The STRIDE Towards IPv6: A Comprehensive Threat Model for IPv6 Transition Technologies

M. Georgescu, H. Hazeyama, T. Okuda, Y. Kadobayashi and S. Yamaguchi
Nara Institute of Science and Technology, 891-6 Takayama, Ikoma, Nara, Japan

Keywords: IPv6 Transition Technologies, Threat Model, STRIDE, Dual-stack, Single Translation, Double Translation, Encapsulation.

Abstract: The IPv6 worldwide deployment rate is still a single figure. This is due to the many challenges introduced by the transition period through which both IPv4 and IPv6 will need to coexist. One of the biggest concerns related to the IPv6 transition is security, which is more difficult to ensure in a heterogeneous environment. To clarify the security threats introduced by IPv6 transition technologies, this article proposes a comprehensive threat model built around the established STRIDE approach. To verify the usefulness of the proposed model, a threat analysis of four generic categories of IPv6 transition technologies is performed. Existing and new threats are documented, classified and prioritized. To further validate some of the documented threats, preliminary penetration test data is presented.

1 INTRODUCTION

The IPv4 address space exhaustion is imminent and can affect the further expansion of the Internet. The Internet Assigned Numbers Authority (IANA) has allocated on February 3rd 2011 the last blocks of IPv4 addresses (NRO, 2014). Four out of the five Regional Internet Registries (RIR) have entered the last stage of IPv4 exhaustion. A detailed report is presented in (Huston, 2015) by APNIC's G. Huston. IPv6 was introduced in 1998. However, the IPv6 worldwide deployment rate is still very low, approaching 5% as the APNIC Labs (APNIC, 2015) report. The root cause for this low deployment status is the lack of backwards compatibility between IPv6 and IPv4. In other words, IPv4-only nodes and IPv6-only nodes cannot communicate directly. That means transition mechanisms have to be used and also that the Internet has to undergo a period through which both protocols have to coexist. This period can be simply referred as the IPv6 transition.

Aside from the larger address space, IPv6 has, in theory, a number of advantages over its predecessor in terms of design: a more efficient and extensible datagram, improved routing with easier route computation and aggregation, stateless autoconfiguration and mandatory security. Over the years, however, some of these new features have proved to be either challenges for enforcing security (e.g. extension headers, stateless autoconfiguration), or not-feasible (e.g. widespread deployment of IPv6 with IPsec). The IPv6 transition has further aggravated these challenges as transition technologies are generally exposed to the threats associated with both IP versions and hybrid blends, depending on the subcomponents.

When building an IPv6 transition plan, security is arguably the biggest concern for network operators, as a heterogeneous IPv4 and IPv6 environment greatly increases the attack surface. To that end, building a threat model for IPv6 transition technologies can help clarify and categorize the associated security threats. In turn, this should facilitate the search for mitigation techniques and can lead to a security quantification method for IPv6 transition implementations. Considering all of the above, this article proposes a threat model built around the well established STRIDE approach described in (Hernan et al., 2006). The STRIDE mnemonic is used to classify the documented threats. The correlations between elements of the Data Flow Diagrams (DFD) and the STRIDE threat categories detailed in (Hernan et al., 2006) are used for the initial basic assessment of the threats for each of the sub-elements.

The generic STRIDE approach represents only the base of our proposal. The main contribution lies in identifying the threat modeling steps necessary for IPv6 transition technologies in particular. To prove the validity of the proposal, the model is used to de-

Georgescu, M., Hazeyama, H., Okuda, T., Kadobayashi, Y. and Yamaguchi, S.
The STRIDE Towards IPv6: A Comprehensive Threat Model for IPv6 Transition Technologies.
DOI: 10.5220/0005652402430254
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 243-254
ISBN: 978-989-758-167-0

fine and categorize existing and new threats for the four generic types of IPv6 transition technologies. The resulting non-exhaustive threat analysis and penetration test data can be considered another important part of the contribution of this work.

The rest of the paper is organized as follows: Section 2 gives an overview of IPv6 transition technologies, Section 3 presents related literature, in Section 4, we introduce the proposed threat model, section 5 discusses our approach and lastly section 6 states the conclusions.

2 IPv6 TRANSITION

IPv6 was not designed to be backwards compatible. Consequently, in a heterogeneous environment coexistence and transition technologies need to be employed. Initially, three basic transition mechanisms were proposed: dual-stack, translation and tunneling. The associated implementation standards are presented in RFC 4213 (Nordmark and Gilligan, 2005) and RFC 6144 (Baker et al., 2011).

For dual-stack, IPv4 and IPv6 are implemented on the same node. This method is used mostly for host-side nodes and edge nodes. The biggest challenge introduced by dual-stack is overhead. Translation is the only method which ensures direct communication between IPv4 and IPv6 by translating the message format and information between different versions of Internet Protocol. The complication introduced by translation is breaking the end-to-end characteristic of the Internet, something that IPv6 was supposed to bring back. Tunneling or encapsulation is used to traverse heterogeneous network environments, by encapsulating the IPvX packets into the payload of IPvY packets, where $X, Y \in \{4, 6\}$. At the border of the IPvY and IPvX networks the packets are decapsulated back into IPvX by an edge router. Tunneling mechanisms are mainly confronted with fragmentation problems because of encapsulation.

In an attempt to compensate for the design simplicity of the two IP versions, IPv6 transition technologies grew in complexity. Most of the modern transition technologies use one or more basic transition technologies. For instance, Dual-Stack Lite (DSLite)(Durand et al., 2011) used dual-stack and translation at the edge nodes and encapsulation in the core. Considering all of the above, a generic classification of the transition technologies can prove useful.

2.1 IPv6 Transition Technologies Generic Categories

We can consider a basic production IP-based network as being constructed using the following components:

- Customer Edge (CE) segment: connects the customer network to the production network's core.
- Core network segment: the main part of the production network, which connects the CE and PE segments.
- Provider Edge (PE) segment: connects the core network to the up-link provider.

According to the technology used for the core network traversal, the IPv6 transition technologies can be categorized as follows:

1. Dual-stack: the core network devices implement both IP protocols
2. Single translation: either IPv4 or IPv6 is used to traverse the core network, and translation is used at one of the edges
3. Double translation: a translation mechanism is employed for the traversal of the core network; CE nodes translate IPvX packets to IPvY packets and PE nodes translate the packets back to IPvX.
4. 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.

