

Vulnerabilities in IPv6

Project ID: 6778

**Students: Jamal Tannous
Salah Kadry**

Supervisor: Mordechai Hagiz

Networked Software Systems Lab

Electrical Engineering | Technion



Technion
Israel Institute of Technology



THE ANDREW & ERNA VITERBI
**FACULTY OF
ELECTRICAL
ENGINEERING**

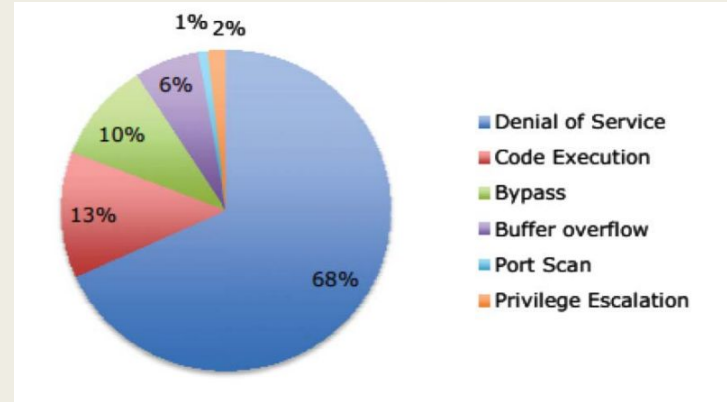
Background

- **IPv6 - Internet Protocol version 6; is the most recent version of the Internet Protocol.**
- **It's widely regarded as the most promising solution to the lack of sufficient IPv4 addresses in the world, and is intended to replace IPv4.**

Emerging Problems

As in all new inventions and protocols:


- **Unforeseen scenarios pop up.**
- **Security issues.**
- **New features might be a gateway to vulnerabilities.**



Project Goals

Our project would have these main goals:

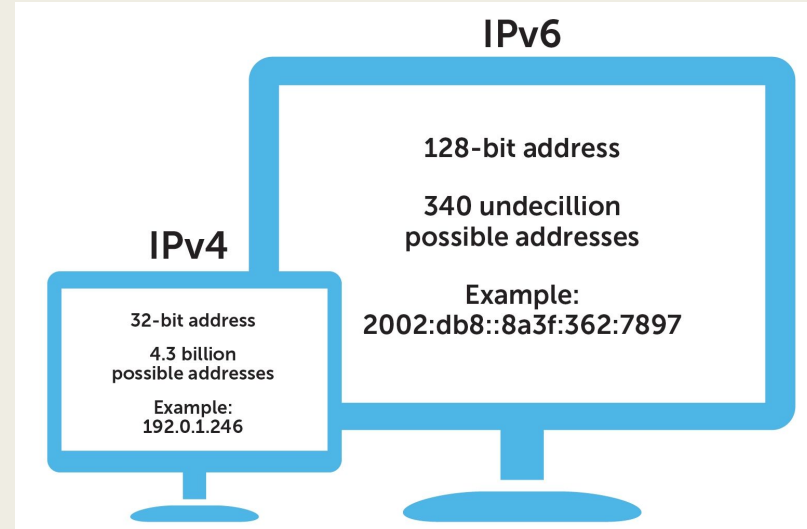
- **Learn and research about IPv6 and its features.**
- **Research and deduce some vulnerabilities in this protocol.**
- **Simulate attack that exploit those vulnerabilities and propose mitigation techniques against them.**

