Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 1, 2017

M. Georgescu, Ed.
NAIST

June 30, 2016

# The STRIDE towards IPv6: A Threat Model for IPv6 Transition Technologies

draft-georgescu-opsec-ipv6-trans-tech-threat-model-01

## Abstract

This document provides a structured approach for analyzing the threats associated with the various IPv6 transition technologies specified by the IETF. The threat model is built around the established STRIDE threat classification and is aimed at existing IPv6 transition technologies, as well as their future developments.

## Status of This Memo

## Copyright Notice

Table of Contents

## 1. Introduction

When building an IPv6 transition plan, security is arguably one of the biggest concerns 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 solutions.

The security considerations of IPv6 transition technologies has generally been analyzed in each of the corresponding specifications, and some documents have discussed the general threats associated with transition technologies (see e.g. [RFC4942]).

However, more structured threat modeling has proved useful for understanding the security of intricate systems. Structured approaches 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. This document follows a structured approach for analyzing the threats asociated with transition technologies, that considers the functions of a transition technology as well as the cntext in which the technology is used.

The threat model uses the established STRIDE mnemonic and threat classification. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service and Elevation of Privilege, a generic list of threats which can be used to classify various threats and provides some basic mitigation directions. Since similar transition technologies can be associated with a similar list of threats, the document considers the generic classification of IPv6 transition technologies described in [draft-bmwg-v6trans].

## 2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

## 3. The Generic Categories of IPv6 Transition Technologies

Table 1 presents the generic categories described in [draft-bmwg-v6trans] and some sample IPv6 transition technologies specified by the IETF.

Table 1. IPv6 Transition Technologies Categories

| | Generic category | IPv6 Transition Technology |
|---|---|---|
| 1 | Dual-stack | Dual IP Layer Operations [RFC4213] |
| 2 | Single translation | NAT64 [RFC6146], IVI [RFC6219] |
| 3 | Double translation | 464XLAT [RFC6877], MAP-T [RFC7599] |
| 4 | Encapsulation | DSLite [RFC6333], MAP-E [RFC7597]<br>Lightweight 4over6 [RFC7596]<br>6RD [RFC5569] |

## 4. Building The Threat Model

To build a threat model for IPv6 transition technologies a series of steps is recommended. The steps were inspired by the threat modelling approach described in [stride-shostack]. These steps are detailed in the following subsections.

### 4.1. 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.

### 4.2. Identify the generic category

The category should be identified considering the generic classification defined in Section 3. This step can help reuse the threat analysis data for technologies which are part of the same category.

### 4.3. 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. The IP protocol suite and the protocols used for the designated function should be identified as well. This can narrow down the attack surface.

Figure 1 presents the basic elements of a data flow diagram as well as general rules for their association with network elements.

```
 +----------+
 | External |  Represents a network node which is outside
 | Entity   |  the control of a network provider
 +----------+
      ___
    ,'   `.    Represents a middle-box or a network node
   |  Pro  |   which processes translated or encapsulated
    \ cess/    traffic
     `---'

 ============
  Data store   Represents a node where user and provider
 ============  data is stored

  Data Flow
------------>  Data in transit exchanged between network elements

    Trust
     ()       The border which marks the part of the
     ()       network considered outside the control
     ()       of a network provider
  boundary
```

Figure 1.  DFD Elements

## 4.4.  Identify the threats

### 4.4.1.  STRIDE-DFD Association

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 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.

Table2.  DFD-STRIDE Associations

| S | T | R | I | D | E |
|---|---|---|---|---|---|
| # |  | # |  |  |  |
| O | O | O | O | O | O |
|  | = | = | = | = |  |
|  | > |  | > | > |  |

| | |
|---|---|
| # | External entity |
| O | Process |
| = | Data store |
| > | Data flow |

### 4.4.2.  Level of Trust

We associate a level of trust with each entry point.  Entry points that are trusted are assumed to behave as expected.  That is, if the entry point is considered trusted, we can assume the likelihood of an attack is low.  Furthermore, the six categories of STRIDE attacks could be assigned a likelihood by considering their association with the DFD elements that are entry points.

