



WILLIAM & MARY

CHARTERED 1693

CSCI 667: Concepts of Computer Security

Prof. Adwait Nadkarni

Wireless Security



Wireless makes network security much more difficult

- Wired:
 - If Alice and Bob are connected via a wire, Eve can only eavesdrop if she has physical access to that wire* (exceptions?)
- Wireless:
 - Everybody shout (broadcast) as loud as you can
 - Friendly to eavesdropping



Evil Toaster
(with wireless card)



Access Point



Internet

Infrastructure mode



Evil Toaster
(with wireless card)



Internet

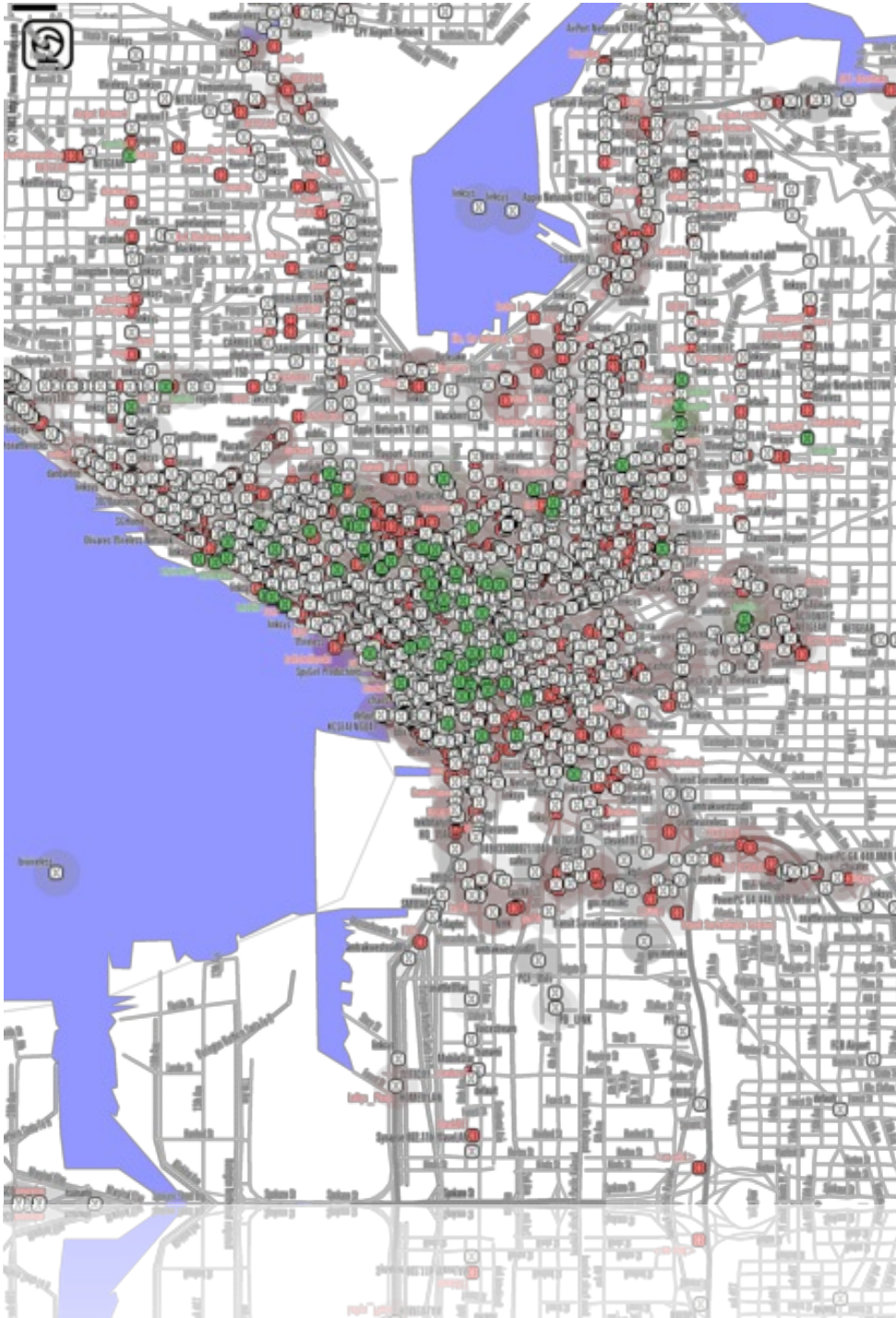
Ad hoc mode

Finding wireless networks is easy

- wardriving
- warbiking
- warwalking
- warrailing
- warkitteh



(http://thehackernews.com/2014/08/how-to-weaponize-your-cat-to-hack-your_9.html)



Several online repositories
Check out <https://wgle.net/>

Wireless Networking: 50,000 ft view

- Protocols defined in IEEE 802.11 standards
- Access points (APs) may periodically broadcast *beacon frames* to advertise its presence (and some configuration parameters)
- Authentication:
 - client sends *authentication frame* to AP
 - if successful, client sends *association request frame* to AP, requesting allocation of resources
 - if successful, AP responds with *association response frame*
- Data sent via *data frames*
- Session Termination:
 - AP sends *disassociation frame* and *deauthentication frame*



Unsecured wireless:
Problem #1:
Everybody is the receiver.



Unsecured wireless:
Problem #2:
Any one can join.



MAC Filtering

