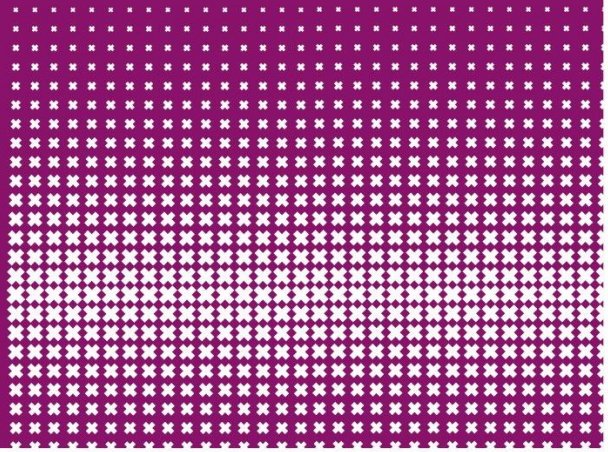
University of Amsterdam

Robert Diepeveen & Ruben de Vries



Bypassing 802.1X

In an IPv6 environment

Introduction and motivation

- What is 802.1X?
  - IEEE standard
  - Port-based network access protocol
  - Authentication mechanism for devices wishing to attach to a network
- Why in an IPv6 environment?

Research question

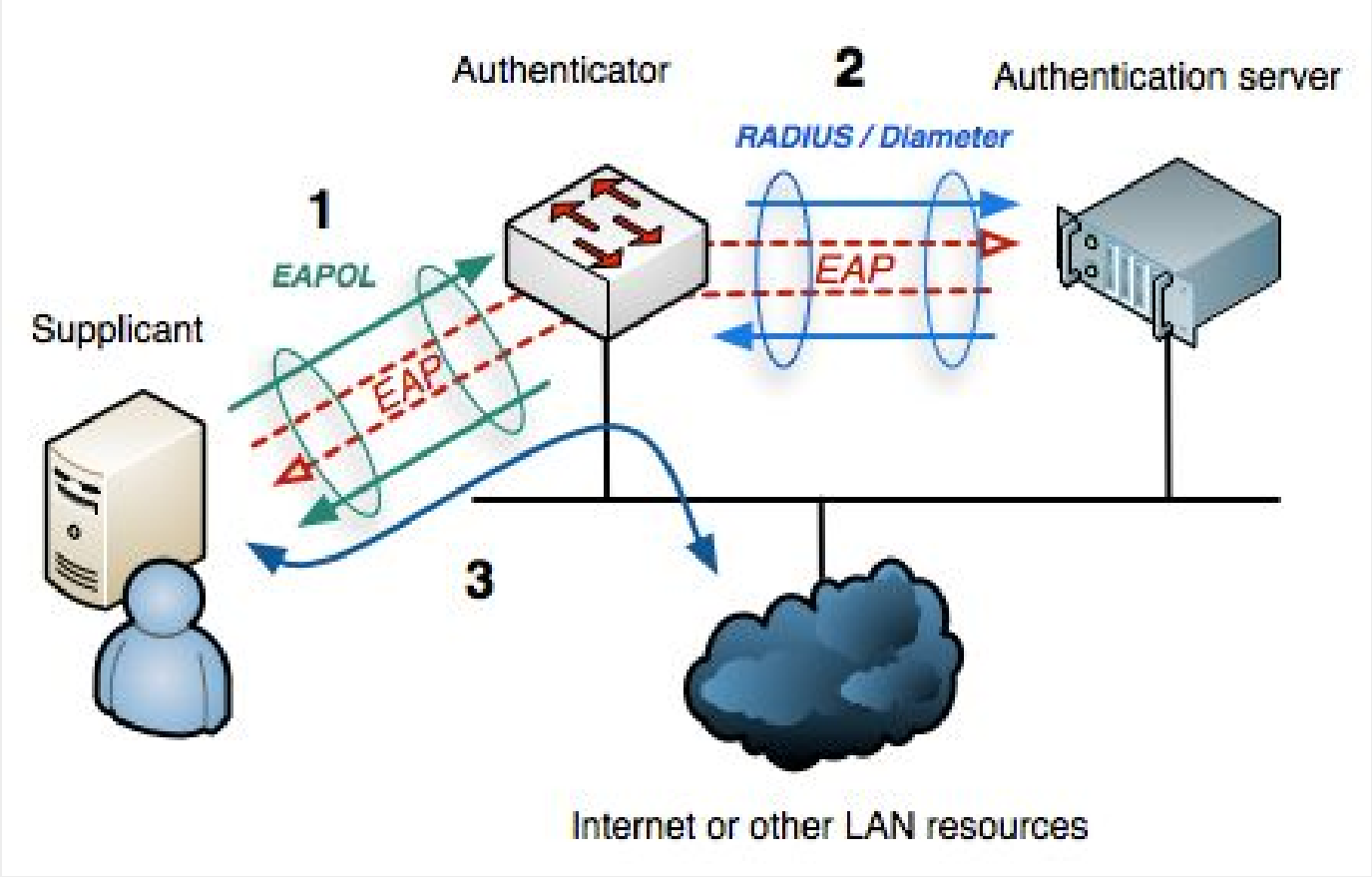
Is it possible to bypass 802.1X in an IPv6 environment?

