llss, a Hardware Address Based MTD for Ad-Hoc Wireless Networking

In other words: you can’t hit me, I’m moving too fast

Wireless security is difficult

- Wireless is broadcast by definition
  - Packets are easily sniffable

- Many networking protocols are even easier to attack over wireless
- Systems are often security-second (or no security…)

- ARP
  - Insecure
  - Abusable

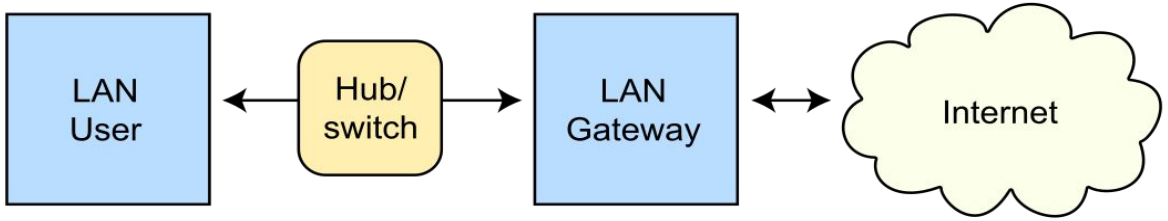
Problem statement

- ARP is inherently insecure
  - First Come First Serve
  - Requests are broadcast
    - In a wireless setting, this is **BAD**

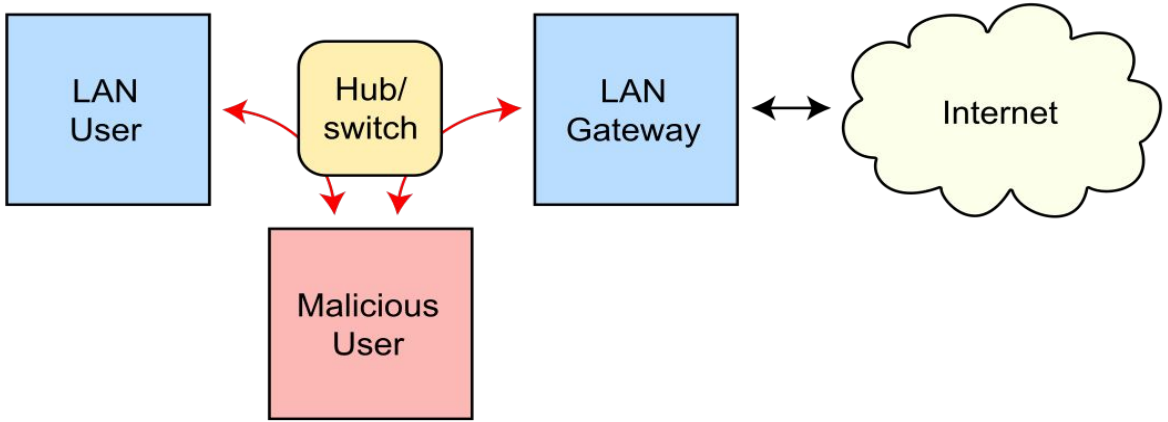
- ARP cache poisoning
  - Very bad
  - Helps establish a MITM (Man In The Middle) for adversaries

- MITM
  - A malicious host places itself in between two legitimate hosts
  - The ultimate goal of a network attack

Routing under normal operation



Routing subject to ARP cache poisoning



llss, basic description

- llss is a hardware address based MTD
  - Hardware Address = MAC address
- MTD
  - Moving Target Defense
  - Moves an attackers target, thus making it harder to attack.

- What does this mean?
  - **llss is a MAC address shuffling tool taken to the extreme.**
- UDP Transport mechanism

MAC Address Shuffling?

