Plans for the Security Analysis of IPv4aaS Technologies

Ameen Al-Azzawi
Department of Networked Systems and Services
Budapest University of Technology and Economics
Budapest, Hungary
alazzawi@hit.bme.hu

***Abstract*— This paper focuses on the IPv6 transition technologies, our aim is to identify the potential security issues within these technologies infrastructure and finding the best implementation platform for the technology itself. The paper surveys many transition technologies, their security analyses, their vulnerabilities and what are the best applicable ones in terms of smooth transition and more secured network.**

Moreover, the paper focuses on 464XLAT, its mechanism, architecture, DFD diagram and it gives a summarized overview on the technology, its possible gaps and prioritize these vulnerabilities from the most vulnerable point to the least one.

Keywords—IPv6, DNS64, DNS system, NAT64, Dual Stack, Tunneling, NATing, STRIDE, 464XLAT.

I. Introduction

After the wide spread of the internet usage all over the globe, IPv4 public addresses started to be liable to depletion which happened in 2011[1]. The transition operation itself is expected to be on the run for three decades [2].

Some of the protocols have security vulnerabilities and they are sensitive to different kinds of attacks.

IPv6 was defined in a draft RFC in 1998 [3], while the actual deployment of it took way longer than it should have because of the technical issue it faced with the old equipment and its compatibility with the new proposed IPv6. A lot of technologies were presented to overcome the depletion of IPv4 and to start the transition process to IPv6, such as Dual Stack, Tunnelling and Natting.

A very informative book by Adam Shostack[4] presents us STRIDE theory, which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, those are the terms that can be applied on each possible potential security threat and can be analysed accordingly.

So, this paper's goal is tackle some network security concerns with the idea designing a systematic method to identify the possible security issues of IPv6 transition technologies using STRIDE Theory[5] with understating its DFD (data flow diagram) and trying to come up with new enhanced DFD for the transition structure.

The remainder of this paper is organized as follows. Section II is an overview of the IPv6 transition technologies. Section III is a short summary of the STRIDE method. Section IV is the application of SRIDE to the 464XLAT transition technology.

II. Transition Technologies

❖ Dual stack

The main idea of dual stack is to have a certain node where both IPv4 & IPv6 are usable, with a priority to IPv6. According to [6], dual stack has what is called "Happy Eye-Balls" to choose the better IP version for the packet delivery. However, it doesn't handle the shortage of IPv4 addresses and it isn't a cost-effective solution.

❖ *Tunneling*

There are different types of tunnling used for IPv4aas puposes

6 in 4 Tunnelling

Due to the unfinished infrastructure of IPv6, 6in4 tunnelling was used to carry IPv6 address through IPv4 tunnel to connect IPv6 islands. It normally uses static preconfigured tunnels between two ports [7].

4 in 6 Tunnelling

The idea is to encapsulate IPv4 datagram over IPv6 packer header as defined by RFC 2473 [8].

❖ Natting

NATting is a solution to handle several problems including the shortage of IPv4 addresses, and it has various types: static, dynamic, PAT, etc [9].

A. Translation Type Technologies

1) Single Translation

There are several single translation technologies who caught the attention of many researchers in the field.

[10] classified some of those technologies as their priority goes such as DNS64, NAT64, SIIT, etc.

❖ DNS64 + NAT64

In [11], the process of NAT64 + DNS64 was carefully explained in detail. As shown in Fig. 1, the process consists of 10 steps. It starts with the IPv6 only client

