FORESCOUT

SYNACKTIV
DIGITAL SECURITY

LIVE:
SECURITY PEN TEST

Exploring the Limitations of 802.1x and Beyond

Andrew Noonan (Forescout)
Florian Guilbert (Synacktiv)
Infosecurity Europe, 4th June 2019

About Synacktiv

- Consulting company in offensive security
  - French and independent
  - Specializing in performing penetration tests and security audits
  - 54 employees including 50 security experts
- Came across Forescout during penetration testing

Physical and Logical Penetration Testing

Key steps of a physical and logical penetration test:

1. Physical intrusion on companies’ premises often simple
2. Connection of a miniature implant

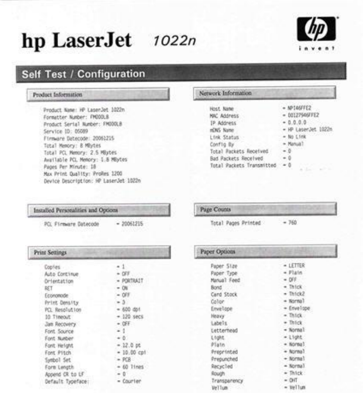
3. Establishing a communication channel (HTTPS, DNS, Wi-Fi hotspot, 3G/4G, SMS, etc.)
4. Intrusion of the internal network

Source: copy goes here

SYNACKTIV DIGITAL SECURITY

MAC Address Filtering

- MAC (Media Access Control) address: unique identifier of the network card



hp LaserJet 1022n

Self Test / Configuration

Product Information

Product Name: HP LaserJet 1022n
Formatter Number: FM000L8
Product Serial Number: FM000L8
Service ID: 05089
Firmware Datecode: 20061215
Total Memory: 8 MBytes
Total PCL Memory: 2.5 MBytes
Available PCL Memory: 1.8 MBytes
Pages Per Minute: 18
Max Print Quality: ProRes 1200
Device Description: HP LaserJet 1022n

Network Information

Host Name	= NPI46FFE2
MAC Address	= 00127946FFE2
IP Address	= 0.0.0.0
mDNS Name	= HP LaserJet 1022n
Link Status	= No Link
Config By	= Manual
Total Packets Received	= 0
Bad Packets Received	= 0
Total Packets Transmitted	= 0

Installed Personalities and Options

PCL Firmware Datecode	= 20061215

Page Counts

Total Pages Printed	= 760

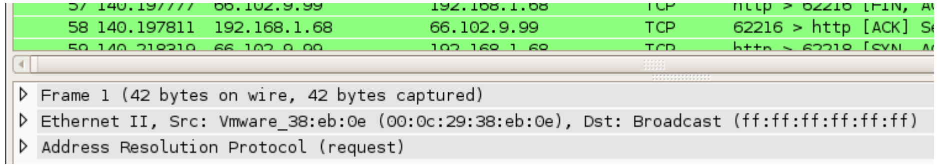
Print Settings

Copies	= 1
Auto Continue	= OFF
Orientation	= PORTRAIT
RET	= ON
Economode	= OFF
Print Density	= 3
PCL Resolution	= 600 dpi
IO Timeout	= 120 secs
Jam Recovery	= OFF
Font Source	= I
Font Number	= 0
Font Height	= 12.0 pt
Font Pitch	= 10.00 cpi
Symbol Set	= PC8
Form Length	= 60 lines
Append CR to LF	= 0
Default Typeface:	= Courier

Paper Options

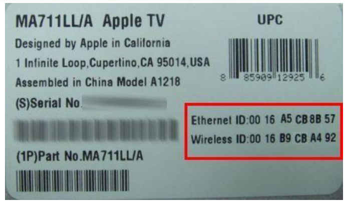
Paper Size	= LETTER
Paper Type	= Plain
Manual Feed	= OFF
Bond	= Thick
Card Stock	= Thick2
Color	= Normal
Envelope	= Envelope
Heavy	= Thick
Labels	= Thick
Letterhead	= Normal
Light	= Light
Plain	= Normal
Preprinted	= Normal
Prepunched	= Normal
Recycled	= Normal
Rough	= Thick
Transparency	= OHT
Vellum	= Vellum

- Bypass
  - Discovery via network sniffing… or just reading the label!



```
57 140.197777  66.102.9.99     192.168.1.68    TCP   http > 62216 [FIN, A
58 140.197811  192.168.1.68    66.102.9.99     TCP   62216 > http [ACK] Se
59 140.218319  66.102.9.99     192.168.1.68    TCP   http > 62218 [SYN, A
```

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```



MA711LL/A Apple TV
Designed by Apple in California
1 Infinite Loop,Cupertino,CA 95014,USA
Assembled in China Model A1218
(S)Serial No.[redacted]
(1P)Part No.MA711LL/A