Yes it is!

Research outline

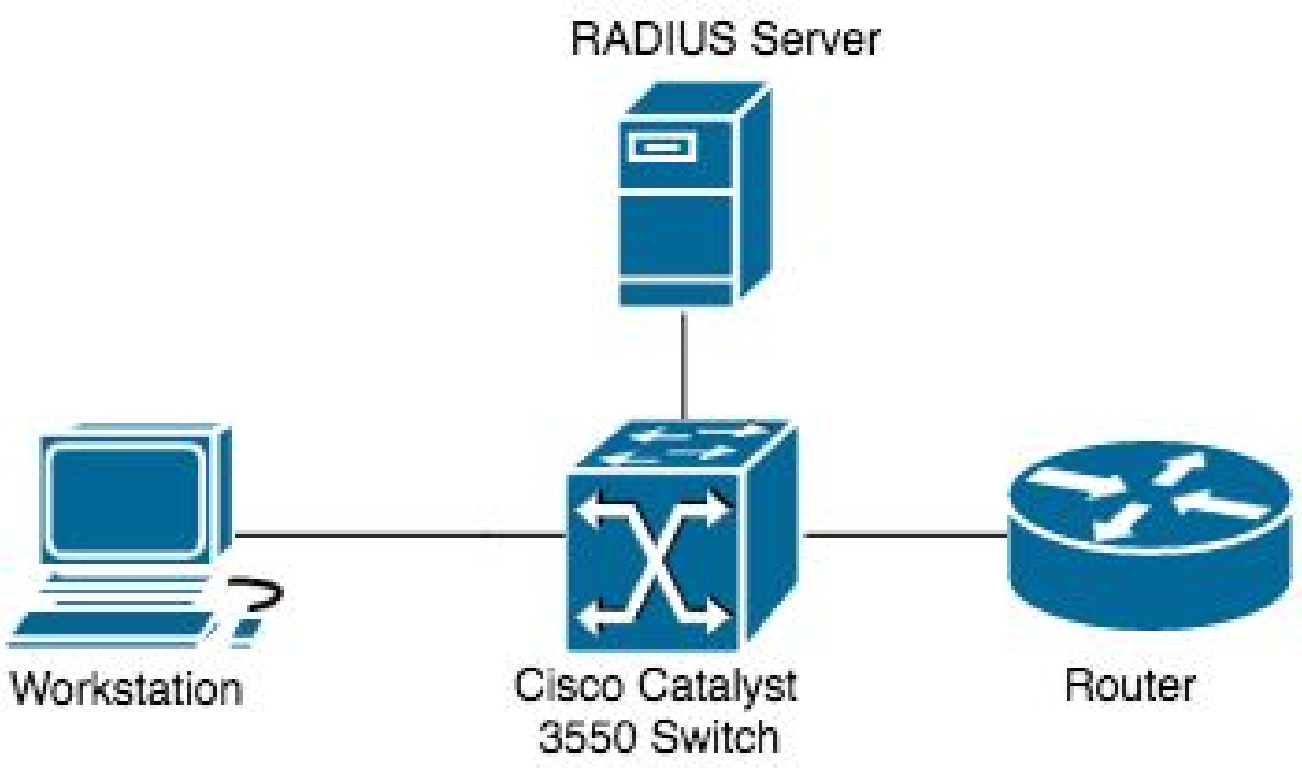
- What is 802.1X?
- How is this attack performed in an IPv4 environment?
  - Key components
- What are the theoretical differences between IPv4 and IPv6?
  - How do these key components translate?