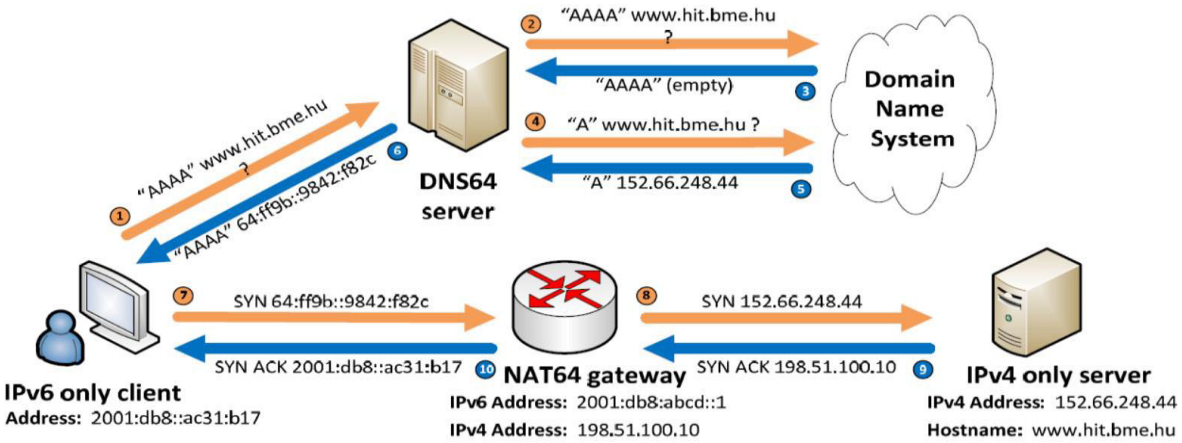

Fig. 1 DNS64+NAT64 Process, IPv6 Only Client contacting IPv4 Only Server [12]

sending a request (AAAA query) to DNS64 asking for an address of IPv4 only server and ends up with the IPv6 only client contacting the IPv4 only server and receives an acknowledgment as well.

The solution is good enough but not perfect as another distinctive drawback emerged to the surface. Some IPv4 only applications don't work with this solution like Skype, Netflix, etc.

- SIIT

  SIIT is the well-known stateless IP/ICMP Packet header translator as defined by RFC 7915s. The idea of SIIT being stateless does put some restrictions on it, while facing with public IPv4 pool depletion [9]. However, it proved to be a sufficient solution coupling with other technologies such as 464XLAT [13].

- SIIT-DC

  This technology focuses on Data centres and its servers' compatibility with IPv6 in terms of serving IPv4 only clients [14].

- NAT-PT

  The old conventional terminology of NAT refers to translate of IPv4 to another IPv4. While NAT-PT is about translating an IPv4 to IPv6 and vice versa. As defined by [15], NAT-PT is to be used when there are no native IPv6 or IPv6 over IPv4 tunnelled ways of communication exists, which means that the main function of NAT-PT is to translate between IPv6 only node and IPv4 only node, without depending of Dual stack whatsoever.

2) Double Translation

This type of translation involves translating an IPv4 packet, when it reaches boundaries of an IPv6 Network into IPv6 packet and then translates it back to IPv4, when they leave IPv6 network and gets back to an IPv4 network. There is one drawback though, and it is that IPv6 packet cannot be carried upon IPv4 packet due to size & data storage limitation issues [10]. There are several Double-Translation methods such as 464XLAT, MAP-T, 4rd, dIVI, etc. In this paper, we are focusing on some of them due to their importance.

- 464XLAT

  So, to go around the problem that NAT64 +DNS64 couldn't solve by their own, a new solution emerged, and it's called 464XLAT [16], the technology was adopted by an American company called T-Mobile. According to [1], this new technology allows IPv6 only networks to run on IPv4 only devices and applications.

  RFC 6877 described 464XLAT as single/dual translation technology [13]. 464XLAT allows ISPs to use only IPv6 in their infrastructure.

  According to [13], CLAT device always placed at the client edge, which performs stateless NAT64 and it normally translates the packets of IPv4 only network into IPv6. It also translates back the returned IPv6 packets to IPv4 so it can be readable within IPv4 only network applications. So, CLAT performs SIIT (stateless Translation algorithm).

  Meanwhile, in the ISP side, there is another device called PLAT which performs Stateful NAT64.