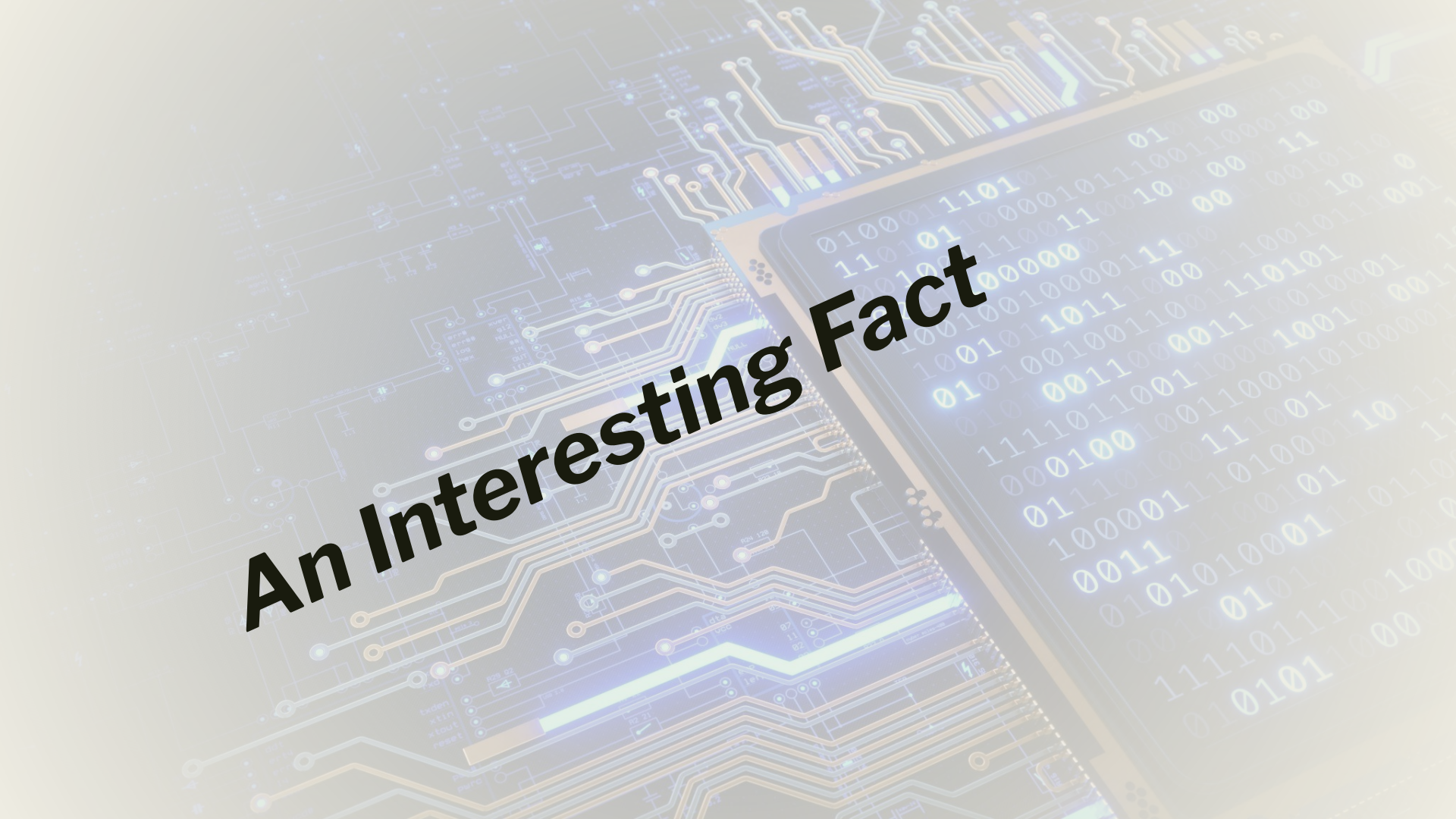


Project's Challenges

Project's Challenges

- The project deals with an enormous field, that is still under development and far from being optimal.
- IPv6 is harder and more complex than IPv4.
 - Harder to find “good quality” studies and explanations regarding it (compared to IPv4).
- Harder to simulate attacks that target some of its vulnerabilities (is not supported on Mininet yet).

