DATA SECURITY IN THE TRANSITION FROM IPV4 TO IPV6

VISHAL S. DHOLE

NITA V. JAISWAL

PROF. D. M. DAKHANE

ABSTRACT

IPv4 is a foundation of Internet communication. Designed many years ago the protocol is inadequate in modern networks. New sixth ersion is replacing the older one. It is often repeated that IPv6 was designated to solve some security problems. This statement is true only to some extent. IPv6 deployment for the future infrastructure IPv6DFI (especially in the transition phase) will have large impact, not always positive on many aspects of Internet services: network performance, data security, economy. As number of IPv6 networks grow, new threat awareness and understanding become more important. The paper attempts to present comprehensive survey on IPv6 security and to identify many issues of data security in the transition from IPv4 to IPv6 phase.

Index Terms— *IPv6, transition, security, network, IPv4*

INTRODUCTION

Internet evolution from IPv4 to IPv6 is the biggest transformation in Internet infrastructure since its beginning. The process is (and will be for many years) very complex and resources (human, money) consuming. It must be expected that the transformation will have huge impact on many aspects of Internet services: network performance, data security, economy. In general, security issues in IPv6 are not better or worse than in IPv4, they are just different. There are risks related to all security features: confidentiality, integrity and availability. For many years we will live in a dual IPv4/IPv6 environment. The security issues could become complex to deal with in terms of implementation and configuration. In dual-stack architecture used in transition phase the problems resulting from IPv6 introduction may have unforeseen effects on IPv4 processing, affecting not only new services but also old services (based on IPv4). The IP transition phase is an important research area of many teams (e.g., 6net [1], IPv6fix [2] in Japan, USGv6 [3] in the USA). There are some resources on different aspects of IPv6 security (e.g., [4] [5] [6]). Complete list of new threats and risks related to IPv6 is very long and it is very probable that we do not know all threats and risks. In the paper we try to present comprehensive survey on IP security issues with emphasis on the security in IPv4 to IPv6 transition phase. Later presents some remarks on solutions to the transition period problems. Main part of the paper is dedicated to several issues related to security of IPv6 deployment and transition phase. General conclusions are given in the last part of the paper.

FROM IPV4 TO IPV6

IPv6 had been proposed at IETF as the next generation of IP at early in the 1990's. IP transformation is long-term and complex process. Changes in software (operating systems, applications) as well as in hardware are needed on different TCP/IP layers. The process is not limited to IP version exchange. Many supplementary protocols, such as ICMP (Internet Control essage Protocol), DNS (Domain Name System), BGP (Border Gateway Protocol), OSPF (Open Shortest Path First), RIP (Routing Information Protocol) need to be modified or upgraded. Unfortunately there is no single, commonly adopted solution to the IP transformation problem. We could not switch from IPv4 to IPv6 in one single point in time. We have to maintain existing IPv4 networks and slowly introduce IPv6 networks. So the two networks have to coexist and

cooperate for most likely long time. It is expected that the phase will last for many years. Some reports (e.g., [7]) suggest the phase will reach 2025 year, with cost estimated in USA at $25 billion. And even in 2025 IPv6 global penetration will not achieve 100%. We have just started and so far some plans of IPv6 adoptions did not materialize. For example, according to Action Plan, published in 2008 for EU,

Europe should widely implement IPv6 by 2010. It was predicted that by 2010 at least 25% of users will be able to connect to the IPv6 Internet and to access their most important content and service providers without noticing a major difference compared to IPv4 [8]. RIPE Survey [9] from mid 2009 leads to conclusion that achieving this 25% market penetration will be very difficult. There are many obstacles: cost, IT staff preparation (and also some form of human inertia), software implementations availability and maturity. The dangers of transition phase arise from many general reasons among them: a lack of information and a lack of documented operational experience, on which network administrators can draw. One of the important concerns in adopting IPv6 is security. Operators and enterprises are reluctant to deploy technology that may compromise security and eventually cause significant financial loss. Most transition alternatives are a combination of dualstack or dual-layer environments and packet tunnelling. Dual-stack means that both versions are running on the.

SECURITY ISSUES

There are many security issues related to IPv6 deployment and transition phase. The security issues related to IP transformation phase may be divided into 2 groups. First group of security problems is associated with IPv6 features and implementations, such as cryptography tools, addressing scheme, security model, host mobility, software bugs. The second group is related to particular methods for IPv4/IPv6 cooperation. Security (especially resources availability) in a broad sense is affected by performance. Poor network performance could lead to availability threats. In order to boost performance security regulations may be loosen by administrators.