- Hardware address shuffling is an under researched field
  - Apple and Microsoft currently have pseudo implementations
  - At session layer, or when connecting to a network initially
- llss
  - Shuffling takes place at the packet layer
  - Every. Single. Packet. is sent to a new MAC address

The Setup

1. Raspberry Pi 4-8GB (Sender)
2. Raspberry Pi 4-4GB (Receiver)
3. Raspberry Pi 3 (Adversary)
4. 8 Port Ethernet Switch (control)
5. 3 Port HDMI Switch (if failure)
6. 2 Port HDMI Switch (to/from PC)
7. 4in2out USB switch (Pi control)
8. Keyboard to control Pi's
9. Mouse to Control Pi's
10. My super cool keyboard I got as a birthday gift from my girlfriend
11. Logitech G502 Mouse (The best mouse no contest).
12. Cup
13. Hand Sanitizer (stay safe)
14. lofi (stay sane)

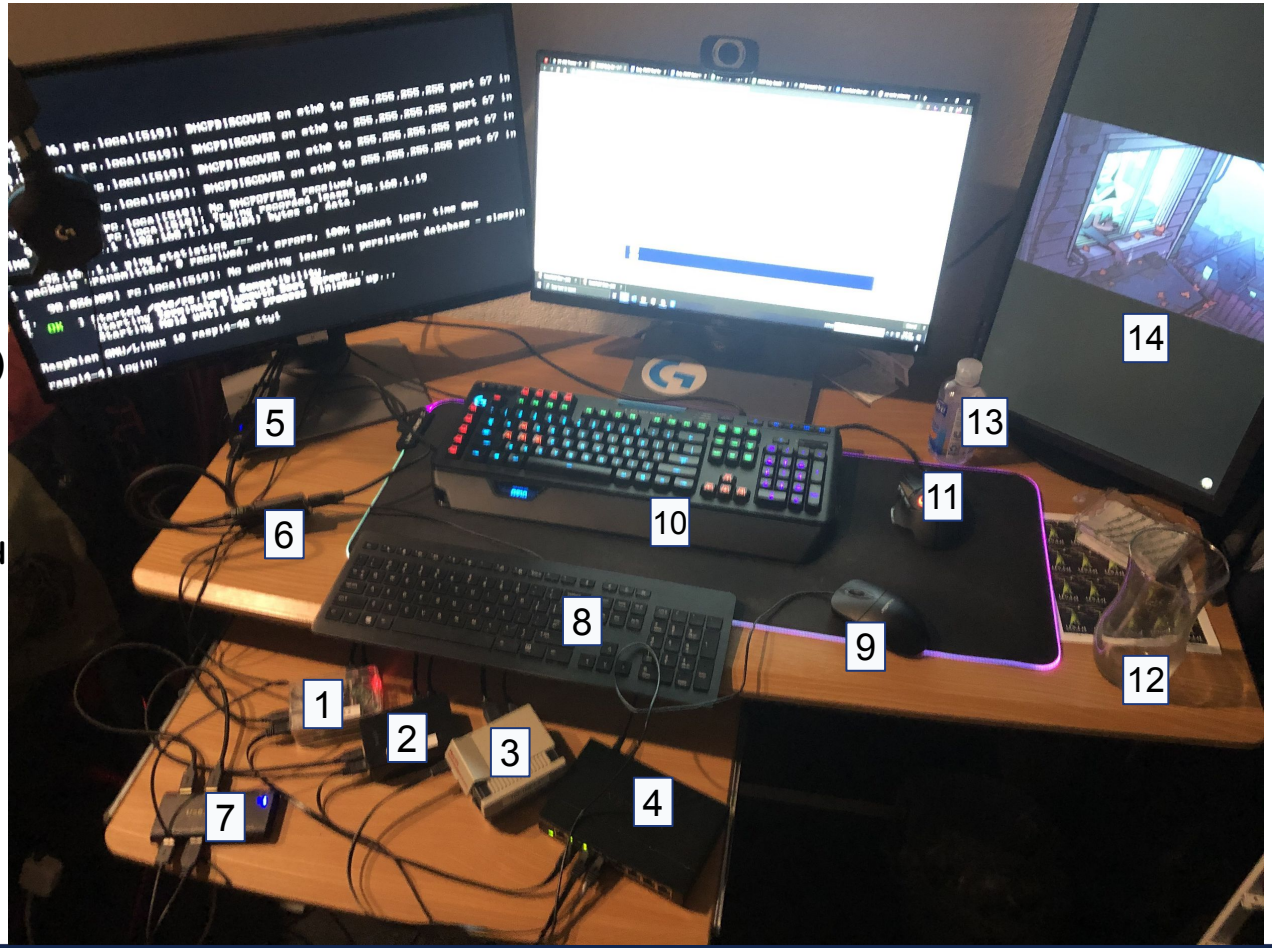
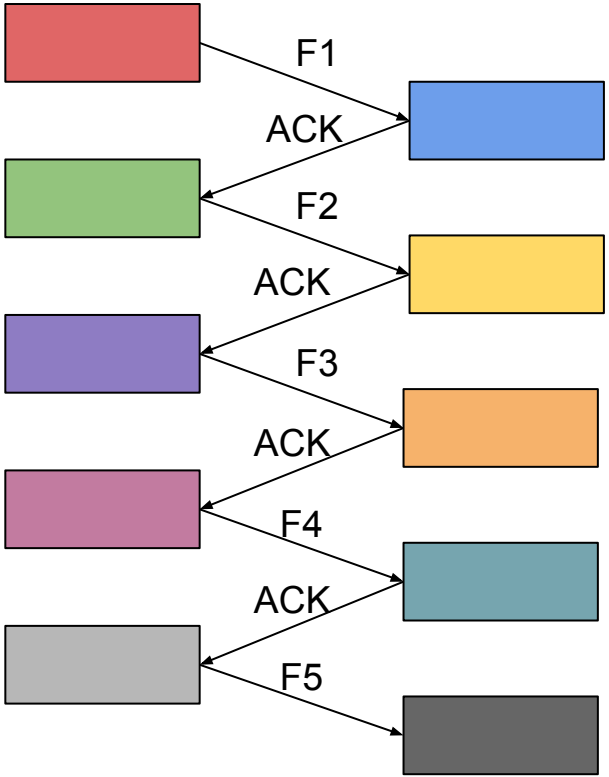