802.1X in detail



source: Wikipedia

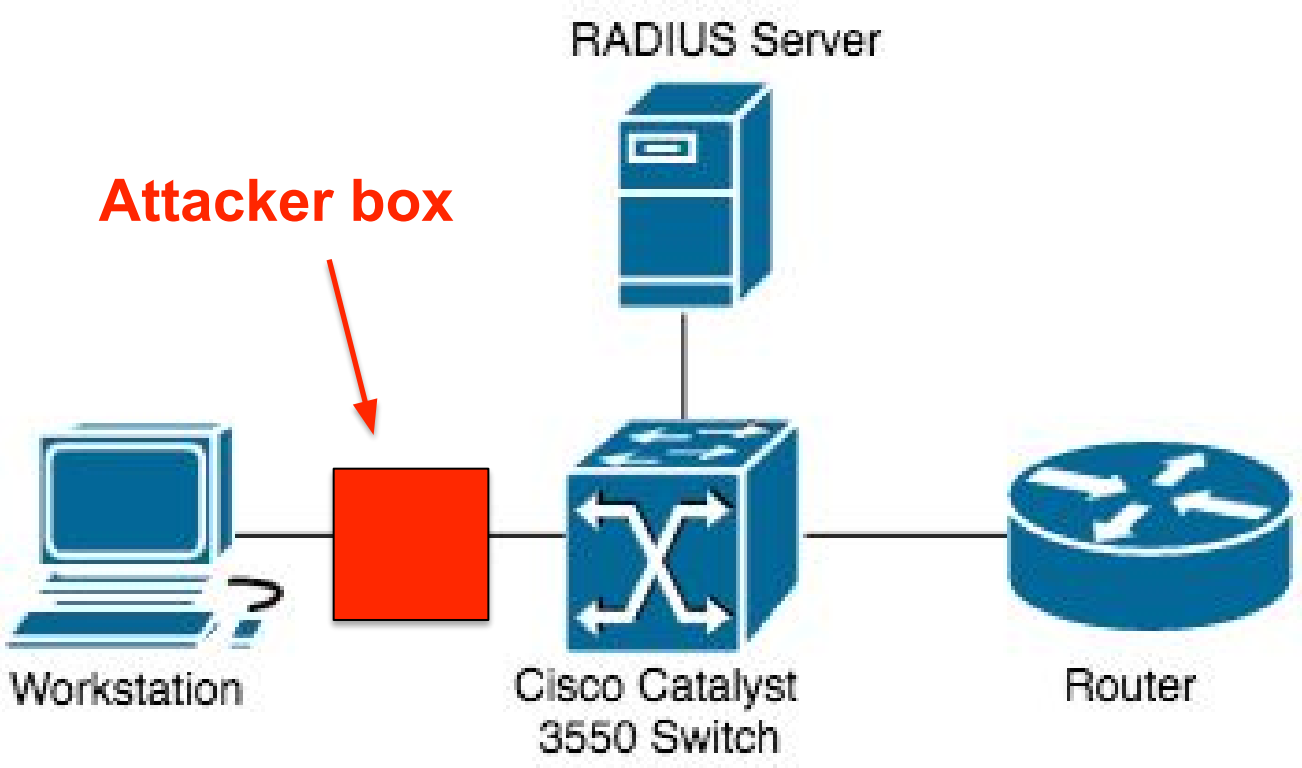
Test environment



Bypassing 802.1X in IPv4

- Place device on the physical link between victim workstation and authenticator
- Make sure the victim host remains connected to the network while setting up the device
  - Be *invisible*
- Gain access to the network via the attacker box