For instance, let's suppose we have an untrusted entry point (High likelihood of exploitation) which is also an external entity. Spoofing and repudiation are potential threats for an external entity.  By association, the two types of attacks can be considered to have a high likelihood of being exploited.  Using this logic, we can assign a likelihood value to each found threat.  This can represent a base for prioritizing mitigation solutions.  The likelihood levels can be defined in accordance with the levels of trust assigned to the the entry points.

### 4.4.3.  Documenting the Threats

Each discovered threat should be documented using the format presented in Table 3.

Table2.  Threat Info 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 possible mitigation solutions |
| Likelihood | Likelihood of the threat being exploited |
| Validation | Empirical validation data |

The Threat-ID is supposed to be an easy way to refer and identify the threat within the IETF.  The tentative format is IETF-TDB-[associated protocol/technology]-[serial number].  IETF-TDB stands for IETF Threat Database in the hope that in the future a threat database will be maintained within the IETF.  The serial number is incremented with each threat found for a particular protocol or technology.

#### 4.4.4.  Complex Threats

As the subcomponents and subprotocols interact, 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.

### 4.5.  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.

The next sections applied the proposed threat modeling approach to the IPv6 transition technologies identified in Section 3.

## 5. Dual Stack Threat Model

### 5.1. 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.

### 5.2. Identify the Generic Category

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

### 5.3. Decompose the Technology

A DFD for dual-stack transition technologies is presented in Figure 2. The diagram represents a basic use case and includes a minimal set of elements.

```
     Domain A-DS                Core  ___   Domain       Domain B-DS
         +----------+     (         ,'   `.         )    ============
         | Customer |-----(------->|  DS    |------- )--->  Provider
         | Device   |<----(-------- \ node/<--------)---- Data Store
         +----------+     (          `---' IPv4/IPv6)    ============
            E  P                     E  P                    E  P
   ______________________________________________________________________
   Legend           ___                                Trust
    +----------+  ,'   `.   ============    Data Flow   ()  E=Entry
    | External | |  Pro  |   Data store   ------------> ()    point
    | Entity   |  \ cess/   ============                ()  P=Protected
    +----------+   `---'                                     boundary
```

Figure 2. Data Flow Diagram (DFD) for Dual Stack (DS) technologies

In Domain A, which is assumed to be 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 important 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 assumed network provider. 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 protected as well.  The Dual-stack node forwards in turn the data request to the provider data store.  The Data store is the last entry point in the system and it is assumed to contain valuable data.  The data reply is forwarded back to the customer device.

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 both IP protocol suites.  Furthermore, the possibility of using security and routing protocols should be considered.

## 5.4.  Identify the threats

### 5.4.1.  STRIDE-DFD Assoctiation

By analyzing the DFD in association with the STRIDE threats per element chart, we can make the associations depicted in Table 3.

Table3.  DFD-STRIDE Associations DS

| S | T | R | I | D | E |
|---|---|---|---|---|---|
| #-H |  | #-H |  |  |  |
| O-L | O-L | O-L | O-L | O-L | O-L |
|  | =-H | =-H | =-H | =-H |  |
|  | >-H |  | >-H | >-H |  |

| | |
|---|---|
| # | Customer device |
| O | DS node |
| = | Provider data store |
| > | Data flow |

### 5.4.2. From Trust to Likelihood

Looking at the associations in Table 3, The Customer Device can be subject to spoofing and repudiation attacks. It being an untrusted entry point, that means there is a high likelihood of an attack. This is marked in Table 3 with H.

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.

### 5.4.3. Documenting the Threats

The Tables 5-10 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 6), IPv6 suite(Table 7), routing (Table 10) and switching (Table 5) could potentially be exploited from the 3 entries of the system: the untrusted (High likelihood of exploitation) Customer device, the trusted (Low likelihood of exploitation) Dual-stack node (Process) and untrusted (High likelihood of exploitation) Provider 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 IETF-TDB-ND-3 to IETF-TDB-ND-6 and the Layer 2 technologies' threats (Table 5) can only be associated with routers or switches. In the context of the DFD, they could only be associated with the Dual-stack node. That means they have a low likelihood of occurrence. Similarly, the routing protocols

(Table 10) can only be associated with the Dual-stack node. By association, they also have a low likelihood of being exploited.

