TALLINN UNIVERSITY OF TECHNOLOGY
Department of Computer Science
TUT Centre for Digital Forensics and Cyber Security

ITC70LT
Christian Ponti 144704

WHAT APPROACH CAN BE USED TO GAIN NETWORK ACCESS FROM OUTSIDE BY USING ICMPv6?

Master Thesis

Supervisor: Bernhards Blumbergs
PhD

Tallinn 2016

Autorideklaratsioon

Autorideklaratsioon on iga lõputöö kohustuslik osa, mis järgneb tiitellehele. Autorideklaratsioon esitatakse järgmise tekstina:

Olen koostanud antud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud. Käsolevat tööd ei ole varem esitatud kaitsmisele kusagil mujal.

Autor: [Ees− ja perenimi]

[April 1, 2016]

Annotatsioon

Annotatsioon on lõputöö kohustuslik osa, mis annab lugejale ülevaate töö eesmärkidest, olulisematest käsitletud probleemidest ning tähtsamatest tulemustest ja järeldustest. Annotatsioon on töö lühitutvustus, mis ei selgita ega põhjenda midagi, küll aga kajastab piisavalt töö sisu. Inglisekeelset annotatsiooni nimetatakse Abstract, venekeelset aga

Sõltuvalt töö põhikeelest, esitatakse töös järgmised annotatsioonid:

- kui töö põhikeel on eesti keel, siis esitatakse annotatsioon eesti keeles mahuga $\frac{1}{2}$ A4 lehekülge ja annotatsioon *Abstract* inglise keeles mahuga vähemalt 1 A4 lehekülg;
- kui töö põhikeel on inglise keel, siis esitatakse annotatsioon (Abstract) inglise keeles mahuga $\frac{1}{2}$ A4 lehekülge ja annotatsioon eesti keeles mahuga vähemalt 1 A4 lehekülg;

Annotatsiooni viimane lõik on kohustuslik ja omab järgmist sõnastust:

Lõputöö on kirjutatud [mis keeles] keeles ning sisaldab teksti [lehekülgede arv] leheküljel, [peatükkide arv] peatükki, [jooniste arv] joonist, [tabelite arv] tabelit.

Abstract

Võõrkeelse annotatsiooni koostamise ja vormistamise tingimused on esitatud eestikeelse annotatsiooni juures.

The thesis is in [language] and contains [pages] pages of text, [chapters] chapters, [figures] figures, [tables] tables.

Glossary of Terms and Abbreviations

Lühendite ning mõistete sõnastikku lisatakse kõik töö põhitekstis kasutatud uued ning ka mitmetähenduslikud üldtuntud terminid. Näiteks inglisekeelne lühend PC võib tähendada nii Personal Computer kui ka Program Counter, sõltuvalt kontekstist. Lühendid ja mõisted esitatakse tabuleeritult kahte tulpa selliselt, et vasakul on esitatud lühend või mõiste ja paremal tulbas seletus. Inglisekeelsed sõnad seletustes esitatakse kaldkirjas. Alltoodud näited esitavad lühendite ja mõistete sõnastiku korrektset vormistamist.

IPv6	Internet Protocol version 6
ICMPv6	Internet Control Message Protocol version 6
Node	ll
NAT	dd
IANA	Internet Assigned Numbers Authority
BYID	Bring Your Own Device
OS	Operating System
IoT	Internet of Things
rootkit	ff

Contents

1 Introduction **10**

2 Background and Related Work **15**

2.1 Background 15

2.1.1 Terminology 17

2.1.2 RFC 2460 18

2.1.3 RFC 4443 19

2.1.4 RFC 4861 24

2.2 Covert Channel 33

2.2.1 The Prisoners' Problem 33

2.2.2 Definitions 34

2.2.3 Related Research 35

3 Methodology **40**

4 Implementation **41**

5 Experiment **42**

6 Results **43**

7 Conclusions **44**

References **45**

Appendix 1 **47**

Appendix 2 **52**

List of Figures

1 Communication Scenarios 35

List of Tables

1 ICMPv6 General Header Format . . . 19
2 ICMPv6 Error Messages . . . 19
3 ICMPv6 Informational Messages . . . 20
4 Destination Unreachable Codes . . . 21
5 Time Exceeded Codes . . . 22
6 Parameter Problem Codes . . . 22
7 Echo Request Fields . . . 23
8 Echo Reply Fields . . . 23
9 RFC 4861 Messages . . . 24
10 Router Solicitation Fields and Options . . . 25
11 Router Advertisement Fields and Options . . . 26
12 Neighbor Solicitation Fields and Options . . . 27
13 Neighbor Advertisement Fields and Options . . . 28
14 Redirect Fields and Options . . . 29
15 Options Type and Names . . . 30
16 Source/Target Link-layer Address Fields . . . 30
17 Prefix Information Fields . . . 31
18 Redirect Header Fields . . . 32
19 MTU Fields . . . 32
20 Investigated Protocols . . . 38
21 IPv6 Header . . . 47
22 Destination Unreachable . . . 47
23 Packet Too Big . . . 48
24 Time Exceeded . . . 48
25 Parameter Problem . . . 48
26 Echo Request . . . 48
27 Echo Reply . . . 49
28 Router Solicitation . . . 49
29 Router Advertisement . . . 49
30 Neighbor Solicitation . . . 50
31 Neighbor Advertisement . . . 50
32 Redirect . . . 50
33 Source/Target link-layer Address . . . 50
34 Prefix Information . . . 51

35 Redirect Header 51
36 MTU 51
37 RFC 4443 - Message Processing Rules 52
38 RFC 4443 - Destination Unreachable 53
39 RFC 4443 - Packet Too Big 53
40 RFC 4443 - Time Exceeded 54
41 RFC 4443 - Parameter Problem 54
42 RFC 4443 - Echo Request 54
43 RFC 4443 - Echo Reply 55
44 RFC 4861 - Validation of Router Solicitation 56
45 RFC 4861 - Validation of Router Advertisement 57
46 RFC 4861 - Validation of Neighbor Solicitation 58
47 RFC 4861 - Sending Neighbor Solicitation 59
48 RFC 4861 - Reception of Neighbor Solicitation 59
49 RFC 4861 - Validation of Neighbor Advertisement 60
50 RFC 4861 - Solicited Neighbor Advertisement 61
51 RFC 4861 - Receipt of Neighbor Advertisement 61
52 RFC 4861 - Validation of Redirect 62
53 RFC 4861 - Redirect, specifications 63
54 RFC 4861 - Options 63

1. Introduction

IPv6 is the designated successor of IPv4, a protocol specified and implemented in a context with a limited number of users and hosts, most of them circumscribed to the scientific world. The need of a new protocol arose because of a changed context: the evolution of new powerful devices and their spread in many field of the society, which in turn modified the behavior and the requests of new entities, being them individuals or big organizations. The new IP protocol has been specified and rewritten in many aspects, taking in consideration the evolution of the requirements and the future needs of the involved actors.

IPv6[1], with respect to his predecessor, changed in many aspects. The headers have been modified to accommodate new functionalities and improved capabilities, mainly it provides "expanded addressing capabilities", "header format simplification", "improved support for extensions and options", "flow labeling capability", and “authentication and privacy capabilities". One of the most relevant aspect is the increased address space from 32 bits to 128 bits, which deals with the demand of new communicating devices to fulfill organization’s requirements.

Despite IPv6 specifications have been formalized in 1998, its spread and adoption by the world community is far from being accomplished. Among the many possible reasons that could explain this behavior, two of them deserve particular attention. The first one is related to the lack of address space, which has been mitigated by the introduction of Network Address Translation (NAT)[2]: the use of NAT allows to use a private, not routeable, address space for the internal network of an organization, and the use of one, or limited number, public IPv4 address at the network boundary. This technique mitigated the need to introduce the 128 bits address space of IPv6, because organization’s requirements to allocate new IPv4 address from IANA[1] have been reduced. The second reason is related to the applications and services offered by organizations. Networked applications have been written for, and tested against, IPv4. Many of them represents IT assets which are critical for the business assets and goals of enterprises: the introduction of new applications written for IPv6 represents a great effort in terms of financial investment, time for implementation and testing, and use of enterprises’ resources.

