

# A Comparative Security Evaluation for IPv4 and IPv6 Addresses

Vincent van der Eijk & Erik Lamers

# Comparing IPv4 port security to IPv6 port security

Scanning the Internet for profit, ethically.

# Why do we need to know this?

IPv6 adoption is growing:

- More exposed hosts?
- More exposed ports every day?

Until recently scanning the IPv6 address space was considered unfeasible.

# Research Question

Has the state of IPv6 port based security compared to IPv4 port based security shifted over the last four years?

# Is IPv6 port security that different?

Previous work has shown that misconfigurations when enabling IPv6 are common. This can leave (IPv6) ports exposed to the Internet.

## Related work (1)

Czyz et al. (2016), have shown that IPv6 port security is leaking compared to IPv4.

Borgolte et al. (2018), have shown that enumerating IPv6 addresses using DNSSEC is possible, and found similar security issues.

## Related work (2)

Durumeric et al. (2013), developed ZMap a Internet wide scanning tool.

# Ports to probe

- In total: 19 TCP and 4 UDP ports

Some examples:

- Basic protocols: FTP, HTTP, SSH
- DB protocols: MongoDB, MSSQL, MySQL
- Outdated protocols: SNMPv1, Telnet

# Host definition

- Only dual-stack hosts
- A host must be reachable via ICMP echo request either on IPv4 or IPv6

# Methodology

1. Datasets (Rapid7, Alexa, IPv6 hitlist)
2. ICMP scan
3. Scan reachable hosts for responding services
4. Banner grab responsive TCP protocols

# Lab setup

- Two servers running Ubuntu 18.04;
  - 8 vCPUs, 16 GB Mem
- 1 GB uplink / Server NIC 200K pps cap.
- ZMap and ZGrab(2) scanning tools

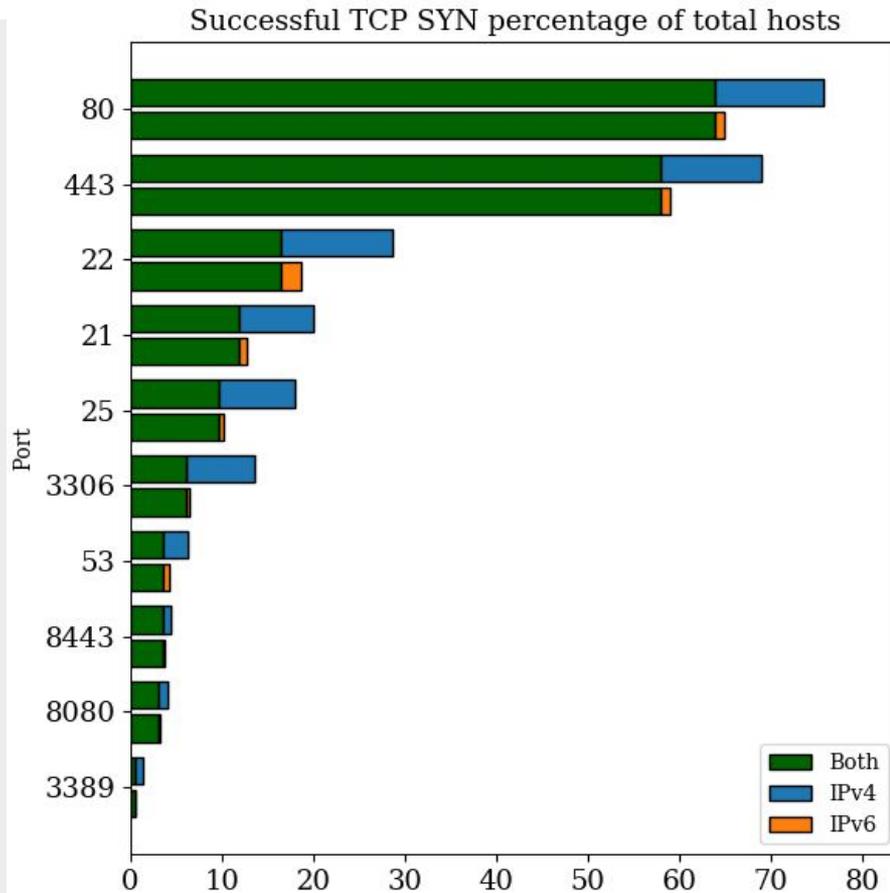
# Then we scanned the Internet

... or at least a part of it.

# Results (1)

Top (blue): IPv4

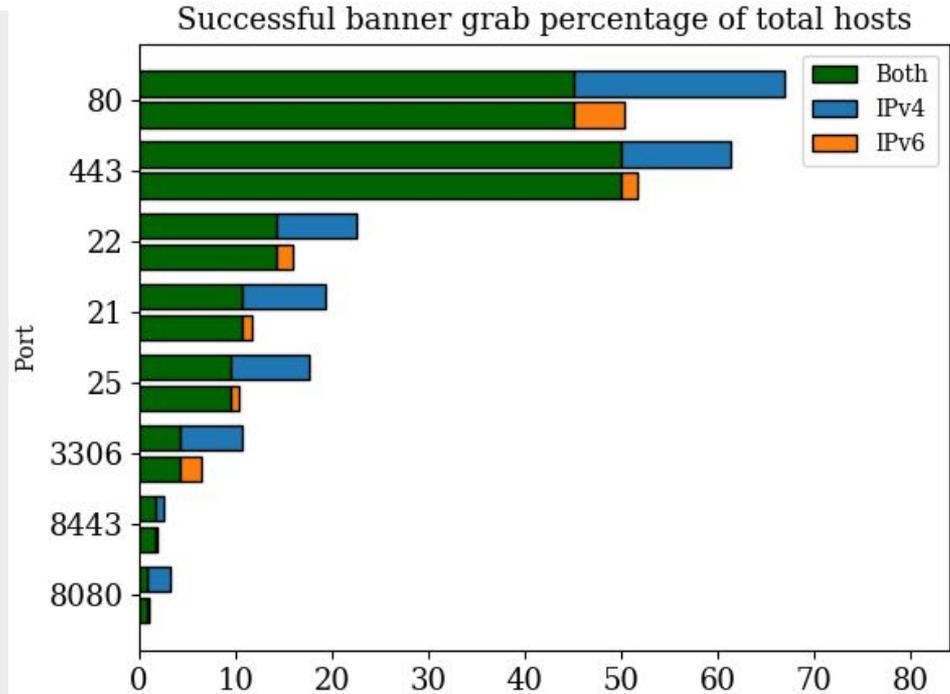
Bottom (orange): IPv6



# Results (2)

## Banner-grab

Average response:  
85%



# Conclusions

According to our findings a higher percentage of IPv4 ports are exposed to the Internet than IPv6 ports are.

Has the trend really shifted in the past four years towards IPv6 security?

# Key findings

- IPv4 is still the dominant protocol
- 4 times more open ports over IPv4 than IPv6
- Is there a shift in port security?