### 5.4.4. Complex Threats

By analyzing the interaction between the three elements of the DFD and the protocols used by Dual stack transition technologies, we can uncover other threats. For example, if the IETF-TDB-ARP-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 IETF-TDB-ND-10 (ND Replay Attacks) threats. IETF-TDB-ARP-1 could be replaced by any other DoS threat associated with the IPv4 protocol suite. This complex threat could 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 4.

Table4. Complex Threats

| | ThreatID | Description | S | T | R | I | D | E | Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| 1 V | IETF-TDB-DS-1 | IETF-TDB-ARP-1 + IETF-TDB-ND-4 | H | H | H | H | H | | DoS Mitigation for IPv4 suite |
| 2 V | IETF-TDB-DS-2 | IETF-TDB-ARP-1 + IETF-TDB-OSPFv3-1 | H | H | H | H | H | H | Crypto authen |
| 3 X | IETF-TDB-1transl-1 | IETF-TDB IP/ICMP-3 + IETF-TDB-ICMPv6-1 | H | | H | H | H | | No widely accepted mitigation |
| 4 V | IETF-TDB-1transl-2 | IETF-TDB-TCP-1 + IETF-TDB-ND-4 | H | H | H | H | H | | Block non-internal traffic |
| 5 X | IETF-TDB | IETF-TDB-IP/ICMP-4 | L | L | L | L | L | | No widely accepted |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | -2transl-1 | + IETF-TDB -ND-4 | | | | | | | mitigation |
| 6 V | IETF-TDB -2transl_2 | IETF-TDB -IP/ICMP-1 + IETF-TDB -OSPFv3-1 | L | L | L | L | L | L | reverse path checks |
| 7 | IETF-TDB -encaps-1 | IETF-TDB -IPv6-1 + IETF-TDB -4encaps_1 | | | | H | H | | IPv4 firewall before decaps |

| Legend | | | |
|---|---|---|---|
| H | associaced with High likelihood | L | associaced with Low likelihood |

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 IETF-TDB-OSPFv3-1, IETF-TDB-OSPFv2-1 or IETF-TDB-RIPv2-1. 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.

The list of threats can help technology implementors and network operators alike prioritize the threats and mitigate accordingly.

### 5.5. 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 3. MAP-T [RFC7599] was used as transition technology. Asamap [asamap2014], 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 first column of Table 4. 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.

```
                                +----------+
      +---------+---------------+ Kali     |
      |---------|+--------------> Attacker |
      ||        ||              +---+^-----+
      ||        ||                  ||
      ||        ||           ___    ||     __
   +--v-------+ ||  (      ,'   `.  ||   ,'   `.      )      ===========
   | Win8     +-+|--(---->+  amap +-+|->+  amap +-----)----->  Ubuntu
   | Host     <--+--(-----+\ CE  /<--+--+\ BR  /<-----)-----+  Server
   +----------+     (       `+-+'  IPvY   `+-+'  IPvX )      ===========
      E  P                  E  P          E  P                   E  P
```

Figure 3.  Pentestbed Setup

## 6. Single Translation Threat Model

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 4.

### 6.1. Decompose the Technology

A DFD for single translation transition technologies is presented in Figure 4. The diagram represents a basic use case and includes a minimal set of elements.

```
     Domain A-IPvX                Core___   Domain      Domain B-IPvY
         +----------+ IPvX (        ,'   `.  IPvY   )    ============
         | Customer |------(------>|  Tra  |------- )--->  Provider
         | Device   |<-----(------- \ nsl /<--------)---- Data Store
         +----------+ IPvX (         `---'   IPvY   )    ============
            E  P                     E  P                    E  P
   ________________________________________________________________________
   Legend           ___                                Trust
    +----------+  ,'   `.   ============    Data Flow   ()  E=Entry
    | External | |  Pro  |   Data store   ------------> ()    point
    | Entity   |  \ cess/   ============               ()  P=Protected
    +----------+   `---'                                   boundary
```