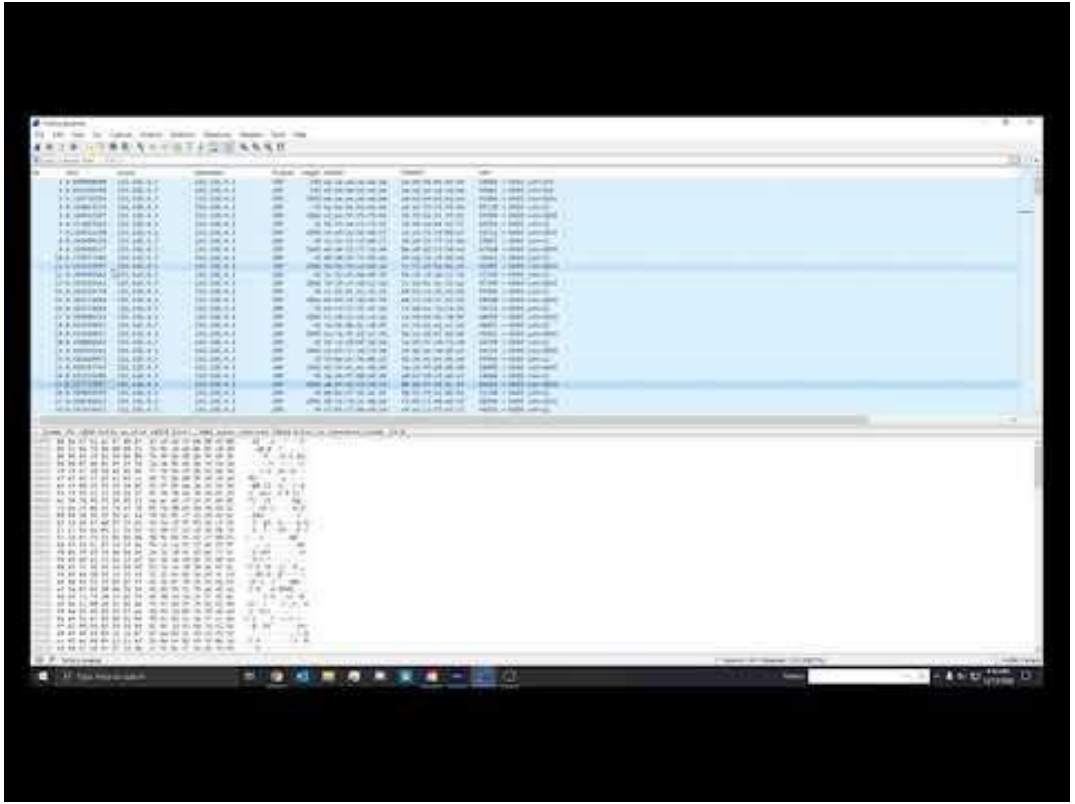
Figure 4 - Frame > Advance > Ack > Advance