The IPv6 world is composed by a number of protocols, which are used by nodes to fulfill their requirements: some of them, with respect to their IPv4 version, have been obsoleted by new concepts and specifications of IPv6, while others have been rewritten with few changes. In this galaxy of protocols, one of them, present also in its version 4, deserves particular at-

[1] http://www.iana.org/

tention: ICMPv6.

ICMPv6, despite it shares almost the same naming convention with respect with the predecessor, could be considered a new protocol for a number of reasons, which make it a critical subject of research by the scientific community. The reasons behind its criticality arise because it holds a backward compatibility with the functions of its version 4, but at the same time it introduces a number of new functionalities, and responsibilities, for the correct behavior of an IPv6 node.

ICMPv4 has been used by IPv4 to manage error and informational messages to allow for a better management and troubleshooting of the network. While it is an important aspect of the network and it has been used by network administrators to manage network issues, it is not crucial for the correct working of the communication. This version has been tested for many years, with the identification of vulnerabilities which can be potentially be exploited by malicious actors. Many best practices[2] [3] suggested to filter ICMPv4 messages at network boundaries to mitigate the risk of the exploitation of some vulnerabilities without compromising the network functionalities. Nowadays the network evolved in more sophisticated designs, and new concepts, like Bring Your Own Device (BYOD) and wireless networks, partially obsolete the very same concept of boundaries, bringing new threats to the internal network. The security controls could no more be applied only at the boundaries, but must be introduced in other segments of the network. This new security controls applies to the ICMPv4 protocol as well, and filtering must be introduced where such messages are not strictly required by network administrators.

"ICMPv6 is used by IPv6 nodes to report errors encountered in processing packets, and to perform other internet-layer functions, such as diagnostics (ICMPv6 "ping"). ICMPv6 is an integral part of IPv6, and the base protocol (all the messages and behavior required by this specification) MUST be fully implemented by every IPv6 node."[3]

This paragraph of RFC 4443 describes broadly the purpose of ICMPv6, but the most important part is the last sentence, which states that the base protocol must be fully implemented by every IPv6 node. In the RFC terminology, the word "MUST, or the terms REQUIRED or SHALL, mean that the definition is an absolute requirement of the specification"[4]. The real distinction between ICMPv4 and ICMPv6 in this context is formal: RFC 792 states that "ICMP ... must be implemented by every IP module"[5], which means that an implementation is required. The ICMPv6 specification is more precise because it refers to every IPv6 node, which covers the implementation inside the module, but also, with the concept of node,

[2] http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc29, accessed 20.03.2016

[3] http://www.cisco.com/c/en/us/about/security-center/firewall-best-practices.html#_Toc332805964, accessed 20.03.2016

implies that the node must be able to use its functionalities.
This is a fundamental distinction, because the best practices in use with ICMPv4, with ICMPv6 are no more relevant, at least with some message types. As it is written in this paper[6], which cites RFC 4861[7], "ICMPv6 is used for basic functionalities and used by other IPv6 protocols ... Neighbor Discovery Protocol is a protocol used with IPv6 to perform various tasks like router discovery, auto address configuration of a node, neighbor discovery, Duplicate Address Detection, determining the Link Layer addresses of other nodes, address prefix discovery, and maintaining routing information about the paths to other active neighbor nodes".
This is the first critical point to consider: version 4 and version 6 of the ICMP protocol share some functionalities, but are different protocols. ICMPv6 is not a protocol modified to adapt itself to IPv6, a new analysis must be performed in an exhaustive way taking into account new scenarios, and new best practices must be applied to mitigate the risk of exploitation of new vulnerabilities related to its functionalities.
Another important aspect to take into consideration when dealing with IPv6 in general, and with ICMPv6, is the transition from version 4 to version 6. For the aforementioned reasons mentioned, many organizations delayed as much as they could the deployment of a full IPv6 network. Nevertheless the scientific community continued to improve the new version and its related protocols, and Operating Systems (OS) started to include them in their network implementations. At the same time, techniques to allow a slow transition have been developed: examples of that are the dual stack, the presence and coexistence of both protocol versions in the same node, or the encapsulation of IPv6 inside IPv4, in those network segments where IPv6 has not been deployed yet. In addition, in many OS, IPv6 is active by default and preferred over IPv4.
These aspects must not be underestimated and show again how critical and urgent is an in-depth analysis of ICMPv6: not only this protocol is fundamental for IPv6 and the best practices can be used only against the old version, but it is already present and activated in OS that users employ in their everyday life. This last distinction is very important because it introduces another aspect to take into account: network administrator and security officer must not deal only with threats deriving from the exploitation of technical vulnerabilities, but also with behavioral procedures shaped around years of practice. IPv6 and ICMPv6 are not protocol that will be introduced in the future, they are already present in this transition period and we must deal with them now. Countermeasures must be in place, at the network boundaries and inside critical network segments above all, that take into consideration version 6 of the protocols. Such countermeasures must follow new best practices carefully shaped around the new version.

The underlined elements, the differences between the two ICMP version and the transition period with the coexistence of IPv4 and IPv6, lead to another topic: the impact of the full deployment of IPv6, and ICMPv6, and the implications for the involved actors, being them users, enterprises, states, or malicious actors.
The scientific community has been involved in the specification, in the improvement, and testing of the protocols since time. But, with respect with the preceding version of the protocols, version 6 of the suite must deal with a very different situation. The electronic communication is spread around the world in a pervasive way, and the near future, with the Internet of Things (IoT) [4], will further the spread. ICMPv6, and IPv6, will be fully deployed in a world strongly dependent on the electronic communication, where critical infrastructures (CI) must be managed and protected, where enterprises relies on its IT infrastructure to support their business assets, and where users are tight to their online experience for their everyday needs. This change in the very basic infrastructure of the network will have an impact which has no terms of comparison with respect to IPv4, whose slow deployment allowed to discover the concept of security and to learn by experience. The transition period, which introduced some security issues, in this case works as a mitigation technique to allow researcher to test the protocols in an exhaustive way, without waiting that the fully deployed IPv6 infrastructures reveals potential weaknesses.
This urgency can be better understood by taking into consideration the evolution of the threats, the sophistication of malware, and the malicious actors involved in the research of vulnerabilities to exploit, as well as their purposes and means to reach their goals.
The term Advanced Persistent Threat (APT) is used to define "any sophisticated adversary engaged in information warfare in support of long-term strategic goals"[8]. One of the main characteristic of APT detected in the wild is the sophistication of the attack. One example is the Uroburos rootkit[9], which "modular structure allows extending it with new features easily, which makes it not only highly sophisticated but also highly flexible and dangerous". The analysis of the rootkit suggests that "the development of a framework like Uroburos is a huge investment" and "that it was designed to target government institutions, research institutions or companies dealing with sensitive information as well as similar high-profile targets". There are other example of APT that suggested an evolution of the threat landscape, like Stuxnet[10]. Even if the aforementioned APT do not target directly IPv6, they share a common characteristic which is important to underline: the sophistication, the investment behind them, and the presence of an Advanced Persistent Adversary (APA)[11], term that "depicts not only the threat, but the threat actors as well".

[4] IoT, http://www.theinternetofthings.eu/what-is-the-internet-of-things, accessed 21.03.2016

The evolution of the threat landscape depicts a situation where APA, often associated with groups sponsored by state actors, have unlimited budget to develop very sophisticated attacks to reach their goals. In the current situation, given the impact that the full deployment of IPv6 will have, those actors have the resources and the motivation to research and discover vulnerabilities in IPv6, ICMPv6, and other protocols involved. Moreover, if this research will succeed, APA can gain a considerable advantage over their opponents, because a possible vulnerability at network layer may allow to bypass more easily the security mechanisms in place and give more robust mechanisms to stay undetected for longer.

While research and tests on ICMPv6 are an ongoing process, the urgency and criticality of the subject require a more in-depth analysis which take into account the full deployment, but also the transition period. To pursue this goal it is important to start from the specifications of the protocol, the RFCs. Those documents represent a guideline, the result of an agreement between many stakeholders. As a guideline, there is no guarantee that the implementation will follow the suggestion, even in the sections specified with a ”must“.