A. General Remarks

IPv6 was designed to improve data security. It introduced obligatory implementation (but its use is not required) of IPsec security mechanisms: AH (Authentication Header), ESP (Encapsulating Security Payload), IKE (Internet Key Exchange) Protocol. In general this makes protection (for higher layer protocols and applications) easier and more cost effective. The mechanisms are used to satisfy the requirements of access control, connectionless integrity, data origin authentication, confidentiality and protection against replay attacks [12]. It must be added that not all network devices are equipped with IPsec. For example, some printers, faxes, scanners do not use IPsec. Furthermore such IPv6 features of the protocol as simplified header, greater number of available addresses have also impact on security. Simplified header makes routers more resistive to DoS attacks – packets are processed more rapidly. Greater number of addresses makes exhaustive host scanning (reconnaissance attack) of a typical /64 subnet unpractical. IPsec is available for IPv4 but only as an option. Furthermore, IPsec means whole datagram protection so it is not attuned to work with NAT (Network Address Translation) used concurrently with IPv4. IPsec protects the whole datagram, so any modification of the header (NAT modifies addresses and port numbers) violates the security of the datagram. In the transition phase NAT is still used in some dual-stack solutions (e.g., [13]). Only in full IPv6 deployment phase NAT is not needed and full end-to-end IP security is deployable without those issues. Common methods for preventing unwanted traffic from the Internet are firewalls and IPSes (Intrusion Prevention System). The security is based on the assumption that all the traffic is inspected at the edge of protected network. The problem is not all of the security devices and software are currently IPv6-capable (e.g., IPS may detect the traffic associated with common attacks and malicious behavior for IPv4 and at the same time might not be able to detect similar traffic when it is sent over IPv6) – in the consequence IPv6 may be used as a backdoor to the protected network. IP transformation phase takes place at the moment of very dynamic Internet rowth. Some forecasts estimate IP traffic will increase at a compound annual growth rate of 40% in 2008-2013 [14]. As a result current firewall systems that perform security screening through a common checkpoint will be increasingly degraded due to increasing number of datagrams to process. IPv6 was designed to protect data. Unreasonably, its deployment may sometimes lead to decreasing security level, especially in the transformation period. The operating system vendors long ago started to support IPv6 in their products.

Nevertheless interoperability and compatibility tests (e.g., [15]) of IPv6 implementations show some implementation problems. The problem occurs in network security systems that deal only with IPv4 datagrams. Operating system implementing both IP versions may use IPv6 without user explicit configuration – IPv6 datagrams are not screened and the protocol may be used to form a backdoor [6]. For example, Teredo, an IPv6 tunnelling tool developed by Microsoft is enabled by default in the Microsoft Windows Vista.

B. Cryptography Strength

IPsec uses various cryptographic techniques and tools: symmetric and asymmetric encryption algorithms, hash functions, pseudorandom number generators, key exchange protocols. For a given transmission process cryptography tools are negotiated with a use of IKE. It is assumed that the ultimate set of optionally available tools is changing. At the same time, in order to ensure interoperability, all IPv6 devices (and IPv4 with IPsec implementations) are required to employ some mandatory algorithms. The first problem is the requirements should be met in all devices, without regard to their processing power. This leads to some compromises in the algorithms strength. As for now according to [16] set of mandatory algorithms contains: AES-CBC with 128-bit keys, Triple DES-CBC and HMAC-SHA1-96. Another problem is the existing algorithms and their implementations are continuously attacked (and sometimes broken) and will be attacked and broken in the future. This is more probable due to long period of IPv6 deployment. Strong algorithm may become weak. Well known examples are DES and MD5, included in the IPsec mandatory list in 1998 [17] but removed from the list in 2005 [18]. SHA1 hash function, which is mandatory at this moment is also known to have some weaknesses [19] and is a possible candidate for removal from the mandatory list. Prospective replacement of the broken algorithms in all network devices will be very painful and resource consuming task. In some cases (e.g., devices with hardware implementations of cryptographic mechanisms) the task may be impossible to complete. It may be assumed that, in outcome older, broken cryptography will be used for data protection.