Table 1 shows how some of the existing IPv6 transition technologies can fit into the generic categories.

3 RELATED WORK

Threat models have been proposed and used for the security analysis of online applications for some time. Probably the most popular is the one introduced in (Hernan et al., 2006), more commonly known as the STRIDE approach. At the heart of the proposal is the STRIDE mnemonic, which stands for **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service and **E**levation of privilege, a set of generic security threats. The mnemonic offers a simple and comprehensible classification base. Using STRIDE in conjuncture with a good understanding of the system's components, can result in a good overview of the threats and possible mitigation directions. As a measure of its success, the STRIDE categories are used as well in (OWASP, 2015), the threat

Table 1: IPv6 transition technologies association.

	Generic category	IPv6 Transition Technology
1	Dual-stack	Dual IP Layer Operations(Nordmark and Gilligan, 2005)
2	Single translation	NAT64(Bagnulo et al., 2011), SIIT-DC(Anderson, 2015), SA46T-AT(Matsuhira, 2015), IVI(Li et al., 2011b)
3	Double translation	464XLAT(Mawatari et al., 2013), MAP-T(Li et al., 2015), dIVI(Bao et al., 2014)
4	Encapsulation	DSLite(Durand et al., 2011), Lightweight 4over6(Tsou et al., 2015), MAP-E(Troan et al., 2015)

modeling process used by the Open Web Application Security Project (OWASP). Furthermore, in (Gervais, 2012), the STRIDE approach has been used to model the threats of industrial control systems.

As for the security of IP-based systems, there are many articles in current literature dedicated to the issues introduced by IPv4 and IPv6. In terms of IPv4 security, we have consulted the following references: (Harris and Hunt, 1999), (Gont, 2011),(Low, 2001), (Abad et al., 2007), (Khallouf et al., 2005). As for IPv6 security, the following documents were very helpful: (Davies et al., 2007), (Convery and Miller, 2004), (Pilihanto, 2011). These documents have done a fine job of documenting existing threats for the two protocols and basic transition mechanisms. However, a threat model for IPv6 transition technologies has not emerged so far.

Threat modeling has proved useful for understanding the security of intricate systems. The main reason is its structured approach, which allows one to discover, categorize and classify the threats according to their potential impact on the system. Considering the complicated nature of IPv6 transition technologies, threat modeling makes a good candidate for better understanding their security implications. The proposed model aims to open this path, which could lead as well to a better understanding of the inner-workings of IPv6 transition technologies.

4 THREAT MODEL

The proposed threat model involves a series of steps which were inspired by the STRIDE modeling approach presented in (McRee, 2009) and the Open Web Application Security Project (OWASP) foundation's application threat modeling guidelines (OWASP, 2015). In the context of IPv6 transition technologies we recommend the following steps.

(1) Establish the Function: the function of the IPv6 transition technology needs to be clearly documented. Depending on the context, the technology can incorporate multiple services, which need to be clearly identified in order to perform an effective threat analysis.

(2) Identify the IPv6 Transition Technology Category: the category should be identified considering the generic classification defined in Section 2.1. This step will help build the data flow diagram (DFD) used in the following steps.

(3) Decompose the Technology: build a data flow diagram (DFD) and highlight the entry points, protected resources and trust boundaries. The entry points should be assigned a level of trust considering the trust boundaries. The external entities, process, data store and data flow elements should be depicted in the same diagram as defined in (Hernan et al., 2006). The IP protocol suite and the protocols used for the designated function should be identified as well. This can narrow down the attack surface.

(4) Identify the Threats: The STRIDE model associates the six categories of threats to each of the elements described in the DFD. Based on this association, we get an initial assessment of the threats as shown in Table 2. To clarify, a data flow, for example, is more susceptible to tampering, information disclosure and denial of service threats. The initial threat assessment must be followed by a detailed analysis which should consider the protocols used in conjuncture with the transition technology.

Considering the level of trust assigned to each entry point, an associated likelihood of attack from that entry point can be deduced. For example, if the entry point is considered trusted, we can assume the likelihood of an attack is low. By extrapolating, the six categories of STRIDE attacks could be assigned a likelihood, considering that their association with the DFD elements that are entry points. For instance, if we have an untrusted entry point which is also an external entity, for which we can have spoofing and repudiation as potential threats, the two types of attacks can be considered to have a high likelihood, as they would be exploited from an untrusted entry. Using this logic, by associating the detailed threats with the STRIDE model and the DFD elements they could be applied to, we can assign each threat a likelihood value. This can represent a base for prioritizing mitigation solutions. Each discovered threat should be documented by using the following format.

Field Name	Description
Threat_ID	A code associated with each identified threat
Description	A summarized description of the threat
STRIDE	The association with the STRIDE categories
Mitigation	Details about existing mitigation solutions
Likelihood	Likelihood of the threat being exploited
Validation	Empirical validation data

For an easy reference in future publications the **[Threat_ID]** should follow the format: *[Code]-[First*

Table 2: STRIDE threats per element.

	Spoofing	Tampering	Repudiation	Info Disclosure	Denial of Service	Elevation of Privilege
External	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store		✓	†	✓	✓	
Data Flow		✓		✓	✓	

Author Initials]-[Publication Submission Year]-[Serial number]. For an author named John Doe, who is submitting a publication proposal in 2015, an example ThreatID is: *IPv6-JD-2015-1*. The serial number is incremented with each threat found for a particular protocol or technology. A list of codes for the basic transition technologies and generic transition technologies can be found in the Appendix, Table 4. For the well-known TCP/IP protocol suite we have used the usual acronyms as codes. As the subcomponents interact and the used protocols stack, the threats can fuse and result in convoluted threats with a higher likelihood of exploitation. Depending on the list of discovered threats, the possibility of a fusion between threats should be analyzed.