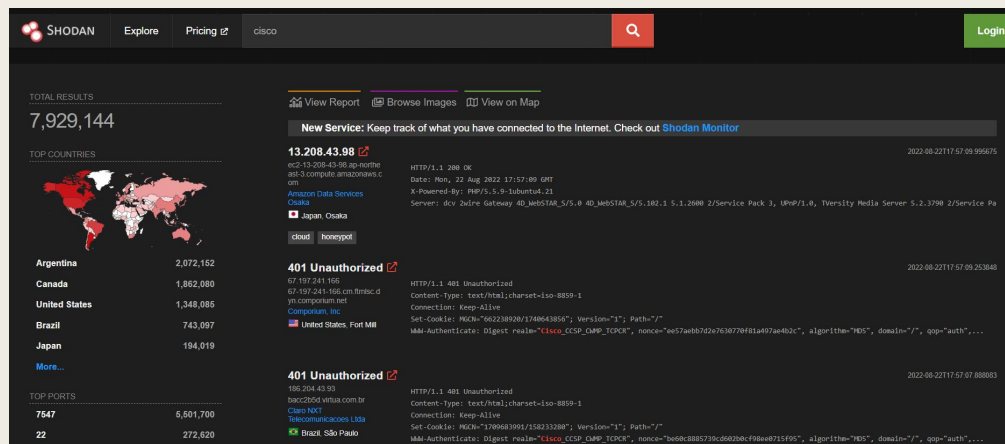


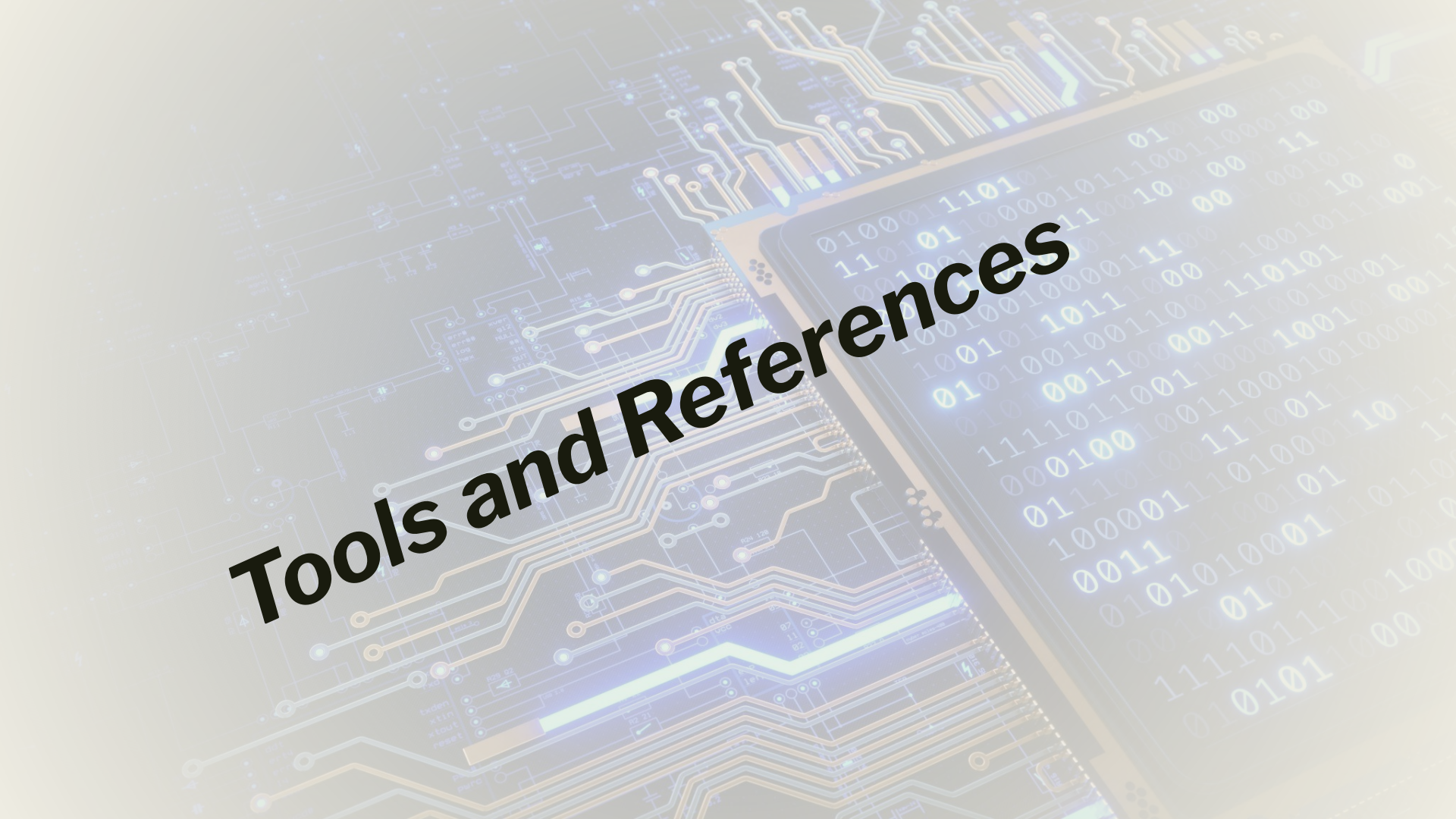


An Interesting Fact

An Interesting Fact

shodan.io has been crawling IPv6 for several years but until now it wasn't possible to search for specific IPv6 network ranges.





Tools and References

Tools and References

- Scapy (Simulating mitm6 and TCP-Syn Flood).
- THC (Researching some vulnerabilities).
- IPvSeeYou (Attack that targets CPE routers).
- C++ (Simulating Copycat attack on RPL).

IDEs and Tools

Scapy

- **Scapy** is a powerful and flexible packet manipulation tool in Python.
- It allows you to capture, analyze, and manipulate network packets, making it a popular tool for network security and testing.
- Scapy is widely used by security professionals, system administrators, and network engineers for various purposes such as network analysis, penetration testing, and protocol development.

IDEs and Tools

Scapy

We used Scapy to perform two attacks

- MITM.
- TCP Syn Flood.

These attacks were performed using Kali Linux based virtual machines, as one of the machines was the attacker and the others were the victims.

IDEs and Tools

THC

A group of international hackers which does IT security work that is publicly accessible.

THC also publishes tools to enhance the IT security movement.

In our project we specifically used THC's IPv6 attack toolkit.

IDEs and Tools

THC

A group of international hackers which does IT security work that is publicly accessible.

In our project we specifically used THC's IPv6 attack toolkit.

A variety of IPv6 attacks, some examples:

- “too_big6”: an attack through which the attacker manages to decrease the MTU in the network.



Some Attack and Simulations

Some Attacks and Simulations

We will discuss four attacks:

- TCP Syn-Flood (over IPv6).
- IPvSeeYou: Exploiting Leaked Identifiers in IPv6 for Street-Level Geolocation.
- MITM with Spoofed ICMPv6 Router Advertisement.
- Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Some Attack and Simulations

TCP Syn-Flood (over IPv6)

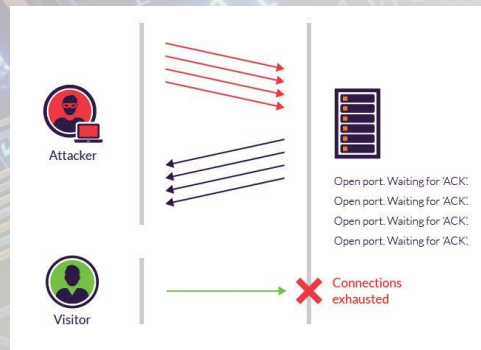
Some Attacks and Simulations

TCP Syn-Flood

A classic DoS/DDoS attack.