C. End-to-End Security Model

There are two fundamental security models for communication protection: end-to-end and network-based. In end-to-end security model the end hosts provide the security services necessary to protect transmitted data. This model is used in banking applications. Network-based security refers to the practice of hardening the elements of a network to protect other devices. Both models have advantages and weaknesses. The two models may be integrated. Hybrid solutions can be used in the transition period. IPv6 is integrated with IPsec transport mode dedicated to end-to-end security model. Switching on IPsec does not solve all security problems. First of all, it may not be assumed that communication endpoints can be trusted. Internal threats to data security occur more often than external. If an endpoint is not trusted then entire end-to-end security system could not be trusted to [20]. Additional weakness of the solution is caused by the fact that data are secured at the source and devices located inside the communication channel (gateways, firewalls, …) are not able to scrupulously analyze the traffic. For example, if inbound datagram is encrypted with ESP then it is possible to check IP address in a header but it is not possible to check if data field contains malicious load. For a firewall it is not possible to provide DoS (Denial of Service) prevention based on the expected TCP protocol behaviour – TCP segments inside IP data fields are encrypted so firewall could not check for example, the settings of particular TCP flags. In the same way outbound transmission analysis is also affected. DLP (Data Leakage Protection) is network sniffer, installed on gateway, looking for outbound transmission with predefined sensitive data that should not be transferred outside protected zone. DLP is called also Extrusion Prevention System. DLP systems could not perform their functions since they could not identify sensitive data in encrypted outbound datagrams. There is a problem with fragmentation – since datagram defragmentation may be done only at the destination host firewall is not able to reassemble the datagram and eventually sanitize it. Another problem is related to users' negligence. In the case of end-to-end security, users (not administrators) are responsible for data security. If users do not understand the security mechanisms they will not use them appropriately. For example, web browsers may display a warning about invalid server certificates, but users can override the warning and still make vulnerable connection. A solution to the problem is proposed in the form of distributed firewall [21] [22]. The architecture consists of two firewalls: one at the network perimeter and the other integrated with end host. Firewall at the network perimeter performs general datagram filtering (e.g., based on source IP address) while host-based firewall inspects datagram more precisely. Only the end-host is able to decrypt datagram in order to check

it thoroughly. The solution has negative impact on performance. Additional problems are related to NAT and Quality of Service enforcement. Full end-to-end security is possible if NAT is not used, but some dual-stack solutions to the transformation phase use NAT for address conversion. Furthermore end-to-end security model makes QoS policy enforcement impossible.

D. ICMPv6 Issues

For a new version of IP a new version of ICMP is needed. The old version of ICMP dedicated to IPv4 may not be used with IPv6. ICMPv6 is more functional than its predecessor. It also replaces ARP (Address Resolution Protocol) – NDP (Neighbor Discovery Protocol) is a part of ICMPv6. Without secure network configuration ICMPv6 may lead to many new threats, for example, covert channel, NDP cache poisoning (similar to ARP cache poisoning) or DoS. The functions added to ICMPv6 are the source of problems for firewall configuration. ICMP messages (used with IPv4) could be dropped by firewall without disturbing normal network operation. In the case of ICMPv6 firewall needs to allow some messages through the firewall and also messages to and from the firewall. Without the authorizations IPv6 procedures (e.g., neighbor discovery or stateless address configuration) could not work properly. As a result covert channel between firewall protected LAN and intruder may be established – for example, malicious IPv4 datagrams (in normal case rejected by firewall) could be hidden inside ICMPv6 messages (which are not rejected by firewall). NDP is a new function added to TCP/IP stack for host IPv6 address autoconfiguration and address resolution. It has been shown [23] that NDP messages may be used to execute an attack on router resulting in network congestion and degradation of QoS. Another DoS attack may be launched with a use of multicast transmission. IPv6 specifications forbid the generation of ICMPv6 datagrams in response to messages to global multicast addresses. But there are two exceptions (the *datagram too big* message and the *parameter problem* message). The attack uses these exceptions – error messages are returned as the responses when unprocessable (e.g., greater than Maximum Transmission Unit) datagrams are sent to multicast addresses. If datagram source address is spoofed (replaced with victim address) then many datagrams from multicast group are sent to a victim [5].