Figure 4.  DFD for 1transl technologies

## 6.2. Identify the threats

For both translation directions 4->6 and 6->4, the threats for the IPv4 suite (Table 6), IPv6 suite (Table 7), routing (Table 10) and switching (Table 5) should be considered.  There are technologies that use stateful mapping algorithms e.g.  Stateful NAT64 [RFC6146], 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 9) as part of the attack surface.  The threats presented in Table X, 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 IETF-TDB-IP/ICMP-3 threat (IPAuth does not work with IP/ICMP) which would increase the likelihood of IETF-TDB-ND-4 (Default router is killed) or IETF-TDB-ND-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 IETF-TDB-ND-4 and IETF-TDB-ND-5 could not be validated empirically, as Asamap [asamap2014] does not accept RA messages when IPv6 forwarding is enabled.

If the IETF-TDB-TCP-1 threat (SYN flood) is exploited from an untrusted entry point, it increases the likelihood of a IETF-TDB-ND-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.

## 7. Double Translation Threat Model

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 5). Another important difference would be that in the untrusted zone, the Customer device and Data store would employ the same IP suite.

### 7.1. Decompose the Technology

A DFD for double translation transition technologies is presented in Figure 5. The diagram represents a basic use case and includes a minimal set of elements.

```
      Domain A-IPvX          ___  Core Dom ___           Domain B-IPvX
     +----------+ IPvX(    ,'   `. IPvY  ,'   `.     )      ============
     | Customer |-----(---|  Tra  |---->|  Tra  |--- )----->  Provider
     | Device   |<----(----\ nsl /<------\ nsl /<----)------ Data Store
     +----------+     (     `---'  IPvY   `---'  IPvX)      ============
        E  P                 E  P          E  P                 E  P
   _____________________________________________________________________
    Legend           ___                                Trust
     +----------+  ,'   `.   ============    Data Flow   ()  E=Entry
     | External | |  Pro  |   Data store   ------------> ()    point
     | Entity   |  \ cess/   ============                ()  P=Protected
     +----------+   `---'                                     boundary
```

Figure 5. DFD for 2transl technologies

### 7.2. Identify the threats

The considered threats for the untrusted elements would be either the IPv4 suite (Table 6) or the IPv6 suite (Table 7) protocol threats. Similar to the single translation technologies, the routing (Table 10), switching (Table 5), transport layer (Table 9) and IP/ ICMP (Table 8) threats should be analyzed as well.

The use of stateful translation mechanisms can expose a double translation technology to the IETF-TDB-IP/ICMP-4 threat (DoS by exhaustion of resources). A convoluted threat can result by exploiting this threat on one of the translators and the IETF-TDB-ND-4 or IETF-TDB-ND-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 IETF-TDB-IP/ICMP-4 threat was replicated with success, the IETF-TDB-ND-10 or IETF-TDB-ND-5 could not be emulated because of a simple built-in mitigation mechanism

implemented by Asamap [asamap2014]. Router advertisement (RA) messages are not accepted while in IPv6 forwarding mode.

The IETF-TDB-IP/ICMP-4 threat can also fuse with the simple authentication threats such as IETF-TDB-OSPFv3-1 , IETF-TDB-OSPFv2-1 or IETF-TDB-RIPv2-1 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 [asamap2014].

## 8. Encapsulation Threat Model

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 6). 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.

### 8.1. Decompose the Technology

A DFD for encapsulation transition technologies is presented in Figure 6. The diagram represents a basic use case and includes a minimal set of elements.

```
     Domain A-IPvX          ___ Core Dom  ___            Domain B-IPvX
    +----------+ IPvX(    ,'   `. IPvY  ,'   `.      )      ============
    | Customer |-----(---|  Enc  |---->|  Dec  |---- )----->  Provider
    | Device   |<----(----\ aps /<------\ aps /<-----)------ Data Store
    +----------+     (     `---'  IPvY   `---'  IPvX )      ============
       E  P                E  P          E  P                   E  P
   _____________________________________________________________________
   Legend           ___                                 Trust
    +----------+  ,'   `.   ============    Data Flow   {}  E=Entry
    | External | |  Pro  |    Data store   ------------> {}    point
    | Entity   |  \ cess/    ============                {}  P=Protected
    +----------+   `---'                                       boundary
```

Figure 6.  DFD for encaps technologies

### 8.2. Identify the threats

For the untrusted domain devices we would consider either the IPv4 suite (Table 6) or the IPv6 suite (Table 7) threats. In addition the routing (Table 10), switching (Table 5), transport layer (Table 9) and encapsulation-related (Table 8) threats should be considered.