Exploits a weakness specifically in TCP protocol.

Consumes resources on the targeted server and rendering it unresponsive through exploiting the three-way handshake process of the protocol.



Some Attacks and Simulations

TCP Syn-Flood

The attack is as follows:

- 1) Attacker sends repeatedly SYN packets to every port on the targeted server (victim).
- 2) Server receives these requests, and replies with a SYN-ACK.

Some Attacks and Simulations

TCP Syn-Flood

- 3) Attacker ignores the server's SYN-ACK.
- 4) Server should keep the connection alive for a certain timeout.
- 5) While the server waits for the timeout, the attacker sends another SYN request on the same port, keeping the connection “half-open”.

Some Attacks and Simulations

TCP Syn-Flood

But where does IPv6 come into play?

For now, we've spoken about an attack that targets TCP. In other words, the attacker does not care whether the server is using TCP over IPv4 or IPv6.

But we found a very interesting encounter on [Linux Mint forum](#) stating scenarios with both IPV4/IPV6 TCP SYN Flood traffic using network simulation tools towards targets which have SYN Cookie enabled.

The results were as follows:

Observed legitimate users able to access the target properly when there is IPv4 TCP SYN Flood attack from random sources.

But when it comes to IPv6, the server was unreachable from legitimate users and its CPU was high while there is IPv6 a TCP SYN Flood attack.

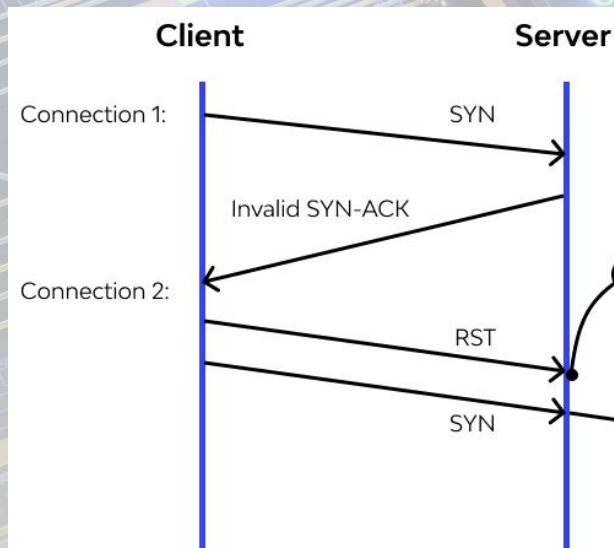
This issue was for Linux Kernel version 4.19.81, and very recent, namely April 2022.

Some Attacks and Simulations

RST Cookies

There are several techniques for mitigating this attack, we will discuss **RST Cookies**.

This technique is very simple yet very effective.



Some Attacks and Simulations

TCP Syn-Flood

Simulation:

We simulated the attack with TCP SYN-Cookies disabled (another mitigation technique which we discussed in the final report).

Here is the link to our simulation with TCP Synflood while Syn_Cookies are off: [Video](#)

Some Attack and Simulations

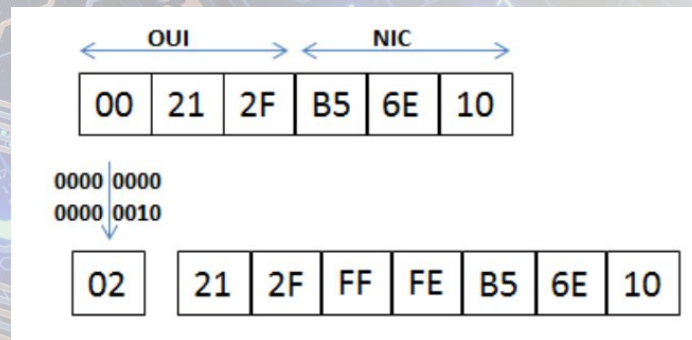
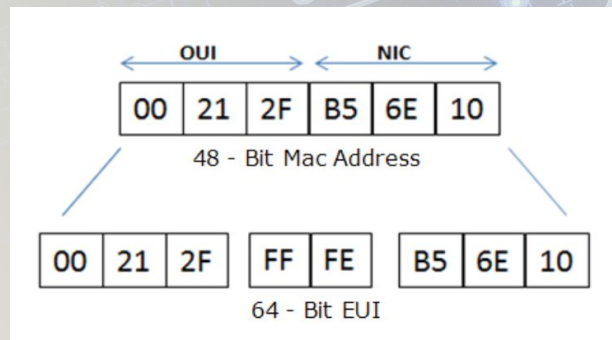
IPvSeeYou: Exploiting Leaked Identifiers in IPv6 for Street-Level Geolocation

Some Attacks and Simulations

IPvSeeYou

An attack that targets residential low cost routers that are deployed widely.