The screenshot displays the Linksys Wireless-G ADSL Gateway web interface, specifically the 'Wireless Access' page. The interface is viewed through a Microsoft Internet Explorer browser window. The main page has a purple header with the Linksys logo and 'A Division of Cisco Systems, Inc.' The firmware version is 1.01.15. The navigation menu includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'Wireless' tab is selected, and the 'Wireless Access' sub-tab is active. The 'Wireless Network Access' section shows two radio buttons: 'Allow All' and 'Restrict Access'. The 'Restrict Access' option is selected. Below this, there are two sub-options: 'Prevent computers listed below from accessing the wireless network' and 'Permit only computers listed below to access the wireless network'. The 'Permit only' option is selected. A smaller window titled 'http://192.168.1.1 - MAC Address Access List - Microsoft Internet Explorer' is overlaid on the main page. This window displays the 'MAC Address Filter List' with a text input field for the MAC address format (xxxx:xx:xx:xx:xx:xx) and a table of 16 MAC addresses. The first row is filled with '00:91:4C:89:9E:D1'.

Wireless Access - Microsoft Internet Explorer

Address: http://192.168.1.1/Wireless_MAC.asp

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: 1.01.15

Wireless-G ADSL Gateway WAG54G V.2

Wireless

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings | Wireless Security | Wireless Access | Advanced Wireless Settings

Wireless Network Access

More...