llss features

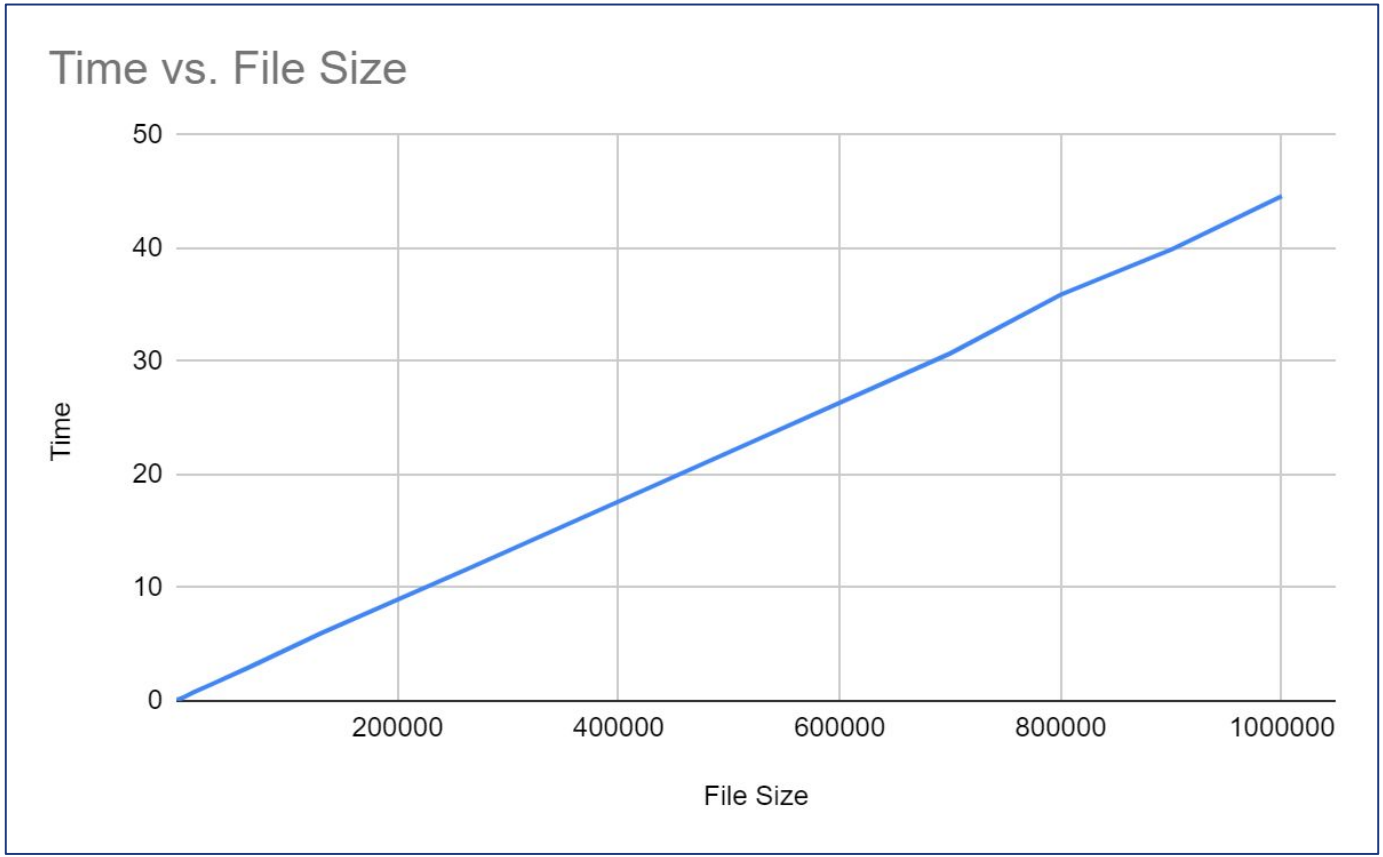
- MAC address shuffling every packet!
- AES-256 Bit Encryption
- File Transfer
- Considerable user agency (lots of options)
- A fully functioning Wizard!
- ~1500 Lines of code
    - Line count doesn’t really matter, it's just a fun statistic.