These routers use a form of legacy IPv6 addressing (IPv6 EUI-64 Bit Address).



Some Attacks and Simulations

IPvSeeYou

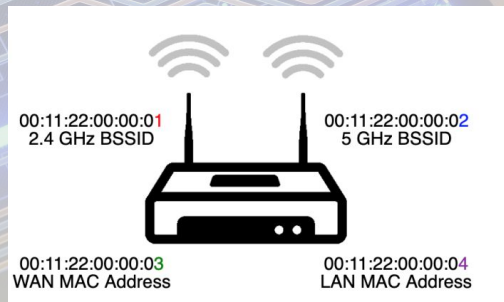
Mapping WAN MAC to WiFi BSSID

Most of the cheap customer premise equipment (CPE) routers are all-in-one CPE devices, e.g. cable modem with built-in WiFi.

Each interface gets its own MAC address.

These MAC addresses are normally related in these devices, for example, +/- 1.

This fact would prove to be of great significance to the attack which we will discuss.

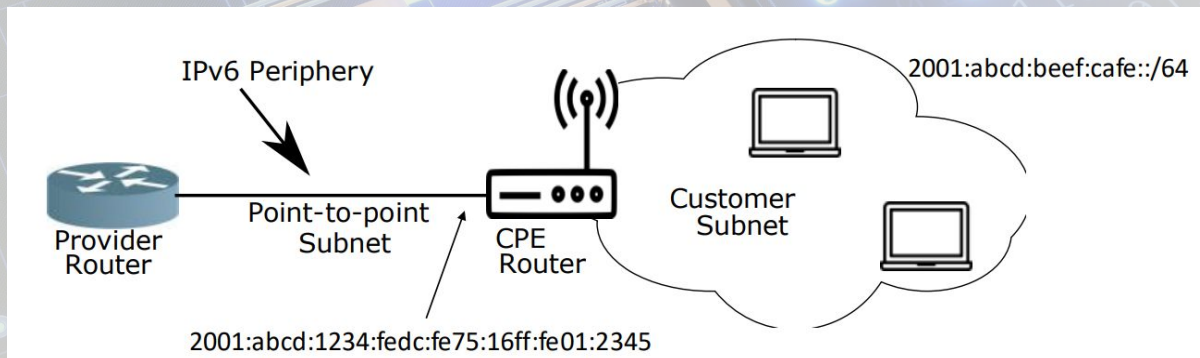


Some Attacks and Simulations

IPvSeeYou

The IPvSeeYou attack

Combines EU-I64 addresses with WiFi geolocation data.



Some Attacks and Simulations

IPvSeeYou

The IPvSeeYou attack

In order to implement the attack, a corpus of about 60 million EUI-64 derived WAN addresses was assembled, through active probing of random IPv6 addresses.

The attack amassed a corpus of about 450 million BSSID-geolocation pairs (using WiFi geolocation services).

Some Attacks and Simulations

IPvSeeYou

The IPvSeeYou attack

And thus the attack can be done as follows:


- 1) Traceroute6 to a random IPv6 address and hope that an “ICMPv6 time exceeded message”, and hopefully this CPE router will have an EUI-64 address.
- 2) Lookup the CPE router using IPvSeeYou tool which matches the EUI-64 address to a possible BSSID and searches for this BSSID's geolocation.

Some Attacks and Simulations

IPvSeeYou

The IPvSeeYou attack

Simulation of the attack: [Video](#)



Some Attack and Simulations

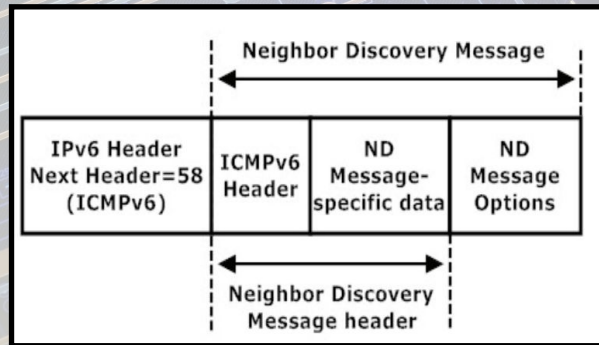
MITM with Spoofed ICMPv6 Router Advertisement

Some Attacks and Simulations

MITM with Spoofed ICMPv6 Router Advertisement

Firstly we need to present Neighbor Discovery Protocol. This protocol presents one of the most significant differences between IPv4 and IPv6.

A mechanism, through which new devices can connect to the network and get an IPv6 address assigned to them.

