Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

Covert Channels in IPv6

Dr.Dhananjay M. Dakhane[1], Akash P. Bhad[2]

[1]Computer Science, Sipna C.O.E.T. Amravati
[2]Computer Science ,Sipna C.O.E.T. Amravati

Abstract-*Covert channels are communication mechanisms that were never intended nor designed to carry information. As such, they are often able to act "below" the notice of mechanisms designed to enforce security policies. Therefore, using covert channels it might be possible to establish a covert communication that escapes notice of the enforcement mechanism in place. Any covertchannel present in digital communications offers a possibility of achieving a secret, and therefore unmonitored, communication. One of the most ubiquitous protocols in deployment is the Internet Protocol version 4 (IPv4). Its universal presence and range make it an ideal candidate for covert channel investigation.This imminent exhaustion of IPv4 address space will soon force a mass migration towards Internet Protocol version 6 (IPv6) expressly designed as its successor. While the protocol itself is already over a decade old, its adoption is still in its infancy.An active warden is there so that it can observe and modify network traffic in its area of responsibility. And active wardens performs the task to prevent and disrupt covert channel communication by modifying the content of network traffic. As much as possible an active warden should maintain the syntactic and semantic integrity of the modified traffic to avoid breaking the cover communication.*

Keywords-*Covert channel, Covert Channel, Active warden, Storage covert channel,Timing covert channel*

I. INTRODUCTION

Keeping in mind, it is not surprising that many communication channels are subject to policies imposing restrictions on the flow of information in the channels. We can divide existing communicationchannels into two broad categories: overt communication channels and covertcommunication channels. Overt channels are acknowledged communicationmethods that are widely known, and if intended to carry sensitive information, they are subject to communication policies. Obviously, in order to make the policies effective, all communications channels should be overt.

Security policies governing information flow in overt channels will be unaware of the existence of covert channels and the information flow therein will go not only unrestricted but entirely unnoticed. If that is the case, covert channels are able to deliver what cryptography cannot, that is they allow one to send "invisible" messages where not only message content is secret, but the very fact that the message exists is hidden.

The covert channels allow sending hidden messages within a single computer, covert channels exist in computer networks as well and they provide the ability to secretly communicate between remote computers in network.Network covert channelsmanipulate network protocols themselves.

Since network protocols are expressly designed for communication, the network covertChannels operate by making a distinction between protocol's control messages and its payload, and by exploiting the fact that it is generally only the payload that is the subject of security checks.Various studies have found multiple covert channels existing in a variety of network protocol. Currently, one of the most ubiquitous protocols in deployment is the Internet Protocol version 4 (IPv4). Its universal presence and global range make it an ideal candidate for covert channel exploits. And now, IPv4 is approaching the end of its dominance as its address space nears exhaustion that will soon force a mass migration towards Internet Protocol version 6 (IPv6), expressly designed as its successor. Therefore, we turn our attention to networkcovert channels present in IPv6 protocol. However, covert channels are a definite security risk, by the virtue of allowing an undetected (and therefore unmonitored) communication.

II. DEFINITIONS

2.1. Covert channel:

Covert channels were first proposed by Lampson in the context of the confinement problem as communication channels that are neither designed nor intended to carry information. The definition was later expanded to include all 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 communication.

2.2. Cover traffic:

Cover traffic is the traffic that is being manipulated by covertchannel participants. It might originate from one of the participants but it is also possible to “hijack" a 3rd party communication for the purpose of covert communication.

2.3. Storage covert channel:

A 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.

2.4Timing covert channel:

A timing covert channel is a signaling mechanism based on influencing system response times. Again, the definition wasinitially created to describe an intra-machine channels and subsequentlyextended to network convert channels. Network timing covert channelsrely on modifying timing of network messages to convey information.

2.5Active warden:

An active warden is positioned so that it can observe and modify network traffic in its area of responsibility. The task of activewardens is to prevent and disrupt covert channel communication bymodifying the content of network traffic. As much as possible a wardenshould maintain the syntactic and semantic integrity of the modified traffic to avoid breaking the cover communication.