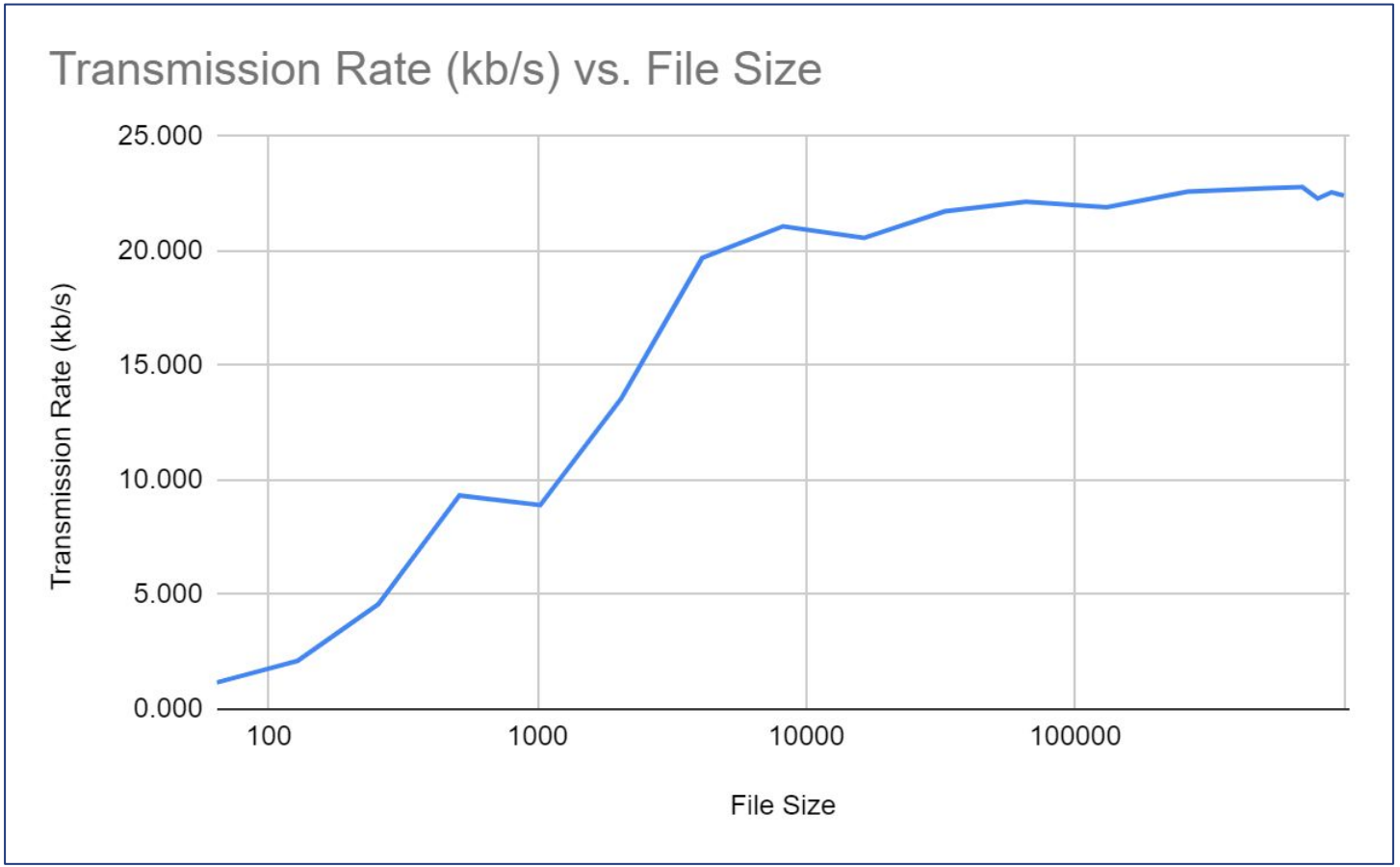
Demonstration



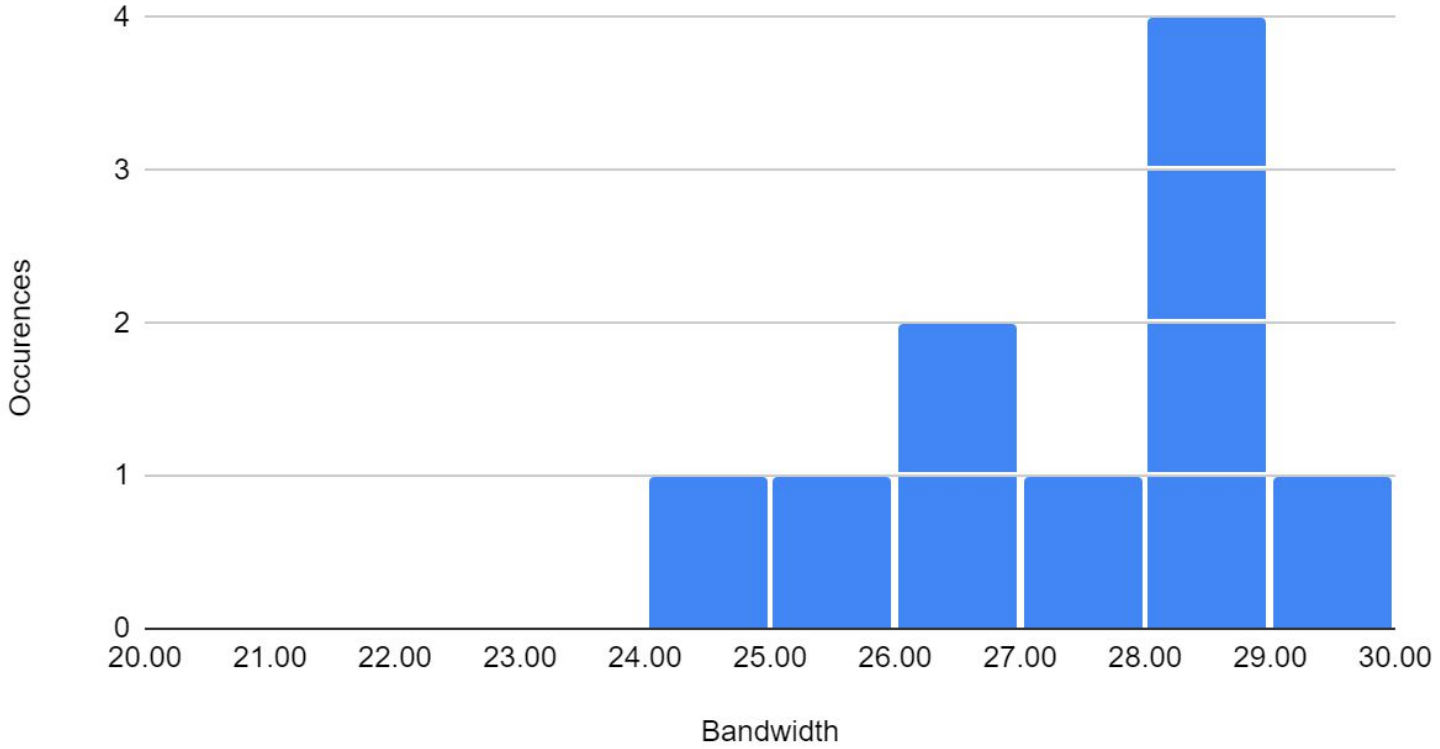
Results

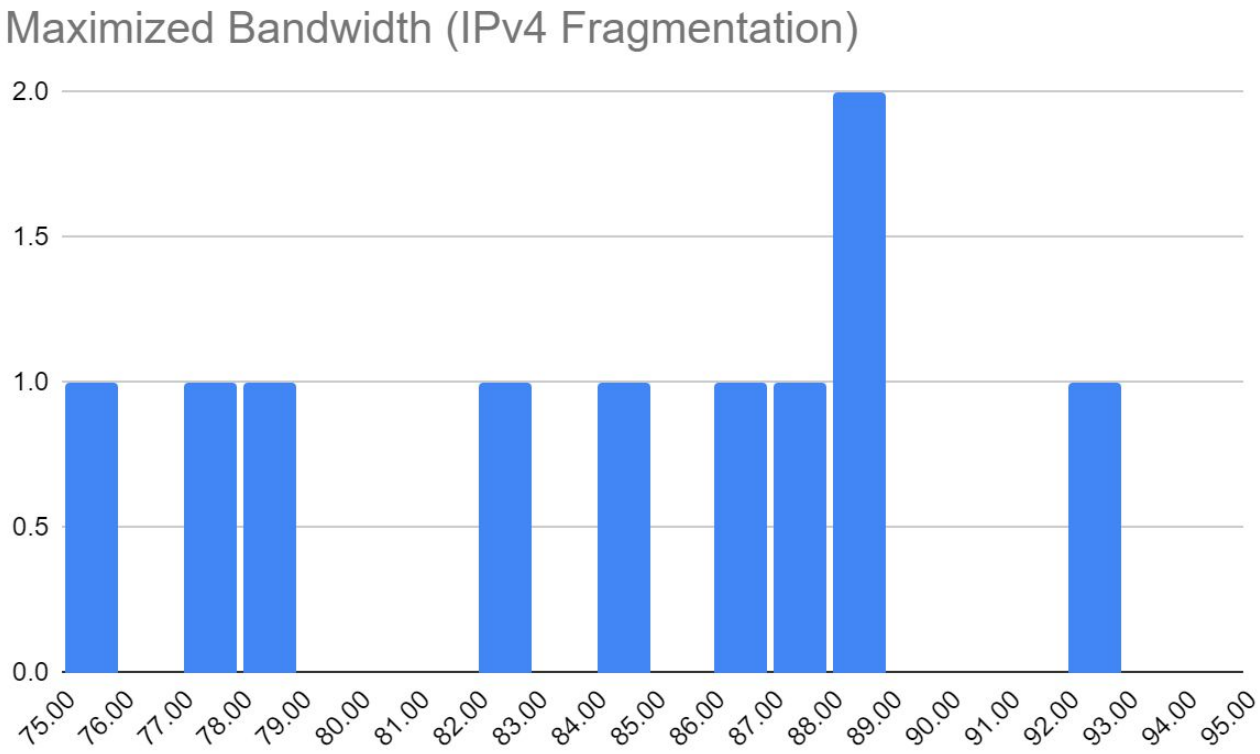
- Success?
  - Yes! Packets could be sent and decrypted!
- Files could be successfully transmitted up to 1MB
- At 1MB, strange socket issues arose
  - Closing and opening rapidly?
- Sniffable
  - Not as easily!
- MITM-Able
  - Very difficult!
  - No ARP Messages!
- Metrics
  - Maximum single-packet bandwidth = 27.37kb/s
  - Maximum no-limits bandwidth = 84.24kb/s
  - Slow, but good enough for text files.


Time vs. File Size
50
40
30
20
10
0
Time
200000
400000
600000
800000
1000000
File Size


Transmission Rate (kb/s) vs. File Size
25.000
20.000
15.000
10.000
5.000
0.000
Transmission Rate (kb/s)
100
1000
10000
100000
File Size

Bandwidth (KBps) Occurences




Maximized Bandwidth (IPv4 Fragmentation)
2.0
1.5
1.0
0.5
0.0
75.00
76.00
77.00
78.00
79.00
80.00
81.00
82.00
83.00
84.00
85.00
86.00
87.00
88.00
89.00
90.00
91.00
92.00
93.00
94.00
95.00

Learning Opportunities

- Do not be a victim of hubris
- Other people know how to help you
- Workflow optimisation is an absolute godsend
- Networking becomes more difficult as you interface with lower layers
- Never roll your own crypto
- Never write your own crypto methods

Conclusion

- MAC address based Moving Target Defense is possible, and practical for small amounts of data.
- Further optimizations could increase the practicality of llss
  - Reliability
  - Timing optimization
  - Kernel optimization

Further information

Please visit

llss.page