Bypassing 802.1X in IPv4



Attacker box properties

- Bridging network traffic
  - At least two ethernet interfaces
  - Forward EAPOL packets
- Invisible for the switch
  - E.g. do not respond to ARP requests
- Mimic the victim workstation
  - *SNAT* with iptables —> IP
  - *SNAT* with ebtables —> MAC

Differences between IPv4 and IPv6

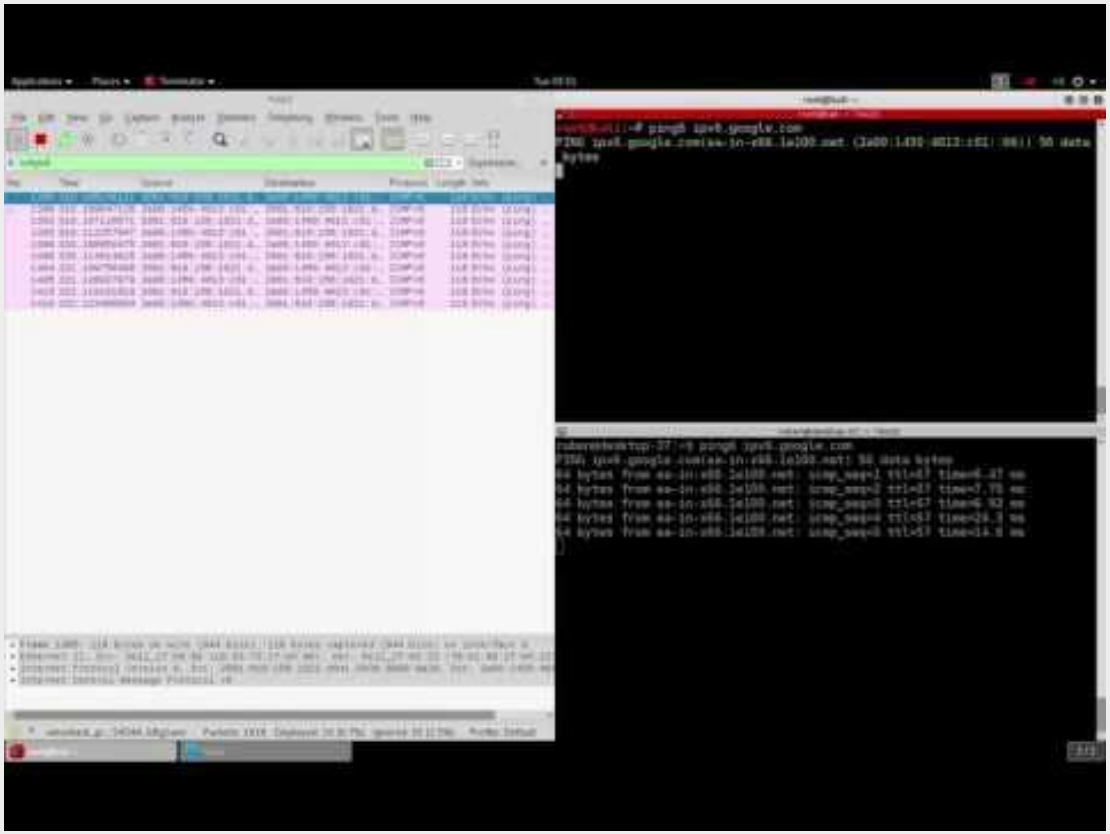
- MAC to IP address mapping
  - IPv4: ARP
  - IPv6: NDP
- Neighbor Advertisements/Sollicitations

- Generally no NAT needed in IPv6
  - However, people insisted (NAT66)

Bypassing 802.1X in IPv6

- Similar to IPv4 bypass
- Bridge needs to learn neighbours by sniffing NDP messages
  - Same for ARP
- Victim host to bypass device communication