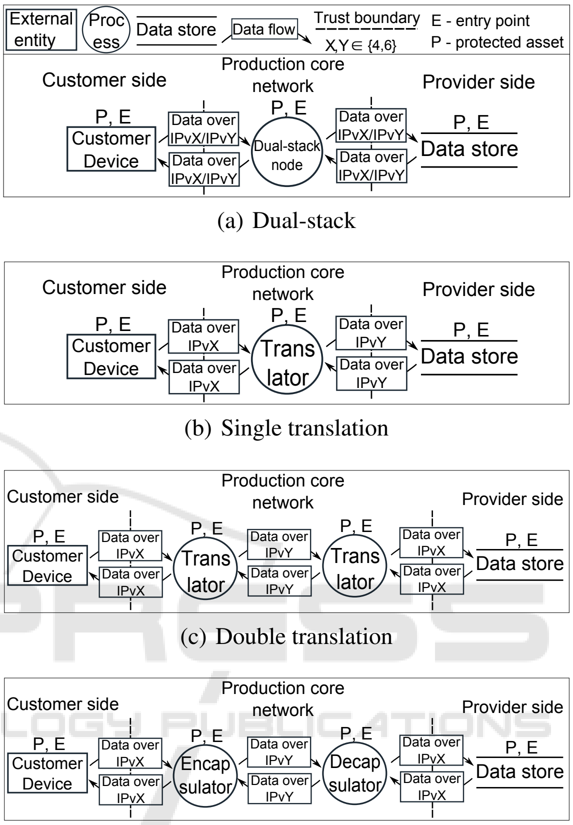
(6) Review, Repeat and Validate: steps 1 and 3 have to be reviewed in the context of potential changes in the technology function and associated protocols. Step 4 should be repeated periodically, as threats may have been overlooked, or the context set by steps 1 and 3 may have changed. If the transition technologies have existing implementations, the analysis should be confirmed with empirical data. To that end, penetration testing can be used.

In the following subsections, the proposed threat modeling technique is used for the four generic IPv6 transition technologies categories defined in Section 2.1. The threat models can be viewed as a starting point for IPv6 transition technologies associated with each category.

4.1 Dual-stack IPv6 Transition Technologies

4.1.1 Establish the Function

The function for dual-stack transition technologies is to ensure a safe data exchange over a dual-stack infrastructure. In other words, the data can be transfered over both IPv4 and IPv6. From a network service perspective, the main function is data forwarding. This includes interior gateway routing solutions. We start with the assumption that services such as address provision, DNS resolution or exterior gateway routing are performed by other nodes within the core network. This assumption in common for all the four generic categories of IPv6 transition technologies.



(a) Dual-stack

(b) Single translation

(c) Double translation

(d) Encapsulation

Figure 1: Data Flow Diagrams for the generic IPv6 transition technologies categories.

4.1.2 Identify the IPv6 Transition Technology Category

This step is meant for more specific transition technologies. Since we are targeting the generic category itself, the step is unnecessary here. This stands for the other three categories as well.

4.1.3 Decompose the Technology

A DFD for dual-stack transition technologies is presented in Figure 1(a). The diagram represents the basic use case and includes a minimal set of elements. On the customer side, we have a Customer Device which initiates the data exchange. It represents one of the entry points of the system and contains im-

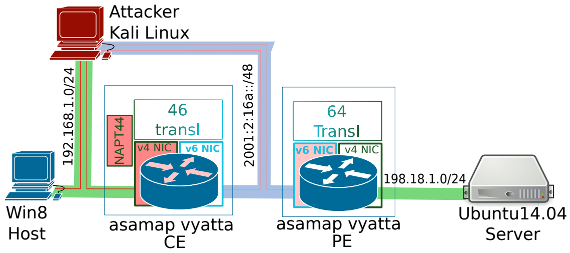


Figure 2: MAP-T Penetration Testbed

portant data, which should be regarded as an asset and protected. The Customer Device is regarded as an external element because it is outside the control zone of the production network. The data request is transmitted over IPv4 or IPv6 to a Dual-stack node. The Dual-stack node is another entry point and contains valuable topology information which should to be protected as well. The Dual-stack node forwards in turn the data request to the provider data store. The Data store is another entry point in the system and it is assumed to contain valuable data. The data reply is forwarded back and makes its return on the same path.

The only trusted entry point in the system is the Dual-stack node. The other two entry points are considered untrusted, since they are outside the control of the production network.That means they can be exploited with a higher likelihood by an attacker. Considering the data can be transferred over both IPv4 and IPv6, we need to consider IP protocol suites. Furthermore, the possibility of using security and routing protocols should be considered.

4.1.4 Identify the Threats

By analyzing the DFD in association with the STRIDE threats per element chart, we can observe that the Customer Device can be subject to spoofing and repudiation attacks. It being an untrusted entry point, it means there is a high likelihood of an attack. The Dual-stack node can be subject to all six types of attacks. However, the likelihood of that happening is low, considering it is a trusted entry point. The Data flow is vulnerable to tampering, information disclosure and denial of service. Considering it traverses untrusted parts of the system, the level of likelihood of an attack on the data flow is high. Lastly, the Data store could potentially be targeted by tampering, repudiation, information disclosure and denial of service attacks. The likelihood for these to happen is high as well, the data store being an untrusted entry point.

Tables 5,7, 6, 8, 9 and 10 of the Appendix contain a non-exhaustive collection of existing threats, which have been collected by surveying a part of existing literature on this subject. For further documentation, each threat has been provided with a reference in the first column. For reuse purposes, the threats are organized according to the categories of protocols which would be necessary for accomplishing the function of the IPv6 transition technologies.

For dual-stack transition technologies the protocol threats associated with the IPv4 suite (Table 5), IPv6 suite(Table 7), routing (Table 8) and switching (Table 10) could potentially be exploited from the 3 entries of the system: the **untrusted - High likelihood of exploitation** Customer device (External entity), **trusted - Low likelihood of exploitation** Dual-stack node (Process) and **untrusted - High likelihood of exploitation** Provider Data store (data store).

The IPv4 suite, transport layer and most of the IPv6 suite protocols are associated with all the elements of the DFD. By extrapolation, their threats have a high likelihood of occurrence. Some of the IPv6 protocol threats (Table 7), namely ND-MG-2015-3 to ND-MG-2015-6 and the Layer 2 technologies' threats (Table 10) can only be associated with routers or switches. In this context, they could only be associated with the Dual-stack node. That means they have a low likelihood of occurrence. Similarly, the routing protocols can only be associated with the Dual-stack node. By association, they also have a low likelihood of being exploited.

