A Holistic Threat Analysis of IPv6 Transition Technologies

Marius Georgescu
liviumarius-g@is.naist.jp

Internet Engineering Laboratory
Nara Institute of Science and Technology
Japan

November 5, 2015

The IPv6 transition

- IPv6 is not backwards compatible
- The Internet is undergoing a period through which both protocols will coexist
- Currently only approx. 4 % of worldwide Internet users have IPv6 connectivity [1]

[1] APNIC. *IPv6 measurements for The World*. Asia-Pacific Network Information Centre, July 2015. URL: http://labs.apnic.net/ipv6-measurement/Regions/.

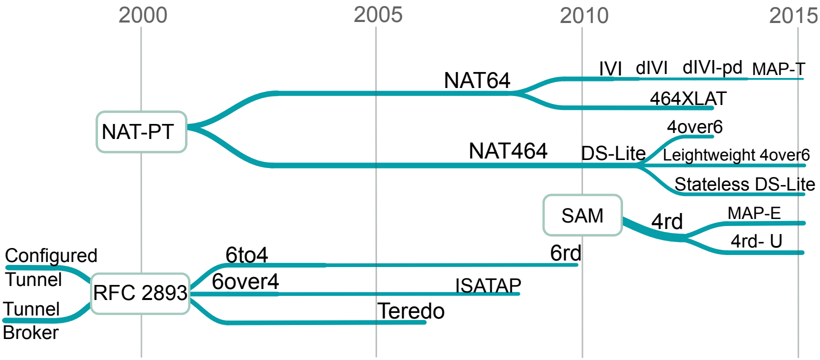
[2] **Original drawing by Andrew Bell @ www.creaturesinmyhead.com** .

The Motivation

What are the security implications of using an IPv6 transition technology?

- What is the use case?
- What are the protected assets ?
- What are the threats ?
- What are the mitigations?

IPv6 Transition Technologies Evolution



[3] inspired by the APNIC35 presentation "The evolution of IPv6 transition technologies" by Jouni Korhonen.

IPv6 transition tech generic categories

1. **Single Translation**: either IPv4 or IPv6 is used to traverse the core network and translation is used at one of the edges
2. **Dual-stack**: the core network devices implement both IP protocols
3. **Encapsulation**: an encapsulation mechanism is used to traverse the core network; CE nodes encapsulate the IPvX packets in IPvY packets, while PE nodes are responsible for the decapsulation process.
4. **Double Tarnslation**: a translation mechanism is employed for the traversal of the network core; CE nodes translate IPvX packets to IPvY packets and PE nodes translate the packets back to IPvX.

[4] M. Georgescuand and G. Lencse. *Benchmarking Methodology for IPv6 Transition Technologies*. I-D (Informational). Internet Engineering Task Force, Oct. 2015. URL: http://tools.ietf.org/html/draft-ietf-bmwg-ipv6-tran-tech-benchmarking-00.

Threat analysis: a step-by-step approach

1. What is the role played by the IPv6 transition technology?
2. What is the category the technology would fit in?
3. What is the technology composed of?
   3.1 What are the subcomponents and associated protocols?
   3.2 What are the protected assets and the potential entry points for an attacker?
   3.3 What are the trust boundaries, and how is that reflecting on the entry points? boundaries ?
4. What are the threats?
   4.1 What are the basic threats introduced by the subcomponents and protocols?
   4.2 How can we associate these threats with the STRIDE categories?
   4.3 Can any complex threats result from the interactions between the basic threats?
5. How can we mitigate these threats?
6. How valid are things we discovered in the previous steps?

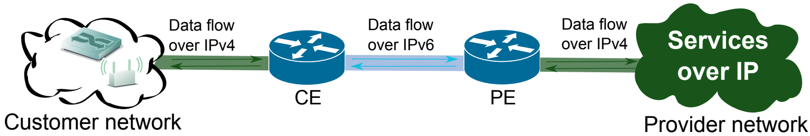
[5] Adam Shostack. *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

The STRIDE threat cassification

Threat	**Desired property**	**Examples**
Spoofing	Authetication	IP address spoofing
Tampering	Integrity	Modify the contents of a state table
Repudiation	Accountability	Hide the source IP of an attack
Information disclosure	Confidentiality	packet analysis
Denial of Service	Availability	ICMP flooding
Elevation of privilege	Authorization	Access privileged parts of the network

A study case: MAP-T

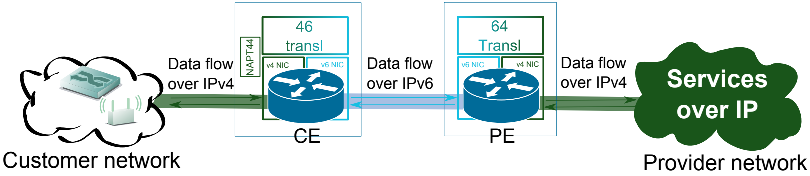
1. What is the role played by the IPv6 transition technology?
   - A secure data exchange between a Customer and a service provided over IPv4. That includes data processing and routing.
2. What is the category the technology would fit in?
   - Double Translation. A basic use case would need a CE device to translate from 4 $\rightarrow$ 6 and a PE to translate back from 6 $\rightarrow$ 4.