Convoluted threats can arise by exploiting the IETF-TDB-4encaps-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.

## 9. Acknowledgments

The author would like to thank Fernando Gont for his review and useful suggestions.

This document was derrived from a template contributed by the xml2rfc project.

## 10. IANA Considerations

This memo includes no request to IANA.

All drafts are required to have an IANA considerations section (see Guidelines for Writing an IANA Considerations Section in RFCs [RFC5226] for a guide). If the draft does not require IANA to do anything, the section contains an explicit statement that this is the case (as above). If there are no requirements for IANA, the section will be removed during conversion into an RFC by the RFC Editor.

## 11. Security Considerations

This memo attempts to build a threat model for IPv6 transition technologies. The author would like to encourage the use of a similar threat modeling approach when writing the security considerations of standards developed in the IETF. To be more concrete the following steps could be reused:

R1 Identify the function

R2 Associate the technology with a generic category (if any)

R3 Decompose the technology

R4 Identify the threats

R5 Review, repeat and validate

## 12. References

### 12.1. Normative References

[draft-bmwg-v6trans]
Georgescu, M. and G. Lencse, "Benchmarking Methodology for IPv6 Transition Technologies", 2015, <https://tools.ietf.org/html/draft-ietf-bmwg-ipv6-tran-tech-benchmarking-01>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4942] Davies, E., Krishnan, S., and P. Savola, "IPv6 Transition/Co-existence Security Considerations", RFC 4942, DOI 10.17487/RFC4942, September 2007, <http://www.rfc-editor.org/info/rfc4942>.

### 12.2. Informative References

[arps] Abad, C. and R. Bonilla, "An analysis on the schemes for detecting and preventing ARP cache poisoning attacks", 2007.

[asamap2014]
Asama, M., "MAP supported Vyatta", 2014, <http://enog.jp/~masakazu/vyatta/map/>.

[bellovin89]
Bellovin, S., "Security Problems in the TCP/IP Protocol Suite", 1989.

[harris99]
Harris, B. and R. Hunt, "TCP/IP security threats and attack methods", 1999.

[icmps] Low, C., "ICMP attacks illustrated", 2001.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998, <http://www.rfc-editor.org/info/rfc2328>.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <http://www.rfc-editor.org/info/rfc2629>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <http://www.rfc-editor.org/info/rfc3552>.

[RFC3756] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, DOI 10.17487/RFC3756, May 2004, <http://www.rfc-editor.org/info/rfc3756>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <http://www.rfc-editor.org/info/rfc3971>.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, DOI 10.17487/RFC4213, October 2005, <http://www.rfc-editor.org/info/rfc4213>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, DOI 10.17487/RFC4443, March 2006, <http://www.rfc-editor.org/info/rfc4443>.

[RFC4552] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, DOI 10.17487/RFC4552, June 2006, <http://www.rfc-editor.org/info/rfc4552>.

[RFC4822] Atkinson, R. and M. Fanto, "RIPv2 Cryptographic Authentication", RFC 4822, DOI 10.17487/RFC4822, February 2007, <http://www.rfc-editor.org/info/rfc4822>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC5569] Despres, R., "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", RFC 5569, DOI 10.17487/RFC5569, January 2010, <http://www.rfc-editor.org/info/rfc5569>.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, DOI 10.17487/RFC6052, October 2010, <http://www.rfc-editor.org/info/rfc6052>.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, DOI 10.17487/RFC6145, April 2011, <http://www.rfc-editor.org/info/rfc6145>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <http://www.rfc-editor.org/info/rfc6146>.