☐ Allow All

☒ Restrict Access

☐ Prevent computers listed below from accessing the wireless network

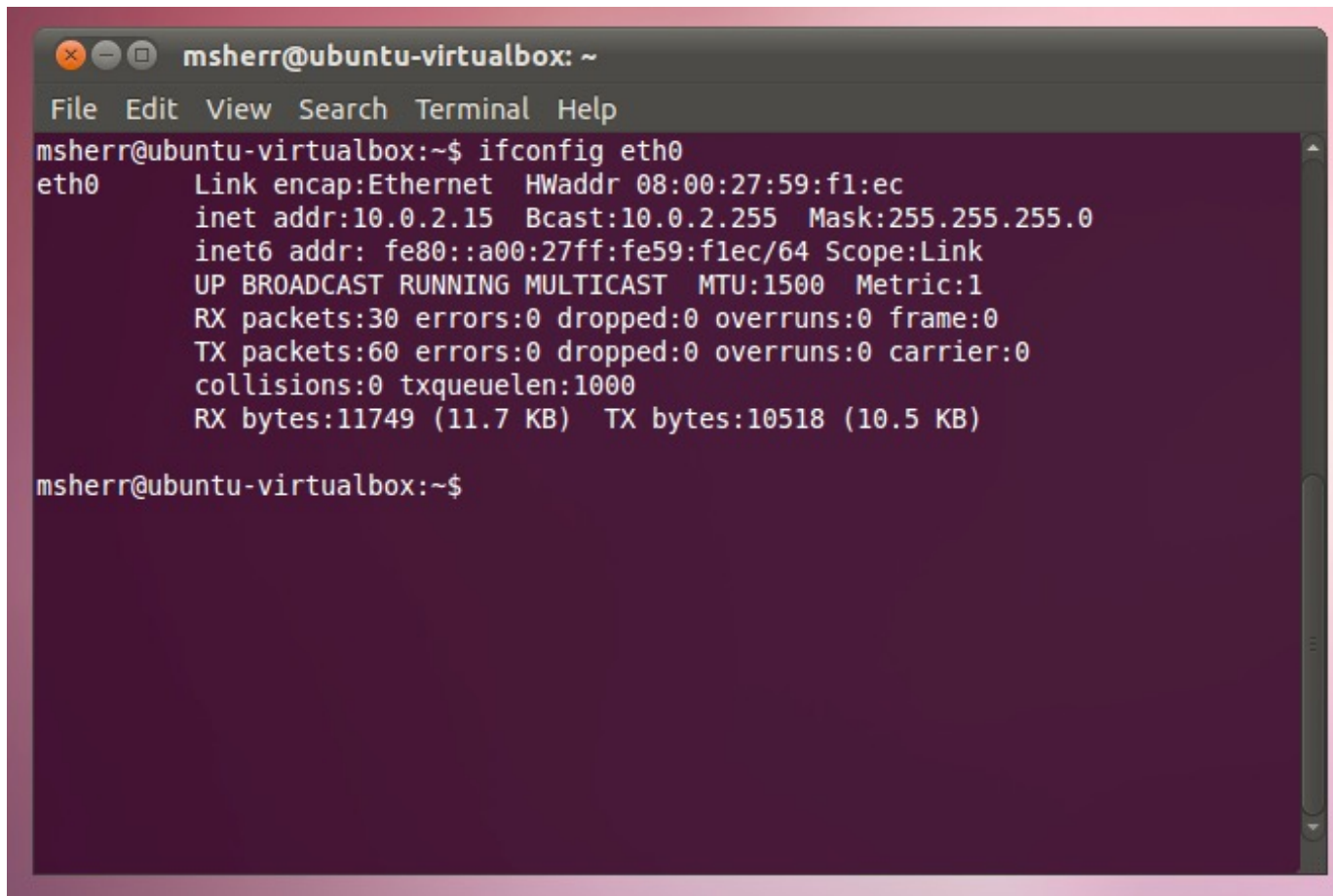
☒ Permit only computers listed below to access the wireless network

http://192.168.1.1 - MAC Address Access List - Microsoft Internet Explorer

MAC Address Filter List

Enter MAC Address Format: xxxxxxxxxx/xx:xx:xx:xx:xx:xx

MAC 01:	00:91:4C:89:9E:D1	MAC 11:	
MAC 02:		MAC 12:	
MAC 03:		MAC 13:	
MAC 04:		MAC 14:	
MAC 05:		MAC 15:	
MAC 06:		MAC 16:	

