



iplab

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

draft-georgescu-opsec-ipv6-trans-tech-threat-model-00

Marius Georgescu

Nara Institute of Science and Technology  
Internet Engineering Laboratory

5 Apr. 2016

# DRAFT MOTIVATION: IPV6 TRANSITION

- ▶ IPv6 is not backwards compatible
- ▶ The Internet will undergo a period through which both protocols will coexist
- ▶ Currently only 5% of worldwide Internet users have IPv6 connectivity<sup>1</sup>

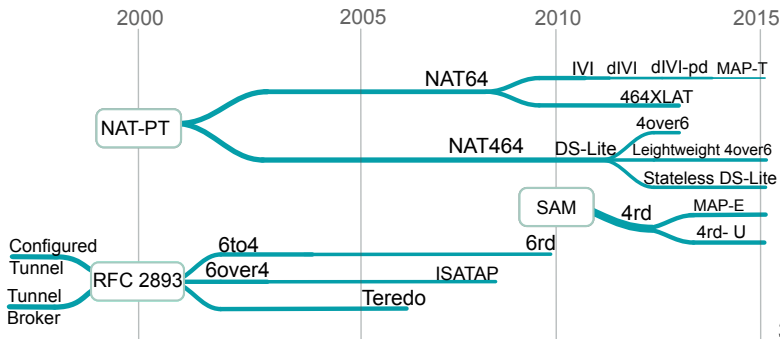


<sup>1</sup>APNIC. *IPv6 measurements for The World*. Asia-Pacific Network Information Centre, Apr. 2016. URL: <http://labs.apnic.net/ipv6-measurement/Regions/>.

<sup>2</sup>Original drawing by Andrew Bell @ [www.creaturesinmyhead.com](http://www.creaturesinmyhead.com).



# IPv6 TRANSITION TECHNOLOGIES EVOLUTION



3

<sup>3</sup>inspired by the APNIC35 presentation "The evolution of IPv6 transition technologies" by Jouni Korhonen.

# DRAFT OVERVIEW

- ▶ Provides complementary security considerations to RFC4942<sup>4</sup>
  - ▶ Proposes a threat modeling approach based on the established STRIDE threat classification<sup>5</sup>
  - ▶ Considers the generic classification on IPv6 transition technologies defined in draft-ietf-bmwg-ipv6-tran-tech-benchmarking-01<sup>6</sup>
  - ▶ Contains a list of threats and mitigation solutions for protocols (associated with IPv6 transition technologies functions) proposed in the IETF
- ▶ Collateral contributions:
  - ▶ A format to maintain threats associated with protocols proposed in the IETF
  - ▶ A way to organize the *Security Considerations* section for protocols proposed in the IETF

---

<sup>4</sup>E Davies, S Krishnan, and P Savola. *IETF RFC4942, IPv6 Transition/Coexistence Security Considerations*, 2007. .

<sup>5</sup>Adam Shostack. "Experiences threat modeling at microsoft". In: *Modeling Security Workshop*. Dept. of Computing, Lancaster University, UK. 2008.

<sup>6</sup>Marius Georgescu and Gabor Lencse. *Benchmarking Methodology for IPv6 Transition Technologies*. draft-georgescu-bmwg-ipv6-tran-tech-benchmarking-01.txt. Internet Engineering Task Force, Mar. 2016. URL: <https://tools.ietf.org/html/draft-ietf-bmwg-ipv6-tran-tech-benchmarking-01>.

# THREAT MODELING STEPS

1. Establish the function
2. Identify the generic category
3. Decompose the technology
4. Identify the threats
  - 4.1 STRIDE-DFD Association
  - 4.2 Level of Trust
  - 4.3 Documenting the Threats
  - 4.4 Complex Threats
5. Review, Repeat and Validate

# THE STRIDE THREAT CLASSIFICATION

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

# ESTABLISH THE FUNCTION

## Text in Section 4.1:

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.

## ESTABLISH THE FUNCTION

### Text in Section 4.1:

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.

### Text in Section 5.1:

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 transferred 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.