It is worth to underline the contribution of this research, which start by producing the necessary awareness with regard to IPv6 and ICMPv6. This is the starting point to understand the need to analyze the protocols in detail. Furthermore, it is important to see the big picture, which include not only ICMPv6, but also its relationship with the devices involved in the communication, the target hosts, and the firewalls through which the packets must transit. Firewalls are devices configured by human beings, which may commit mistakes and use different best practices. Each configuration can produce a different scenario, which is worth to analyze because in the real world each system may differ from another, and the goal of an APA is to find these slight differences between them to take advantage. A scenario-based experiment needs also a test set, based on RFC specifications, and the implementation of a software to conduct the experiments.

The next chapters of this work will explore the backgrounds, the specification inside RFCs, and the related work(see 2), which includes existing tools and projects to test ICMPv6, and a review of the literature. Then the analysis proceeds with definition of the methodology(see 3) of this research, which is based on the scientific method of the experimentation; the chapter includes the motivation behind this choice and behind the choice of the technology to conduct the experiments. The implementation is the next chapter(see 4), which deal with the details of the technology, followed by the experiment(see 5), which describes the set of performed tests. The chapter related to the results(see 6) includes a discussion about the results of the experiment and its meaning. Finally, the conclusions(see 7) summarizes the research, discuss about suggestions and future work.

2. Background and Related Work

2.1. Background

”The Internet Standards process is an activity of the Internet Society that is organized and managed on behalf of the Internet community by the Internet Architecture Board (IAB)[5] and the Internet Engineering Steering Group (IESG)[6]. ... an Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet. ... Each distinct version of an Internet standards-related specification is published as part of the "Request for Comments" (RFC) document series. This archival series is the official publication channel for Internet standards documents and other publications of the IESG, IAB, and Internet community.“[12]

This work starts by analyzing the RFCs related to ICMPv6, which specify the protocol and the features to which each implementation must adhere. The main goal of an agreement on a protocol is interoperability [7], but, since this is not a binding process, and even though implementations follow the main specifications, it is always possible that some of them do not adhere completely. This could lead to some interoperability issues, which may introduce vulnerabilities in the protocol.
The background of this research is represented by two RFCs, ”Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification“[3], and ”Neighbor Discovery for IP version 6 (IPv6)“[7]. These two RFCs specify the general header for ICMPv6 messages, and each specific message header to which each implementation must adhere.
The IPv6 specification[1] is only partially in the scope of this research, but it must be mentioned, because of its tight relationship with ICMPv6, and because in each ICMPv6 message type specification some of its fields are cited, as it will be underlined later in the chapter.

[5] https://www.iab.org/
[6] https://www.ietf.org/iesg/
[7] http://www.merriam-webster.com/dictionary/interoperability

RFCs use a specific set of words to express the requirements of the implementations [4]. Words like ”must“, or ”should“ have a particular meaning, as expressed in the cited document, that should be well understood by implementors. The reason is that a lack of compliance may lead to the introduction of some vulnerabilities, where a node is especting a particular behavior from another peer, while the peer's implementation follows slightly different specifications. This research, inside next sections, will try to underline where, under each message type, and along the general specifications (e.g. general processing rules), it is possible to insert vulnerabilities in the protocol if the interpretation of the specifications were different between the implementations.

Since the list of possibilities may be long, this research will use criteria in order to generate a subset of specification to test. The followed mechanism is to first select specifications and insert them into a set of tables, each related to a specific message, and then select from each table the test to be performed during the experiment. The criteria are presented at the end of this chapter, after the related works' analysis.

2.1.1. Terminology

This research background's analysis starts from the terminology, since it is important to define and understand the terms which will be spread across the RFCs. The definition's sources are the RFCs.

Node:	a device that implements IPv6.
Link:	a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IPv6.
Interface:	a node's attachment to a link.
Neighbors:	nodes attached to the same link.
Prefix:	a bit string that consists of some number of initial bits of an address.
On-link:	an address that is assigned to an interface on a specified link.
Off-link:	an address that is not assigned to any interfaces on the specified link.
Longest prefix match:	the process of determining which prefix in a set of prefixes covers a target address. A target address is covered by a prefix if all of the bits in the prefix match the left-most bits of the target address. When multiple prefixes cover an address, the longest prefix is the one that matches.
Reachability:	whether or not the one-way "forward" path to a neighbor is functioning properly. In particular, whether packets sent to a neighbor are reaching the IP layer on the neighboring machine and are being processed properly by the receiving IP layer.
Packet:	an IPv6 header plus payload.
Link MTU:	the maximum transmission unit, i.e., maximum packet size in octets, that can be conveyed over a link.
Path MTU:	the minimum link MTU of all the links in a path between a source node and a destination node.
Multicast capable:	a link that supports a native mechanism at the link layer for sending packets to all (i.e., broadcast) or a subset of all neighbors.
Point-to-point:	a link that connects exactly two interfaces.

Link-local address:	a unicast address having link-only scope that can be used to reach neighbors.
All-nodes multicast address:	the link-local scope address to reach all nodes, FF02::1.
All-routers multicast address:	the link-local scope address to reach all routers, FF02::2.
Solicited-node multicast address:	a link-local scope multicast address that is computed as a function of the solicited target's address. The function is chosen so that IP addresses that differ only in the most significant bits will map to the same solicited-node address thereby reducing the number of multicast addresses a node must join at the link layer.
Unspecified address:	a reserved address value that indicates the lack of an address. It is never used as a destination address, but may be used as a source address if the sender does not know its own address. The unspecified address has a value of 0:0:0:0:0:0:0:0.

2.1.2. RFC 2460

The table (see 21) shows the specification of the IPv6 header. From the point of view of this research, there are four interesting fields which are strictly involved in the ICMPv6 specification:

- **Next Header**: 8-bit, identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field. The ICMPv6 value is 58. The complete list is available on IANA's website[8]
- **Hop Limit**: 8-bit, decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.
- **Source Address**: 128-bit address of the originator of the packet.
- **Destination Address**: 128-bit address of the intended recipient of the packet.

[8] http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml, accessed on 27.03.2016

2.1.3. RFC 4443

The Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification categorizes two broad type of messages, error and informational messages.
As shown in the table (see 1), the general ICMPv6 header format is composed by an 8 bit **type** field, an 8 bit **code** field, and a 16 bit **checksum** field. The message body suggests specific header fields which are characteristic of each message type.
ICMPv6 messages are categorized by its type field, while the code field in this specification identifies a specific message under the category.
Error messages are characterized by a 0 in the high order bits of the type field, which gives a value range between 0 and 127. Informational message are instead characterized by a 1 in the high order bits, for a possible value range between 128 and 255.

Type	Code	Checksum
Message Body		

Table 1. ICMPv6 General Header Format

The next two table (see 2 and 3) summarize the type of ICMPv6 messages described in this RFC.

Type field	Error Message
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
100	Private experimentation
101	Private experimentation
127	Reserved for expansion of ICMPv6 error messages

Table 2. ICMPv6 Error Messages

The RFC, besides ICMPv6 fields, gives directives also for IPv6 fields of interest. For all the error messages and Echo Reply is the Destination Address field, which is ”copied from the

Type field	Informational Message
128	Echo Request
129	Echo Reply
200	Private experimentation
201	Private experimentation
255	Reserved for expansion of ICMPv6 informational messages

Table 3. ICMPv6 Informational Messages

Source Address field of the invoking packet“. For an Echo Request, the IPv6 field is ”any legal IPv6 address“.
The RFC includes a ”Message Processing Rules“ section, which underlines the rules that a node must observe while processing an ICMPv6 message. The complete list is in table 37 in Appendix 2.
During the preparation for the experiment it is important to identify tests that may lead to unexpected, from the RFC specification point of view, results. One example of that, taking the first rule in the aforementioned table, may be:
what would happend in the case that an ICMPv6 error message of unknown type is received at its destination, and it is passed to the upper-layer process **with a forged malicious payload**?
As this research will show, some test may be spread across different scenarios, while other are more suitable to be performed only in a specific scenario; the example above is a good candidate for an outside-to-inside direction scenario, in order to test the behavior of an internal node.

Destination Unreachable

The first inspected message type is Destination Unreachable. Its purpose is to generate an error ”in response to a packet that cannot be delivered to its destination address for reasons other than congestion“.
For a detailed view of the header, table (see 22) in 7.
The table (see 4) summarizes the type and code fields of the header, with the corresponding code name of the message.