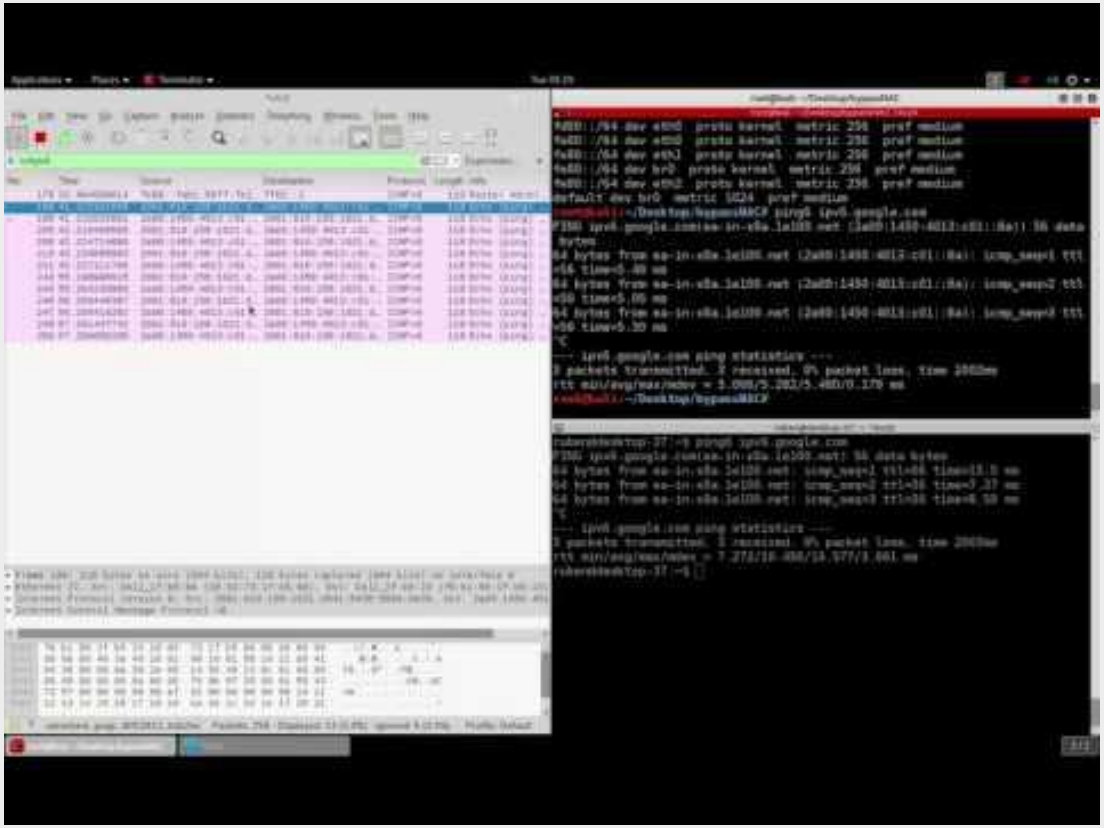
Bypassing 802.1X in IPv6



Dot1X security violation

```
%DOT1X-5-SECURITY_VIOLATION: Security violation on the interface
FastEthernet0/17, new MAC address 000e.c68f.f9e0 is seen.
```

Bypassing 802.1X in IPv6



Discussion

- Not every packet/frame is encrypted or authenticated
- Layer 2 vs layer 3 security
- Mitigation techniques
  - MACsec, IPsec, SEND, HIDS
- Kernel bug
  - Linux Kali used on Raspberry (4.1.7)
  - NAT66 bug in Linux kernel versions < 4.3

Conclusion

- **Is it possible to bypass 802.1X in an IPv6 environment?**
  - *Yes it is!*
  - Attacks in both environments are not that different

Future work

- Mitigation techniques
  - Investigate feasibility of the attack in a MACsec/IPsec/.. enabled environment
- Remote access
  - Add a third (4G) interface to access the attacker box remotely
- Device portability
  - Patch kernel
  - Different Linux distribution
- Open-source wired 802.1X switches