# IDENTIFY THE GENERIC CATEGORY

	Generic Category	IPv6Transition 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] Lightweight 4over6 [RFC7596] 6RD [RFC 5569]

# DECOMPOSE THE TECHNOLOGY: DFD ELEMENTS

```
+-----+
| External | Represents a network node which is outside
| Entity   | the control of a network provider
+-----+
```

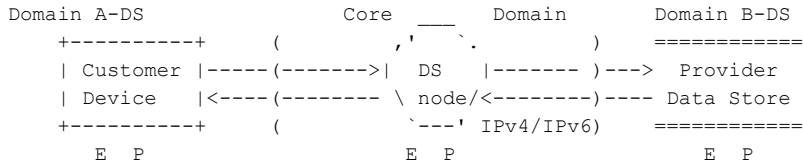
```
  _____
 / '   ' \
|  Pro   | Represents a middle-box or a network node
|  cess/  | which processes network data
 \_____/
```

```
=====
Data store  Represents a node where data is stored
=====
```

```
Data Flow
-----> Data exchanged between network elements
```

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

# DECOMPOSE THE TECHNOLOGY: DFD FOR DS TRANS TECH



## Legend

```

+-----+
| External |
| Entity   |
+-----+
  
```

```

, ' ' \ .
| Pro |
\ cess/
' ' '
  
```

```

=====
Data store
=====
  
```

Data Flow

-----&gt;

## Trust

() E=Entry

() point

() P=Protected

boundary

# IDENTIFY THE THREATS: STRIDE-DFD ASSOCIATIONS

```

+---+---+---+---+---+---+
| S | T | R | I | D | E |
+---+---+---+---+---+---+
| # |   |   | # |   |   |
+---+---+---+---+---+---+
| O | O | O | O | O | O |
+---+---+---+---+---+---+
|   | = | = | = | = |   |
+---+---+---+---+---+---+
|   | > |   | > | > |   |
+---+---+---+---+---+---+
| # | External entity |
+---+---+---+---+---+---+
| O | Process          |
+---+---+---+---+---+---+
| = | Data store       |
+---+---+---+---+---+---+
| > | Data flow        |
+---+---+---+---+---+---+

```

7

<sup>7</sup>Shostack, see n. 5.

# DECOMPOSE THE TECHNOLOGY: LEVEL OF TRUST

```

+---+---+---+---+---+---+
| 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         |
+---+---+---+---+---+---+

```

# IDENTIFY THE THREATS: DOCUMENTING THE THREATS

```

+-----+-----+
| 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 |
+-----+-----+

```

# IDENTIFY THE THREATS: BASIC THREATS

	ThreatID	Description	S	T	R	I	D	E	Mitigation
1	IETF-TDB	ARP	H	H	H	H	H		Static
V	-ARP-1	cache							ARP
	[8]	poisoning							entries, arpwatch
2	IETF-TDB	Default			L	L	L		No widely
V	-ND-5	router							accepted
	[RFC3756]	is 'killed'							mitigation technique
3	IETF-TDB	OSPFv3	L	L	L	L	L	L	no
V	-OSPFv3-2	used							manual
	[RFC4552]	without							keys
		IPsec							
Legend									
H		associated with			L				associated with
		High likelihood							Low likelihood

<sup>8</sup>Cristina L Abad, Rafael Bonilla, et al. "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*. IEEE, 2007, pp. 60–60.

<sup>9</sup>M. Gupta and N. Melam. *Authentication/Confidentiality for OSPFv3*. RFC 4552 (Proposed Standard). Internet Engineering Task Force, June 2006. URL: <http://www.ietf.org/rfc/rfc4552.txt>.

<sup>10</sup>P. Nikander, J. Kempf, and E. Nordmark. *IPv6 Neighbor Discovery (ND) Trust Models and Threats*. RFC 3756 (Informational). Internet Engineering Task Force, May 2004. URL: <http://www.ietf.org/rfc/rfc3756.txt>.

# IDENTIFY THE THREATS: COMPLEX THREATS

	ThreatID	Description	S	T	R	I	D	E	Mitigation
1	IETF-TDB	IETF-TDB	H	H	H	H	H		
V	-DS-1	-ARP-1							DoS
		+							Mitigation
		IETF-TDB							for
		-ND-4							IPv4 suite
2	IETF-TDB	IETF-TDB	H	H	H	H	H	H	Crypto
V	-DS-3	-ARP-1							authen
		+							
		IETF-TDB							
		-OSPFv3-2							
Legend									
H		associated with				L			associated with
		High likelihood							Low likelihood



# COLLATERAL CONTRIBUTION

- ▶ The threat format
  - ▶ Following the presented pattern a threat database could be maintained for the protocols proposed in the IETF
- ▶ *Security Considerations* section of technologies/protocols proposed in the IETF could be structured on the lines of:
  - ▶ Identify the function
  - ▶ Associate the technology with a generic category (if any)
  - ▶ Decompose the technology
  - ▶ Identify the threats
  - ▶ Validate the threats

## NEXT STEPS

### ★ Questions for OPSEC:

- ▶ How adoption-ready is this draft?

### ★★ Side Questions for OPSEC

- ▶ Does it make sense to maintain a structured threat database for protocols proposed in the IETF ?
- ▶ If writing a new protocol draft, would you follow a similar pattern to the one proposed?

# CONTACT