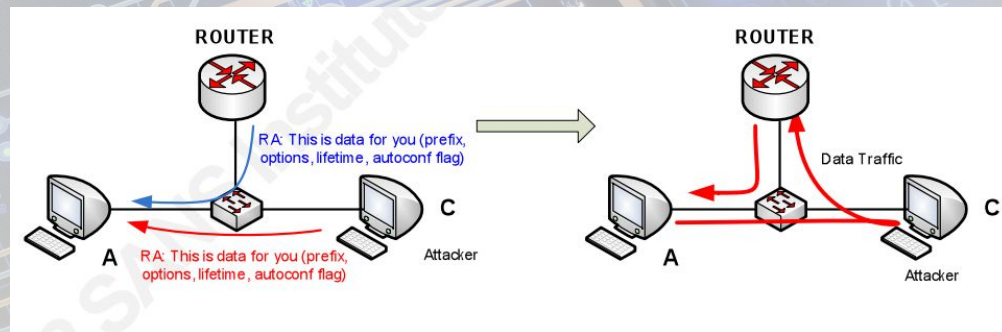


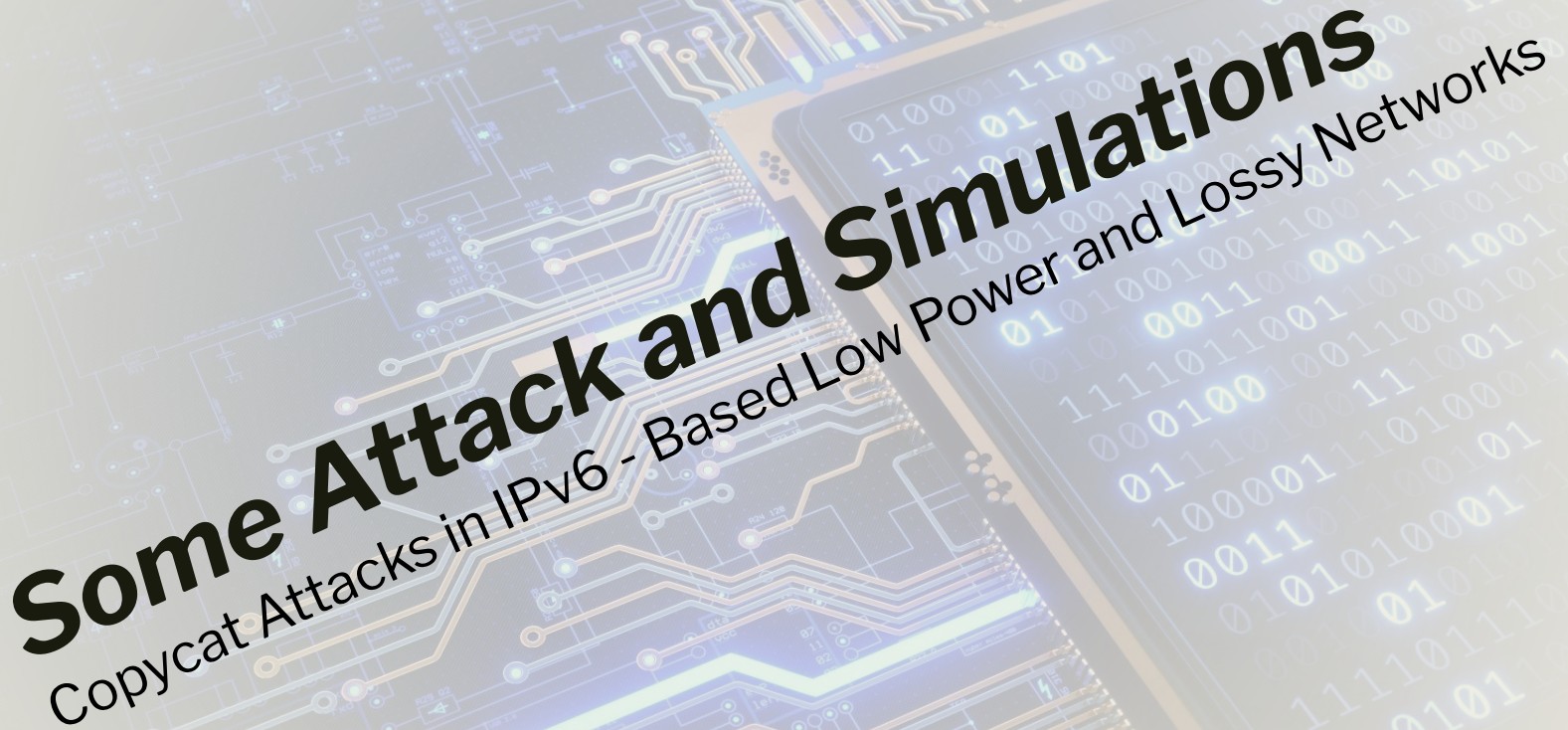
Some Attacks and Simulations

MITM with Spoofed ICMPv6 Router Advertisement

So this attack can be used in two different ways:

- 1) Violate the privacy of devices on the network.
- 2) Function as a type of DoS attack to render the network non functioning.



The background of the slide is a stylized, semi-transparent image of a computer circuit board. It features intricate patterns of gold and blue lines representing circuit traces. Overlaid on the right side of the circuit is a grid of binary code (0s and 1s) in a light blue color. The overall aesthetic is high-tech and digital.

Some Attack and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

One of the most interesting attacks that we found.