By analyzing the interaction between the three elements of the DFD (Figure 1(a)) and the protocols used by Dual stack transition technologies, we can uncover other threats. For example, if the ARP-MG-2015-1(ARP cache poisoning) is used to perform a Denial of Service attack on the Dual-stack node from the Customer device, the likelihood of exploitation rises for the ND-MG-2015-10 (ND Replay Attacks) threats. Table 7. ARP-MG-2015-1 could be replaced by any other DoS threat associated with the IPv4 suite protocols. This complex threat could only be prevented by ensuring that the IPv4 suite DoS threats are properly mitigated. Examples of convoluted threats for the four generic IPv6 transition technologies are presented in Table 3.

Another convoluted threat can result from exploiting IPv4 or IPv6 spoofing threats to increase the likelihood of an attack on routing protocols with simple authentication, such as or OSPFv3-MG-2015-1, OSPFv2-MG-2015-1 or RIPv2-MG-2015-1. Since the attack could be performed from an untrusted entry point (Customer device or Data store), the likelihood of the threat being exploited rises to High. This type of attack can be mitigated by using cryptographic authentication for the routing protocols.

Table 3: Generic IPv6 Transition Technologies Convoluted Threats.

	ThreatID	Description	S	T	R	I	D	E	Mitigation	Validation
Generic IPv6 Transition Technologies										
1	DS -MG-2015-1	ARP-MG-2015-1 + ND -MG-2015-10	H	H	H	H	H		Ensure DoS mitigation for IPv4 suite protocols; use SEND	✓
2	DS-MG-2015-2	ARP-MG-2015-1 + OSPFv3-MG-1	H	H	H	H	H	H	Use OSPv3 with IPsec	✓
3	1transl -MG-2015-1	IP/ICMP -MG-2015-3 + ND-MG-2015-5	H		H	H	H		No widely accepted mitigation	X
4	1transl -MG-2015-2	TCP-MG-2015-1 + ND-MG-2015-10	H	H	H	H	H		Block packets with non-internal addresses; use SEND	✓
5	2transl -MG-2015-1	IP/ICMP -MG-2015-4 + ND -MG-2015-4	H	H	H	H	H		No widely accepted mitigation	X
6	2transl -MG-2015-2	IP/ICMP-MG-2015-4 + OSPFv3-MG-2015-1	H	H	H	H	H	H	OSPFv3 with IPsec	✓
7	encaps -MG-2015-1	IPv6-MG-2015-1 + 4encaps -MG-2015-1				H	H		Use IPv4 firewall before decapsulating	

Legend

L	Associated with low likelihood of exploitation	H	Associated with high likelihood of exploitation

The list of threats can help technology implementors and network operators alike prioritize the threats and mitigate accordingly. The protocols which have threats with no widely accepted mitigation techniques have been highlighted and should be treated as first priority.

4.1.5 Review, Repeat and Validate

This step is necessary if the technology analyzed or associated protocols change. For example if the routing system were to be only OSPFv3, then the threats associated with other routing protocols could be ignored. Also, the detailed analysis of threats is far from exhaustive. In terms of convoluted new threats, only a few are presented as an example. If this was to be an updated database of threats, it would need constant update. To further validate the presented threats, a simple penetration testbed was built. The details of the testbed are presented in Figure 2. MAP-T (Li et al., 2015) was used as transition technology. Asamap (Asama, 2014), a transition implementation developed in Japan, was used as the base for MAP-T. The threats which were successfully emulated, have been marked accordingly in the last column of Table 3. In the case of the convoluted threats identified for Dual-stack transition technologies, both threats were emulated successfully by performing ARP Cache Spoofing, Neighbor Advertisement (NA) flooding and simple traffic analysis.

4.2 Single Translation Transition Technologies

To avoid redundant information, the following three subsections will only mark the differences with the threat modeling process presented for Dual-stack transition technologies.

One of the fundamental differences is that the single translation technologies would require a node to algorithmically translate the IPvX packets to IPvY, as shown in Figure 1(b). For both translation directions (4 → 6 and 6 → 4) the threats for the IPv4 suite (Table 5), IPv6 suite (Table 7), routing (Table 8) and switching (Table 10) should be considered.

There are technologies that use stateful mapping algorithms e.g. Stateful NAT64 (Bagnulo et al., 2011), which create dynamic correlations between IP addresses or {IP address, transport protocol, transport port number} tuples. Consequently, we need to consider the protocols used at the transport layer (Table 6) as part of the attack surface. The threats presented in Table 9, associated with the IP/ICMP translation algorithm (IP/ICMP), should be considered as well.

In terms of convoluted threats, one example could be exploiting the IP/ICMP-MG-2015-3 threat (IPAuth does not work with IP/ICMP) which would increase the likelihood of ND-MG-2015-4 (Default router is killed) or ND-MG-2015-5 (Good router goes bad) threats being exploited. Since there is no widely-accepted mitigation for any of the three threats, this convoluted threat is laking a mitigation solution as well. Fortunately, both complex threats could not be validated empirically. An IPsec VPN connection was successfully established using UDP encapsulation between the Windows Host and the Ubuntu Server. Moreover, the ND-MG-2015-4 and ND-MG-2015-5 could not be validated empirically, as Asamap (Asama, 2014) does not accept RA messages when IPv6 forwarding is enabled.

If the TCP-MG-2015-1 threat (SYN flood) is exploited from an untrusted entry point, it increases the likelihood of a ND-MG-2015-10 (ND Replay attacks) threat. This threat can be mitigated by blocking packets with non-internal addresses from leaving the network. Both the SYN flood attack and the Neighbor Advertisement (NA) flooding attacks were staged successfully.

4.3 Double Translation Transition Technologies

The main difference between the Single translation case and the double translation case is the need for an extra translation device as part of the core network (Figure 1(c)). Another important difference would be that in the untrusted zone, the Customer device and Data store would employ the same IP suite. Hence, the considered threats for the untrusted elements would be either the IPv4 suite (Table 5) or the IPv6 suite (Table 7) protocol threats. Similar to the single translation technologies, the routing (Table 8), switching (Table 10), transport layer (Table 6) and IP/ICMP (Table 9) threats should be analyzed as well.

