Gateway doing NAT-PT but it also breaks the end-to-end reachability promise of IPv6. IETF RFC 6092 [i.38] lists several recommendations to design such a CPE;
- open/transparent: allowing all internally and externally initiated connections, therefore restoring the end-to-end nature of the Internet for the IPv6 traffic but having a different security policy for IPv6 than for IPv4.

IETF RFC 6092 [i.38] REC-49 states that a choice can be given to the user to select one of those two policies.

There is also an alternate solution which has been deployed notably by Swisscom: open to all outbound and inbound connections at the exception of a handful of TCP and UDP ports known as vulnerable.

8 Cybersecurity

8.1 Introduction

Cybersecurity is a very balanced mix of policy and technology. However, according the finding obtained from the European Commission funded research project SAINT, it is abundantly clear that Cybersecurity is more of a policy while technology is just a tool to empower the cybersecurity policy to exercise the cybersecurity laws that should be prescribed in the constriction of any country. Cybersecurity is agnostic of any technology and applies to all technologies.

From the European Commission funded project SAINT's own findings, see Figure 1, Finland ranks as one the most cybersecure nations in the world with a host exploit of just 14,3 from a scale of 1 000 and ranks 221 country among the 224 investigated countries.

NOTE: Lower number corresponds to higher cyber threats mitigation.