[6] X. Li et al. *Mapping of Address and Port using Translation (MAP-T)*. . RFC 7599 (Proposed Standard). Internet Engineering Task Force, July 2015. URL: https://tools.ietf.org/html/rfc7599.

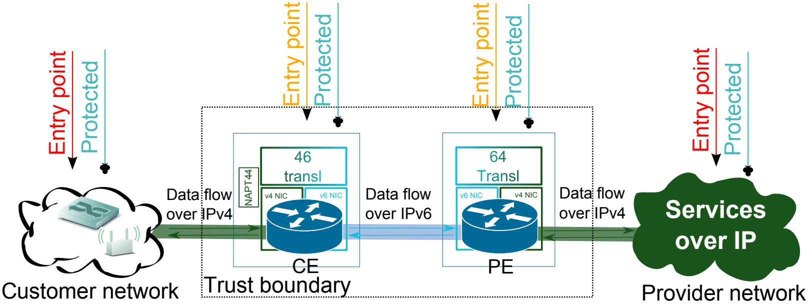
MAP-T: subcomponents

3. What is the technology composed of?
   3.1 What are the subcomponents and associated protocols?



MAP-T: entry points, protected assets

3. What is the technology composed of?
   - 3.2 What are the protected assets and the potential entry points for an attacker?
   - 3.3 What are the trust boundaries, and how is that reflecting on the entry points?



MAP-T: some of the basic threats

4. What are the threats?
   4.1 What are the basic threats introduced by the subcomponents and protocols?
   4.2 How can we associate these threats with the STRIDE categories?
5. How can we mitigate these threats?

No	Description	Protocol /Entry point	S	T	R	I	D	E	Mitigation	Likelihood
1	ARP Cache Poisoning	IPv4 suite CN, CE,PE, PN	✓	✓	✓	✓	✓		Use static ARP entries or arpwatch	High
2	Port set exhaustion	NAPT44 CN, CE					✓		Filter depending on IP Address	High
3	Authentication Headers cannot be used over an IPv6-to-IPv4	64transl PE, PN				✓			No widely-accepted mitigation	Low
4	ND Good router goes bad	IPv6 suite CE, PE	✓	✓	✓	✓	✓	✓	No widely-accepted mitigation	Low
5	NS/NA Spoofing	IPv6 suite CE, PE	✓	✓	✓	✓	✓	✓	Use SEND	Low
6	ICMPv6 flooding	IPv6 suite, transl CE, PE					✓		ICMP error ratelimiting mechanism	Low
7	OSPFv2 simple password authentication	OSPFv2 CE, PE	✓	✓	✓	✓	✓	✓	The use of cryptographic authentication	Low
8	OSPFv3 used without IPsec	OSPFv2 CE, PE	✓	✓	✓	✓	✓	✓	The use of IPsec	Low

MAP-T: some convoluted threats

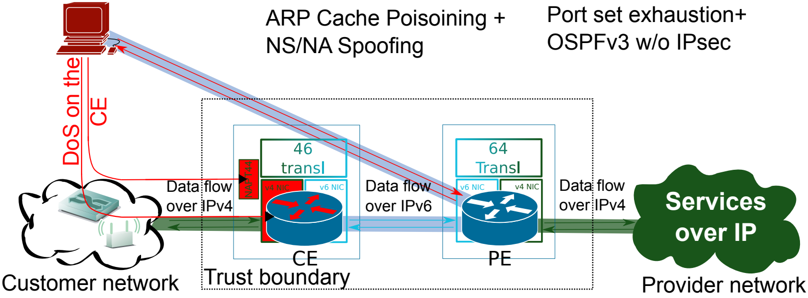
4. What are the threats?
   4.3 Can any complex threats result from the interactions between the basic threats?