III. COVERT CHANNELS IN IPv6

3.1.IPv6 Header:

The field wise plausible covert channels:

- Traffic class: Here the traffic class bit can set false it can work bandwidth of 8bit/packet[5].
- Flow label: In this also this bit is set false and bandwidth here is 20bit/packet.
- Payload length: Some modification is done with this values that is the value is increased to insert more data and the bandwidth varies as the value.
- Next Header: Valid value is modified to add an extra extension header.
- Hop value: this value is increased or decreased, with the bandwidth of approximate 1bit/packet.
- Source: False source address is set and bandwidth is 16bytes/packet.

3.2. Hop-by-Hop Options Header:

This extension header has high bandwidth covert channels, because of its different type, defined and undefined and its variable length.

Next Header (1 byte)	***Extension Header Length (1 byte)***	***Option Type (1 byte)***	***Option Data Length (1 byte)***	***Option Data***

Figure: Format of Hop-by-Hop Header.

1.3. Routing Header:

It contains a list of intermediate nodes a packet in transit should visit on the way to itsdestination. In this the reserved bytes are altered with bandwidth of 4 byte/packet by hiding data in it and the addresses are setfalse.

Next Header (1 byte)	***Header Extension Length (1 byte)***	***Routing Type=0 (1 byte)***	***Segment Left (1 byte)***
Reserved (4 byte)			
Addresses (16 byte each)			

Figure: Format of Routing Header

.

1.4. Fragment Header:

Routers along the path does not fragmented the packets in IPv6 , rather the sending nodesuse path MTU discovery to determine the allowed maximum packet size on the way to a specific destination and fragment packets as needed.One can refragment a packet solely toincrease the bandwidth of existing covert channelthat does not involve thefragment header.

1.5. Destination Options Header

The Destination Options header carries optional information relevant to the destinationnodes. As theoptions of both options headers, hop-by-hop and destination,follow the same format, the covert channels identified are similar to thoseshown in Figure. The option data is padded with false padding value and type of optionis fabricated on or more option.

Next Header (1 byte)	***Extension Header Length (1 byte)***	***Option Type (1 byte)***	***Option Data Length (1 byte)***	***Option Data***

Figure: Destination Option Header

1.6. Authentication Header:

It gives connectionless integrity and data origin authentication of individual IP packets, by calculating an integrity check value (ICV) per packet based on particular fields from other extension headers and from theIPv6 header as well. In this communication is covert by either hiding the data in unused field or using fake header.

Next Header (1 byte)	***Payload Length (1 byte)***	***Reserved (2 byte)***
Security Parameters Index (SPI) (4 byte)		
Sequence Number Field (4 byte)		
Authentication Data (Variable Length)		

Figure: Format For Authentication Header

1.7. Encapsulating Security Payload Header:
The Encapsulating Security Payload (ESP) Header provides confidentiality for all data transmitted end-to-end in IP packets.in this thefalse padding value is set or entire header is inserted fake.

1.8. Mobility Header:
Mobility header is required for mobility support in IPv6 and is defined by RFC 3775 [2]. It is used to carry messages and special mobility options. Mobility Header contains Reserved field, and additionally, different mobility messages and mobility options that it can carry, have their own reserved fields. They can be used by Alice in the same way as other similar fields inother headers.

1.9. ICMPv6 Header:
The structure of an ICMPv6 message is defined by RFC 4443 [3]. And it is an IPv6 equivalent of ICMP. It performs similar error reporting, diagnostic and discovery functions and uses similarly formatted messages, with a number of changes. Code field can be altered for the purpose of covert communication, it provides the potential bandwidth of 8 bit/packet. Also one can abuse ICMPv6 checksum to carry covert data.