The Unused field accordingly to the RFC must be initialized to zero by the originator and

Type	Code	Description
1	0	No Route to Destination
	1	Communication with destination administratively prohibited
	2	Beyond scope of source address
	3	Address unreachable
	4	Port unreachable
	5	Source address failed ingress/egress policy
	6	Reject route to destination

Table 4. Destination Unreachable Codes

ignored by the receiver.
The following illustrates the meaning behind codes and description:

No Route to Destination: lack of a matching entry in the forwarding node's routing table
Communication with destination administratively prohibited: administrative prohibition (e.g., a "firewall filter")
Beyond scope of source address: the destination is beyond the scope of the source address (e.g., when a packet has a link-local source address and a global-scope destination address)
Address unreachable: the reason for the failure to deliver cannot be mapped to any of other codes
Port unreachable: generated in response to a packet for which the transport protocol (e.g., UDP) has no listener
Source address failed ingress/egress policy: the packet with this source address is not allowed due to ingress or egress filtering policies
Reject route to destination: the route to the destination is a reject route (may occur if the router has been configured to reject all the traffic for a specific prefix).

Packet Too Big

A Packet Too Big must be sent by a router in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link.
The table (see 23) in Appendix 1 shows the header fields.
For this message the type field must always be 2 and the code set to 0 and ignored by the receiver. The MTU value represent "the Maximum Transmission Unit of the next-hop link".

Time Exceeded Message

The table (see 24) in Appendix 1 underlines the header fields of this type of message, table 5 shows the codes.

Type	Code	Description
3	0	Hop limit exceeded in transit
	1	Fragment reassembly time exceeded

Table 5. Time Exceeded Codes

If a router receives a packet with a Hop Limit of zero, or if a router decrements a packet's Hop Limit to zero, it must discard the packet and originate an ICMPv6 Time Exceeded message with Code 0 to the source of the packet. An ICMPv6 Time Exceeded message with Code 1 is used to report fragment reassembly timeout.

Parameter Problem Message

"If an IPv6 node processing a packet finds a problem with a field in the IPv6 header or extension headers such that it cannot complete processing the packet, it must discard the packet and should originate an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem".
The table (see 25) in Appendix 1 underlines the header fields of this type of message.
Table 6 shows a mapping between each code and a description of the error.

Type	Code	Description
4	0	Erroneous header field encountered
	1	Unrecognized Next Header type encountered
	2	Unrecognized IPv6 option encountered

Table 6. Parameter Problem Codes

Accordingly to the specification, the pointer field "identifies the octet offset within the invoking packet where the error was detected. The pointer will point beyond the end of the ICMPv6 packet if the field in error is beyond what can fit in the maximum size of an ICMPv6 error message".

Echo Request

The RFC states that each node must implements an Echo mechanism in order to produce Echo Requests and answer with Echo Replies. It also mentions the implementation of an application layer interface, for diagnostics purposes, to originate requests and receive replies. The table (see 26) in Appendix 1 shows the header fields of an Echo Request message.
An Echo Request code is always 0. Identifier and Sequence Number are considered helping fields, which, in fact, could be expected to be zero, as depicted in table 7.

Field	Value/Description
Type	128
Code	0
Identifier	An identifier to aid in matching Echo Replies to this Echo Request. May be zero.
Sequence Number	A sequence number to aid in matching Echo Replies to this Echo Request. May be zero.
Data	Zero or more octets of arbitrary data.

Table 7. Echo Request Fields

Echo Reply

For the Echo Reply Header (see 27), while table 8 shows the fields with the value, where present, or the function.

Field	Value/Description
Type	129
Code	0
Identifier	The identifier from the invoking Echo Request message.
Sequence Number	The sequence number from the invoking Echo Request message.
Data	The data from the invoking Echo Request message.

Table 8. Echo Reply Fields

The RFC reiterate the implementation of the same mechanism as underlined in the Echo Request. In addition, it highlights that if the message is in response to a request to the unicast

address of the node, the source address of the Echo Reply must be copied from the destination address field of the Echo Request.
An Echo Reply should be also originated in the case that the Request has been made to an IPv6 multicast or anycast address, in this case with the source address of the interface that received the message.
The data, which has no limitations in size, must be the same which has been received inside the Echo Request.

2.1.4. RFC 4861

The Neighbor Discovering Protocol has many functionalities and it is used by an IPv6 nodes in order to determine the link-layer address of neighbors, hosts and routers, and to discover which router is able to forward their packets to another off-link networks. In addition, it is used as a reachability mechanism to determine if a host is still alive.
The RFC defines five additional messages, characterized by the type field (for these messages the code is always zero), as summarized in table 9.

Type field	Message
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

Table 9. RFC 4861 Messages

This RFC defines in addition five options, with the possibility to be extended in the future, that ”provide a mechanism for encoding variable length fields, fields that may appear multiple times in the same packet, or information that may not appear in all packets“. Options defined in the document are:

- Source Link-Layer Address
- Target Link-Layer Address
- Prefix Information
- Redirected Header
- MTU

Router Solicitation

The function of a Router Solicitation message, for a host, is to inform a router to generate a Router Advertisement. The format of a Router Solicitation is shown in Appendix 1 (see 28).

Router Solicitation specifies three IPv6 fields:

Source Address	An IP address assigned to the sending interface, or the unspecified address if no address is assigned to the sending interface.
Destination Address	Typically the all-routers multicast address.
Hop Limit	255

The next table (see 10) summarizes the requirements of the fields.

Field	Value/Description
Type	133
Code	0
Reserved	This field is unused. It must be initialized to zero by the sender and must be ignored by the receiver.
Valid Options	
Source link-layer address	The link-layer address of the sender, if known.

Table 10. Router Solicitation Fields and Options

Router Advertisement

Router Advertisement are sent by routers periodically, or in response to a Router Solicitaion, to help hosts in their configuration processes. Examples of such processes are the mechanism to configure their addresses, how to obtain information about DNS servers, prefix information for the link.
The table 29 in Appendix 1 shows the header of a Router Advertisement.
Router Advertisement specifies three IPv6 fields:

Source Address	must be the link-local address assigned to the interface from which this message is sent.
Destination Address	Typically the Source Address of an invoking Router Solicitation or the all-nodes multicast address.
Hop Limit	255

The table (see 11) summarizes the fields with their specifications.

Field	Value/Description
Type	134
Code	0
Cur Hop Limit	The default value that should be placed in the Hop Count field of the IP header for outgoing IP packets. A value of zero means unspecified
M	"Managed address configuration" flag. When set, it indicates that addresses are available via Dynamic Host Configuration Protocol
O	"Other configuration" flag. When set, it indicates that other configuration information is available via DHCPv6.
Reserved	It must be initialized to zero by the sender and must be ignored by the receiver.
Router Lifetime	The lifetime associated with the default router in units of seconds.
Reachable Time	The time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation.
Retrans Timer	The time, in milliseconds, between retransmitted Neighbor Solicitation messages.
Valid Options	
Source link-layer address	The link-layer address of the interface from which the Router Advertisement is sent.
MTU	should be sent on links that have a variable MTU.
Prefix Information	These options specify the prefixes that are on-link and/or are used for stateless address autoconfiguration.

Table 11. Router Advertisement Fields and Options

Neighbor Solicitation

Neighbor Solicitation is used by nodes to request the Link-layer address of a neighbor, or to verify if a neighbor's reachability.
See table 30 in Appendix 1 for the detailed header format.
Neighbor Solicitation specifies three IPv6 fields:

Source Address	Either an address assigned to the interface from which this message is sent or (if Duplicate Address Detection is in progress) the unspecified address.
Destination Address	Either the solicited-node multicast address corresponding to the target address, or the target address.
Hop Limit	255

Table 12 summarizes the fields with their specifications.

Field	Value/Description
Type	135
Code	0
Reserved	It must be initialized to zero by the sender and must be ignored by the receiver.
Target Address	The IP address of the target of the solicitation. It must not be a multicast address.
Valid Options	
Source link-layer address	The link-layer address for the sender.

Table 12. Neighbor Solicitation Fields and Options

Neighbor Advertisement

A Neighbor Advertisement is sent by a node in response to a Neighbor Solicitation, or to spread information quickly. The latter is called unsolicited Neighbor Advertisement.
Neighbor Advertisement specifies three IPv6 fields:

Source Address	An address assigned to the interface from which the advertisement is sent.
Destination Address	For solicited advertisements, the Source Address of an invoking Neighbor Solicitation or, if the solicitation's Source Address is the unspecified address, the all-nodes multicast address. For unsolicited advertisements typically the all-nodes multicast address.
Hop Limit	255

The table (see 13) shows the fields with the specifications.