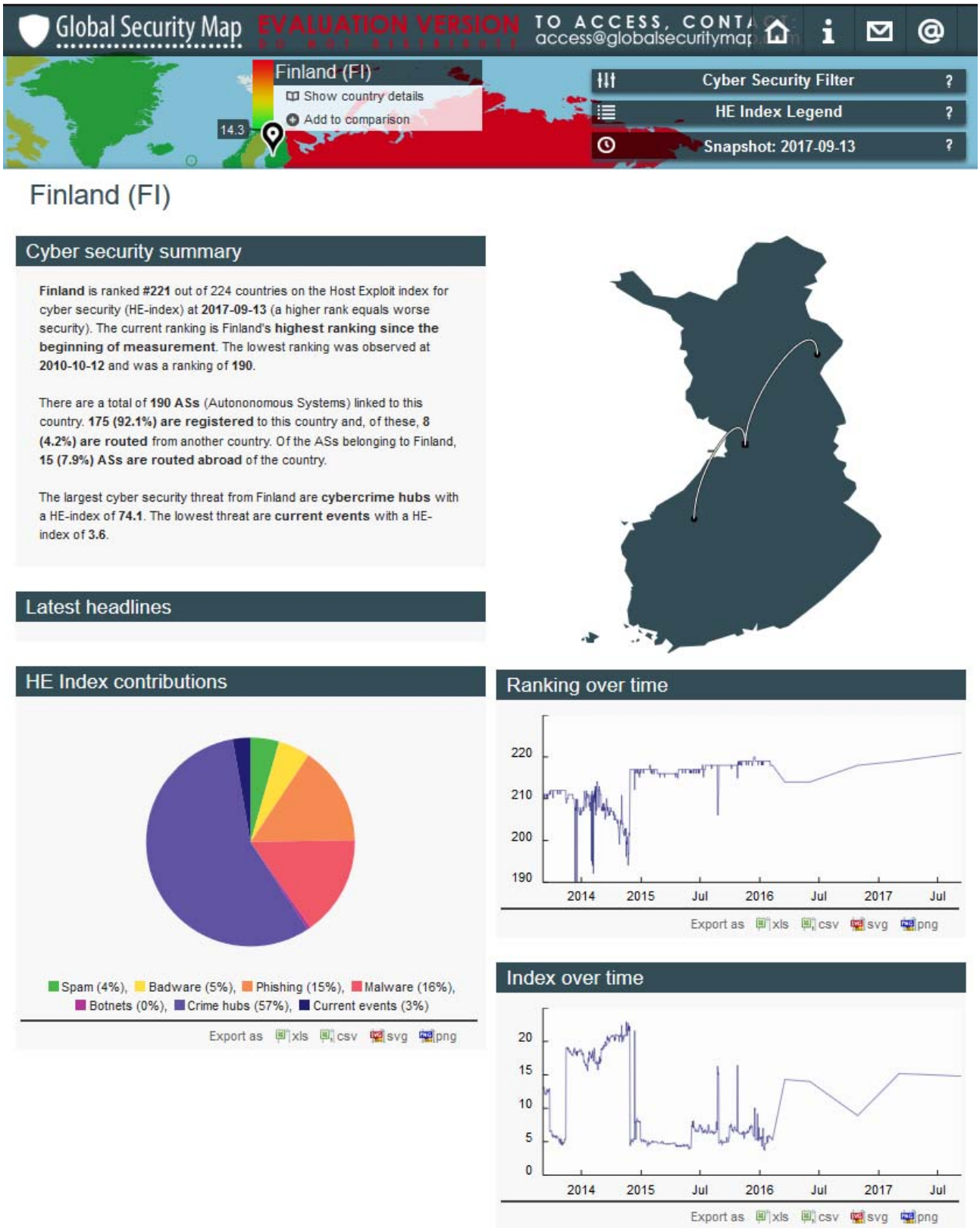

Figure 1: SAINT globalsecuritymap.com

The most important reason for this highly positive model is that the Finnish Transport and Communications Agency (Traficom, as a regulator, is the prime interface for cybersecurity empowered to issue direct instructions to the ISPs. It also cooperates with industry to achieve the same level of service, a Cybersecurity as a Service (CaaS). The second important vehicle is that the ISPs are empowered by the Finnish legislation to take actions, such as, for example, automatic prevention or limitation of message transmission or reception, in order to safeguard information security of their networks and services. This helps in directly stopping hacking of hostings and individuals.

Another viewpoint from OECD shows Finland as the lowest on a scale of businesses that have encountered IT security problems (see Figure 2).

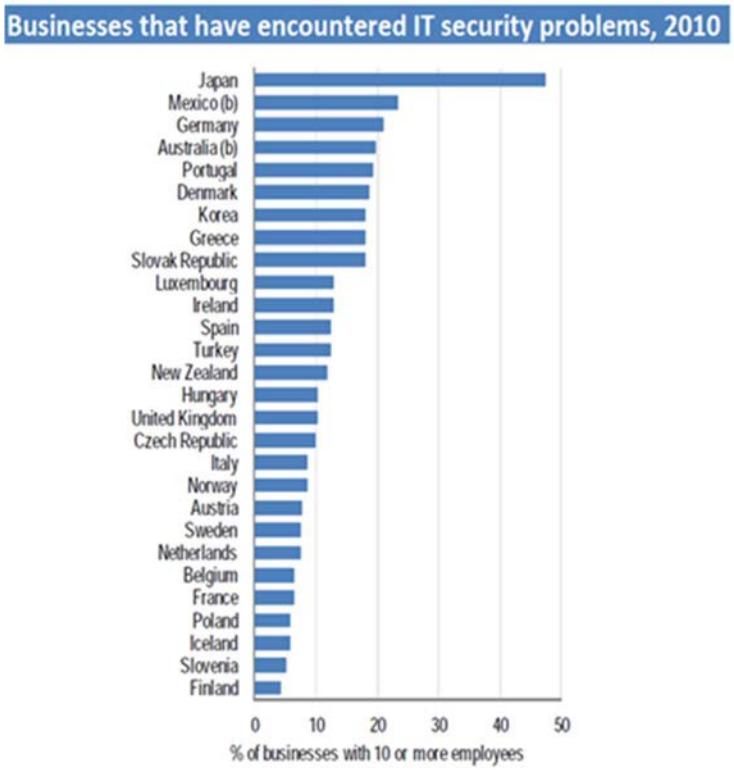

Figure 2: OECD 2010

Traficom boldly monitors and promotes communications markets and services in the interests of the general public, business and industry. It also ensures that everyone has access to versatile, effective and secure communications in Finland. The authority's activities contribute to a reliable information society and secure the status and rights of users of communications services by ensuring that society, business and citizens have access to, for example:

- fast and reliable telecommunications connections;
- effective communications markets;
- efficiently-used radio frequencies, numbers and codes;
- reasonably-priced communications services of good quality;
- versatile electronic media services;
- information on development, pricing and service level of communications markets/services.

Traficom maintains an overview of the functionality of electronic communications networks and information security, and reports of eventual information security threats. Another objective is to increase the awareness of information security in homes and companies for example by means of guidelines. Traficom also ensures the compatibility of communications networks and services.

The centralized administration of radio frequencies ensures that frequencies are used in as effective and disturbance-free manner as possible. This responsibility is significant both at national and international level.

Traficom supervises the .fi domain name registrars' technical information security and maintains the fi-domain name register. Traficom also grants telecoms operators the numbers and codes they need. This ensures that numbers are equally accessible to all telecom operators, that there are enough numbers available and that the numbers are uniform.

Also, the authority enhances the provision of versatile electronic media services. Regarding these duties, Traficom performs the following functions:

- collects license fees;
- grants programming licenses for TV and radio;
- monitors the content and advertising of TV and radio programs;
- monitors the functionality and service level of universal broadband, telephone and postal services;
- handles undeliverable postal items.

Traficom functions under the Ministry of Transport and Communications Finland. Traficom is responsible for steering and supervising communication networks and services together with other operators in the field. The aims are to ensure that new service providers can enter the market, there is sufficient spectrum for new needs, and consumer rights are respected. Traficom provides government services related to information security for citizens, businesses and the public administration.