A terminal window titled 'msherr@ubuntu-virtualbox: ~' with a menu bar containing 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'ifconfig eth0' and its output. The output lists network details for the 'eth0' interface, including link type, hardware address, IP address, broadcast address, netmask, IPv6 address, and various statistics like MTU, metric, and packet counts. The prompt 'msherr@ubuntu-virtualbox:~\$' is visible at the bottom.

```
msherr@ubuntu-virtualbox: ~  
File Edit View Search Terminal Help  
msherr@ubuntu-virtualbox:~$ ifconfig eth0  
eth0      Link encap:Ethernet  HWaddr 08:00:27:59:f1:ec  
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe59:f1ec/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:11749 (11.7 KB)  TX bytes:10518 (10.5 KB)  
  
msherr@ubuntu-virtualbox:~$
```

```
msherr@ubuntu-virtualbox: ~  
File Edit View Search Terminal Help  
msherr@ubuntu-virtualbox:~$ sudo ifconfig eth0 hw ether 00:12:34:56:78  
msherr@ubuntu-virtualbox:~$ ifconfig eth0  
eth0      Link encap:Ethernet  HWaddr 00:12:34:56:78:00  
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe59:flec/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:64 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:24452 (24.4 KB)  TX bytes:14003 (14.0 KB)  
  
msherr@ubuntu-virtualbox:~$
```

SSID hiding

- APs broadcast **Service Set Identifiers (SSIDs)** to announce their presence
- In theory, these should identify a particular wireless LAN
- In practice, SSID can be anything that's 2-32 octets long
- To join network, client must present SSID
- Crappy security mechanism for preventing interlopers:
 - Don't advertise SSID
 - Problem:
 - To join network, client must present SSID
 - This is not encrypted, even if network supports WEP or WPA

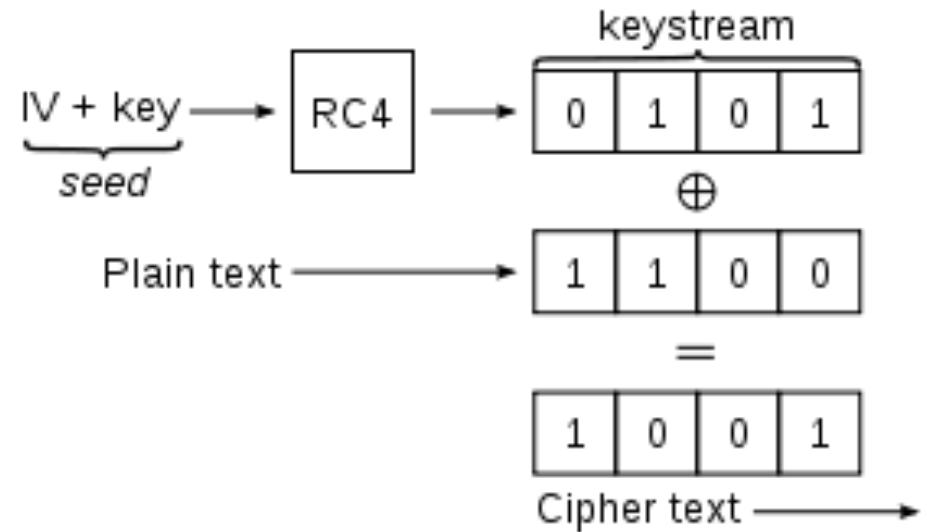
Wireless Security

Let's sprinkle on some of that
crypto magic sauce

Wired Equivalent Privacy (WEP)

- Part of original 802.11 standard
- Uses stream cipher:
 - Stream cipher crypto
 - $C = M \oplus S$, where S is pseudo-random sequence produced using a key K and an IV
 - $M = C \oplus S \rightarrow (M \oplus S) \oplus S = M$
- WEP uses RC4: supports seed up to 256 bits
 - seed = 24-bit IV + WEP key
- In WEPv1, key was 40 bits \Rightarrow 64bit seed
- Later versions supported seeds of 128 and 256 bits

Wired Equivalent Privacy (WEP)



- Data transmission:
 - Produce keystream S using RC4 with seed function $f(K, IV)$
 - $C = M \oplus S$
 - send (IV, C) frames
 - knowledge of IV and K sufficient to decrypt C

WEP Authentication Modes

- **Open System:**

- client doesn't need to provide any credentials
- immediate association with access point
- but can only send and receive info if using correct key

- **Shared Key:**

- client must prove knowledge of WEP key before associating
- AP sends client plaintext challenge; response is challenge encrypted with the correct key
- Q: Which is more secure?