Field	Value/Description
Type	136
Code	0
R	Router flag. When set, the R-bit indicates that the sender is a router.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address.
O	Override flag. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address.
Reserved	It must be initialized to zero by the sender and must be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address must not be a multicast address.
Valid Options	
Target link-layer address	The link-layer address for the target, i.e., the sender of the advertisement.

Table 13. Neighbor Advertisement Fields and Options

Redirect

Redirect messages are used by routers to inform a node about a better first-hop node on the path to a destination.

Redirect specifies three IPv6 fields:

Source Address	Must be the link-local address assigned to the interface from which this message is sent.
Destination Address	The Source Address of the packet that triggered the redirect.
Hop Limit	255

Table 14 shows the fields with the specifications.

Field	Value/Description
Type	137
Code	0
Reserved	It must be initialized to zero by the sender and must be ignored by the receiver.
Target Address	An IP address that is a better first hop to use for the ICMP Destination Address. When the target is the actual endpoint of communication, i.e., the destination is a neighbor, the Target Address field must contain the same value as the ICMP Destination Address field. Otherwise, the target is a better first-hop router and the Target Address must be the router's link-local address so that hosts can uniquely identify routers.
Destination Address	The IP address of the destination that is redirected to the target.
Valid Options	
Target link-layer address	The link-layer address for the target.
Redirected Header	As much as possible of the IP packet that triggered the sending of the Redirect without making the redirect packet exceed the minimum MTU.

Table 14. Redirect Fields and Options

Options

RFC 4861 specifies a set of options, which can be included in the messages. The general form includes an 8 bit identifier (Type) and an 8 bit length field, which represents "the length

of the option in units of 8 octets. Options should be padded when necessary to ensure that they end on their natural 64-bit boundaries“.

Type	Option Name
1	Source Link-Layer Address
2	Target Link-Layer Address
3	Prefix Information
4	Redirected Header
5	MTU

Table 15. Options Type and Names

Source/Target Link-layer Address

Field	Value/Description
Type	1 for Source Link-layer Address
	2 for Target Link-layer Address
Length	The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1
Link-Layer Address	The variable length link-layer address.

Table 16. Source/Target Link-layer Address Fields

”The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and Router Advertisement packets. The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets. These options must be silently ignored for other Neighbor Discovery messages.“

Prefix Information

The Prefix Information is used by routers to inform hosts about on-link prefixes of the network segments, and allow them to perform address autoconfiguration.

Field	Value/Description
Type	3
Length	4
Prefix Length	The number of leading bits in the Prefix that are valid.
L	On-link flag. When set, indicates that this prefix can be used for on-link determination. When not set the advertisement makes no statement about on-link or off-link properties of the prefix.
A	Autonomous address-configuration flag. When set indicates that this prefix can be used for stateless address configuration.
Reserved1	It must be initialized to zero by the sender and must be ignored by the receiver.
Valid Lifetime	The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity.
Preferred Lifetime	The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. A value of all one bits (0xffffffff) represents infinity.
Reserved2	It must be initialized to zero by the sender and must be ignored by the receiver.
Prefix	An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and must be initialized to zero by the sender and ignored by the receiver.

Table 17. Prefix Information Fields

Redirect Header

This options is used by Redirect messages and contains, in IP header and data, the original packet that triggered the redirect.

Field	Value/Description
Type	4
Length	The length of the option in units of 8 octets.
Reserved	They must be initialized to zero by the sender and must be ignored by the receiver.
IP header + data	The original packet truncated to ensure that the size of the redirect message does not exceed the minimum MTU required to support IPv6.

Table 18. Redirect Header Fields

MTU

The MTU option is used to ensure that all the nodes on the link use the same MTU value, in such case where ”heterogeneous technologies are bridged together“.

Field	Value/Description
Type	5
Length	1
Reserved	It must be initialized to zero by the sender and must be ignored by the receiver.
MTU	The recommended MTU for the link.

Table 19. MTU Fields

This ends the background analysis. Next, this research takes on the related work, in which other researches are taken into consideration in order to understand what have been done in the field, and to take suggestions about possible scenarios that are worth to test.

In the context of an attack, malicious actors can exploit a vulnerability to gain a foothold in the internal perimeter. This is a kind of scenario that concerns many actors, but it is not the only one. There is another scenario to take into consideration, especially if APT and the amont of resources that APA have are recognized. The case that the malicious actor has already gained a foothold and want to exfiltrate data without authorization. The absence of a proper authorization is an important concept, because it includes in the scenario also persons that are authorized to access the network, like employees, but have no authorization to send information outside the internal perimeter.
This scenario is characterized by the flow of the attack, from the internal perimeter to the outside, and by the need, from an attacker point of view, to stay undetected and, at the same time, to be able to pursue its goals. The analysis of this scenario is presented next, and it is usually referred to with the presence of a covert channel.

2.2. Covert Channel

Before attempting to analyze the scenario characterized by a covert channel in a networked communication, it is necessary to describe the context in which it came out first, that is, the Prisoners' Problem.

2.2.1. The Prisoners' Problem

The Prisoners' Problem[13] involves two actors that "have been arrested and are about to be locked in widely separated cells", and a warden, who "is willing to allow the prisoners to exchange messages in the hope that he can deceive at least one of them into accepting as a genuine communication from the other either a fraudolent message created by the warden himself or else a modification by him of a genuine message".
In the context of a networked communication, "Alice and Bob exploit an already existing communication path, corresponding to two arbitrary communicating processes: the sender and the receiver. Wendy is a warden, located somewhere along the communication path, monitoring all possible messages exchanged by Alice and Bob"[14].
In the analyzed scenario the attacker represents both the sender process located in the inside network, and the receiver process, located outside. The warden is a firewall, or a router, which allows specific communications from the inside to the outside, regulated by the orga-

nization's security policy, standards, and procedures. The challenge for the attacker is to find a communication path, which is allowed in the specific traffic direction flow, and use it as a covert channel, in order to deceive the countermeasures in place to consider it as a legitimate traffic.

Policy: A formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area [9].
Standard: A mandatory action or rule designed to support and conform to a policy [9].
Procedure: Procedures describe the process: who does what, when they do it, and under what criteria [9].

2.2.2. Definitions

Covert Channel is a "communication paths that allow information transfer in violation of a system's security policies. In the context of network protocols, covert channel communication is generally achieved by manipulating an overt[10] communication"[14].

Cover traffic "is the traffic that is being manipulated by covert channel participants"[14].

Storage Covert Channel "manipulates a storage location in such a way that it conveys information to an observer. This definition was initially applied only to covert channels within a single machine or at least with a shared storage location. It was then extended to network covert channels and in this context, a storage channel is understood to be a channel that relies on modification of network traffic content"[14].

An **active warden** "is positioned so that it can observe and modify network traffic in its area of responsibility. The task of active wardens is to prevent and disrupt covert channel communication by modifying the content of network traffic"[14]

[9] http://www.slu.edu/its/policies-and-processes, accessed 1.4.2016
[10] "open to view or knowledge; not concealed or secret", http://www.dictionary.com/browse/overt, accessed 1.4.2016

2.2.3. Related Research

The aforementioned Lewandowski's research defines a communication model for network storage channels, which involves two parties who wish to communicate covertly. "As a cover, Alice and Bob might either select a suitable, already ongoing communication or generate an appropriate one if they can do so without arousing suspicion, and then they proceed to modify the cover communication's content to transmit their information. Meanwhile a third party, Wendy, positioned somewhere on the covert communication's path, attempts to disrupt Alice and Bob's efforts while preserving the integrity of the cover traffic".
The author extracted six scenarios (see Figure 1) from the model, based on the work of Lucena[15].