[RFC6219] Li, X., Bao, C., Chen, M., Zhang, H., and J. Wu, "The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition", RFC 6219, DOI 10.17487/RFC6219, May 2011, <http://www.rfc-editor.org/info/rfc6219>.

[RFC6274] Gont, F., "Security Assessment of the Internet Protocol Version 4", RFC 6274, DOI 10.17487/RFC6274, July 2011, <http://www.rfc-editor.org/info/rfc6274>.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011, <http://www.rfc-editor.org/info/rfc6333>.

[RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, DOI 10.17487/RFC6877, April 2013, <http://www.rfc-editor.org/info/rfc6877>.

[RFC7596] Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture", RFC 7596, DOI 10.17487/RFC7596, July 2015, <http://www.rfc-editor.org/info/rfc7596>.

[RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, Ed., "Mapping of Address and Port with Encapsulation (MAP-E)", RFC 7597, DOI 10.17487/RFC7597, July 2015, <http://www.rfc-editor.org/info/rfc7597>.

[RFC7599] Li, X., Bao, C., Dec, W., Ed., Troan, O., Matsushima, S., and T. Murakami, "Mapping of Address and Port using Translation (MAP-T)", RFC 7599, DOI 10.17487/RFC7599, July 2015, <http://www.rfc-editor.org/info/rfc7599>.

[stride-shostack] Shostack, A., "Experiences threat modeling at microsoft", 2008, <http://mail.homeport.org/~adam/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf>.

[sws] Rouiller, S., "Virtual LAN Security: weaknesses and countermeasures", 2003.

[udps] Garg, A. and A. Reddy, "Mitigation of DoS attacks through QoS regulation", 2004.

[x1037] ITU-T, "IPv6 technical security guidelines. Recommendation X.1037", 2013, <https://www.itu.int/rec/T-REC-X.1037/en>.

## Appendix A.  Appendix A

Table5. L2 Technologies Threats

| | ThreatID | Description | S | T | R | I | D | E | Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| 1 | IETF-TDB -VLAN-1 [x1037] | Exhaust a the FIB of an L2switch | | | | | L | | IEEE 802.1x authentication |
| 2 | IETF-TDB -VLAN-2 [sws] | CAM Overflow | | | | | L | | port -security features |
| 3 | IETF-TDB -VLAN-3 [sws] | Basic VLAN Hopping | L | | | | | | Software update |
| 4 | IETF-TDB -VLAN-4 [sws] | Double encapsulation VLAN Hopping | L | | | | | L | Disable Auto -trunking |
| 5 | IETF-TDB -VLAN-5 [sws] | Spanning Tree Attack | | | | L | L | | Disable STP; BPDU Guard |
| Legend | | | | | | | | | |
| H | associaced with High likelihood | | | | | L | associaced with Low likelihood | | |

Table6. IPv4 Protocol Suite Threats

| | ThreatID | Description | S | T | R | I | D | E | Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| 1 | IETF-TDB -IPv4-1 [harris99] | IP source address spoofing | H | H | H | H | | | Apply ACLs filter source address traffic |
| 2 | IETF-TDB | Mal | | H | | | | | Version |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | -IPv4-2 [RFC6274] | formed version field | | | | | | | checked to be 4 |
| 3 | IETF-TDB-IPv4-3 [RFC6274] | forged DSCP field | H | | | | H | | Filter unrecognized DSCP |
| 4 | IETF-TDB-IPv4-4 [RFC6274] | Buffer overflow IP fragmentation | | | | | H | | avoid illegitimate reassembly |
| 5 | IETF-TDB-ICMP-1 [harris99] | Ping o'death | | | | | H | | do not accept oversized ICMP |
| 6 | IETF-TDB-ICMP-2 [bellovin89] | ICMP redirects | H | H | H | H | H | | don't update routing tables with ICMP Redirects |
| 7 | IETF-TDB-ICMP-3 [icmps] | ICMP sweep for recon | | | | H | | | Selective filtering of ICMP |
| 8 | IETF-TDB-ICMP-6 [icmps] | ICMP flooding | | | | | H | | Selective filtering of ICMP |
| 9 | IETF-TDB-ARP-1 [arps] | ARP cache poisoning | H | H | H | H | H | | Static ARP entries, arpwatch |
| 10 | IETF-TDB-ARP-2 [RFC6274] | ARP cache overrun | | | | | H | | Selective drop of packets |