Traficom develops and monitors the operational reliability and security of communications networks and services. It produces and publishes situational awareness of cyber security and acts as the National Communications Security Authority.

8.2 National Cyber Security Centre Finland, NCSC-FI

The National Cyber Security Centre Finland (NCSC-FI) at Traficom has been in operation since 1 January 2014. CERT (Computer Emergency Response Team Finland), NCSA (National Communications Security Authority Finland) and NRA (National Regulatory Authority) duties are part of the NCSC-FI's information security services. To support its operations, the NCSC-FI also maintains nationwide situational awareness of cyber security.

The NCSC-FI is a national information security authority. It develops and monitors the operational reliability and security of communications networks and services. NCSC-FI can mandate telecommunications providers to take corrective action to support incident response.

Its CERT duties consist of preventing, detecting and resolving security breaches, as well as of informing about the information security threats. The Centre's NCSA duties include the responsibility for security matters related to electronic transfer and processing of classified information. The NRA duties aim to safeguard via guidance and supervision the confidentiality of electronic communication as well as operation and information security of Finnish networks and services.

The Centre's operations aim at ensuring that public communications networks and communications services are safe and interference-free, as well as securing critical societal functions. In accordance with the agreement entered with the National Emergency Supply Agency (NESA), the NCSC-FI is, for its part, responsible for ensuring the functionality of technical systems critical to the security of supply. The NCSC-FI wants to develop and diversify its information security services by means of e.g. development work and extensive partnership networks.

The English name National Cyber Security Centre Finland is intended for international use. In Finnish and Swedish, the Centre is called Kyberturvallisuuskeskus and Cybersäkerhetscentret respectively. The operational names CERT-FI and NCSA-FI are used in international stakeholder cooperation in accordance with established practice.

NCSC-FI provides various services that are mostly free of charge and belong to everyone. Some of these services are aimed especially at public administration and critical infrastructures. The organization defines 3 groups of its services, namely *situational awareness and network coordination*, *detection and assistance* and *other authoritative services* (Figure 3).

The first group of services include situational awareness, guidelines and recommendations, vulnerability coordination, cooperation networks and cyber-exercises. The *situational awareness* service implements proactive assistance via dissemination through mailing lists and online publications. NCSC-FI produces alerts, bulletins, vulnerability reports and articles. All incident reports are divided on the following categories: vulnerabilities, malware, spam, system break-in, denial-of-service attack, information security problems and social engineering. NCSC-FI also provides guidelines, advice, and tips (*guidelines and recommendations* service). These materials are intended to organizations, individuals as well as service administrators and they are available on organization's website.

