

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

Research Project #2

• Why in an IPv6 environment?



Research question

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

Yes it is!

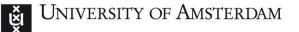




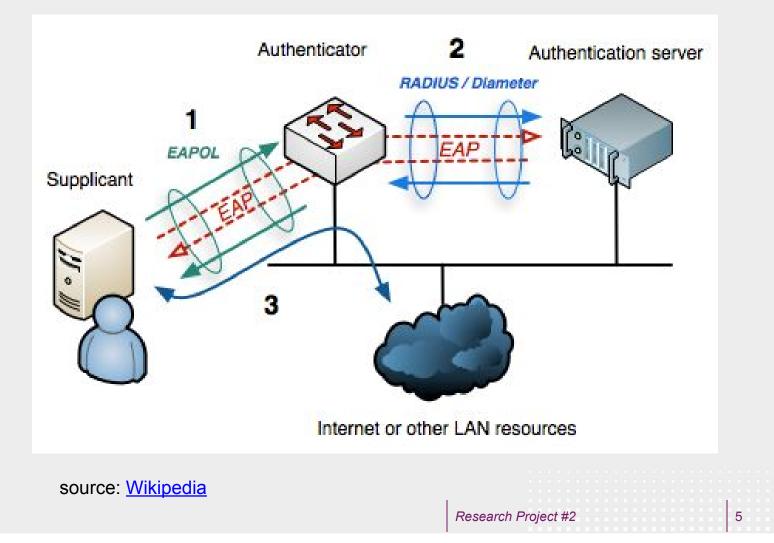
Research outline

- 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?





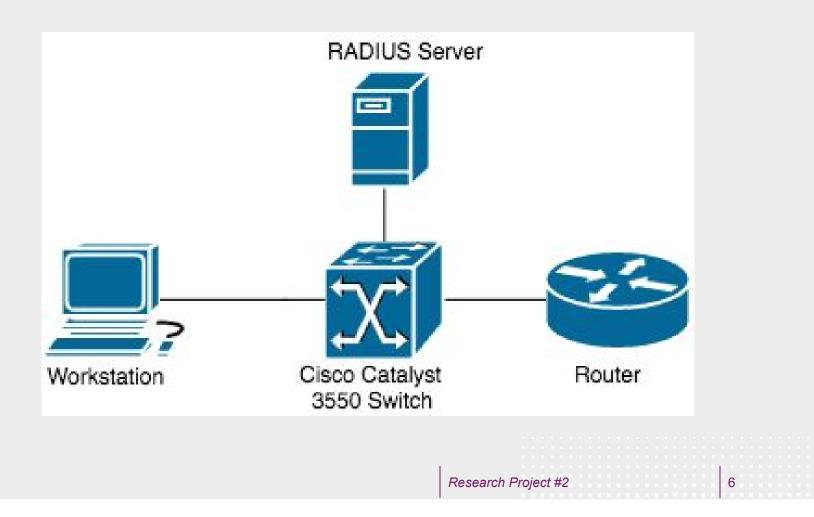
802.1X in detail





University of Amsterdam

Test environment

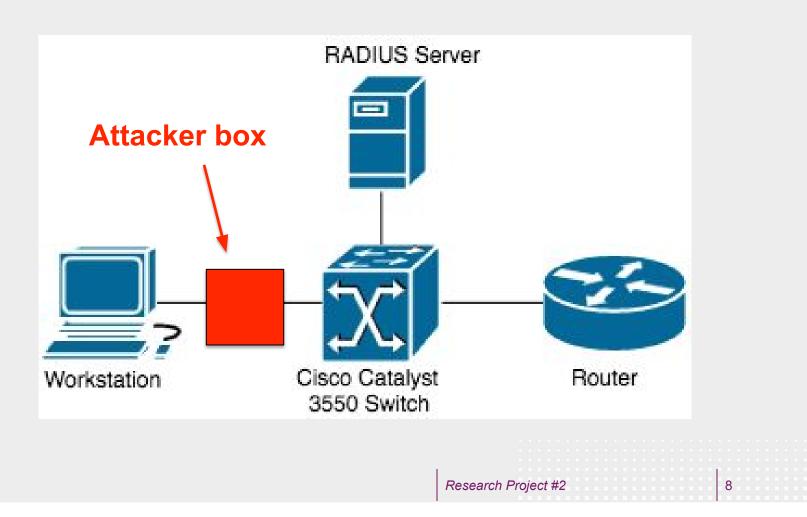




- Place device on the physical link between victim workstation and authenticator
- Make sure the victim host remains connected to the network while setting up the device
 - Be invisible
- Gain access to the network via the attacker box

Research Project #2







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

Research Project #2

- 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)





- Similar to IPv4 bypass
- Bridge needs to learn neighbours by sniffing NDP messages

Research Project #2

- Same for ARP
- Victim host to bypass device communication



		5483		田 = +0.
in the latter many from	frames from fair and	Distances	Concession of the local distance of the loca	10.0
D'SCO		Contraction of the second	pingh inve.genglw.com	an ante entri las i fat ante
		ant - Supreme a Patter		
See land	Domaton Potenti	Lange Into		
		All and a grant a second and a second a		
		Pittin, gave - go 64 hg/tari, Pro 64 hg/tari, Pro	p-37/-4 provpt yers progle rom byla iverae in sta laiss ent to device e de databa Salida est ivery ward thi e e-34 sida Salida est ivery ward thi	-17 time-7.75 em
a dama dala kacamatan dala dalah		tia toptad fra	9 88-07,205.36109 πet διαφ ₂ 9000 τη 8 48-07,205.36100 πet διαφ ₂ 9000 τη 8 48-07,205.36100 πet διαφ ₂ 9000 τη 8 48-07,205.36100 πet διαφ ₂ 9000 τη	157 time-24.3 us
	the last start store have been	Contraction and		
sentence blitting av Paters II	18. Dataset 20. N. Pal growth 10.2	the Actualities		1.00



Dot1X security violation

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





ALC: NOT	Nitracy Summer Summer	4
	fail) 1/64 day hr0: prote kernel: estric: 259 pre	ref medice ref medice of medice s.ise 1400 HELLINGLING() 16 deal 13 CULIES() Comp_seeps1 tt 14 CULIES() Sail Somp_seeps1 tt 14 CULIES() Sail Somp_seeps1 tt 14 CULIES() Sail Somp_seeps1 tt 14 CULIES() Sail Som 14 CULIES() Sail Som
	rt% m(r//wallowAnion = 7 272/10 488/18.577/3.86) referenting Tips 32 -5 □	

Research Project #2



Discussion

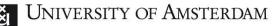
- Not every packet/frame is encrypted or authenticated
- Layer 2 vs layer 3 security
- Mitigation techniques
 - MACsec, IPsec, SEND, HIDS
- Kernel bug
 - Linux Kali used on Raspberry (4.1.7)
 - NAT66 bug in Linux kernel versions < 4.3



Conclusion

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

Research Project #2



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

Research Proiect #2

- Device portability
 - Patch kernel
 - Different Linux distribution
- Open-source wired 802.1X switches