The use of stateful translation mechanisms can expose a double translation technology to the IP/ICMP-MG-2015-4 threat (DoS by exhaustion of resources). A convoluted threat can result by exploiting this threat on one of the translators and the ND-MG-2015-4 or ND-MG-2015-5 threats on the other translator. This threat would have a higher likelihood of exploitation since it is associated with an untrusted entry point. In terms of mitigation, further investigation is needed, as there are no widely accepted mitigation techniques. Although the IP/ICMP-MG-2015-4 threat was replicated with success, the ND-MG-2015-10 or ND-MG-2015-5 could not be emulated because of a simple built-in mitigation mechanism implemented by Asamap (Asama, 2014). Router advertisement (RA) messages are not accepted while in IPv6 forwarding mode.

The IP/ICMP-MG-2015-4 threat can also fuse with the simple authentication threats such as OSPFv3-MG-2015-1 , OSPFv2-MG-2015-1 or RIPv2-MG-2015-1 to affect both translating nodes. The likelihood of the threats become higher by fusing them, since the flooding attack can be performed from an untrusted entry point, the customer network. This threat could be mitigated by using cryptographic authentication or implementing reverse path checks. The convoluted threat was validated by flooding the translation table of the first translator and forcing it to crash. OSPFv3 information disclosure was emulated with simple traffic analysis. To validate the other types of threats, a rogue router instance was created using Asamap.

4.4 Encapsulation Transition Technologies

Similar to double translation IPv6 transition technologies, encapsulation technologies, the core network traffic is forwarded through at least two devices, an Encapsulator and a Decapsulator (Figure 1(d)). As the main difference, the traffic is encapsulated. This means more overhead but also more support for end-to-end security protocols. Packets are encapsulated either over IPv4 or IPv6. Consequently, for the untrusted domain devices we would consider either the IPv4 suite (Table 5) or the IPv6 suite (Table 7) threats. In addition the routing (Table 8), switching (Table 10), transport layer (Table 6) and encapsulation-related (Table 9) threats should be considered.

Convoluted threats can arise by exploiting the 4encaps-MG-2015-1 threat (avoiding IPv4 network security measures with encapsulation). This threat can facilitate IPv6 suite DoS threats on the Decapsulator device. This convoluted threat would increase the likelihood of a successful DoS attack from the Customer Device. The threat could be mitigated by making use of an IPv4 firewall before decapsulating the packets.

5 DISCUSSION

The security of IPv6 transition technologies, as the technologies themselves, are hard to grasp and analyze. Although many documents have targeted different aspects of the security of these technologies, a comprehensive threat model has not been proposed yet. With this article, we want to take a first step in that direction. Our approach is built around the well-established STRIDE model, which has proved to be an adaptive tool for threat modeling. We have used the proposed threat model to analyze the security issues of the generic IPv6 transition technologies defined in Section 2.1.

One of the limitations of the proposed threat model is the lack of specificity of the scenario. However, given the diversity of existing production network this would be close to impossible. This is why we targeted a very common use case of production networks and a very basic network function for the IPv6 transition technologies. The model is a starting point, which we hope to keep developing in the future.

This hindrance can be extended to the generic IPv6 transition technologies. However, by being inclusive, rather than specific and exclusive, we contend that the proposed threat model can be applied to most of the existing IPv6 transition technologies and their future developments.

The use of STRIDE for IPv6 transition technologies can be another discussion point. One can claim that Elevation of Privilege or Repudiation threats are not exploitable at the level the transition technologies are used. However, we contend that these threats are indeed plausible. For instance, by exploiting a VLAN Hopping threat, an attacker can violate the isolation principle and by extension perform an elevation of privilege attack. In terms of repudiation, an attacker could perform a router impersonation attack and cover his tracks.

A more fundamental hindrance of the approach is represented by the lack of an associated risk quantification step. However, we believe this step to have deeper implications, particularly implementation-specific details which should be considered as well. This motivates us to continue this work by associating a risk quantification technique to the current threat model. To that end, staging penetration tests to empirically validate the threats discovered analytically could also be employed to quantify the risk associated with particular implementations.

6 CONCLUSION

In this article, we have proposed a wide-ranging threat model for IPv6 transition technologies. As part of the contribution, this article also provides a mean to generically classify IPv6 transition technologies. To prove the adequacy of the proposed threat model, we have used it to analyze the security threats of the four generic categories of IPv6 transition technologies.

As part of the threat modeling process, for each of the four categories we have defined a common use case, deconstructed the system using Data Flow Diagrams (DFDs), and obtained an initial overview of the security threats by association with the STRIDE approach. Subsequently, we have documented existing threats and mitigation solutions for the IP protocol suites and basic transition technologies representing dependencies of the system. The documented threats have been mapped with the STRIDE elements identified in the DFD, to obtain a rough likelihood for the threats to be exploited. We have shown how existing threats can lead to new threats by the interaction between subcomponents and various protocols. Lastly, we have empirically validated some of the analytically discovered threats by building a simple penetration testbed.

As a summary, the proposed, holistic threat model has revealed that the concerns related to the security of IPv6 transition technologies are well-endowed. Although it is too early to say that certain technologies are more secure than others, we contend that the proposed method can represent the basis for establishing a methodology that can lead us there. As a general observation for double translation and encapsulation technologies, the lack of shared secrets between the CE and PE devices can have serious consequences on the core network exploit-ability.

The main contribution of this article is represented by the proposed threat model. As shown, the threat model can be used to classify and prioritize already documented threats. Moreover the threat model can help discover new threats and indicate their level of mitigation. As a secondary contribution , this article contains a non-exhaustive database of documented threats associated with IP enabled devices. Moreover, preliminary penetration test data was introduced for one of the existing IPv6 transition implementations.

We contend that this approach can be the starting point for analyzing the threats of specific IPv6 transition technologies. Moreover, we intend to extend this work by proposing a risk quantification technique, which should lead to a security quantification method for IPv6 transition technologies. The first steps in this direction were taken by proposing penetration testing as a validation technique. Although the presented data is preliminary, we aim to continue this effort in future work.

