iplab

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

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

Marius Georgescu

Nara Institute of Science and Technology
Internet Engineering Laboratory

20 Jul. 2016

DRAFT MOTIVATION: IPV6 TRANSITION

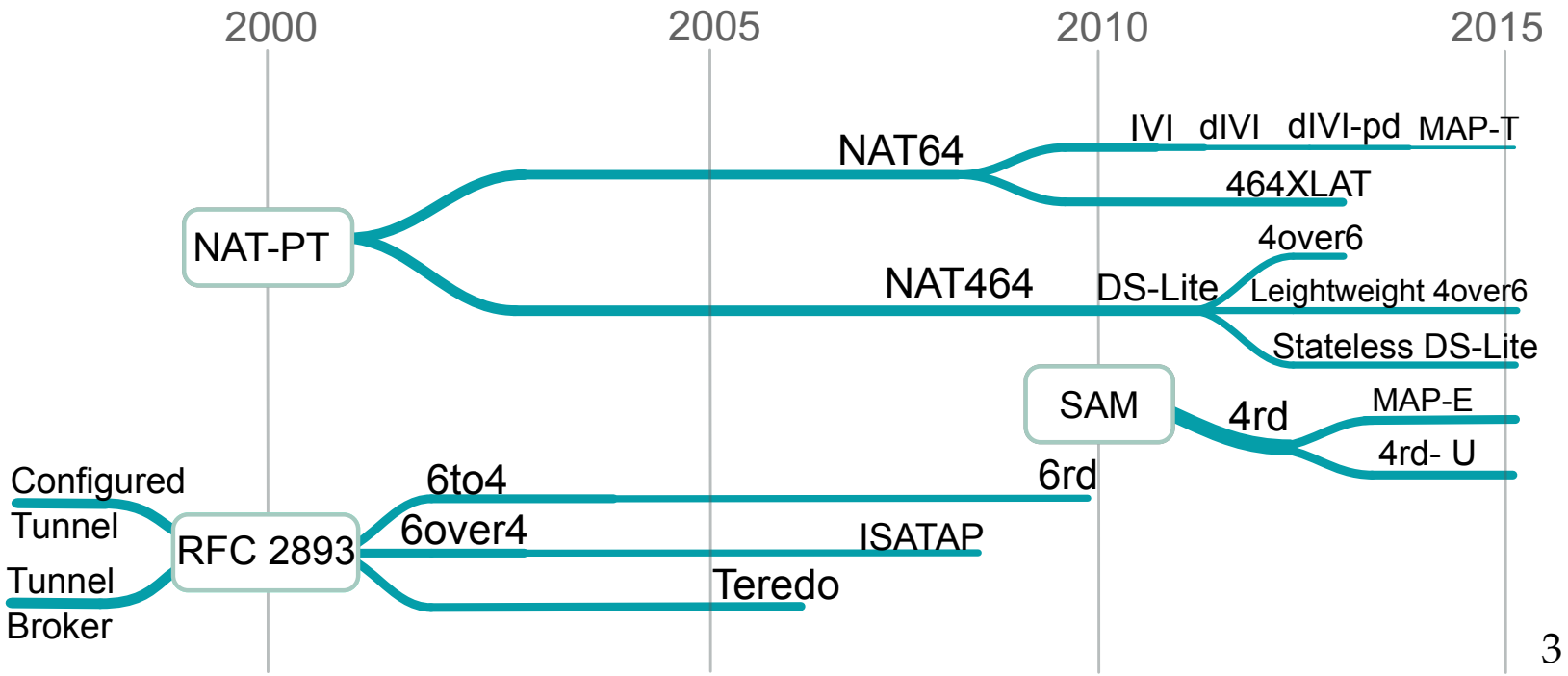
- IPv6 is not backwards compatible
- The Internet will undergo a period through which both protocols will coexist
- Currently only 6% of worldwide Internet users have IPv6 connectivity [1]

[2]

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

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

IPV6 TRANSITION TECHNOLOGIES EVOLUTION



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

DRAFT OVERVIEW

- Provides complementary security considerations to RFC4942[4]
  - Proposes a threat modeling approach based on the established STRIDE threat classification [5]
  - Considers the generic classification on IPv6 transition technologies defined in draft-ietf-bmwg-ipv6-tran-tech-benchmarking-01 [6]
  - 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

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

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

[6] Marius Georgescu and Gabor Lencse. *Benchmarking Methodology for IPv6 Transition Technologies*. draft-ietf-bmwg-ipv6-tran-tech-benchmarking-02.txt. Internet Engineering Task Force, July 2016. URL: https://tools.ietf.org/html/draft-ietf-bmwg-ipv6-tran-tech-benchmarking-02.