1.10. Destination Unreachable Message:
When a packet encounters that cannot be delivered to its destination address for reasons other than congestion, Destination Unreachable ICMPv6 message is generated by a node or by IPv6network stack. It contains a 4 byte long unused field. An attacker can insert data into the field achieving covert transmission bandwidth of 32 bits per packet.

1.11. Packet Too Big Message:
The Code field of Packet Too Big message is not used by the sender and it is supposed to be ignored by the receiver which is the behavior identical to any reserved field. So, one can inject her covert message into the field, resulting in a bandwidth of 8 bits per packet.

1.12. Time Exceeded Message :
Router, when encounters that a packet is with hop limit field equal 0 or by a node when a packet re-assembly time is exceeded it send a Time Exceeded Message. Time Exceeded message contains an unused field of 4 bytes. This field is used to send covert messages.

1.13. Parameter Problem Message:
Parameter Problem Message is sent when an IPv6 node finds a problem within packet's IPv6 header or extension headers and the problem prevents it from completing the packet's processing. It contains an offset pointing to the detected error and as much of the defective packet as possible. And this 32 bit pointer field can be manipulated to carry covert data.

1.14. Echo Request Message:
Every IPv6 node is required to implement Echo Request message, as it is a part of diagnostic ping mechanism. Code is field is always 0,and its body carries Identifier and Sequence Number fields, as well as arbitrary data. The code field can overwrite and transmit 8 bits per packet. The body of Echo Request message carries arbitrary data and it one of the most widely recognized covert channels.

1.15. Echo Reply Message:
All covert channels are exact equivalents as the Echo Reply message is a mirror of the invoking Echo Requestmessage, codefield of Echo Reply message is supposed to be set to zero. And can overwrite the field and transmit 8 bits per packet.

1.16. Router Renumbering for IPv6:
A mechanism for reconfiguring multiple routers simultaneously is defined by Router Renumbering for IPv6 protocol, including environments where the number of routers is unknown. SegmentNumber field is intended to help differentiate between severalRouter Renumbering messages in the same manner SequenceNumber. Sincethe SegmentNumber value does

not imply any ordering, and since manyRouter Renumbering message are likely to have only one segment, one caneasily alter the value without affecting the cover messages.SegmentNumber field is 1-byte wide offering a bandwidth of 1 byte perpacket.

1.17. Router Renumbering Command Message:
Along with header Router Renumbering Command Message includes body, consists of zero or more Prefix Control Operation (PCO) stations, with different length. Even though there exist covert channel in Router Renumbering PCO station they are not listed here as they only appear in command message which are required to be protect by IPsec [1].

1.18. Router Renumbering Report Message:
Report Messages are likely easier targets for covert communicationas the specification does not require that they are protected by IPsec andmoreover, they do not have any effect on the network operations. 14 bit Reserved field as other similar fields in other headers. Present in Router Renumbering MatchReport section offers the same covert communication possibilities.

1.19. Mobility Support in IPv6:
RFC 3775 [2] describes mobility support in IPv6 protocol. The support allows an IPv6 node to remain reachable at its home address despite changing its location within the network. While the mobile node resides in its new location, traffic addressed to the node's home address is transparently routed to the new address. Additionally the new address can be registered with the node's correspondents to allow direct communication with the mobile node bypassing the home address [1].

1.20. Home Agent Address Discovery Request Message:
In case when need to discover the address (or addresses) of available Home Agents, Home Agent Address Discovery Request message is sent by the mobile node.

Type *(1 byte)*	***Code*** *(1 byte)*	***Checksum*** *(2 byte)*
Identifier *(2 byte)*		***Reserved*** *(2 byte)*

Figure: Home Agent Address Discovery Request Format.

Code field can be overwritten to transmit 8 bits of covert information. The Reserved field is initialized to zero and is supposed to be ignored by the receiver. It can be used to transmit 8 bits of covert information.

1.21. Home Agent Address Discovery Reply Message:
In response to a received Home Agent Address Discovery Request the Home Agent Address Discovery Reply Message is sent. Addresses field is used to transmit covert information. If thefield contains only one address, then it should not overwritten, as this would block the Home Agent discovery. In such case, append an extra “address" and fill it with her data as well as adjust payload length in IPv6 header.