ACKNOWLEDGEMENTS

This research has been supported by the Strategic International Collaborative R&D Promotion Project of the Ministry of Internal Affairs and Communication, Japan, and by the European Union Seventh Framework Programme (FP7/2007- 2013) under grant agreement No. 608533 (NECOMA). The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of the Ministry of Internal Affairs and Communications, Japan, or of the European Commission.

REFERENCES

Abad, C. L., Bonilla, R., et al. (2007). An analysis on the schemes for detecting and preventing arp cache poisoning attacks. In *Distributed Computing Systems Workshops, 2007. ICDCSW'07. 27th International Conference on*, pages 60–60. IEEE.

Anderson, T. (2015). SIIT-DC: Stateless IP/ICMP Translation for IPv6 Data Centre Environments. draft-ietf-v6ops-siit-dc-01.

APNIC (2015). IPv6 measurements for The World.

Arkko, J., Kempf, J., Zill, B., and Nikander, P. (2005). SEcure Neighbor Discovery (SEND). RFC 3971 (Proposed Standard). Updated by RFCs 6494, 6495.

Asama, M. (2014). MAP supported Vyatta [Online]. Available: http://enog.jp/∼masakazu/vyatta/map/.

Atkinson, R. and Fanto, M. (2007). RIPv2 Cryptographic Authentication. RFC 4822 (Proposed Standard).

Bagnulo, M., Matthews, P., and van Beijnum, I. (2011). Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. RFC 6146 (Proposed Standard).

Baker, F., Li, X., Bao, C., and Yin, K. (2011). Framework for IPv4/IPv6 Translation. RFC 6144 (Informational).

Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and Li, X. (2010). IPv6 Addressing of IPv4/IPv6 Translators. RFC 6052 (Proposed Standard).

Bao, C., Li, X., Zhai, Y., and Shang, W. (2014). dIVI: Dual-Stateless IPv4/IPv6 Translation. draft-xli-behave-divi-06.

Bellovin, S. M. (1989). Security problems in the tcp/ip protocol suite. *SIGCOMM Comput. Commun. Rev.*, 19(2):32–48.

Conta, A. and Gupta, M. (2006). Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification. RFC 4443 (Proposed standard).

Convery, S. and Miller, D. (2004). Ipv6 and ipv4 threat comparison and best-practice evaluation.

Davies, E., Krishnan, S., and Savola, P. (2007). IPv6 Transition/Co-existence Security Considerations. RFC 4942 (Informational).

Durand, A., Droms, R., Woodyatt, J., and Lee, Y. (2011). Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion. RFC 6333 (Proposed Standard).

Garg, A. and Reddy, A. N. (2004). Mitigation of dos attacks through qos regulation. *Microprocessors and Microsystems*, 28(10):521–530.

Gervais, A. (2012). Security analysis of industrial control systems. *Aalto University-KTH Stockholm, Jun*, 29.

Gont, F. (2011). Security assessment of the internet protocol version 4. RFC 6274 (Informational).

Gupta, M. and Melam, N. (2006). Authentication/Confidentiality for OSPFv3. RFC 4552 (Proposed Standard).

Harris, B. and Hunt, R. (1999). Tcp/ip security threats and attack methods. *Computer Communications*, 22(10):885–897.

Hernan, S., Lambert, S., Ostwald, T., and Shostack, A. (2006). Threat modeling-uncover security design flaws using the stride approach. *MSDN Magazine-Louisville*, pages 68–75.

Huston, G. (2015). IPv4 Address Report.

ITU-T (2013). ITU-T Rec. X.1037 (10/2013) IPv6 technical security guidelines. Recommendation X.1037.

Khallouf, Z., Roca, V., Moignard, R., and Loye, S. (2005). A Filtering Approach for an IGMP Flooding Resilient Infrastrcuture. 4th Conference on Security and Network Architectures(SAR'05), Batz sur Mer, France.

Li, X., Bao, C., and Baker, F. (2011a). IP/ICMP Translation Algorithm. RFC 6145 (Proposed Standard). Updated by RFC 6791.

Li, X., Bao, C., Chen, M., Zhang, H., and Wu, J. (2011b). The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition. RFC 6219 (Informational).

Li, X., Bao, C., Dec, W., Troan, O., , Matsushima, S., Murakami, T., and Taylor, T. (2015). Mapping of Address and Port using Translation (MAP-T). RFC 7599 (Proposed Standard).

Low, C. (2001). Icmp attacks illustrated. *SANS Institute URL: http://rr. sans. org/threats/ICMP_attacks. php (12/11/2001)*.

Matsuhira, N. (2015). SA46T Address Translator. draft-matsuhira-sa46t-at-05.

Mawatari, M., Kawashima, M., and Byrne, C. (2013). 464XLAT: Combination of Stateful and Stateless Translation. RFC 6877.

McRee, R. (2009). IT Infrastructure Threat Modeling Guide. Microsoft Technet.

Moy, J. (1998). OSPF Version 2. RFC 2328 (INTERNET STANDARD). Updated by RFCs 5709, 6549, 6845, 6860.

Nikander, P., Kempf, J., and Nordmark, E. (2004). IPv6 Neighbor Discovery (ND) Trust Models and Threats. RFC 3756 (Informational).

Nordmark, E. and Gilligan, R. (2005). Basic Transition Mechanisms for IPv6 Hosts and Routers. RFC 4213 (Proposed Standard).

NRO (2014). Free Pool of IPv4 Address Space Depleted [Online]. Available: http://www.nro.net/news/ipv4-free-pool-depleted.

OWASP (2015). Application Threat Modeling. OWASP Foundation.

Pilihanto, A. (2011). A complete guide on ipv6 attack and defense. *Sans. org [online]*.

Rouiller, S. A. (2003). Virtual lan security: weaknesses and countermeasures. *available at uploads. askapache. com/2006/12/vlan-security-3. pdf*.

Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and Taylor, T. (2015). Mapping of Address and Port with Encapsulation (MAP-E). RFC 7597 (Proposed Standard).

Tsou, T., Cui, Y., Boucadair, M., Farrer, I., and Lee, Y. (2015). Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture. RFC 7596 (Proposed Standard).

APPENDIX

Table 4: ThreatID Codes.