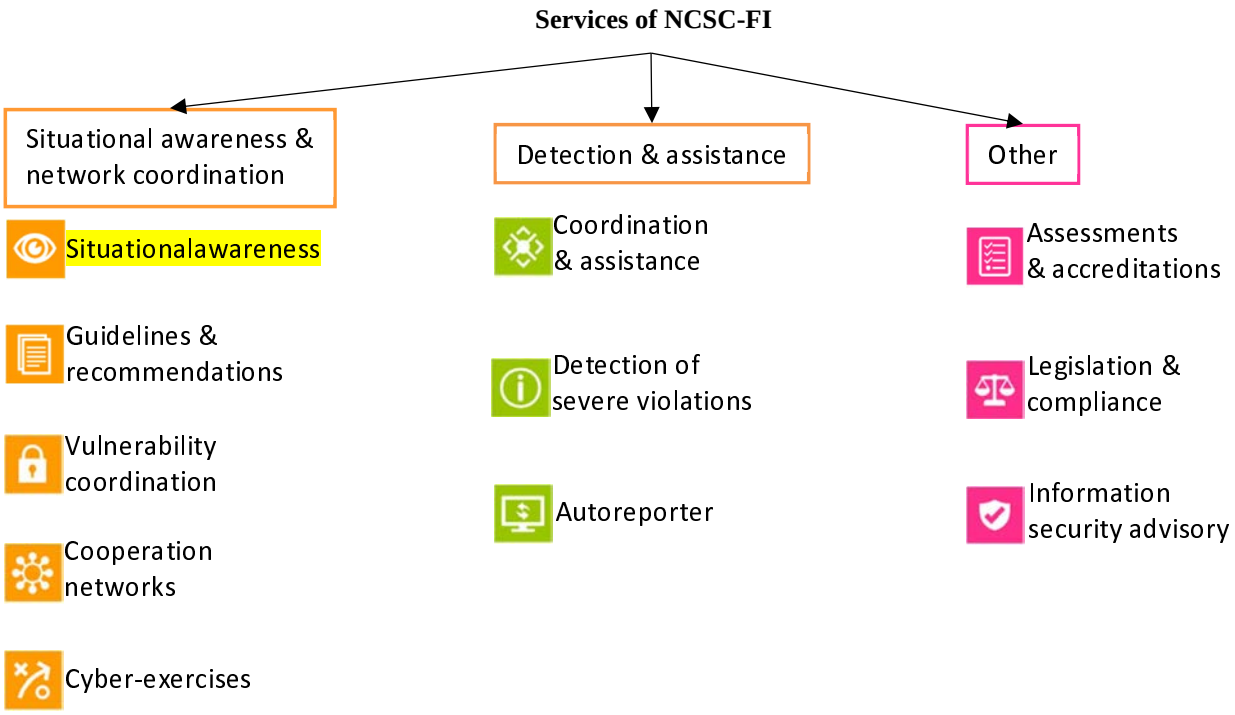

Figure 3: Services of NCSC-FI

The next service, *vulnerability coordination*, assists the discoverers of severe software vulnerabilities in cooperation with the software makers. NCSC-FI promotes responsible handling of vulnerability information throughout the lifecycle of the vulnerability and ensures that the resulting findings are handled in a responsible manner to prevent far-reaching negative impacts on privacy, assets, business, or even national security. The information about the vulnerability and its fix with the updates is made available for everyone, including the end-users.

The *cooperation and networks* service is provided by Information Sharing groups (ISACs). These groups enable confidential information sharing and discussion about information security related matters, improve and enhance information security know-how within participating organizations, and develop the cyber security both within the industry and across the society. Such groups were established on various sites: state administration, internet service providers (ISPs), chemical and forest industry, banks, media, energy sector, food industry and supply chain, healthcare, software industry.

The last service in the first group, *cyber-exercises*, aims to increase the organization's ability to react to cyber incidents. NCSC-FI offers professional support and materials both for conducting the exercise and for planning realistic scenarios based on real-life cyber incidents.

The second group of services consists of the following: coordination and assistance, detection of severe violations and Autoreporter. The first service, *coordination and assistance*, aims to resolve and investigate already occurred information security breaches. NCSC-FI also coordinates the needed follow-up actions, such as information sharing, contacting partners and cooperation networks, technical analysis and legal advisory. The users can send a notification about a threat through an online service.

Detection of severe violations is done by means of the information security breach detection and alerting system HAVARO. This system monitors severe cyber security threats, such as advanced persistent threat activity and information stealing malware, from the network traffic. In case of a confirmed finding, the customer is warned about the detected cyber security breach. NCSC-FI also compiles alerts from the threats detected in other systems to the customers and produces customer and industry-specific reports about their information security posture.

The *Autoreporter* system receives information of malicious network traffic originating from Finland from nearly all over the world. It captures many varying types of bot malware, web server break-ins, DOS and worm-like behaviour. This information is afterwards forwarded to operators who inform their customers about the findings. In such wary, NCSC-FI and telecoms operators perform collaborative actions to fight the malware.

Within the third group, NCSC-FI provides the following services: assessments and accreditations, legislation and compliance and information security advisory.

Assessments and accreditations services are performed by Finnish Communications Regulatory Authority. Accreditation can be performed for governmental organizations' information systems that are related to fulfilling international information security obligations and for the systems of companies that participate in international competitive bidding. Authority also performs assessments and accreditations of cryptographic products.

NCSC-FI provides advice related to interpretations of the legislation under its supervision (*legislation and compliance*). This guidance can be related to the rights and obligations directly derived from the law. In addition, NCSC-FI provide advisory about other instructions, guidance, recommendations, decisions, interpretations, and reports Finnish Communications Regulatory Authority has given in regard to information security, contingency planning and preparedness, strong electronic identification, etc. These services can be provided, for example, via email, phone calls with the specialist and advisory meetings.

Lastly, NCSC-FI serves public administration and organizations critical to the security of supply by providing *advice on information security* related matters. The purpose of the information security advisory is to guarantee the awareness of the cyber threats and possible resolutions in the operational environment within the organizations. The focus and the scope of the support is determined in cooperation with the client case-by-case.

8.3 National Communications Security Authority, NCSA-FI

8.3.1 Overview

Traficom's NCSA-FI duties have been merged into the National Cyber Security Centre Finland (NCSC-FI). It specializes in information assurance matters related to the handling of classified information in electronic communications.

In Finland, several different authorities are responsible for international obligations concerning information security. NCSA-FI operating within the National Cyber Security Centre Finland (NCSC-FI) is a part of the Finnish national security authority organization.

NCSC-FI has the following duties concerning international information security obligations:

- preparation of guidance and agreements concerning national security activities;
- preparation of guidance on the handling of international classified information;
- management and accounting of the crypto material distribution network and guidance on the secure handling of the material;
- approval of cryptographic products for protecting international classified information in Finland;
- accreditation of information systems used for processing international classified information;
- co-ordination of and guidance on national TEMPEST activities.