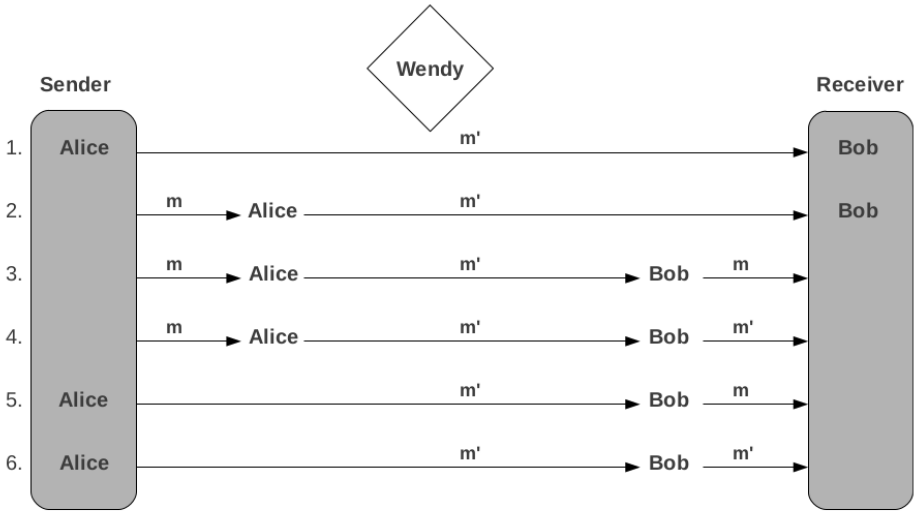

Figure 1. Communication Scenarios

The six scenarios depicts different positions of Bob and Alice in the communication model, and the way the cover traffic (m) is manipulated by the covert channel (m′).
The first scenario is the simplest one, it involves a communication between Bob and Alice, where Alice use directly the covert channel and insert the manipulated message, which is directed to Bob, the receiver. The remaining scenarios explores different combinations, depending on the behavior and identity of the sender, i.e. if Alice is the sender and introduces a manipulated message in the channel or Alice modifies an existing and legitimate one, or on the behavior and identity of the receiver, i.e. whether Bob is the receiver or, where he is not, if he restores or not the original message after reception.

"In these scenarios, Wendy always should be positioned between Alice and Bob so that she can monitor m′ traffic. Were she positioned differently, and were unable to see m′, her presence would be irrelevant to the covert communication".
For the scope of this research, it is assumed that the sender can control the covert channel and insert directly the manipulated message. This reduction in scope, with respect to Lewandowski's study, is justified by the limitation in time, and by the simplicity of the network topology used for the experiment, that will be highlighted later in next chapters. However, it is worth saying that for an exhaustive testing of ICMPv6, related to covert channels, there are interesting implications to analyze inside the other scenarios, like the ability to preserve the covert channel in situations where Alice must modify the original message of the sender, or Bob must restore the original message before forwarding it to the legitimate receiver.
This assumption, however, has some implications:
"Alice can modify the traffic to a greater degree, since Bob does not necessarily expect the traffic to be meaningful and perhaps not even valid. On the other hand, if Alice and Bob use their own traffic to provide cover, they run a greater risk of exposure as they are openly communicating".
Furthermore, in this research, it is assumed that both the sender and the receiver are the same subject.

Another topic to take into consideration, which relates to the behavior of the active warden, is the system and semantics preservation. The concepts have been applied first to preserve steganography [11][16], but "the definitions can be applied to covert channels as well"[14].

System Preservation "guarantees that the stegomessage is well formed within the rules of the protocol; the actual meaning of the stegomessage may be different than the original cover"[16]
Semantic Preservation "means that, as observed at a point along the message's path through the network, the stegomessage has the same meaning as the original cover"[16]

In the context of covert channels, "the property of syntax preservation determines whether the modified traffic m′ adheres to the protocol syntax. On the other hand, the property of

[11] "The art or practice of concealing a message, image, or file within another message, image, or file", http://www.merriam-webster.com/dictionary/steganography, accessed 24.3.2016

semantics preservation guarantees that the meaning of modified traffic m′ is the same as the original traffic m, or in other words that covert channel communication performed by Alice and Bob does not alter the meaning of cover traffic".

The above concepts acquire more relevance in a complex topology scheme, where an IPv6 packet must eventually traverse multiple wardens. Lewandowski's work defines the concept of "location-based syntax and semantics preservation", which is useful to differentiate between nodes, along the path, "performing distinct functions" and with "multiple levels of protocol knowledge and understanding". Each node, with a particular function in the network, may behave differently with respect to the packet in travel, and "as a result, a modified traffic's syntax or semantics might be deemed correct by an IPv6 node with limited protocol knowledge while at the same time be rejected by a more knowledgeable node".

This concepts will assume a particular relevance for this research when building the experiment. As it has been said before, it is important not only to understand the ICMPv6 protocol by itself, but also its relationship with devices like firewalls (the active warden) and the different configurations which produce different scenarios. Each configuration may lead to a different knowledge and understanding of the protocol by the node, which may affect the ability to preserve the covert channel, and must be taken into consideration. For example, an "interesting case is presented by protocol's reserved fields. Since their value is fixed (usually zeroed), and it is supposed to be ignored by the receiver, they do not carry any meaning and modifying such field does not alter packet's semantics. If the modification in question avoids changing packet's syntax as well, the reserved field is ideal for the purpose of embedding covert messages. And indeed, many network covert channel investigations focus on network protocol's reserved fields and find them useful for covert communication". Therefor, choosing a different configuration for the device, a firewall or router, may affect the level of knowledge of the protocol of that device, and the ability to preserve the covert channel. Or, in the other way, each scenario may produce different behaviors with the presence of a covert channel, and allow to assess a particular configuration and its ability to prevent it.

Indeed, "the objective of covert channel participants is to conduct their communication in such way that the necessary modifications of the cover traffic are always syntax and semantics preserving *with respect* to network nodes along the communication's path".

Analyzed RFCs

The following table (see 20) shows the list of protocols and associated RFC from Lewandowski's study that are in scope with this research.

Protocol	RFC
IPv6 [12]	RFC2460[1]
ICMPv6	RFC4443[3]
Neighbor Discovery (ND) for IPv6	RFC4861[7]

Table 20. Investigated Protocols

Properties of Covert Channels

Lewandowski's study proposed six properties of covert channels which are important for the investigation. In this research, given its scope, two of them have been considered:

- "degree of packet alteration – syntax- and semantics-preservation level of altered packets". Since each configuration can have different syntax- and semantics-preservation level, it is important to test each covert channel against each configuration, to assess both the warden configuration and the covert channel in this particular scenario.
- "channel bandwidth – amount of data that can be transfered in given covert channel per packet of cover traffic". This property does not affect the existence of the covert channel, but its ability to be preserved for a longer period. Depending on the bandwidth, a covert channel may be useful, from attacker perspective, only in situations with a low amount of data to be exfiltrated, or when it is possible to insert a delay in the transmission to avoid suspicion on the traffic.

Lewandowski observed that some of the considered protocols, Neighbor Discovering is an example of them, "are designed for operation on a single network segment. In consequence, any covert channel using these protocols as a cover will be similarly limited in its range", and that "the communication can be easily defeated by simple address-based filtering mechanism".
This research, even though the observation may be correct, will not consider its assumption. The reason is given, as stated before, by the fact that it is important to consider also the actual transition period, where the two protocol, IPv4 and IPv6, cohexist in many configurations.

[12] RFC2460 is only partially in scope with this research, but it is worth to mention it because in ICMPv6 specification there are frequently references to IPv6 fields, like source and destination addresses

This scenario implies that both networks are in place, but the active warden is configured to inspect only IPv4-related protocols, thus with a low level of syntax and semantics preservation knowledge, and any IPv6 packet will transit without deep inspection. For the same reason, an address-based filtering mechanism for IPv6 would probably not be in place. Another aspect, still related to the active warden, is the direction of the communication, from the inside to the outside: since it is considered a communication from a trusted to an untrusted network, the default configuration may allow the traffic without restrictions.

3. Methodology

4. Implementation

5. Experiment

6. Results

7. Conclusions

References

[1] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," Internet Requests for Comments, RFC Editor, RFC 2460, December 1998. [Online]. Available: http://www.rfc-editor.org/info/rfc2460

[2] P. Srisuresh and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)," Internet Requests for Comments, RFC Editor, RFC 3022, January 2001. [Online]. Available: http://www.rfc-editor.org/info/rfc3022

[3] A. Conta, S. Deering, and M. E. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," Internet Requests for Comments, RFC Editor, RFC 4443, March 2006. [Online]. Available: http://www.rfc-editor.org/info/rfc4443

[4] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," Internet Requests for Comments, RFC Editor, RFC 2119, March 1997. [Online]. Available: http://www.rfc-editor.org/info/rfc2119

[5] J. Postel, "Internet Control Message Protocol," Internet Requests for Comments, RFC Editor, RFC 792, September 1981. [Online]. Available: http://www.rfc-editor.org/info/rfc792

[6] M. Chakraborty, N. Chaki, and A. Cortesi, "A New Intrusion Prevention System for Protecting Smart Grids from ICMPv6 Vulnerabilities," *Conference: 2014 Federated Conference on Computer Science and Information Systems*, vol. 2, 2014.