E. Host Authentication vs. User Anonymity

IPv6 addressing scheme is very complicated. There are many different types of addresses and many methods for address generation. For ease of configuration a 64-bit part identifying a particular host in the network may come from the interface identifier (e.g., Ethernet MAC address extended to 64 EUI (Extended Unique Identifier)). This ease of configuration leads to privacy problems. All communications of the given user can be linked together using constant interface identifier very easily. On the margin it may be added that IP addresses attributed to Internet users are personal data and are protected by EU Directives 95/46 and 97/66 [24]. In order to prevent such threats to privacy another method (pseudorandom) for address generation was established. Among various methods for address acquirement we have stateless address autoconfiguration with pseudorandom host identifier selection [25]. The purpose is to change the interface identifier (and public address) from time to time. This way it is much harder for any eavesdropper to correlate Internet transactions to a specific network subject and the user anonymity is better protected. It must be added that a global routing prefix (usually /48), added to pseudorandom host identifier, is fixed for hosts in a given network and some privacy concerns remain. Full anonymity protection is almost impossible. An attacker, who is on path, may be able to draw some conclusions with a use of: the payload contents of the transmitted datagrams and the characteristics of the datagrams such as datagram size and timing. Use of pseudorandom addresses will not prevent such payloadbased correlation. The same change in the address used for privacy protection could make it harder for a security administrator to define an address-based firewall policy access rule. Another problem is that such node behaviour with relatively high rate of address changes may be interpreted as DDoS (Distributed DoS), like SYN flood, attack and the transmission from the node may be blocked by firewall [5]. Address autoconfiguration has one more weakness. First 24 bits of MAC (Medium Access Control) addresses used in the process are related to specific vendor equipment. An attacker may scan network in order to discover specific vendor device reachability and facilitating an attack on known, specific for the given device security weaknesses. Here we see typical development scenario: new feature in the protocol (address autoconfiguration) leads to a new security problem (threat to privacy), solution to the problem

(pseudorandom address generation) leads to another difficulty (false DDoS alert). Privacy is important feature of communication. Nevertheless it must be added that the feature may be used also to hide the source of illegal and nasty activities.

F. Software Bugs in IPv6 Implementations

Software implementing IPv6 is relatively new, less mature and has not been tested thoroughly. So far many bugs have been found in the software developed by all the major vendors of IT. It is very probable that numerous bugs will be found in the future. A question is if the bugs will be patched quickly? If not so, many new attack methods will emerge. Furthermore it may not be excluded that essential security features may be missing from early releases of software. For example, Symantec discovered IPv6-related flaw in Vista. Fortunately it was patched by Microsoft (MS07-038 security update from July 2007). The flaw was related to Teredo tunnelling interface, which did not properly handled certain traffic, allowing to bypass firewall filtering and to obtain sensitive information with a use of IPv6 transmission. Similar problems occur in other operating systems. For example, bug number 6797796 in Solaris 10 may be used to execute DoS attack [26]. Old JUNOS (Juniper router operating system) versions (before May 2006) had a security bug, which could lead to router crash [27].

G. Mobile IP

Both Mobile IP and the increase of moveable IP devices will mean they will be in uncontrollable networks. In Mobile IP environment mobile host is reachable with a use of host routing protocol – normal route to a host is modified for a given recipient host. The method changes the way a datagram is sent to a host. In the effect it may be expected some forms of attacks will use the feature [28]. In the mobile IP environment new security threats will materialize in networks designated for use by foreign, visiting hosts. Such a network will have to loosen firewall rules. Mobile host needs to transmit some IP and ICMP packets (e.g., binding updates, datagrams with optional routing headers) necessary to maintain associations with home agent and other hosts. Firewall should be open for these datagrams – obviously this leads to a security risk. Mobile IPv6 devices are often equipped with scarce resources and have low processing power. The resources

and processing power may be not enough to protect the device: to filter incoming datagrams, to automatically update software (especially implementations of cryptography algorithms), to resist DoS attacks. Of course this problem is common and not related to a particular IP version but IPv6 users may mistakenly believe they are better protected.