8.3.2 National Regulatory Authority, NRA

NCSC-FI also has several duties concerning national information security obligations. They are the following:

- steering and supervision of telecoms operators' operations, information security and preparedness, for example, monitoring compliance with the information security regulation (regulation no 67);
- steering and supervision of strong electronic identification and the provision of qualified certificates, for example, monitoring compliance with regulation no 72 issued by Traficom and carrying out annual audits of certification authorities providing qualified certificates.

8.3.3 CERT-FI

NCSC-FI's CERT-FI has 2 main objectives: to safeguard functions that are vital to society, and to ensure that public communications networks and communications services function safely and properly. The duties of CERT-FI include:

- solving information security violations and threats against network, communications and value-added services;

- gathering information on such incidents;
- disseminating information on information security matters.

8.3.4 Targets and methods for steering and supervision

Traficom and its NCSC-FI steer and supervise compliance with the provisions and regulations that apply to its field of activity. Steering and supervision apply to telecommunications operators, TV and radio operators, users of radio frequencies, postal operators, and other several players related to electronic communications networks.

The matters of interpretation often concern how to define telecommunications and a telecommunications operator or other conveyance of communications. The last-mentioned is supervised by Traficom as of the beginning of 2015. Traficom does not supervise the content or marketing of communications. Traficom is in favor of preventive and extensive measures and also aims at improving the operational possibilities of companies.

8.3.5 Players subject to NCSC-FI's regulation

The legislation concerning electronic communications and supervised by Traficom concerns, among others:

- traditional telecommunications operators, also in television and radio networks (telecommunications);
- several commercial and non-commercial providers of communications networks and communications services which have not traditionally been perceived as telecommunications operators (telecommunications);
- corporate or association customers that process their customers' identification data (corporate or association subscribers);
- as of 1 January 2015, also other parties than telecommunications operators and corporate or association subscribers that convey electronic communications as a third party with regard to the parties to the communications (other communications provider);
- housing companies and other holders of internal communications networks in real estate buildings;
- telecommunications and antenna contractors that install internal networks to real estate buildings;
- public authority networks;
- providers of directory inquiry services;
- providers of electronic remote controls (information society services);
- users of radio frequencies;
- manufactures of radio and telecommunications terminal equipment and network equipment, importers, retailers, and inspection bodies;
- providers of a qualified certificate;
- providers of strong electronic identification;
- authorities responsible for authorities' information systems and telecommunications arrangements and companies that implement them;
- authorities and companies that process international classified information;
- inspection bodies of the information security of information systems and telecommunications arrangements;
- postal operators, particularly universal postal service.

The legislation supervised by Traficom does not concern the content of communications at all, for example the content provided on the internet. However, requirements concerning the program content have been imposed on television and radio operators, and on providers of Video-on-Demand (VoD) services.

8.3.6 Proactive supervision

Traficom performs proactive supervision, some of the examples are:

- planning of radio frequencies, and related international and national stakeholder cooperation;
- drafting regulations specifying obligations in the legislation;
- imposing universal service obligations and obligations based on significant market power on telecommunications operators;
- drafting guidelines, recommendations and interpretation principles;
- sectoral working groups and other national stakeholder cooperation;
- drafting clarifications and reports;
- producing information concerning the sector and other monitoring of the development in the sector.

8.3.7 The goals of Traficom's supervision

The goals of Traficom's supervision are to:

- recognize problems in time and prevent them;
- settle matters in cooperation with players, but by ensuring the confidentiality of the information;
- act in such a manner that the effects of the measures are as effective as possible and apply to a large group;
- act flexibly in such a manner that unnecessary litigations are avoided;
- invest in steering and supervision of basic services;
- issue, always when necessary, a written decision which may be appealed to an administrative court.

8.4 Operators' rights and obligations

Communications providers, such as telecommunications operators, have the obligation to ensure that the information security of their network and communications services is not compromised. Ensuring information security may require measures that affect customers' communications.

The Finnish legislation requires that telecoms operators to maintain the information security of its network and communications services by ensuring:

- operating security;
- communications security;
- hardware and software security;
- data security.

Operators are not required to take unreasonable measures for ensuring information security as long as the measures are commensurate with:

- the seriousness of threats;
- the level of technical development;
- the costs.

In order to prevent information security violations and to ensure information security, a telecoms operator has the right to:

- prevent the conveyance and reception of messages;
- remove from messages malware that pose a threat to information security;
- take any other comparable technical measures in its communications network.

An operator may undertake these measures only if they are necessary for safeguarding the network or communications services or the communications ability of a message recipient. The measures taken to ensure information security may not limit freedom of speech or the protection of privacy any more than what is necessary.

A telecoms operator can notify its customers and Traficom's NCSC-FI of significant information security violations or threats to information security in the services and of anything else that prevents or significantly interferes communication services.