WEP Shared Key Vulnerability

- Random Challenge: “jk4533hfdsa9”
- Response: $\{IV, \text{“jk4533hfdsa9”} \oplus RC4(K,IV)\}$
 - here, $RC4(K,IV)$ denotes RC4 encryption using a key derived from key K and IV
- Eavesdropper can observe plaintext challenge and encrypted response, and can produce:
 - $\text{challenge} \oplus \text{response} = RC4(K,IV)$
 - $RC4(K,IV)$ sufficient to authenticate:
 - next challenge: “abcdef”
 - Eve responds (without knowing K!): $\{IV, \text{“abcdef”} \oplus RC4(K,IV)\}$

WEP Problems: IV Collisions

- IVs are too small... likely collision(s) after a few hours
- when IVs are the same, two ciphertexts can be xor'ed together to produce the xor of the plaintexts
 - statistical analysis will then yield plaintexts
 - redundancy in IP packets makes this easy!
 - knowledge of protocols further limits the possibilities
 - or, attacker sends message thru Internet to a wireless client in a manner that will result a known response (e.g., ping message)
- if multiple messages share same IV, once one is recovered, others can be trivially/immediately recovered --**WHY?**

WEP Problems:

Exploiting RC4 Weaknesses

- RC4 has a weakness: first few bytes of keystream are sometimes not particularly random looking [Fluhrer, Mantin and Shamir Attack; 2001]
- Mathematical result: Given enough keystreams, it's possible to construct the key [ciphertext-only attack]
- Attacker's goal: Get a lot of keystreams!
 - Basic approach: replay a bunch of ARP packets
 - AP will respond to replayed ARP
 - Sufficient number of AP's encrypted packets will yield key
- An aside: standard RC4 fix: discard first n bytes of keystream (usually $n \geq 3072$)

Story Time: TJX Data Breach



- TJX (TJMaxx + Marshalls + Bob's) main database compromised in 2007
 - ~94M credit and debit cards stolen
 - one of nation's largest (2nd only to Heartland Payment Systems -- 130M!)
- Scanning devices, cash registers, and PCs in Minnesota Marshalls wirelessly communicated to server, which communicated to backend database
- Wireless data encrypted using WEP
- WEP key stolen from MN parking lot. Uh-oh.
- **Lesson: Don't use WEP!**

Wi-Fi Protected Access (WPA)

- Engineered to be the “secure replacement” for WEP
- Authentication stages:
 - Shared secret used to derive encryption keys
 - Client authenticates to AP
 - Encryption keys are used to produce keystreams for encrypting traffic

Wi-Fi Protected Access (WPA)

- Two Modes:
 - **PSK (Pre-shared Key):**
 - also called “WPA Personal”
 - shared secret manually entered into all devices
 - designed for home use
 - **802.1x Mode:**
 - also called “WPA Enterprise”
 - authentication handled by backend service (e.g., RADIUS server) via Extensible Authentication Protocol (EAP)
 - may make use of certificates or other authentication techniques
 - e.g., SaxaNet

Wi-Fi Protected Access (WPA)

- Encrypting Traffic (2 confidentiality protocols):
 - **Temporal Key Integrity Protocol (TKIP):**
 - uses RC4, but designed to improve upon WEP's shortcomings
 - increases size of IV to 48 bits
 - rather than just concatenate IV, uses more complex key mixing routine

Wi-Fi Protected Access (WPA)