H. Security of the Interoperability Methods

There are several means to operate in IPv4+IPv6 environment. The methods enable to transfer datagrams between hosts located in two generations of networks: IPv4 and IPv6. For example, datagram between hosts belonging to two separated IPv6 networks (islands) may be transferred (tunnelled) across IPv4 network – IPv6 datagram is encapsulated in data field of IPv4 datagram. In the future, as IPv6 deployment will spread and IPv4 use will diminish, the roles of IP versions will change. IPv4 datagrams will be encapsulated in data fields of IPv6 datagrams – new types of problems will emerge. Some security problems are independent of tunnelling method, others are related to a particular tunnelling procedure. In the case of tunnelled datagrams devices enforcing security may inspect only the outer layer of the datagrams, which may be prepared by intruder to avoid filtering while malicious contents of the datagram remain unnoticed. If such datagrams reach a tunnel end-point inside the protected network they are decapsulated and from there can potentially be very harmful since within a network itself, defence levels are usually much lower. It is obvious that in the case of tunnelling unencrypted IPv6 datagrams in IPv4 network all IPv4 security concerns influence data security. And this problem is regardless of tunnelling method. There are many tunnelling/interoperability methods, for example: 6to4, Teredo, ISATAP and tunnel broker. Each method has individual impact on data security

Teredo

Teredo uses UDP to tunnel IPv6 datagrams through IPv4 network. IPv6 datagrams are put into UDP segments, which are sent to the destination system via IPv4. Teredo requires a lot of datagram-sanity checks, which can prevent a number of attacks. The program also includes some decent anti-spoofing mechanisms. Nevertheless Teredo tunnelling may lead to new threats. In Teredo architecture encapsulation/decapsulation is performed by end host. Any of internal (inside

LAN protected by firewall) network's Teredo-enabled systems that can receive UDP datagrams can then act as an endpoint for IPv6 tunnels. It is much difficult to secure all such endpoints instead of a single firewall at the network boundary. In the case of a single firewall it is relatively easy for network administrator to control the traffic. But if malicious datagrams are hidden in Teredo tunnel then firewall is not able to discern them and block. Of course firewall could entirely block Teredo traffic (UDP predefined destination port 3544) but attack may be carried with a use of another UDP port. An attacker can send arbitrary IPv6 datagrams to a Teredo-enabled machine inside LAN. The machine may route the datagrams (with source routing mechanism of IPv6) to other host [29]. The problem is particularly related to MS Windows Vista, which in default configuration has both IPv6 and Teredo turned on [11].

6to4

6to4 dual-stack is used to connect IPv6 networks across an IPv4 network. Unique 2002::/16 prefix is reserved for 6to4 systems. Network address with 2002::/prefix has IPv4 address 32 bits embedded immediately after the prefix. The IPv4 address indicates 6to4 router located between IPv6 and IPv4 network. All nodes inside IPv6 network have addresses with 48 bits prefix (2002 and 32 bits of IPv4 router address). If a 6to4 router receives an IPv6 datagram with 2002::/16 prefix then it sends it through IPv4 network, inside IPv4 datagram with IPv4 receiver address taken from 32 next (after 16 bits prefix) bits of IPv6 address. It is assumed that IPv4 traffic from every address is accepted and decapsulated by 6to4 routers. The routers can be tricked to send spoofed datagrams anywhere. Anyone can send tunnelled spoofed traffic to a 6to4 router, and the router will believe that it is coming from a legal relay. There is no simple way to prevent such attacks, and longer-term solutions are needed in both IPv6 and IPv4 networks [30].In addition it is suggested that 6to4 routers can be abused to carry DoS attack [31].

ISATAP

ISATAP is Intra-site Automatic Tunnel Addressing Protocol. SATAP uses unusual form of IPv6 addresses. Address is made of 64-bit network prefix and interface identifier. Network prefix is received from ISATAP router while interface identifier contains an embedded IPv4 address (last

32 bits of IPv6 address). The IPv4 address is used in IPv4 headers when IPv6 traffic is tunnelled across an IPv4 network. Risks related to ISATAP are similar to those related to 6to4.

Tunnel broker

Tunnel broker is based on third party servers (tunnel broker servers, tunnel servers) distributed in Internet. Tunnel broker provides tunnels for IPv6 datagrams in IPv4 networks. User/client has to register with the broker system, which sets up a tunnel to one of its tunnel servers. Client gets configuration settings from the broker and uses tunnel servers for communication. The problem is related to the requirement that all traffic passes through third party servers. Service availability as well as confidentiality are threatened. Exemplary DoS attack may be performed by malicious user demanding to establish such number of tunnels that exhausts the resources available in tunnel server [32].