Basic IPv6 transition technologies		
IP/ICMP Translation Algorithm	RFC6145	IP/ICMP
Encapsulation of IPv6 in IPv4	RFC4213	4encaps
Generic IPv6 transition technologies		
Dual Stack	-	DS
Single Translation	-	1transl
Double Translation	-	2transl
Encapsulation	-	encaps

Table 5: IPv4 suite protocols threats.

	ThreatID	Description	S	T	R	I	D	E	
IPv4 Suite Protocols			#		#				Mitigation
			O	O	O	O	O	O	
				=	=	=	=		
				>		>	>		
1	IPv4-MG-2015-1 (Harris and Hunt, 1999)	IP source address spoofing	H	H	H	H			Apply ACLs and filter source address routed traffic
2	IPv4-MG-2015-2 (Gont, 2011)	Malformed version field		H					Version field must be checked to be 4
3	IPv4-MG-2015-3 (Gont, 2011)	Packets with a forged DSCP field	H				H		Filter packets with unrecognized DSCP
4	IPv4-MG-2015-4 (Gont, 2011)	Buffer overflow with IP fragmentation					H		IP module should implement measures to avoid illegitimate reassembly
5	ICMP-MG-2015-1 (Harris and Hunt, 1999)	Ping o'death					H		Patch software to not accept oversized ICMP messages
6	ICMP-MG-2015-2 (Bellovin, 1989)	ICMP redirects	H	H	H	H	H		routing tables should not be modified in response to ICMP Redirect messages
7	ICMP-MG-2015-3 (Low, 2001)	ICMP sweep for recon				H			Selective filtering of ICMP messages
8	ICMP-MG-2015-4 (Low, 2001)	ICMP traceroute				H			Selective filtering of ICMP messages
9	ICMP-MG-2015-5 (Low, 2001)	ICMP firewalk				H			Selective filtering of ICMP messages
10	ICMP-MG-2015-6 (Low, 2001)	ICMP flooding					H		Selective filtering of ICMP messages
11	ARP-MG-2015-1 (Abad et al., 2007)	ARP cache poisoning	H	H	H	H	H		Static ARP entries, arpwatch
12	ARP-MG-2015-2 (Gont, 2011)	ARP cache overrun					H		Selectively drop packets
13	IGMP-MG-2015-1 (Khallouf et al., 2005)	IGMP flooding					H		selective filtering of IGMP messages, multicast group authentication

Legend

H	associated with High likelihood	**# external, O process**	#	Untrusted element with High likelihood of being exploited
L	associated with Low likelihood	**>data flow, = data store**	O	Trusted element with Low likelihood of being exploited

Table 6: Layer4 Protocols Threats.

	ThreatID	Description	S	T	R	I	D	E	
Transport Layer Protocols			#		#				Mitigation
			O	O	O	O	O	O	
				=	=	=	=		
				>		>	>		
1	TCP-MG-2015-1 (Harris and Hunt, 1999)	SYN flood					H		Block packets with non-internal addresses from leaving the network
2	TCP-MG-2015-2 (Harris and Hunt, 1999)	SYN/ACK flood	H		H		H		L3/L4 Packet Filtering
3	TCP-MG-2015-3 (Harris and Hunt, 1999)	ACK or ACK-PUSH Flood	H		H		H		L3/L4 Packet Filtering
4	TCP-MG-2015-4 (Harris and Hunt, 1999)	Fragmented ACK Flood					H		L3/L4 Packet Filtering
5	TCP-MG-2015-5 (Harris and Hunt, 1999)	TCP Spoofing based on sequence number prediction	H						Block packets with non-internal addresses from leaving the network
6	TCP-MG-2015-6 (Harris and Hunt, 1999)	TCP session hijacking based on sequence number prediction	H	H	H	H	H	H	Block packets with non-internal addresses from leaving the network
7	TCP-MG-2015-7 (Harris and Hunt, 1999)	RST and FIN DoS					H		L3/L4 Packet Filtering; Stateful Flow Awareness
8	UDP-MG-2015-8 (Garg and Reddy, 2004)	UDP flood					H		QoS regulation; L3/L4 Packet Filtering
6	NAT44-MG-2015-9 (ITU-T, 2013)	Port set exaustion					H		Address-Dependent Filtering

Table 7: IPv6 suite protocols threats.