UPC
8 85909 12925 6

Ethernet ID:00 16 A5 CB 8B 57
Wireless ID:00 16 B9 CB A4 92

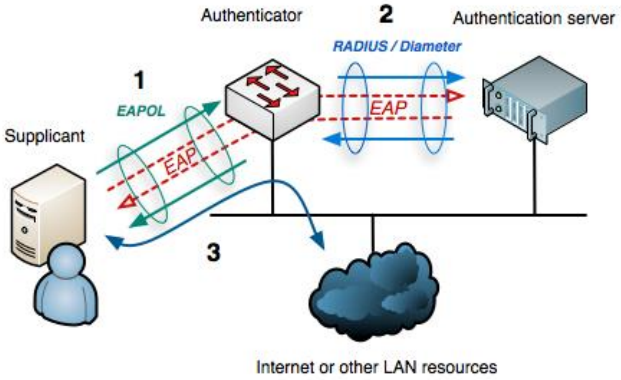
  - Edition simple on the attacker device

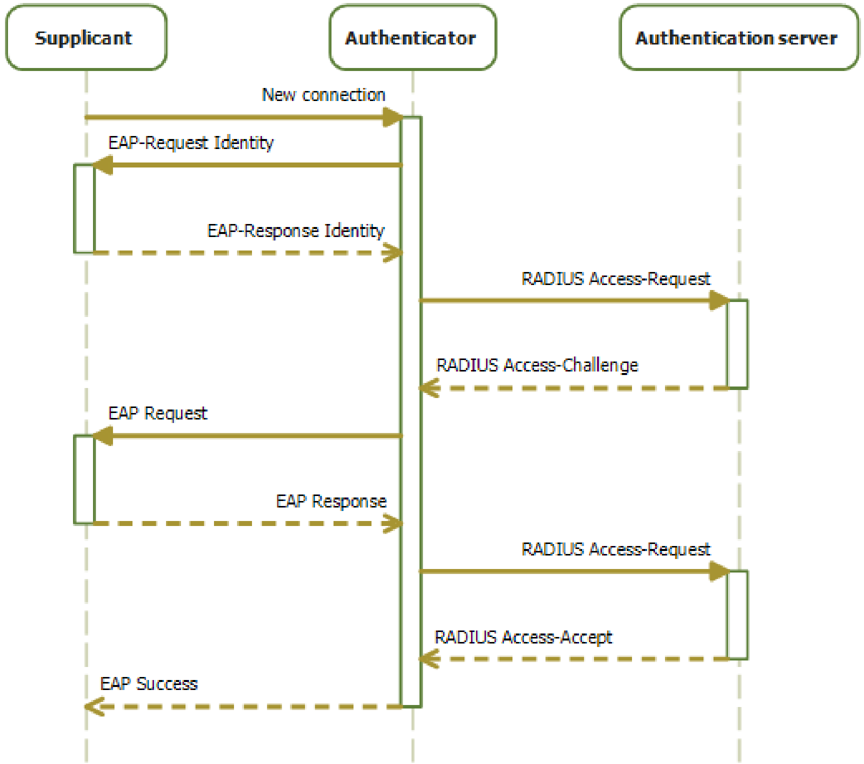
```
$ ip link set eth0 address 00:16:A5:CB:88:57
```

- Filtering often used because simple to deploy and sometimes, the only supported solution
- Inoperable in large scale infrastructure and difficult to maintain
- The recommendation is to implement 802.1x

802.1x Protocol

- IEEE standard requesting an authentication to allow accessing the switch ports





- Not supported by every device
  - IoT, printers, card readers, IP cameras, etc.

- Robust?

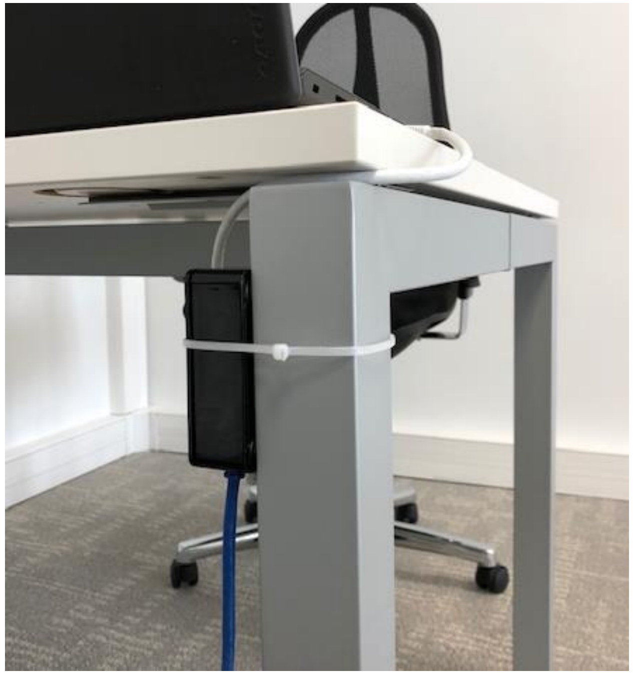
- Improved by 802.1AE (MACsec)
  - But not widely supported