A telecoms operator also has to notify its customers of:

- measures available to customers for protecting themselves against the information security threats identified and the costs of such measures;
- sources of further information on the threats.

8.5 Conclusion

From SAINT's own findings, it is abundantly clear that Finland has empowered itself with Cybersecurity legislation, partnership with ISPs and industry with tools and resources to reach the top rank as one the most cybersecure nations in the world.

The most important reason for this highly positive model is that the Finnish Transport and Communications Agency (Traficom) and especially the National Cyber Security Centre (NCSC-FI) which is a department of Traficom, as a regulator, is the prime interface for cybersecurity empowering it to issue direct instructions to the ISPs and cooperates with industry to achieve the same level of service, a Cybersecurity as a Service (CaaS).

The second important vehicle is that the ISPs are empowered by the Finnish legislation to take actions, such as for example automatic prevention or limitation of message transmission or reception, to safeguard information security of their networks and services. This helps indirectly stopping hacking of hostings and individuals.

From the SAINT's project point of view, the Finnish model is to serve the EU member States and Associates states and probably worldwide as the most effective model to garner support and get strong consensus among all key stakeholders to fence off the dramatic onslaught of Cybersecurity threats in the end of this decade and the next one.

9 Blockchain/DataBlockMatrix

9.1 Blockchain/DLT and Privacy Regulation

Blockchain and other forms of Distributed Ledger Technology (DLT) are a valuable tool for many networked systems, but existing DLT implementations often present challenges when applied to many types of application. At the root of this difficulty is the fact that blockchain was designed as a way to prevent double-spending in digital currency. Alternative approaches can make DLT components more practical for use in a broad range of distributed system applications.

Although the blockchain data structure originated with in cryptocurrencies, designers are beginning to find interesting ways to solve system problems using blockchain and other forms of Distributed Ledger Technology (DLT). The most commonly used data structure for distributed ledgers is the blockchain. The central property of a blockchain-based system is the decentralized, replicated data synchronized among separate network nodes, which may be geographically dispersed. DLT systems are often characterized as either public or private, but a better way to categorize blockchain systems is based on their permission model: permissioned or permissionless; since it is directly tied to the technology; where private or public may apply to the visibility of the network or ledger itself. This clause discusses a DLT data structure designed primarily for use in permissioned systems, although use in permissionless systems may be appropriate in some applications.

With its features providing distributed, trusted data using no central server, DLT seems a natural tool for many complex distributed systems, and a number of implementations have been proposed. However, some environments and applications are not well suited to using an append-only ledger. For example, an analysis of DLT for the international banking consortium SWIFT found that the permissionless model used by Bitcoin and other cryptocurrencies "does not provide the level of trust, transparency, and accountability required by the financial industry". The SWIFT analysis noted that permissioned ledgers are helpful, but "existing implementations of permissioned ledgers remain basic". Of particular concern is the "immutable" aspect of transactions recorded in blockchains. As noted by the European Banking Institute, "once an error is embedded in the blockchain, this may be highly problematic, legally, in that often law requires the ability to rectify errors as a matter of law in a way foreign to DLT". One option is to correct errors by issuing a new transaction which supersedes the older erroneous transaction. In this way, the ledger provides a full history of events as they happened. While this is possible and desirable for some applications, privacy laws may lead to additional complications, because they may require user transactions to be deleted at the user's request. In addition to making it difficult to comply with privacy rules, other properties of conventional blockchains are not a good match for applications beyond cryptocurrency, and modifications to distributed ledger designs are being developed to meet new needs. Blockchains are a valuable distributed ledger technology for providing trust, but there are many ways to construct distributed ledgers.

9.2 DLT and Data Management

A distributed ledger, as the name suggests, is a distributed record of transactions, maintained by consensus among a network of peer to peer nodes (possibly geographically dispersed). The most widely recognized form of DLT is the blockchain structure, which provides the basis for cryptocurrencies and a variety of other applications. Most currently available distributed ledger designs using blockchain provide certain properties:

- *Pseudo-anonymity* - Especially for cryptocurrency, blockchains enable participation using only identifiers, providing a limited form of anonymity. Permissioned blockchains may not include this property.
- *Public access, transparency* - Every participant can see all transactions on the blockchain, although they may be anonymized. This property may also not be provided in permissioned systems.
- *Small transaction size* - Blockchains were originally designed for monetary transactions, so messages are assumed to be relatively small.
- *Immutable records* - As a consequence of the linked chain of cryptographic hashes of records, a change to one record would cause the hash of subsequent records to be invalid, so changes require recomputing the entire chain. As a result, it is generally intractable to change any record in a blockchain.
- *Proof of work or other expensive consensus models* - A consequence of the need to prevent double spending. Permissioned blockchains do not generally need this feature and can use simpler consensus.
- *Block ordering guarantee* - The consensus mechanism ensures ordering of the blocks and therefore transactions, preventing the possibility of double spending.
- *Decentralization* - There is no central authority for records. With each update, records are dispersed to peer nodes simultaneously, who ensure the updates are correct.
- *Replication and Synchronization guarantee* - Transactions are duplicated across all nodes of the network, so that every node has an identical copy of all transaction records, current to the most recent update cycle. Consensus protocols are designed such that when the consensus is complete, all nodes have an identical copy of the distributed ledger records.
- *Integrity protection* - Cryptographic hashes are used to guarantee that records have not been changed.