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.

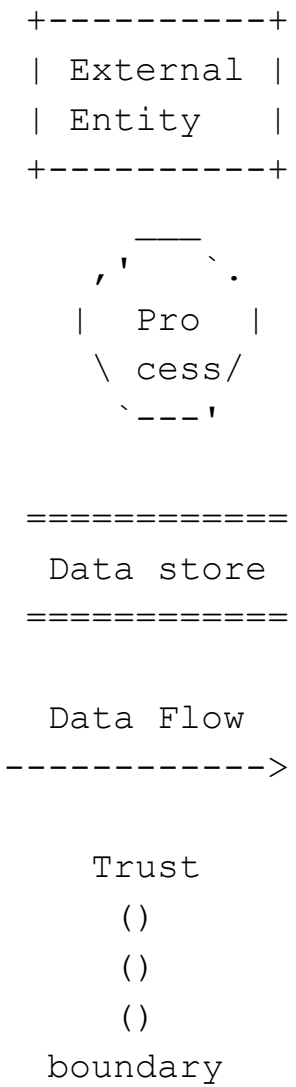
Text in Section 5.1:

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 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.

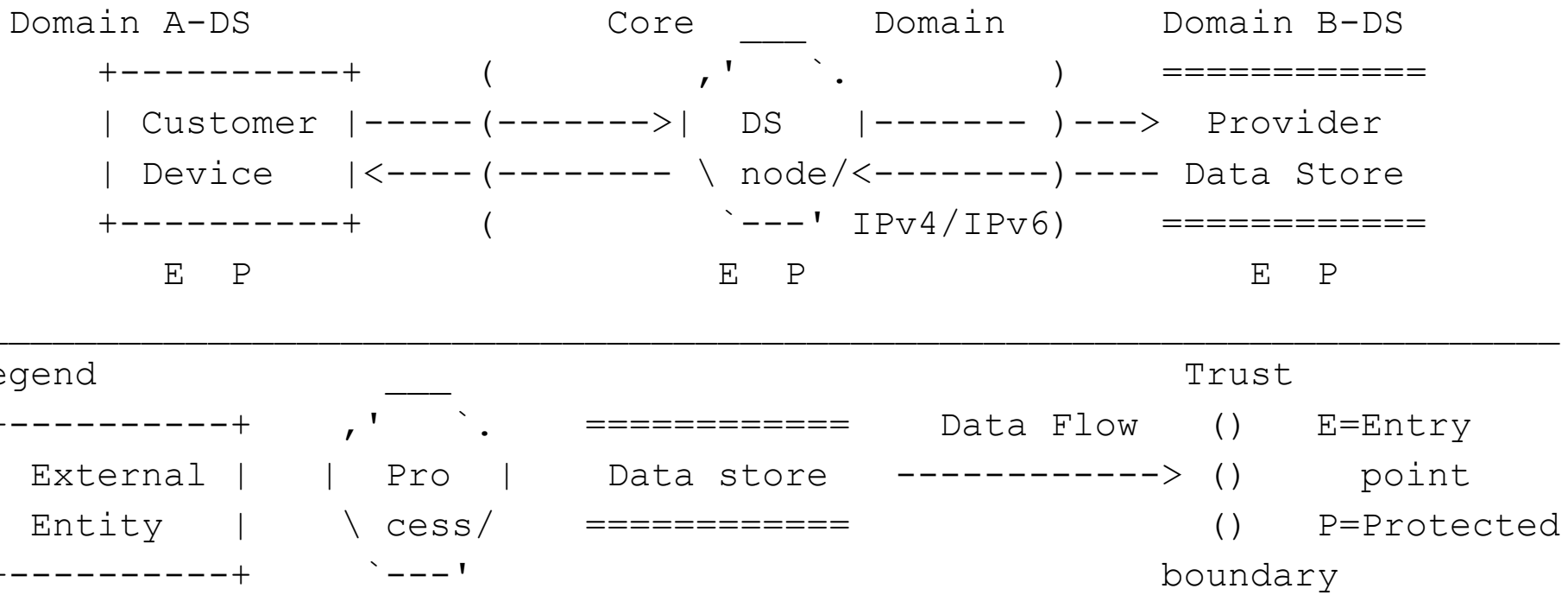
Identify the generic category

	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]