I. Performance Issues

IPv6 was developed to improve network performance. There are many features that aim to fulfill this requirement: simplified header, better addressing scheme, ability to transfer very large datagrams, ban on fragmentation in routers. However, there are some issues of IPv6 with negative impact on performance. This indirectly may influence data security. IPv6 allows transferring very large datagrams (up to gigabytes). On the other hand in the case of IPv6 tunneling in IPv4 network, the IPv6 path MTU for the destination is typically 20 bytes less than the IPv4 path MTU for the destination. IPv6 headers have fewer fields but are longer due to longer addresses. Minimum length of IPv4 header is 20 bytes while minimum length of IPv6 header is 40 bytes. This makes additional load to all the nodes (including routers, firewalls, bridges) in the communication channel. Of course these longer IP addresses are transferred not only in IPv6 headers but also in messages of many higher layers protocols (e.g., DNS, ICMP, BGP, OSPF) increasing network load. In the transition phase routing may be done with two separate protocols and doubling the amount of processing in routers. This may lead to router's CPU overload and increase in routes convergence time. It is obvious that the longer IP header the more timeconsuming packet filtering process in firewalls. The question is if this will not force network

administrator to switching off filtering in order to boost performance? Dual-stack systems use tunneling for datagram transmission in heterogeneous environment. Datagram processing on hosts or routers sitting on tunnel ends adds extra time to total datagram delays. In the case of tunnel broker solution further delay is related to datagram transmission from source host to tunnel server, which may be topologically remote. For example, if hosts in Europe use American tunnel broker then transmission parameters (Round Trip Time, jitter, throughput, packet loss ratio) between two IPv6 hosts in Europe will be downgraded by intercontinental links. Another set of problems is related to DNS. A performance problem is coupled with fallback process. In the IP transformation phase name servers will store two types of address resource records: A for IPv4 and AAAA for IPv6. It is assumed that no explicit information on address preference will be given to a client. The application may receive both IPv4 and IPv6 addresses for the same domain name. The application will have to try respectively addresses received from name server until the connection is successful. It is assumed that IPv6 addresses will be used initially. But if end system has no global IPv6 connectivity then the attempt to connect will be unsuccessful and host will switch to IPv4 address (this is known as fallback process). Due to TCP characteristics the fallback process may last up to about 190 s [33] – the effects on service access time are obvious. Increased number of AAAA queries sent to name servers is another source of performance deterioration. From IP transition point of view DNS is extraordinary service. Name servers and resolvers should be the first to be fully dual-stack capable. In dual-stack architecture the IPv6 datagrams performance deterioration resulting from IPv6 processing may potentially have harmful unforeseen effects on IPv4 processing, affecting availability of services based on both protocols. IPv6 allows to classify datagrams in order to diversify their processing by network devices. Some users (legal as well as hackers) may abuse the function and wrongly classify all sent datagrams as highest-priority. To enforce appropriate QoS policy the network device (e.g., gateway) needs to inspect headers and data fields of the datagrams. If the datagrams are encrypted such inspection (and QoS policy enforcement) will be impossible.

CONCLUSION

Some general conclusions may be drown from IP evolution. The change is rather inevitable. New functions of IPv6 and ICMPv6 lead to new threats. IP transition period has (and will have for many years) great impact on Internet security, performance and economy. Since all popular tunnelling methods (Teredo, 6to4, ISATAP, tunnel broker) use IPv4 networks, the security concerns related to IPv4 are still relevant. In popular dualstack architecture the problems resulting from IPv6 introduction may potentially have unforeseen effects on IPv4 processing, affecting both services. There are many security issues related to IPv6 deployment. Complete list of new threats and risks related to IPv6 is very long. It is probable that the list will grow longer in the future. In general the security issues related to IP transition phase may be divided into 3 classes:

• related to IPv6 internal features,

• related to IPv6 implementations,

• related to IPv4 to IPv6 transition mechanisms.

A variety of risks and threats are results of the problems. In the previous sections we have described examples of threats from several categories:

• DoS attacks,

• covert channels through firewalls,

• privacy problems,

• extra complexity of management/security tasks,

• bugs in immature software,

• performance deterioration.

In the time of full IPv6 deployment IPv6 will be more than 30 years old. It is very unlikely that the protocol will be appropriate for Internet in for example, years 2020-2030. Finally, it must be said that many attacks are targeted at the application layer. Since the attacks are unrelated to a particular IP version IPv6 deployment will not change the security level of the application layer.