One of the key needs for data management systems is for assurance that records are not corrupted, either accidentally or by malicious action. Blockchain's integrity protection guarantee is thus an attractive feature that could be used to provide better assurance than might be possible using conventional database components. However, not all properties of blockchain are as well-suited to building distributed systems. These properties with the needs of more typical applications of distributed data storage and retrieval are compared in Table 1. Note that six of the nine blockchain properties designed for cryptocurrency are at odds with the requirements of many other applications.

Table 1: Comparison of DLT application characteristics

Cryptocurrency	Finance, supply chain, e-commerce, etc.
1. Pseudo-Anonymity	ID required for contracts or government regulation
2. Public access, transparency	Controlled access
3. Small transaction size	Range of message sizes up to large documents, images
4. Immutable records	Changes and deletions, often required by law
5. Proof of work and other expensive consensus models	Flexible consensus models
6. Block ordering guarantee	Timestamps often required
7. Decentralization	Same in many applications
8. Replication and synchronization guarantee	Same in many applications
9. Integrity protection	Same in many applications

9.3 A Distributed Ledger Alternative to Blockchain

The mismatch between blockchain properties and many application needs has led to a number of problems in applying blockchain designs to data management problems. For example, Bitcoin is designed to provide some degree of anonymity in transactions (i.e. only public identifiers, not real-world identities are used), but the law may prohibit anonymity for many types of transactions and require participants to be identified for tax or other purposes. Laws such as the European Union General Data Protection Regulation (GDPR), that require the ability to delete privacy relevant information, may limit the type of information that can be stored in a blockchain.

For system engineers, the price of distributed trust is often added complexity. The design choices that were made to incorporate anonymity and prevent double spending in blockchains often lead to seemingly unnecessary complications when applied to areas beyond cryptocurrency. For example, immutability has resulted in designs where alterable records are kept off of the blockchain, with only pointers to them stored in the blockchain itself. Alternatively, some designs involve encrypting data on the blockchain, then destroying the encryption key to "delete" the data. Neither of these options may be desirable for many applications, as the first option leads to unnecessary complications, and the second risks the data being decrypted in the future, when data will be protected for decades. These are serious design issues for supporting privacy requirements such as those of GDPR, resulting in proposals such as an "editable blockchain" using new forms of hashing. For cryptocurrency, a consensus algorithm is needed to guarantee record ordering in the absence of a central time authority (i.e. transactions are ordered based on group consensus, rather than time of entry into a system), and this ordering is used to prevent double spending. Designs for access control using blockchain may involve tokenizing permissions, then passing these to users, and "spending down" the value to remove a permission from a user. All of these strategies are needed to take advantage of blockchain's trust properties, but blockchains would probably not be used if a more conventional database could provide the desired distributed trust.

At first glance, blockchain solutions for applications such as supply chain, financial settlement, and others may appear to offer nothing more than added complexity in comparison with a conventional database. However, when more than one organization is involved, the decentralized trust of blockchains and other distributed ledgers can be a tremendous advantage. For example, consider regulated industries where audit is a part of doing business. Every node on the system can have a full set of records detailing the movement of assets. Any shared database can keep track of asset movement, but DLT adds trust by maintaining current, integrity-protected records at every organization, making it easy to audit the process. Thus, the financial industry views *full traceability* and *simplified reconciliation* of transactions among the key advantages of DLT. DLT can be considered as adding a layer of distributed trust to the problem of data storage and retrieval, clearly a desirable property, but industry is still struggling with how to use DLT in practical ways.

9.4 Decentralized Trust in a Permissioned Distributed Ledger Model

Much of the current DLT research seems to centre on how to get around properties that were baked into blockchain. Adaptations such as faster consensus algorithms are gradually moving DLT from its origin in cryptocurrency towards a more general-purpose database technology. But instead of tweaking blockchain designs, alternative approaches to distributed ledger may reflect the needs of data management applications as discussed earlier.

The key feature of the data structure described below is to provide the decentralized trust of a blockchain, but otherwise behaves as a conventional database. Two recent developments, a *data block matrix*, and *verified time*, may be used to achieve this goal, helping to make DLT a more practical component for networked system designers. The data block matrix retains hash-based data integrity guarantees, while allowing controlled modification or deletion of specified records, with integrity guarantees for all other records. A data block matrix can be implemented in a decentralized system to provide data replication among peers. The verified time protocol allows guaranteed timestamps to be used in place of consensus algorithms to ensure record ordering.