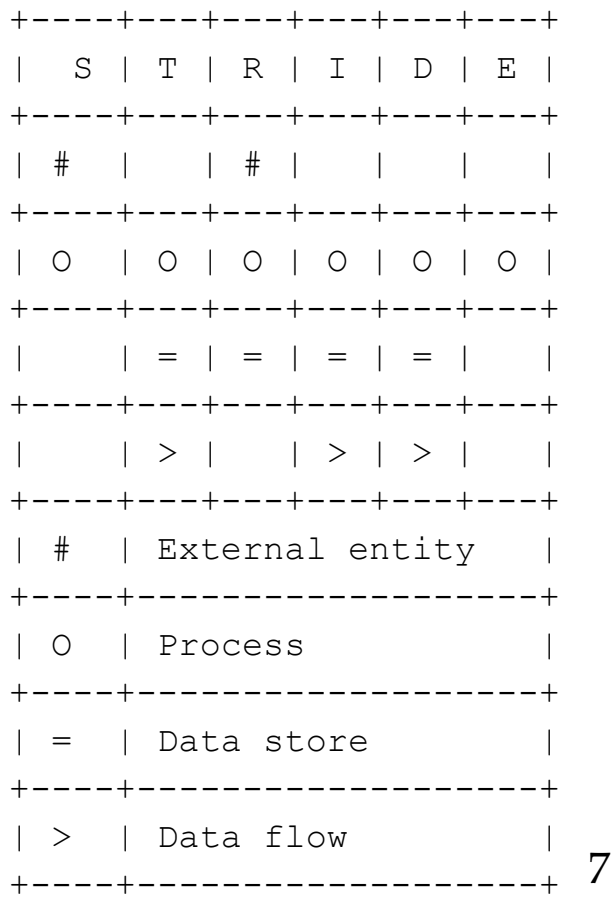
DECOMPOSE THE TECHNOLOGY: DFD ELEMENTS



DECOMPOSE THE TECHNOLOGY: DFD FOR DS TRANS TECH



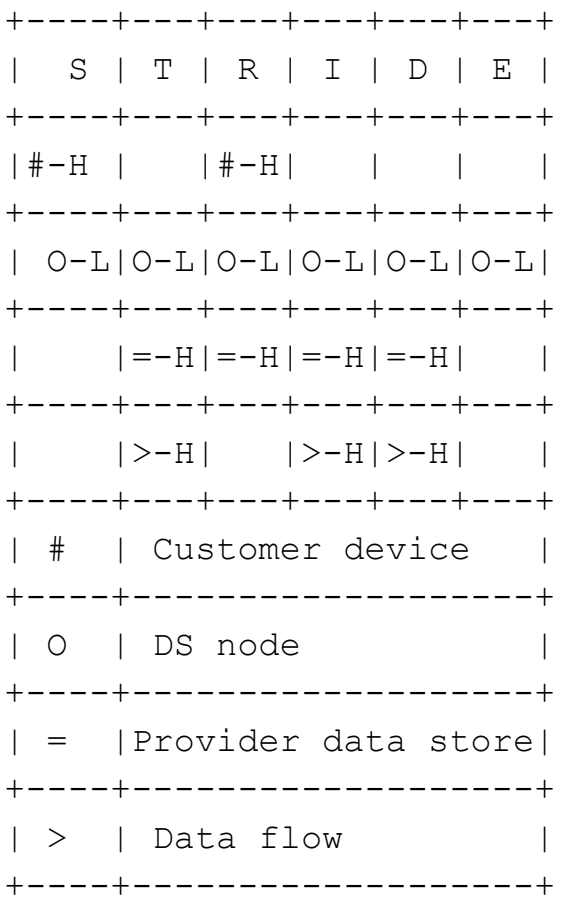
IDENTIFY THE THREATS: STRIDE-DFD ASSOCIATIONS



[7]

[7] Shostack, see n. 5.

DECOMPOSE THE TECHNOLOGY: LEVEL OF TRUST



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 V	IETF-TDB -ARP-1 [8]	ARP cache poisoning	H	H	H	H	H		Static ARP entries, arpwatch
2 V	IETF-TDB -ND-5 [RFC3756]	Default router is 'killed'			L	L	L		No widely accepted mitigation technique
3 V	IETF-TDB -OSPFv3-2 [RFC4552]	OSPFv3 used without IPsec	L	L	L	L	L	L	no manual keys

Legend			
H	associaced with High likelihood	L	associaced with Low likelihood

[8] 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.

[9] 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.

[10] 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 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-3	IETF-TDB -ARP-1 + IETF-TDB -OSPFv3-2	H	H	H	H	H	H	Crypto authen

Legend			
H	associaced with High likelihood	L	associaced with 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


Institute of Science and Technology
NAIST
Nara
Marius Georgescu
liviumarius-g@is.naist.jp
www.ipv6net.ro
IPv6
IPv4