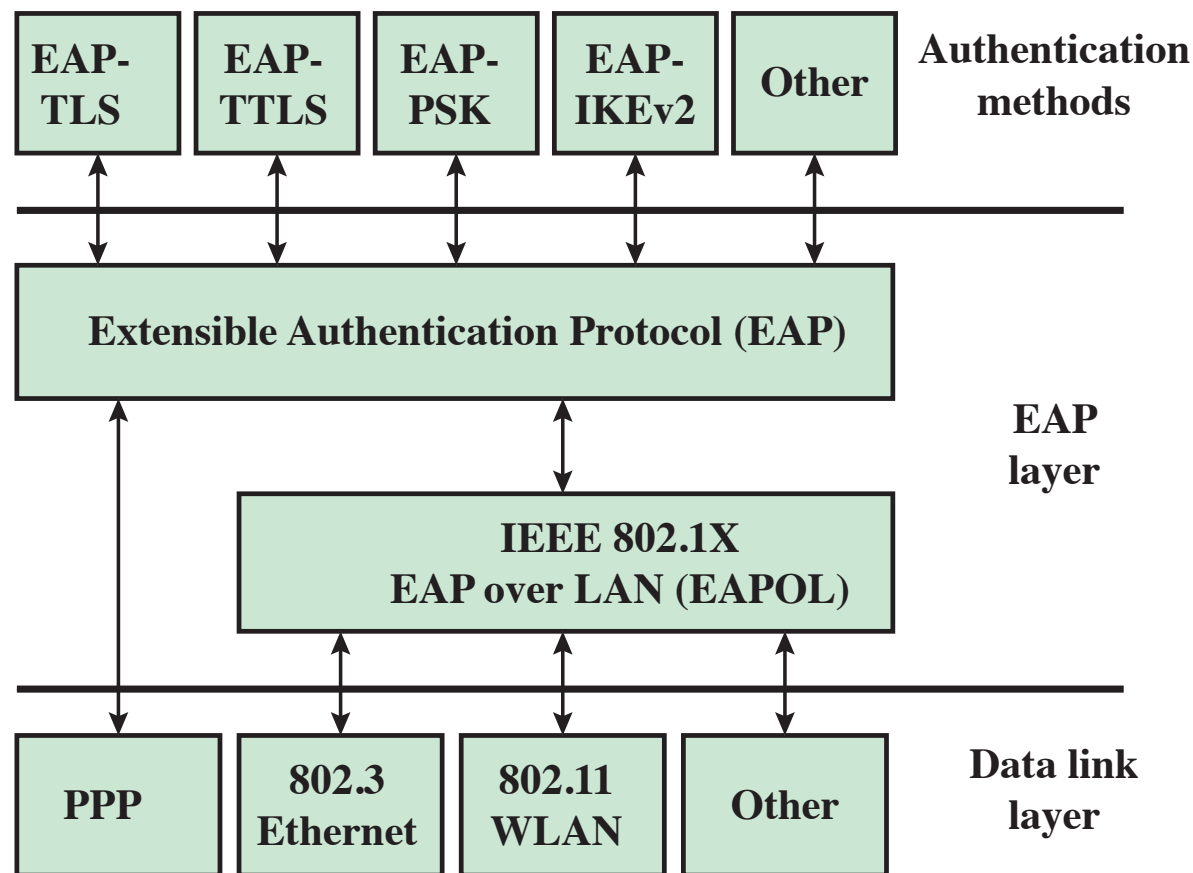
- Encrypting Traffic (2 confidentiality protocols):
 - **AES:**
 - supported in newer WPA2 protocol
 - runs AES in stream-cipher like way (e.g., using something similar to counter mode)

Attacks against WPA

- WPA is a lot stronger than WEP
- Most attacks rely on weak passwords
 - user-supplied keys are either entered as 256-bit string (64 hex digits) or as password
 - password is hashed to produce key using 4096 iterations of HMAC-SHA1 with SSID of AP as salt
 - there exists dictionaries of pre-hashed keys for most popular SSIDs (“linksys”, “redsox”, etc.)