Targets Low Power and Lossy Networks, which is an essential field in the IoT (Internet of Things) world.

Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Low Power and Lossy Networks

- Comprised of thousands of embedded networking devices (with limited resources).
- Network nodes are interconnected over lossy links with low packet delivery rates.

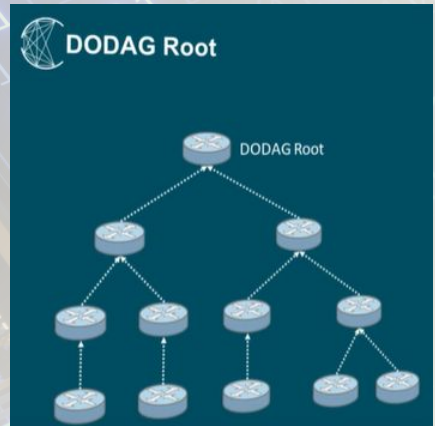
IETF has recently standardized RPL and 6LoWPAN to allow the use of IPv6 on LLNs.

Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

RPL and DODAG

- The functioning of the **RPL** is based on the construction of a Directed Acyclic Graph (DAG).
- RPL routes are optimized for traffic to or from a root that acts as a sink/root for the topology.



Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

RPL Control Messages

There are multiple RPL control messages, we will discuss DIO (which is the message exploited in the Copycat Attack).

DODAG information Object (DIO) : This message is Multicastd downwards.

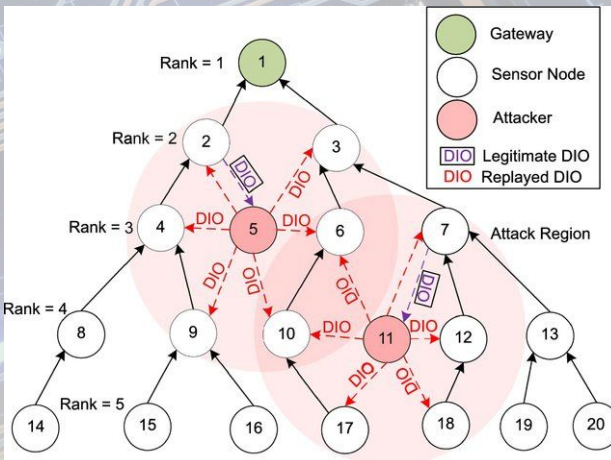
Includes information about the sending node.

Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Copycat Attacks in IPv6-Based LLNs

The main goal of the copycat attack is to degrade the routing performance of RPL based networks so that the Quality of Service (QoS) of real-time applications is affected.



Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Copycat Attacks in IPv6-Based LLNs

Launching a Copycat attack:

- 1) Attacker listens to DIO messages from neighbors.
- 2) After capturing messages, the attacker re-sends those DIO messages again (multicast) many times with a fixed replay interval.
- 3) Victim nodes believe that the packet is from a legitimate sender and makes them perform unnecessary routing related operations.

Some Attacks and Simulations

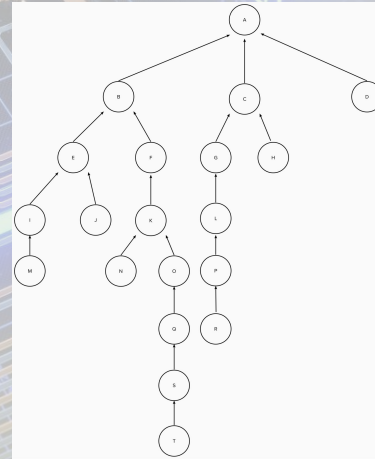
Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Copycat Attacks in IPv6-Based LLNs (Simulation)

Simulated this attack using a C++ simulation (Program) that mimics the behavior and transportation of an RPL network.

There are two types of messages in the simulation: TCP and DIO messages.

We chose the following topology:



Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Copycat Attacks in IPv6-Based LLNs (Simulation Results)

```
Node A average message handle time = 4221.100000
Node C average message handle time = 5554.310000
Node D average message handle time = 3418.250000
Node E average message handle time = 5526.725000
Node F average message handle time = 5515.730000
Node G average message handle time = 6012.380000
Node H average message handle time = 5818.370000
Node I average message handle time = 5670.405000
Node J average message handle time = 5670.625000
Node K average message handle time = 5413.215000
Node L average message handle time = 6055.125000
Node N average message handle time = 5558.290000
Node O average message handle time = 275.785000
Node P average message handle time = 6231.280000
Node Q average message handle time = 6097.310000
Node R average message handle time = 6212.270000
Node S average message handle time = 6221.205000
Node T average message handle time = 3175.445000
```

Regular simulation without a Copycat attack

Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Copycat Attacks in IPv6-Based LLNs (Simulation Results)

**Attacker as a direct child
of the root.**

Node A	average message handle time = 5623.842500
Node C	average message handle time = 7367.550000
Node D	average message handle time = 4941.985000
Node E	average message handle time = 7401.170000
Node F	average message handle time = 7381.815000
Node G	average message handle time = 7914.855000
Node H	average message handle time = 7667.970000
Node I	average message handle time = 7551.275000
Node J	average message handle time = 7553.985000
Node K	average message handle time = 7227.740000
Node L	average message handle time = 7972.175000
Node N	average message handle time = 7381.700000
Node O	average message handle time = 287.195000
Node P	average message handle time = 8169.870000
Node Q	average message handle time = 8076.490000
Node R	average message handle time = 8150.955000
Node S	average message handle time = 8207.455000
Node T	average message handle time = 3371.960000

Simulations with a Copycat attacking node which sends 5 consecutive DIO messages whenever it receives one (each simulation the attacker chooses a different parent).

Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Copycat Attacks in IPv6-Based LLNs (Mitigation Technique)

We came up with a mitigation algorithm that uses the ratio between TCP messages and DIO messages.

The algorithm that runs recursively from the root to the children. Each child chooses its child with the lowest ratio between TCP and DIO messages (in case the child is a root of a subtree, then it calls recursively), the suspect to be hacker is “bubbled” up to the parent and all the way until it reaches the root.

Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Copycat Attacks in IPv6-Based LLNs (Simulation Results)

**Attacker as a direct child
of the root.**

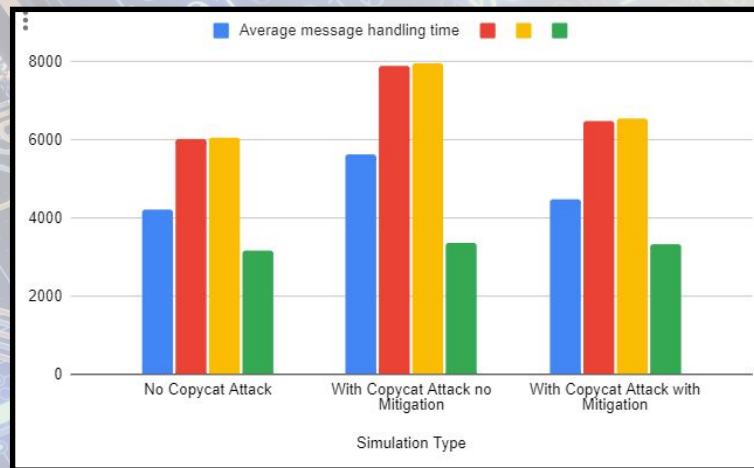
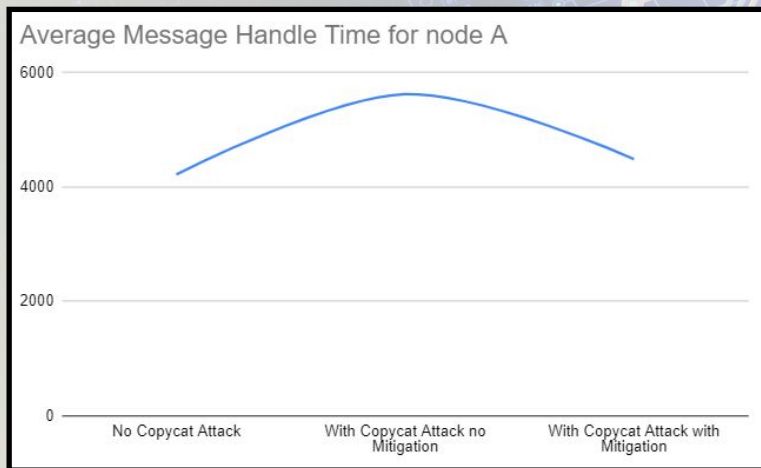
```
Node A average message handle time = 4489.960000
Node C average message handle time = 5987.770000
Node D average message handle time = 4013.485000
Node E average message handle time = 6012.750000
Node F average message handle time = 6002.685000
Node G average message handle time = 6478.240000
Node H average message handle time = 6303.825000
Node I average message handle time = 6175.785000
Node J average message handle time = 6177.155000
Node K average message handle time = 5911.335000
Node L average message handle time = 6544.055000
Node N average message handle time = 6061.015000
Node O average message handle time = 287.195000
Node P average message handle time = 6707.625000
Node Q average message handle time = 6579.335000
Node R average message handle time = 6691.920000
Node S average message handle time = 6705.345000
Node T average message handle time = 3330.205000
Hacker node detected = Node with IP X
```

Same simulations as the one with Copycat attack but with the mitigation technique.

Some Attacks and Simulations

Copycat Attacks in IPv6 - Based Low Power and Lossy Networks

Copycat Attacks in IPv6-Based LLNs (Simulation Results)





Conclusions

Project's Conclusions

- *Learned about a “hot” and fascinating topic that has a significant effect on our daily life.*
- Our study was heavily focused on the weaknesses in IPv6, and we found them to be plenty.

Project's Conclusions

- We got to know new vulnerabilities unique to IPv6 and others that got inherited from IPv4.
- *Managed to explore and simulate attacks that target vulnerabilities in IPv6 and mitigation techniques against them.*

THANK YOU



ANY QUESTIONS?