REFERENCES

[1] 6net Large-Scale International IPv6 Pilot Network, 6NET Consortium, 2008, http://www.6net.org

[2] IPv6 Fix Official Homepage, WIDE Project, 2007, ttp://v6fix.net/index.html

[3] USGv6 Testing Program, NIST, 2010, http://www.antd.nist.gov/usgv6/testing.html

[4] S. Convery and D. Miller, IPv6 and IPv4 Threat Comparison and Best Practice Evaluation, 2004, Cisco Systems, http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf

[5] E. Davies, S. Krishnan, and P. Savola, IPv6 Transition/Coexistence Security Considerations, RFC 4942, IETF, 2007.

[6] S. Hogg and E. Vyncke, IPv6 Security, Addison Wesley, 2008.

[7] M.P. Gallaher and B. Rowe, IPv6 Economic Impact Assessment, NIST, October, 2005.

[8] Advancing the Internet. Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe, Commission of the European Communities, Brussels, 2008, http://www.ipv6.eu/admin/bildbank/uploads/Documents/Commision/ COM_.pdf

[9] M. Botterman, Towards IPv6 Deployment, RIPE 59 Lisbon, 2009, http://ripe59.ripe.net/presentations/botterman-towards-v6-deployment.pdf

[10] E. Nordmark, Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC 4213, IETF, 2005.

[11] J. Hoagland, The Teredo Protocol: Tunneling Past Network Security and Other Security Implications, Symantec, http://www.symantec.com/avcenter/reference/Teredo_Security.pdf, 2007

[12] E. Kent et al., Security Architecture for the Internet Protocol, RFC 4301, IETF, December 2005.

[13] A. Durand, Dual-stack lite broadband deployments post IPv4 exhaustion, Internet-draft, IETF, 2009.

[14] Cisco Visual Networking Index: Forecast and Methodology, 2008- 2013, Cisco, San Jose, 2009.

[15] TAHI Project. Test and Verification for IPv6, http://www.tahi.org

[16] V. Manral, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), RFC 4835, IETF, 2007.

[17] S. Kent and R. Atkinson, IP Encapsulating Security Payload (ESP), RFC 2406, IETF, 1998.

[18] D. Eastlake, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), RFC 4305, IETF, 2005.

[19] V. Rijmen and E. Oswald, Update on SHA-1, Cryptology ePrint Archive Report 2005/010

[20] M.H. Behringer, Why End-to-End Security is Necessary But Not Sufficient, Internet Protocol Journal, Cisco vol. 12. No. 2, Sep. 2009, pp. 20-26.

[21] S. Ioannidis, A. Keromytis, S. Bellovin, and J. Smith, Implementing a Distributed Firewall, Proceedings of Computer and Communications Security (CCS), November 2000.

[22] M. Kaeo, IPv6 Security Technology Paper, North American IPv6 Task Force (NAv6TF) Technology Report, NAv6TF, http://www.ipv6forum.com/dl/white/NAv6TF_Security_Report.pdf.

[23] G. An and J. Nah, Effective Control of Abnormal Neighbor Discovery Congestion on IPv6 Local Area Network, LNCS, Volume 4159/2006, Springer Berlin/Heidelberg, 2006, pp. 966-976.

[24] Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, Data Protection Working Party, European Commission, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58en.pdf, 2002

[25] T. Narten, R. Draves and S. Krishnan, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 4941, IETF, 2007.

[26] Bug ID 6797926, Oracle Corporation, 2011, http://bugs.opensolaris.org/bugdatabase/view_bug.do?bug_id=6797926,

[27] Juniper Security Advisory, UNIRAS, 2006, http://archive.cert.unistuttgart.de/uniras/2006/07/msg00013.html

[28] A. Mankin, Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6, Internet-Draft draft-teammobileip- mipv6-sec-reqts-00, July 2001.

[29] P. Savola, Security of IPv6 Routing Header and Home Address Options, Internet draft, IETF, 2001.

[30] F. Ali, IP spoofing, Internet Protocol Journal, Cisco, volume 10, no 4,Dec. 2007, pp. 2-9.

[31] P. Savola and C. Patel, Security Considerations for 6to4, RFC 3964,IETF, 2004.

[32] A. Durand, P. Fasano, I. Guardini, and D. Lento, IPv6 Tunnel Broker

[33] T. Fujisaki et. al., Operational Problems in IPv6: Fallback and DNS issues, http://www.nttv6.net/~fujisaki/fallback.pdf