Table7. IPv6 Protocol Suite Threats

| | ThreatID | Description | S | T | R | I | D | E | Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| 1 | IETF-TDB-IPv6-1 [RFC4942] | Routing header to evade access controls | H | | | | H | | Access controls based on dest addresses |
| 2 | IETF-TDB-IPv6-2 [RFC4942] | Site-scope multicast addresses reconnaissance | | | | H | | | Drop packets with site-scope dest addresses |
| 3 | IETF-TDB-IPv6-3 [RFC4942] | Anycast traffic identif reconnaissance | | | | H | | | Restrict outside anycast services |
| 4 | IETF-TDB-IPv6-4 [RFC4942] | Extension headers excessive hop-by-hop options | | | | | H | | Drop packets with unknown options |
| 5 | IETF-TDB-IPv6-5 [RFC4942] | Overuse of IPv6 router alert Option | | | | | H | | Filter externally generated Router Alert packets |
| 6 | IETF-TDB-IPv6-6 [RFC4942] | IPv6 fragmentation overload of reconstruct buffers | | | | | H | | Mandating the size of packet fragments |
| 7 | IETF-TDB-IPv6-7 [RFC4942] | IPv4-Mapped IPv6 Addresses | H | | | | H | | Avoid IPv4-mapped IPv6 addesses |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 8 | IETF-TDB-ICMPv6-1 [RFC4443] | ICMPv6 spoofing | H | | | | H | | IPAuth |
| 9 | IETF-TDB-ICMPv6-2 [RFC4443] | ICMPv6 Redirects | H | | H | H | | | IPAuth or ESP |
| 10 | IETF-TDB-ICMPv6-3 [RFC4443] | Back-to-back erroneous IP packets | | | | | H | | ICMP error rate limiting |
| 11 | IETF-TDB-ICMPv6-4 [RFC4443] | Send ICMP Parameter Problem to multicast source | | | | H | H | | Secure multicast traffic |
| 12 | IETF-TDB-ICMPv6-5 [RFC4443] | ICMP passed to upper-layers | | | | | H | | IPSec |
| 14 | IETF-TDB-SLAAC-1 [RFC4942] | Address Privacy Extensions Interaction with DDoS Defenses | | | | | H | | Tune the change rate of the node address |
| 15 | IETF-TDB-ND-1 [RFC3756] | NS/NA Spoofing | H | | | | H | | SEND |
| 16 | IETF-TDB-ND-2 [RFC3756] | NUD failure | | | | | H | | SEND |
| 17 | IETF-TDB-ND-3 [RFC3756] | Malicious Last Hop Router | | | L | L | L | | SEND |
| 18 | IETF-TDB-ND-4 [RFC3756] | Default router is 'killed' | | | L | L | L | | No widely accepted mitigation technique |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 19 | IETF-TDB-ND-5 [RFC3756] | Good Router Goes Bad | | | L | L | L | | No widely accepted mitigation technique |
| 20 | IETF-TDB-ND-6 [RFC3756] | Spoofed Redirect Message | | | L | L | L | | SEND; Still an issue for ad-hoc cases |
| 21 | IETF-TDB-ND-7 [RFC3756] | Bogus On-Link Prefix | | | | | L | | SEND |
| 22 | IETF-TDB-ND-8 [RFC3756] | Bogus Address Config Prefix | | | | | L | | SEND; Still an issue for ad-hoc cases |
| 23 | IETF-TDB-ND-9 [RFC3756] | Parameter Spoofing | L | | L | L | | | SEND; Still an issue for ad-hoc cases |
| 24 | IETF-TDB-ND-10 [RFC3756] | ND Replay attacks | H | | | H | | | SEND |
| 25 | IETF-TDB-ND-11 [RFC3756] | Neighbor Discovery DoS | | | | | H | | Rate limit NS messsages |
| 26 | IETF-TDB DAD_1 [RFC3756] | DAD DoS | | | | | H | | SEND |
| 27 | IETF-TDB-SEND-1 [RFC3971] | Authorization Delegation Discovery DoS | | | | | H | | Cache discovered info and limit the number of discovery processes |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 28 | IETF-TDB -MIPv6-1 [RFC4942] | Obsolete Home Address Option Mobile IPv6 | H | | | | | | Secure Binding Update messages |