[7] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," Internet Requests for Comments, RFC Editor, RFC 4861, September 2007. [Online]. Available: http://www.rfc-editor.org/info/rfc4861

[8] Fortinet, "Threats on the Horizon: The Rise of the Advanced Persistent Threat," *solution report, Fortinet Inc.*, 2013.

[9] G. D. SecurityLabs, "Uroburos: Highly complex espionage software with Russian roots," *tech. rep., G Data Software AG*, 2014.

[10] N. Falliere, L. O. Murchu, and E. Chien. (2011) W32.Stuxnet Dossier. Accessed: 21-03-2016. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[11] F. Rajpari, "Finding the Advanced Persistent Adversary," *SANS Institute*, 2014.

[12] S. Bradner, "The Internet Standards Process – Revision 3," Internet Requests for Comments, RFC Editor, RFC 2026, October 1996. [Online]. Available: http://www.rfc-editor.org/info/rfc2026

[13] J. G. Simmons, "The prisoners' problem and the subliminal channel," *Advances in Cryptology, Proceedings of CRYPTO '83, pages 51–67*, 1984.

[14] G. Lewandowski, "Network-aware Active Wardens in IPv6," *Electrical Engineering and Computer Science - Dissertations*, 2011.

[15] N. Lucena, "Application-level protocol steganography," *PhD thesis, Syracuse University*, 2008.

[16] N. Lucena, J. Pease, P. Yadollahpour, and S. J. Chapin, "Syntax and Semantics-Preserving Application-Layer Protocol Steganography," *Syracuse University*, 2004.

Appendix 1 - Protocol Headers

IPv6

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

Table 21. IPv6 Header

ICMPv6

RFC 4443

The following are the Protocol Headers described in RFC 4443.

Destination Unreachable

Type	Code	Checksum
Unused		
As much of invocking packet as possible without the ICMPv6 packet exceeding the minimum IPv6 MTU		

Table 22. Destination Unreachable

Packet Too Big

Type	Code	Checksum
MTU		
As much of invocking packet as possible without the ICMPv6 packet exceeding the minimum IPv6 MTU		

Table 23. Packet Too Big

Time Exceeded

Type	Code	Checksum
Unused		
As much of invocking packet as possible without the ICMPv6 packet exceeding the minimum IPv6 MTU		

Table 24. Time Exceeded

Parameter Problem

Type	Code	Checksum
Pointer		
As much of invocking packet as possible without the ICMPv6 packet exceeding the minimum IPv6 MTU		

Table 25. Parameter Problem

Echo Request

Type	Code	Checksum
Identifier		Sequence Number
Data		

Table 26. Echo Request

Echo Reply

Type	Code	Checksum
Identifier		Sequence Number
Data		

Table 27. Echo Reply

RFC 4861

Router Solicitation

Type	Code	Checksum
Identifier		Reserved
Options		

Table 28. Router Solicitation

Router Advertisement

Type	Code			Checksum
Cur Hop Limit	M	O	Reserved	Router Lifetime
Reachable Time				
Retrans Timer				
Options				

Table 29. Router Advertisement

Neighbor Solicitation

Neighbor Advertisement

Redirect

Source/Target link-layer Address

Type	Code	Checksum
Reserved		
Target Address		
Options		

Table 30. Neighbor Solicitation

Type			Code	Checksum
R	S	O	Reserved	
Target Address				
Options				

Table 31. Neighbor Advertisement

Type	Code	Checksum
Reserved		
Target Address		
Destination Address		
Options		

Table 32. Redirect

Type	Length	Link-layer Address

Table 33. Source/Target link-layer Address

Prefix Information

Type	Length	Prefix length	L	A	Reserved1
Valid Lifetime					
Preferred Lifetime					
Reserved2					
Prefix					

Table 34. Prefix Information

Redirect Header

Type	Length	Reserved
Reserved		
IP Header + Data		

Table 35. Redirect Header

MTU

Type	Length	Reserved
MTU		

Table 36. MTU

Appendix 2 - ICMPv6 specifications

Processing Rules	
Selected	Specification
	If an ICMPv6 error message of unknown type is received at its destination, it MUST be passed to the upper-layer process that originated the packet that caused the error, where this can be identified
	If an ICMPv6 informational message of unknown type is received, it MUST be silently discarded.
	Every ICMPv6 error message MUST include as much of the IPv6 offending (invoking) packet
	In cases where the internet-layer protocol is required to pass an ICMPv6 error message to the upper-layer process, the upper-layer protocol type is extracted from the original packet and used to select the appropriate upper-layer process to handle the error.
	An ICMPv6 error message MUST NOT be originated as a result of receiving the following: ▪ An ICMPv6 error message. ▪ An ICMPv6 redirect message. ▪ A packet destined to an IPv6 multicast address. (There are two exceptions to this rule: (1) the Packet Too Big Message to allow Path MTU discovery to work for IPv6 multicast, and (2) the Parameter Problem Message, Code 2 reporting an unrecognized IPv6 option that has the Option Type highest- order two bits set to 10). ▪ A packet sent as a link-layer multicast. ▪ A packet sent as a link-layer broadcast. ▪ A packet whose source address does not uniquely identify a single node.
	Finally, in order to limit the bandwidth and forwarding costs incurred by originating ICMPv6 error messages, an IPv6 node MUST limit the rate of ICMPv6 error messages it originates.

Table 37. RFC 4443 - Message Processing Rules

Destination Unreachable	
Selected	Specification
	Unused field: This field is unused for all code values. It MUST be initialized to zero by the originator and ignored by the receiver.
	A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion.
	One specific case in which a Destination Unreachable message is sent with a code 3 is in response to a packet received by a router from a point-to-point link, destined to an address within a subnet assigned to that same link (other than one of the receiving router's own addresses). In such a case, the packet MUST NOT be forwarded back onto the arrival link.
	A destination node SHOULD originate a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender.
	For security reasons, it is recommended that implementations SHOULD allow sending of ICMP destination unreachable messages to be disabled, preferably on a per-interface basis.
	A node receiving the ICMPv6 Destination Unreachable message MUST notify the upper-layer process if the relevant process can be identified

Table 38. RFC 4443 - Destination Unreachable

Packet Too Big	
Selected	Specification
	A Packet Too Big MUST be sent by a router in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link.
	An incoming Packet Too Big message MUST be passed to the upper-layer process if the relevant process can be identified.

Table 39. RFC 4443 - Packet Too Big

Time Exceeded	
Selected	Specification
	If a router receives a packet with a Hop Limit of zero, or if a router decrements a packet's Hop Limit to zero, it MUST discard the packet and originate an ICMPv6 Time Exceeded message with Code 0 to the source of the packet.
	An incoming Time Exceeded message MUST be passed to the upper-layer process if the relevant process can be identified.

Table 40. RFC 4443 - Time Exceeded

Parameter Problem	
Selected	Specification
	If an IPv6 node processing a packet finds a problem with a field in the IPv6 header or extension headers such that it cannot complete processing the packet, it MUST discard the packet and SHOULD originate an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem.
	A node receiving this ICMPv6 message MUST notify the upper-layer process if the relevant process can be identified.

Table 41. RFC 4443 - Parameter Problem

Echo Request	
Selected	Specification
	Every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and originates corresponding Echo Replies. A node SHOULD also implement an application-layer interface for originating Echo Requests and receiving Echo Replies, for diagnostic purposes.
	Echo Request messages MAY be passed to processes receiving ICMP messages.