The data block matrix uses an array of blocks, with hash values for each row and column. This structure makes it possible to delete or modify a particular block with hash values assuring that other blocks have not been affected. An example is shown in Figure 4. Suppose that it is desired to delete block 12, by writing all zeroes to that block, or otherwise modifying it. This change disrupts the hash values of $H_{3,-}$ and $H_{-,2}$ for row 3 and column 2. However, the integrity of all blocks except the one containing "X" is still ensured by the other hash values. That is, other blocks of row 3 are included in the hashes for columns 0, 1, 3, and 4. Similarly, other blocks of column 2 are included in the hashes for rows 0, 1, 2, and 4. Thus the integrity of blocks that have not been deleted is assured. Blocks can be deleted by overwriting with zeroes or other values, with one row and one column hash recalculated; specifically, after deleting block *i, j*, row *i* and column *j* hash values are recalculated.

As shown in Figure 4, the data structure ensures the following properties:

- *Balance*: Upper half (above diagonal) contains at most one additional cell more than the lower half.
- *Hash sequence length*: Number of blocks in a row or column hash proportional to $\sqrt{N}$ for a matrix with *N* blocks, by the balance property.
- *Number of blocks*: The total number of data blocks in the matrix is $N^2 - N$ since the diagonal is null.
- *Block dispersal*: No consecutive blocks appear in the same row or column.

	0	1	2	3	4	
0	•	1	3	7	13	$H_{0,-}$
1	2	•	5	9	15	$H_{1,-}$
2	4	6	•	11	17	$H_{2,-}$
3	8	10	12	•	19	$H_{3,-}$
4	14	16	18	20	•	$H_{4,-}$
	$H_{-,0}$	$H_{-,1}$	$H_{-,2}$	$H_{-,3}$	$H_{-,4}$	etc.

Figure 4: Data block matrix with numbered cells

Clearly, this data structure is not suited to all DLT applications, but it offers features that are difficult to provide with a conventional blockchain. As such, it offers a new form of data storage structure that provides the integrity guarantees of blockchain with the addition of reversibility, which can be used in a wide range of applications. A comparison is shown in Table 2.

Table 2: Blockchain and data block matrix features

Blockchain - provides integrity, sequencing	Data block matrix - provides integrity, erasure
Integrity protection, no erasure possible	Integrity protection for all blocks not erased
Double-spend problem solved by distributed transaction ordering guarantees	Ability to erase values obviates need for ordering guarantees through consensus algorithms
Ordering guarantees require consensus algorithms	Ordering guarantees granted by time authority

In distributed ledger designs, the role of time is often an afterthought. Some DLT systems have no inherit transaction timestamp, to record when the transaction was submitted to the system. Rather the transactions adopt the time in which they were included into the ledger which may occur after a significant amount of time has passed since being submitted. This approach has worked for applications where just having a transaction accepted is good enough (e.g. it is not needed to know that a cryptocurrency transaction was submitted down to the millisecond, just that it was indeed submitted and eventually recorded in the ledger).

However, when time dependent situations arise, a timestamp becomes more important, and knowing when a transaction was submitted to a system may be more important than when it was incorporated into the ledger. Often, systems will rely on local system time, or a network time - both may differ from one system to the next. Distributed ledgers can be able to operate in environments that include rules mandated by government or contract. For some applications, the ordering of transactions into blocks within the blockchain may not be enough, and there is a need for a global timestamp service, providing verified time. Time is a key component of this because things happen outside of the blockchain that matter for applications - orders need to be fulfilled by a specified date and time, legal papers filed on schedule, and so on, requiring timestamps of events that take place outside of the blockchain. A global time-stamping approach includes an agreed upon and accepted service, which uses an algorithm combining times from a user-specified set of atomic clock time servers, to produce a high resolution blockchain time mechanism. This design thus avoids the need for resource-intensive consensus sequence guarantee algorithms, such as proof of work, used in permissionless blockchains for cryptocurrencies.

Summary

The blockchain data structure and proof-of-work protocol were designed to solve the problem of double spending in cryptocurrencies. Although blockchain has found many applications outside of cryptocurrency, many of its features are not well suited to common data management applications, leading many to argue that distributed ledgers are only databases with more complex features. As shown in this clause, alternative architectures can provide the integrity and sequencing trust features of blockchains, with characteristics that allow for simpler designs and greater practicality in conventional data management problems in networked systems.

NOTE: This clause is abstracted from:

1) NIST Cybersecurity Whitepaper [i.92];

2) IEEE Computer, 52(2), 68-72 [i.93].

History

Document history		
V1.1.1	November 2020	Publication