  In conclusion, IPv6-only clients do get IPv6 addresses and they can reach IPv6 servers while they need DNS64+NAT64 to reach IPv4-only servers without the need for double translation process. However, IPv4-only clients need CLAT double translation process to perform the full 464XLAT operation.

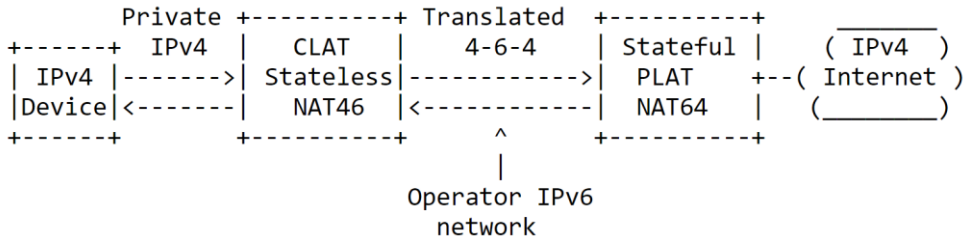

Fig. 2 Overview Architecture of 464XLAT [17]

According to [1], no previous testing process was conducted on CLAT on its different platforms because CLAT run on the customer edge and it could be anything like (iPhone, Android, etc.).

Fig. 2 presents the overview architecture of 464XLAT, it shows the chain of communication and translation steps that being conducted in order to ensure that IPv6 is being used on every platform no matter what even within IPv4-only applications.

❖ MAP-T

MAP-T [18] was adopted by an IETF RFC-7599 and its high-level operation is similar to that of 464XLAT, but MAP-T is much more complicated. It uses different set of terminology and equipment such as: -

- CE (Customer-Edge): according to [18], performs NAT44 in order to maintain a low users port number of TCP /UDP, then it conducts a stateless translation from IPv4 to IPv6 encoding IPv4 source address & port number into the IPv6 source address. The process has two scenarios, the first one is that the packet will be destined to another user within the IPv4 network, where another CE process will occur, but if the packet is heading toward a destination which is outside the IPv4 network, then BR will come in handy as explained below.
- BR (Border-Relay): performs the transformation where a packet has been translated by CE and wants to go out from the IPv4 network.

B. Encapsulation

❖ MAP-E

As defined by [13], MAP-E uses stateless algorithm in order to embed part of IPv4 address into the IPv6 prefix which allows huge number of clients to be provisioned using single MAP rule. At CE, the router runs a stateful NAPT44 operation in order to translate IPv4 private source address and source port into an address and a port range. Moreover, at the CE router begins the encapsulation of IPv4 packet inside IPv6 packet and send it to another host within the MAP domain or to BR if the destined packet to area not covered by MAP rules. The BR will start the decapsulation procedure from his side (decapsulating IPv6 into IPv4).

❖ DUAL-STACK LITE

An IETF RFC 6333 defined DS-Lite.

In CE, DS-Lite uses "Basic Broadband Bridging" B4 to encapsulate IPv4 into IPv6 packet then send it through IPv6 network to AFTR (Address Family Transition Route) which will perform the encapsulation / decapsulation process of the 4in6 data and then it performs a Stateful NAPT44.

❖ LIGHTWEIGHT 4OVER6

Lightweight 4over6 is an extension of DS-Lite, but it has some different aspects where the NAPT function is relocated from AFTR to customer's B4 element which is called "lwB4". In this case, AFTR conducts A+P routing (Address + Port number) and 4in6 encapsulation / decapsulation.

Direct communication between two lwB4s is being done through hair pinning traffic through lwAFTR, RFC 6333.

III. STRIDE IN A NUTSHELL

Stride stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege and they are general attack types explained below in details:

- Spoofing: in general, it is claiming to be someone that it is not you, or someone pretends to be your website [4]. Concerning computer networks, it often means the usage of the IP address of another device as source IP address to gain unauthorized access to some resources or to hide the real identity of the attacker [1].
- Tampering: the attacker might play and change something in the flowing data while it bounces back and forth between two nodes [4].