Man In The Middle on 802.1x

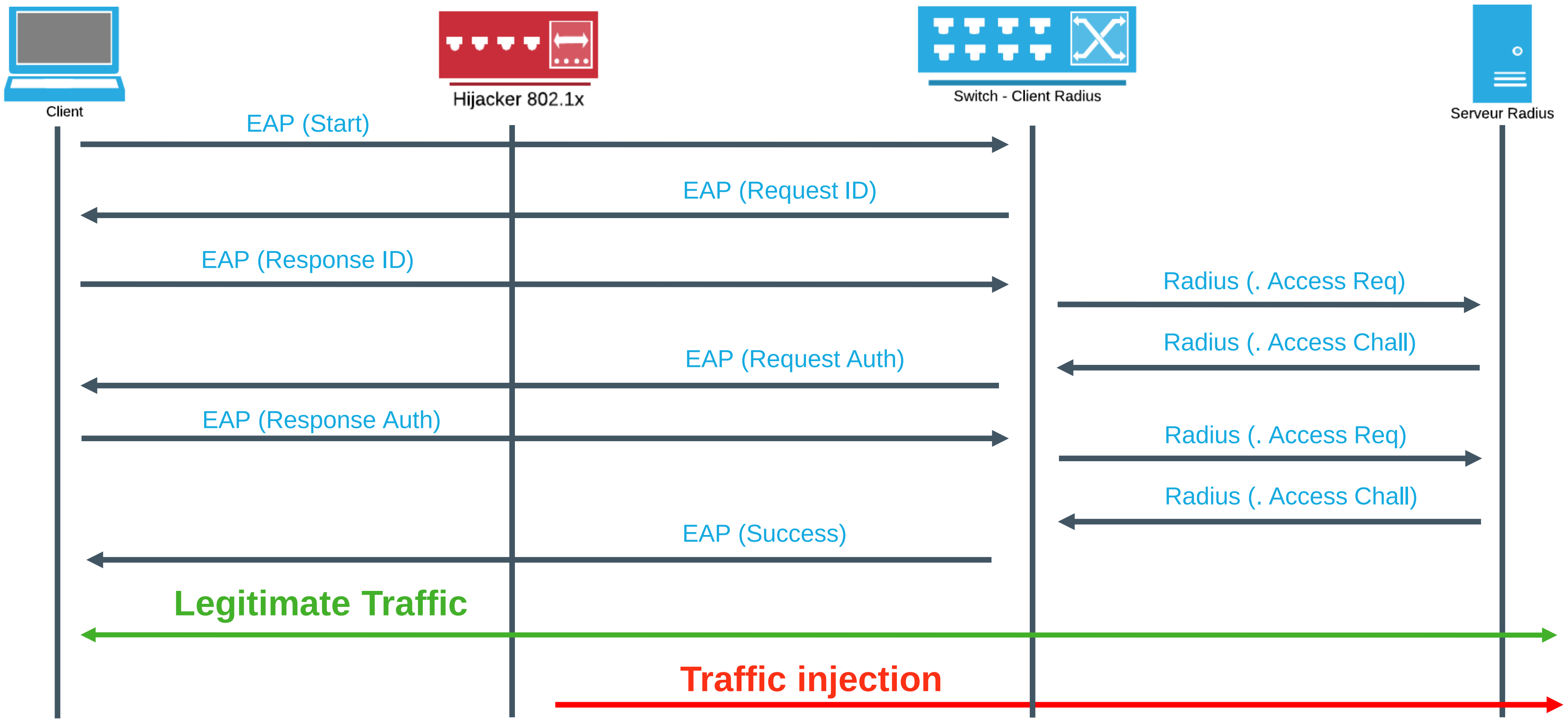
- Man In The Middle attack
  - Connection between the legitimate client and the switch
    - Frames are transparently forwarded
    - Especially the 802.1x authentication frames

- Injection of malicious packets within the legitimate traffic
  - By pretending to be the client
  - Possible due to the absence of packets authentication

- Recommendation to regularly request the authentication is useless



Man In The Middle on 802.1x



Source: copy goes here

SYNACKTIV DIGITAL SECURITY

Live Demo