Table 42. RFC 4443 - Echo Request

Echo Reply	
Selected	Specification
	The source address of an Echo Reply sent in response to a unicast Echo Request message MUST be the same as the destination address of that Echo Request message.
	An Echo Reply SHOULD be sent in response to an Echo Request message sent to an IPv6 multicast or anycast address. In this case, the source address of the reply MUST be a unicast address belonging to the interface on which the Echo Request message was received.
	The data received in the ICMPv6 Echo Request message MUST be returned entirely and unmodified in the ICMPv6 Echo Reply message.
	Echo Reply messages MUST be passed to the process that originated an Echo Request message.
	An Echo Reply message MAY be passed to processes that did not originate the Echo Request message.
	Note that there is no limitation on the amount of data that can be put in Echo Request and Echo Reply Messages.

Table 43. RFC 4443 - Echo Reply

Router Solicitation	
Selected	Specification
	Hosts MUST silently discard any received Router Solicitation Messages.
	A router MUST silently discard any received Router Solicitation messages that do not satisfy all of the following validity checks: ■ The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router. ■ ICMP Checksum is valid. ■ ICMP Code is 0. ■ ICMP length (derived from the IP length) is 8 or more octets. ■ All included options have a length that is greater than zero. ■ If the IP source address is the unspecified address, there is no source link-layer address option in the message.
	The contents of the Reserved field, and of any unrecognized options, MUST be ignored.
	The contents of any defined options that are not specified to be used with Router Solicitation messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Source Link-Layer Address option.

Table 44. RFC 4861 - Validation of Router Solicitation

Router Advertisement	
Selected	Specification
	A router MUST silently discard any received Router Advertisement messages that do not satisfy all of the following validity checks: ■ IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers. ■ The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router. ■ ICMP Checksum is valid. ■ ICMP Code is 0. ■ ICMP length (derived from the IP length) is 16 or more octets. ■ All included options have a length that is greater than zero.
	The contents of the Reserved field, and of any unrecognized options, MUST be ignored.
	The contents of any defined options that are not specified to be used with Router Advertisement messages MUST be ignored and the packet processed as normal. The only defined options that may appear are the Source Link-Layer Address, Prefix Information and MTU options.
	A host MUST NOT send Router Advertisement messages at any time.

Table 45. RFC 4861 - Validation of Router Advertisement

Neighbor Solicitation	
Selected	Specification
	A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks: ■ The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router. ■ ICMP Checksum is valid. ■ ICMP Code is 0. ■ ICMP length (derived from the IP length) is 24 or more octets. ■ Target Address is not a multicast address. ■ All included options have a length that is greater than zero. ■ If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address. ■ If the IP source address is the unspecified address, there is no source link-layer address option in the message.
	The contents of the Reserved field, and of any unrecognized options, MUST be ignored.
	The contents of any defined options that are not specified to be used with Neighbor Solicitation messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Source Link-Layer Address option.

Table 46. RFC 4861 - Validation of Neighbor Solicitation

Neighbor Solicitation - Sending	
Selected	Specification
	If the source address of the packet prompting the solicitation is the same as one of the addresses assigned to the outgoing interface, that address SHOULD be placed in the IP Source Address of the outgoing solicitation.
	If the solicitation is being sent to a solicited-node multicast address, the sender MUST include its link-layer address (if it has one) as a Source Link-Layer Address option.
	Otherwise, the sender SHOULD include its link-layer address (if it has one) as a Source Link-Layer Address option.
	On unicast solicitations, an implementation MAY omit the Source Link-Layer Address option.

Table 47. RFC 4861 - Sending Neighbor Solicitation

Neighbor Solicitation - Reception	
Selected	Specification
	A valid Neighbor Solicitation that does not meet any of the following requirements MUST be silently discarded: ▪ The Target Address is a "valid" unicast or anycast address assigned to the receiving interface. ▪ The Target Address is a unicast or anycast address for which the node is offering proxy service. ▪ The Target Address is a "tentative" address on which Duplicate Address Detection is being performed.
	If the Source Address is not the unspecified address and, on link layers that have addresses, the solicitation includes a Source Link-Layer Address option, then the recipient SHOULD create or update the Neighbor Cache entry for the IP Source Address of the solicitation.
	If the Source Address is the unspecified address, the node MUST NOT create or update the Neighbor Cache entry.

Table 48. RFC 4861 - Reception of Neighbor Solicitation

Neighbor Advertisement	
Selected	Specification
	A node MUST silently discard any received Neighbor Advertisement messages that do not satisfy all of the following validity checks: ■ The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router. ■ ICMP Checksum is valid. ■ ICMP Code is 0. ■ ICMP length (derived from the IP length) is 24 or more octets. ■ Target Address is not a multicast address. ■ If the IP Destination Address is a multicast address the Solicited flag is zero. ■ All included options have a length that is greater than zero.
	The contents of the Reserved field, and of any unrecognized options, MUST be ignored.
	The contents of any defined options that are not specified to be used with Neighbor Advertisement messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Target Link-Layer Address option.

Table 49. RFC 4861 - Validation of Neighbor Advertisement

Sending Solicited Neighbor Advertisement	
Selected	Specification
	If the solicitation's IP Destination Address is not a multicast address, the Target Link-Layer Address option MAY be omitted.
	If the solicitation's IP Destination Address is a multicast address, the Target Link-Layer option MUST be included in the advertisement.
	if the node is a router, it MUST set the Router flag to one; otherwise, it MUST set the flag to zero.
	If the Target Address is either an anycast address or a unicast address for which the node is providing proxy service, or the Target Link-Layer Address option is not included, the Override flag SHOULD be set to zero. Otherwise, the Override flag SHOULD be set to one.
	If the source of the solicitation is the unspecified address, the node MUST set the Solicited flag to zero and multicast the advertisement to the all-nodes address. Otherwise, the node MUST set the Solicited flag to one and unicast the advertisement to the Source Address of the solicitation.

Table 50. RFC 4861 - Solicited Neighbor Advertisement

Receipt of Neighbor Advertisement	
Selected	Specification
	When a valid Neighbor Advertisement is received (either solicited or unsolicited), the Neighbor Cache is searched for the target's entry. If no entry exists, the advertisement SHOULD be silently discarded.

Table 51. RFC 4861 - Receipt of Neighbor Advertisement

Redirect	
Selected	Specification
	A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks: ■ IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers. ■ The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router. ■ ICMP Checksum is valid. ■ ICMP Code is 0. ■ ICMP length (derived from the IP length) is 40 or more octets. ■ The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address. ■ The ICMP Destination Address field in the redirect message does not contain a multicast address. ■ The ICMP Target Address is either a link-local address (when redirected to a router) or the same as the ICMP Destination Address (when redirected to the on-link destination). ■ All included options have a length that is greater than zero.
	The contents of the Reserved field, and of any unrecognized options, MUST be ignored.
	The contents of any defined options that are not specified to be used with Redirect messages MUST be ignored and the packet processed as normal. The only defined options that may appear are the Target Link-Layer Address option and the Redirected Header option.
	A host MUST NOT consider a redirect invalid just because the Target Address of the redirect is not covered under one of the link's prefixes.

Table 52. RFC 4861 - Validation of Redirect

Redirect - Router and Host Specifications	
Selected	Specification
	A router MUST NOT update its routing tables upon receipt of a Redirect.
	A host receiving a valid redirect SHOULD update its Destination Cache accordingly so that subsequent traffic goes to the specified target.
	If no Destination Cache entry exists for the destination, an implementation SHOULD create such an entry.
	If the Target and Destination Addresses are the same, the host MUST treat the Target as on-link.
	If the Target Address is not the same as the Destination Address, the host MUST set IsRouter to TRUE for the target.
	A host MUST NOT send Redirect messages.

Table 53. RFC 4861 - Redirect, specifications

Options Processing	
Selected	Specification
	In order to ensure that future extensions properly coexist with current implementations, all nodes MUST silently ignore any options they do not recognize in received ND packets and continue processing the packet.
	All options specified in this document MUST be recognized.
	A node MUST NOT ignore valid options just because the ND message contains unrecognized ones.
	The option MUST NOT depend on the presence or absence of any other options.
	Options in Neighbor Discovery packets can appear in any order; receivers MUST be prepared to process them independently of their order.
	The amount of data to include in the Redirected Header option MUST be limited so that the entire redirect packet does not exceed the minimum MTU required to support IPv6.
	The size of an ND packet including the IP header is limited to the link MTU. When adding options to an ND packet, a node MUST NOT exceed the link MTU.

Table 54. RFC 4861 - Options