Element	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data Flows		✓		✓	✓	
Data Stores		✓		✓	✓	
Processes	✓	✓	✓	✓	✓	✓
Interactors	✓		✓			

Table. 1 Vulnerability of different DFD Elements to different Threats [1]

- Repudiation: is the claim that a host didn't do something or not responsible or a specific act / behaviour [4].
- Information Disclosure: An attacker getting confidential information that he shouldn't have got it [1], like the TTL value of specific packet within DNS64 server.
- Denial of Service: The attacker floods the targeted network server with huge number of useless requests (queries) which causes preventing the legitimate user from contacting or accessing the designated server [1]
- Elevation of Privilege: incorrectly allowing a user /hacker to access an un-authorized server/ service [4].

The STRIDE method uses the DFD (Data Flow Diagram) of the examined system for its security analysis. The DFD is build up by four types of elements: Data Flows, Data Stores, Processes and Interactors. Each one of the four elements is susceptible to some of the before mentioned threats but not susceptible to some others. Table. 1 shows the DFD elements and the threats that they are susceptible to marked with a ✓ sign.

IV. Towards the Threat Analysis of 464XLAT

In this chapter, we will be focusing on 464XLAT, its security analysis by applying STRIDE theory and analysing its DFD diagram focusing on possible vulnerable spots and taking in consideration the previous implementation handled by [1].

Fig.3 shows the DFD for the threat analysis of 464XLAT. By applying the STRIDE method on this DFD, the threats that might face each element within 464XLAT architecture may be discovered.

My plan to perform STRIDE on DFD in Fig. 3 is to check all possible vulnerabilities (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) at each DFD element (1-14) and prioritize the level of threat at each element then come up with analysis of the most vulnerable element within the DFD and classify the threats based on number of their possible occurrence in order to tackle them top to bottom.

Conclusion

Among all surveyed transition technologies, 464XLAT proved to be a suitable one while it has some security threats. It solved the problem of IPv4 only applications in an IPv6 environment and the CLAT+PLAT solution is very practical solution for this issue. Further research is required in this area and that requires testing the NAT64 gateway and examine its behaviour under different circumstances using some free (open source) software.

Acknowledgment

Thanks to my Supervisor; Dr. Gabor Lencse, Budapest University of Technology & Economics, who helped me all the way through with my research.

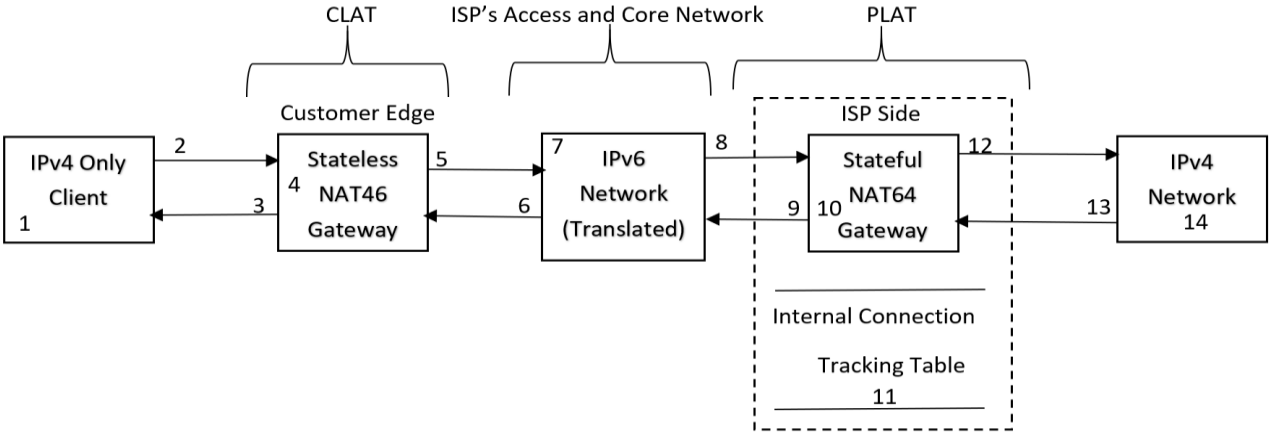

Fig. 3 DFD of the threat Analysis of 464XLAT (CLAT + PLAT)