Convoluted Threat1

ARP Cache Poisoining +
NS/NA Spoofing

Convoluted Threat2

Port set exhaustion+
OSPFv3 w/o IPsec



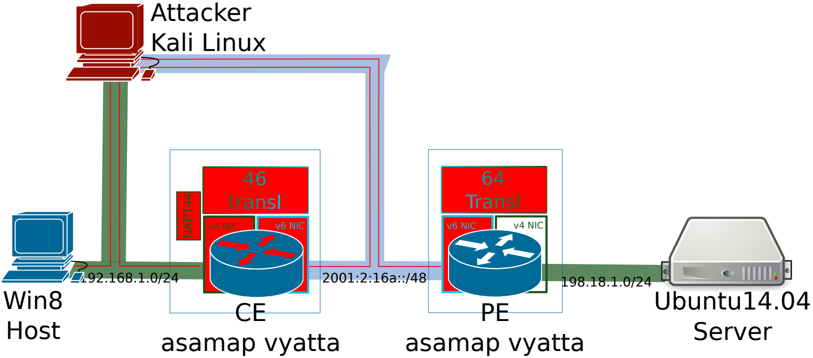
MAP-T: some more convoluted threats

4. What are the threats?
   4.3 Can any complex threats result from the interactions between the basic threats?
5. How can we mitigate these threats?

No	Description	Protocol /Entry point	S	T	R	I	D	E	Mitigation	Likelihood
1	ARP Cache Poisoning+ NS/NA Spoofing	IPv4, IPv6 CN, CE,PE, PN	✓	✓	✓	✓	✓	✓	static ARP entries, arpwatch, SEND	High
2	Port set exhaustion+ OSPFv3 w/o IPsec	NAPT44, OSPFv3 CN, CE, PE, PN	✓	✓	✓	✓	✓	✓	Selective IP filter, IPsec	High
3	OSPFv3 w/o IPsec+ ICMPv6 flooding	OSPFv3, transl CE, PE				✓	✓		IPsec, SEND	High
4	ICMPv6 flooding+ NS/NA Spoofing	IPv6 suite CE, PE	✓	✓	✓	✓	✓	✓	ICMP filtering, SEND	Low
5	OSPFv3 w/o IPsec+ NS/NA Spoofing	OSPFv3, IPv6 CE, PE	✓	✓	✓	✓	✓	✓	IPsec, SEND	Low

MAP-T: PenTestbed

6. How valid are things we discovered in the previous steps?
   - PenTestbed setup



MAP-T: Pentesting the basic threats

6. How valid are things we discovered in the previous steps?
   - Preliminary penetration test data

No	Threat Description	Tool	Emulated
1	ARP Cache Poisoning	Ethercap	✓
2	Port set exhaustion	nmap	✓
3	Authentication Headers cannot be used over an IPv6-to-IPv4	tcpdump	X
4	ND Good router goes bad	fake_router6	X
5	NS/NA Spoofing	fake_advertise6	✓
6	ICMPv6 flooding	smurf6	✓
7	OSPFv2 simple password authentication	tcpdump	✓
8	OSPFv3 used without IPsec	tcpdump & asamap vyatta	✓

MAP-T: Pentesting the convoluted threats

6. How valid are things we discovered in the previous steps?
   - Preliminary penetration test data

No	Threat Description	Tools	Emulated
1	ARP Cache Poisoning+ NS/NA Spoofing	Ethercap + fake_advertise6	✓
2	Port set exhaustion+ OSPFv3 w/o IPsec	nmap+ tcpdump+ asamap vyatta	✓
3	OSPFv3 w/o IPsec+ ICMPv6 flooding	tcpdump+ smurf6	✓
4	ICMPv6 flooding+ NS/NA Spoofing	smurf6+ fake_advertise6	✓
5	OSPFv3 w/o IPsec+ NS/NA Spoofing	tcpdump+ fake_advertise6	✓

OSPF w/o IPsec + NS/NA Spoofing

Implications

- The lack of higher levels of trust (shared secrets) between CE and PE can lead to disastrous consequences on the security of a production network
- A holistic analysis of threats can reveal that what looks like a mediocre backdoor can become a veritable grand entrance
- The concerns related to the deployment of IPv6 transition technologies are justified. The threats from both IP protocol suites need to be considered, as well as the interactions between the protocol stacks and subcomponents.

Take-aways

- IPv6 transition technologies generic classification
- MAP-T (non-exhaustive) threat analysis
- MAP-T: preliminary penetration test data
- A holistic approach to threat modeling can reveal more complex threats
- **STRIDE** seems to work for IPv6 transition technologies as well

Next Steps

- An extended threat analysis for IPv6 transition technologies
- More penetration testing to further validate threat patterns
- A risk quantification approach $\rightarrow$ Security quantification approach for IPv6 transition technologies

Questions for SAAG

- Is RFC4942 enough as security analysis for IPv6 Transition Technologies?
- Would an I-D containing an extension of this work find its place in the IETF?
- Would it make sense to have a similar **Threat Model** in the **Security Considerations** of standards developed in the IETF?

Thank you for your attention!

Marius Georgescu
liviumarius-g@is.naist.jp
www.ipv6net.ro