Table8.  Basic Transition Technologies Threats

|   | ThreatID | Description | S | T | R | I | D | E | Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| 1 | IETF-TDB-IP/ICPM-1 [RFC6052] | IPv4 spoofing with IPv4-embedded IPv6 | L |  |  |  |  |  | Implement reverse path checks |
| 2 | IETF-TDB-IP/ICMP-2 [RFC6145] | ESP fails with IPv6-to-IPv4 translation |  |  |  | L |  |  | Use checksum-neutral addresses |
| 3 | IETF-TDB-IP/ICMP-3 [rfc6145] | Auth Headers cannot be used across IPv6-to-IPv4 |  |  |  | L |  |  | No widely accepted mitigation |
| 4 | IETF-TDB-IP/ICMP-4 [RFC6145] | Stateful translators resources exhaustion |  |  |  |  | L |  | No widely accepted mitigation |
| 5 | 4encaps_1 [RFC4942] | Tunneling IPv6 over IPv4 breaks IPv4 Network's security assumptions |  |  |  | L |  |  | route encaps traffic through IPv4 firewall before decaps |

Table9.  L4 Technologies Threats

|   | ThreatID | Description | S | T | R | I | D | E | Mitigation |
|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | IETF-TDB-TCP-1 [harris99] | SYN flood | | | | | H | | Block non-internal addresses from leaving |
| 2 | IETF-TDB-TCP-2 [harris99] | SYN/ACK flood | H | | H | | H | | L3/L4 Packet Filtering |
| 3 | IETF-TDB-TCP-3 [harris99] | ACK or ACK-PUSH Flood | H | | H | | H | | L3/L4 Packet Filtering |
| 4 | IETF-TDB-TCP-4 [harris99] | Fragmented ACK Flood | | | | | H | | L3/L4 Packet Filtering |
| 5 | IETF-TDB-TCP-5 [harris99] | TCP Spoofing sequence number prediction | H | | | | | | Block non-internal traffic from leaving |
| 6 | IETF-TDB-TCP-6 [harris99] | TCP session hijacking sequence number prediction | H | H | H | H | H | H | Block non-internal traffic from leaving |
| 7 | IETF-TDB-TCP-7 [harris99] | RST and FIN DoS | | | | | H | | L3/L4 Packet Filtering Stateful Flow Awareness |
| 8 | IETF-TDB-UDP-8 [udps] | UDP flood | | | | | H | | QoS regulation;L3/L4 Packet Filtering |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 9 | IETF-TDB -NAT44-9 [rfc7957] | Port set exaustion | | | | | H | | Address Dependent Filtering |

Table10. Routing Technologies Threats

| | ThreatID | Description | S | T | R | I | D | E | Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| 1 x | IETF-TDB -RIPv2-1 [RFC4822] | simple password authen | L | L | L | L | L | L | crypto authen |
| 2 x | IETF-TDB -OSPFv2-1 [RFC2328] | simple password authen | L | L | L | L | L | L | crypto authen |
| 3 x | IETF-TDB -OSPFv2-2 [RFC2328] | OSPFv2 authen sequence number prediction | L | L | L | L | L | L | crypto sequence number |
| 4 | IETF-TDB -OSPFv3-1 [RFC4552] | OSPFv3 using the same manual key | L | L | L | L | L | L | no manual keys |

| Legend | | | |
|---|---|---|---|
| H | associaced with High likelihood | L | associaced with Low likelihood |

## Author's Address

Marius Georgescu (editor)
NAIST
Takayama 8916-5
Nara  630-0192
Japan

Phone: +81 743 72 5216
Email: liviumarius-g@is.naist.jp
URI:   http://www.ipv6net.ro