REFERENCES

[1] G. Lencse and Y. Kadobayashi, "Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64", Computers & Security, vol. 77, no. 1, pp. 397-411, August 1, 2018, DOI: 10.1016/j.cose.2018.04.012.

[2] M. Nikkhah, R. Guerin, "Migrating the Internet to IPv6: An exploration of the when and why", IEEE/ACM Transactions on Networking vol. 24, no 4, (2016) pp. 2291-2304. DOI:10.1109/TNET.2015.2453338.

[3] S. Deering, R. Hinden, Internet protocol, version 6 (IPv6) specification, IETF RFC 2460 (1998). DOI:10.17487/RFC2460.

[4] A. Shostack, Threat Modeling: Designing for Security, Wiley &Sons, Indianapolis, Indiana, USA, 2014.

[5] S. Hernan, S. Lambert, T. Ostwald, A. Shostack, Threat modelling: Uncover security design flaws using the STRIDE approach, MSDN Magazine 6 (11) (2006) 68-75.

[6] Cert, Vulnerability note VU#23495: DNS implementations vulnerable to denial-of-service attacks via malformed DNS queries, VU #23495 2001.

[7] E. Nordmark, R. Gilligan, "Basic transition mechanisms for IPv6 hosts and routers", IETF RFC 4213, Oct. 2005.

[8] A. Conta, S. Deering, "Generic packet tunneling in IPv6 specification", IETF RFC 2473, Dec. 1998.

[9] Network Protocols Handbook, 2nd ed., Javvin Technologies Inc. 2005. p. 27. ISBN 9780974094526. Retrieved 2014-09-16.

[10] G. Lencse and Y. Kadobayashi, "Comprehensive Survey of IPv6 Transition Technologies: A Subjective Classification for Security Analysis" IEICE Transactions on Communications, vol. E102-B, no.10, (to appear in October 2019) DOI: 10.1587/transcom.2018EBR0002.

[11] G. Lencse, A. G. Soós, "Design of a tiny multi-threaded DNS64 server", in: Proc. 38th International Conference on Telecommunications and Signal Processing (TSP 2015), Prague, Czech Republic, 2015, pp. 27-32. DOI:10.1109/TSP.2015.7296218.

[12] Internet Systems Consortium, "BIND: Versatile, classic, complete name server software", [Online]. Available: https://www.isc.org/downloads/bind

[13] G. Lencse, J. Palet Martinez, L. Howard, R. Patterson, I. Farrer, "Pros and cons of IPv6 transition technologies for IPv4aaS", active Internet Draft, Jul. 2019, https://tools.ietf.org/html/draft-lmhpv6opstransition-comparison-03

[14] T.Anderson, "SIIT-DC: Stateless IP/ICMP translation for IPv6 data center environments", IETF RFC 7755, Feb. 2016.

[15] G. Tsirtsis and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", IETF RFC 2766, Feb. 2000.

[16] M. Mawatari, M. Kawashima, C. Byrne, "464XLAT: Combination of stateful and stateless translation", IETF RFC 6877, Apr. 2013.

[17] G. Lencse, D. Bakai, "Design and implementation of a test program for benchmarking DNS64 servers", IEICE Transactions on Communication vol. E100-B, no 6, (2017) pp. 948-954. DOI:10.1587/transcom.2016EBN0007.

[18] X. Li, C. Bao,W. Dec (ed), O. Troan, S.Matsushima, T.Murakami, "Mapping of address and port using translation (MAP-T)", IETF RFC 7599, Jul. 2015.