1.22. Mobile IPv6 Fast Handovers:
RFC 5568 [4] addresses the problem of high \handover latency" resulting from standard Mobile IPv6 operations. It obsoletes and amends older RFC 5268 redefining two of its ICMPv6 messages as Mobility Header messages. As a result, there are no new ICMPv6 covert channels in Fash Handovers Protocol [1].

IV. COUNTERMEASURES

Basically, countermeasures deployed against covert channel communications will result in a complete disruption of covert communication, but it is also possible that only a partial success is achieved. Their effect on specific covert channels is classified as follows [1]:

Channel defeated Covert communication using this channel is impossible, As a result of active warden's actions.
Channel partially defeated It willaffect on some covert channel communications, but not all. Typically a blind attacker will be defeated, while more aware adversaries will be able still succeed in their communication attempts, even though the adjustment will usually result in lowering the available covert channel bandwidth.

4.1.Specification-based Countermeasures:
For a reference used in a covert channel defense the protocol specification is the most obvious choice. Packet scrubbers, traffic normalizers as well as active wardens use methods that are based on the specification.

.4.2.Network-aware Active Warden
Specification-based active wardens that perform according to the rules described in [1] are able to defeat many of the covert channels. Knowledge of the protocol specification allows Active Warden to simulate end-point semantics and then use the simulation to normalize the traffic.The wardens equipped with the new ability will still perform according to similar rules as before. First they will try to establish correct values of protocol fields and enforce the established values. If that is not possible, then they will check whether observed values are clearly incorrect. And then the Packets, headers or options carrying incorrect data will be dropped.

1.23. Network Manipulation
A network-aware active warden can also attempt to manipulate the network itself to assist withDefeating covert channel communications. Two suchmanipulations are:

4.3.1. Multiple equivalent traffic classes
4.3.2. Variable routing:

V. CONCLUSION

It is possible, by the fact that the correct values of IPv6 protocol fields are not always known and contain certain amount of entropy, to attack. The attacker can take advantage of consistingentropy and the protocol field will altered with the foreign data to carry covert communication.The paper describe covert channel to hide information in the IPv6. We have introduced the idea and communication model of covert channels and explained the different application countermeasures used toeliminate, or limit the capacity of covert channels. Some proposed countermeasures could significantly reduce overt channel performance and therefore their applicability in real high-speed networks is questionable. There are a number of directions for further research. At present a complete organization for classifying the different covert channels and countermeasures is missing. Covert channels by now have been used just to leak sensitive information, such as secret keys and passwords. Recently, however an idea of using covert channels to protect the data.A number of directions are left for further study. We must have focused on capacity estimation. Because of capacity estimation include formal methods and channel errors to identify covert channels during protocol design. Finally, it seems likely that the arms race of developing new covert channels with improved stealth and capacity, and developing more effective detection and elimination techniques will continue.

REFERENCES

[1] Grzegorz Lewandowski, Syracuse University, Network-aware Active Wardens in IPv6, 2011.

[2] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6.Retrieved on December 31, 2010 from the World Wide Web: http://www.ietf.org/rfc/rfc3775.txt, June 2004.RFC 3775.

[3] A. Conta, S. Deering, and M. Gupta. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. Retrieved on December 31, 2010 from the World Wide Web: http://www.ietf.org/rfc/rfc4443.txt, March 2006. RFC 4443.

[4] R. Koodli. Mobile IPv6 Fast Handovers.Retrieved on December 31, 2010 from the World Wide Web: http://www.ietf.org/rfc/rfc5568.txt, July 2009.RFC 5568.

[5] K. Nichols, S. Blake, F. Baker, and D. Black.Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.Retrieved on December 31, 2010 from the World Wide Web: http://www.ietf.org/rfc/rfc2474.txt, December 1998.RFC 2474.