	ThreatID	Description	S	T	R	I	D	E	
IPv6 Suite Protocols			#		#				Mitigation
			O	O	O	O	O	O	
				=	=	=	=		
				>		>	>		
1	IPv6-MG-2015-1 (Davies et al., 2007)	Routing header can be used to evade access controls	H				H		Access controls based on destination addresses
2	IPv6-MG-2015-2 (Davies et al., 2007)	Site-scope multicast addresses for reconnaissance				H			Drop packets with site-scope destination addresses
3	IPv6-MG-2015-3 (Davies et al., 2007)	Anycast traffic identification for reconnaissance				H			Restrict the use of outside anycast services
4	IPv6-MG-2015-4 (Davies et al., 2007)	Extension headers excessive hop-by-hop options					H		Drop packets with unknown options
5	IPv6-MG-2015-5 (Davies et al., 2007)	Overuse of IPv6 router alert Option					H		Filter externally generated Router Alert packets
6	IPv6-MG-2015-6 (Davies et al., 2007)	IPv6 fragmentation that would potentially overload the reconstruction buffers					H		Mandating the size of packet fragments; drop non-final fragments smaller than 640 octets
7	IPv6-MG-2015-7 (Davies et al., 2007)	IPv4-Mapped IPv6 Addresses	H				H		Avoid using IPv4-mapped IPv6 addesses
8	ICMPv6-MG-2015-1 (Conta and Gupta, 2006)	ICMPv6 message spoofing	H				H		Use IPAuth
9	ICMPv6-MG-2015-2 (Conta and Gupta, 2006)	ICMPv6 Redirects	H		H	H			Use IPAuth or ESP
10	ICMPv6-MG-2015-3 (Conta and Gupta, 2006)	Back-to-back erroneous IP packets					H		Implement correctely ICMP error rate limiting mechanism
11	ICMPv6-MG-2015-4 (Conta and Gupta, 2006)	Send ICMP Parameter Problem Message to the multicast source				H	H		Secure multicast traffic
12	ICMPv6-MG-2015-5 (Conta and Gupta, 2006)	ICMP messages passed to the upper-layers					H		Use IPSec
13	ICMPv6-MG-2015-6 (Pilihanto, 2011)	ICMPv6 echo request for reconnaissance				H			Deny inbound ICMPv6 echo request
14	SLAAC-MG-2015-1 (Davies et al., 2007)	Address Privacy Extensions Interact with DDoS Defenses					H		Tune the change rate of the node address
15	ND-MG-2015-1 (Nikander et al., 2004)	Neighbor Solicitation/Advertisement Spoofing	H				H		Use SEND
16	ND-MG-2015-2 (Nikander et al., 2004)	Neighbor Unreachability Detection (NUD) failure					H		Use SEND
17	ND-MG-2015-3 (Nikander et al., 2004)	Malicious Last Hop Router	L	L	L	L	L		Use SEND
18	ND-MG-2015-4 (Nikander et al., 2004)	Default router is 'killed'	L	L	L	L	L		No widely accepted mitigation technique
19	ND-MG-2015-5 (Nikander et al., 2004)	Good Router Goes Bad	L	L	L	L	L		No widely accepted mitigation technique
20	ND-MG-2015-6 (Nikander et al., 2004)	Spoofed Redirect Message	L	L	L	L	L		Use SEND; Still an issue for the ad-hoc case
21	ND-MG-2015-7 (Nikander et al., 2004)	Bogus On-Link Prefix					L		Use SEND
22	ND-MG-2015-8 (Nikander et al., 2004)	Bogus Address Configuration Prefix					L		Use SEND; Still an issue for the ad-hoc case
23	ND-MG-2015-9 (Nikander et al., 2004)	Parameter Spoofing	L		L	L			Use SEND; Still an issue for the ad-hoc case
24	ND-MG-2015-10 (Nikander et al., 2004)	ND Replay attacks	H			H			Use roughly synchronized clocks and timestamps; Use SEND
25	ND-MG-2015-11 (Nikander et al., 2004)	Neighbor Discovery DoS threat					H		Rate limit Neighbor Solicitations
26	DAD-MG-2015-1 (Nikander et al., 2004)	Duplicate Address Detection DoS					H		Use SEND
27	SEND-MG-2015-1 (Arkko et al., 2005)	The Authorization Delegation Discovery process may be vulnerable to DoS					H		Cache discovered information and limit the number of discovery processes
28	MIPv6-MG-2015-1 (Davies et al., 2007)	Obsolete Home Address Option in Mobile IPv6	H						Secure Binding Update messages

Legend

H	associaced with High likelihood	**# external, O process**	#	Untrusted element with High likelihood of being exploited
L	associated with High likelihood	**>data flow, = data store**	O	Trusted element with Low likelihood of being exploited

Table 8: Routing Protocols threats.

	ThreatID	Description	S	T	R	I	D	E	
Routing Protocols			#		#				**Mitigation**
			O	O	O	O	O	O	
				=	=	=	=		
				>		>	>		
1	RIPv2-MG-2015-1 (Atkinson and Fanto, 2007)	RIPv2 simple password authentication issues	L	L	L	L	L	L	Use cryptographic authentication
2	RIPv2-MG-2015-2 (Atkinson and Fanto, 2007)	RIPv2 Security Association expiration				L			Let RIPv2 routing fail when the last key expires
3	RIPv2-MG-2015-3 (Atkinson and Fanto, 2007)	RIPv2 Security Association					L		The receiver should not try all RIPv2 Security Associations
4	OSPFv2-MG-2015-1 (Moy, 1998)	OSPFv2 simple password authentication	L	L	L	L	L	L	Use cryptographic authentication
5	OSPFv2-MG-2015-2 (Moy, 1998)	OSPFv2 cryptographic authentication sequence number prediction	L	L	L	L	L	L	Use cryptographic sequence number
6	OSPFv3-MG-2015-1 (Gupta and Melam, 2006)	OSPFv3 using the same manual key	L	L	L	L	L	L	avoid using manual keys

Legend

H	associaced with High likelihood	**# external, O process**	#	Untrusted element with High likelihood of being exploited
L	associaced with Low likelihood	**>data flow, = data store**	O	Trusted element with Low likelihood of being exploited

Table 9: Basic IPv6 Transition Technologies Threats.

	ThreatID	Description	S	T	R	I	D	E	
Routing Protocols			#		#				**Mitigation**
			O	O	O	O	O	O	
				=	=	=	=		
				>		>	>		
1	IP/ICMP-MG-2015-1 (Bao et al., 2010)	IPv4 address spoofing with IPv4-embedded IPv6	L						Implement reverse path checks to verify that packets are coming from an authorized location.
2	IP/ICMP-MG-2015-2 (Li et al., 2011a)	transport mode ESP will fail with IPv6-to-IPv4 translation				L			Use checksum-neutral addresses
3	IP/ICMP-MG-2015-3 (Li et al., 2011a)	Authentication Headers cannot be used across an IPv6-to-IPv4				L			No widely accepted mitigation
4	IP/ICMP-MG-2015-4 (Li et al., 2011a)	Stateful translators can run out of resources					L		No widely accepted mitigation
5	4encaps-MG-2015-1 (Davies et al., 2007)	Tunneling IPv6 through IPv4 networks could break IPv4 Network's security assumptions				L			route the encapsulated through an IPv4 firewall before decapsulating them

Table 10: L2 Technologies Threats.

	ThreatID	Description	S	T	R	I	D	E	
L2 Technologies			#		#				**Mitigation**
			O	O	O	O	O	O	
				=	=	=	=		
				>		>	>		
1	VLAN-MG-2015-1 (ITU-T, 2013)	Exhaust a forwarding information base (FIB) of an L2switch					L		IEEE 802.1x authentication
2	VLAN-MG-2015-2 (Rouiller, 2003)	Content Addressable Memory (CAM) Overflow					L		Use the port-security features
3	VLAN-MG-2015-3 (Rouiller, 2003)	Basic VLAN Hopping	L						Software update
4	VLAN-MG-2015-4 (Rouiller, 2003)	Double encapsulation VLAN Hopping	L					L	Disable Auto-trunking
5	VLAN-MG-2015-5 (Rouiller, 2003)	Spanning Tree Attack				L	L		Disable STP, Use BPDU Guard