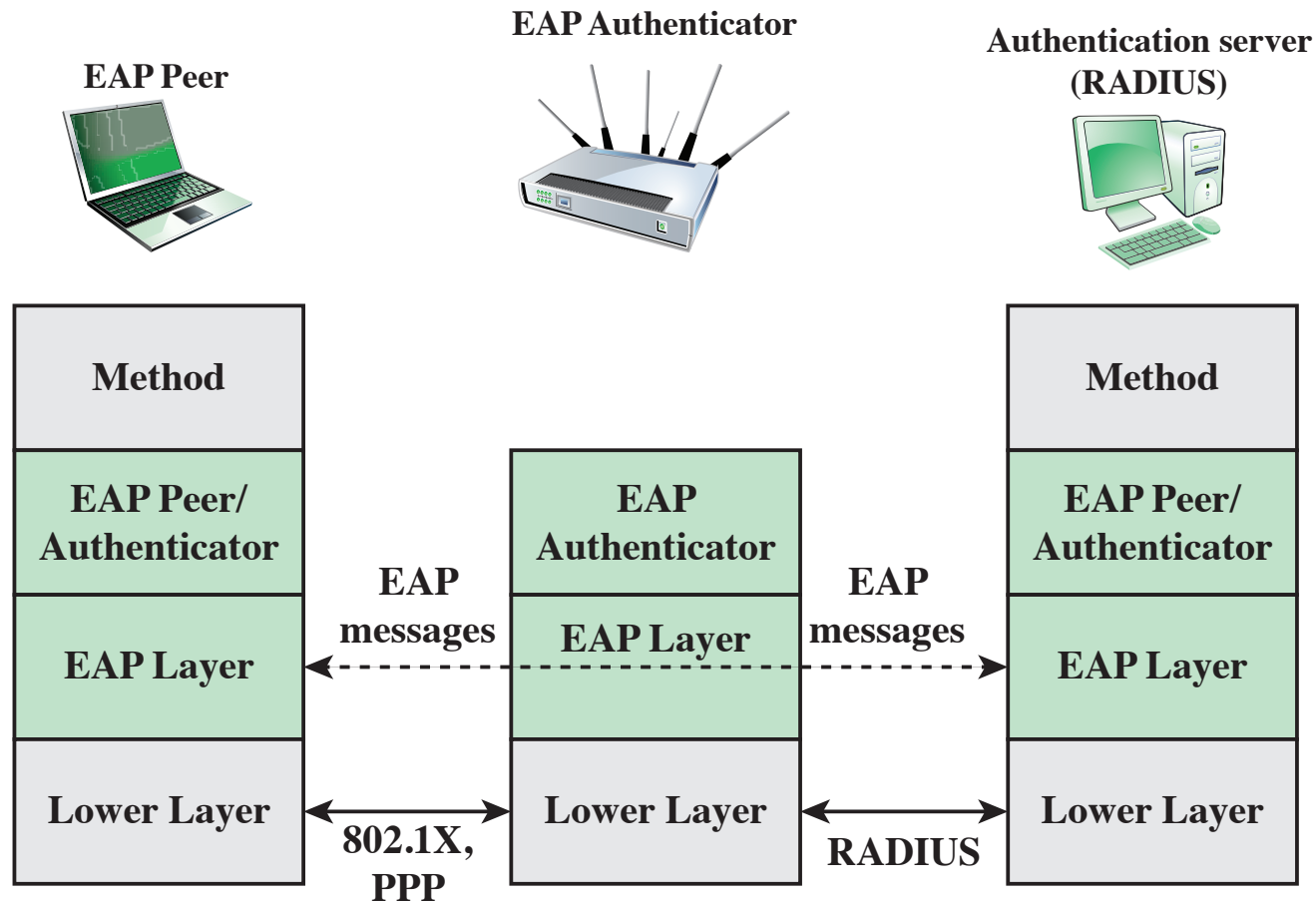
EAP Authentication

- WPA Enterprise using 802.1x for authentication



(from Stallings, Crypto and Net Security)

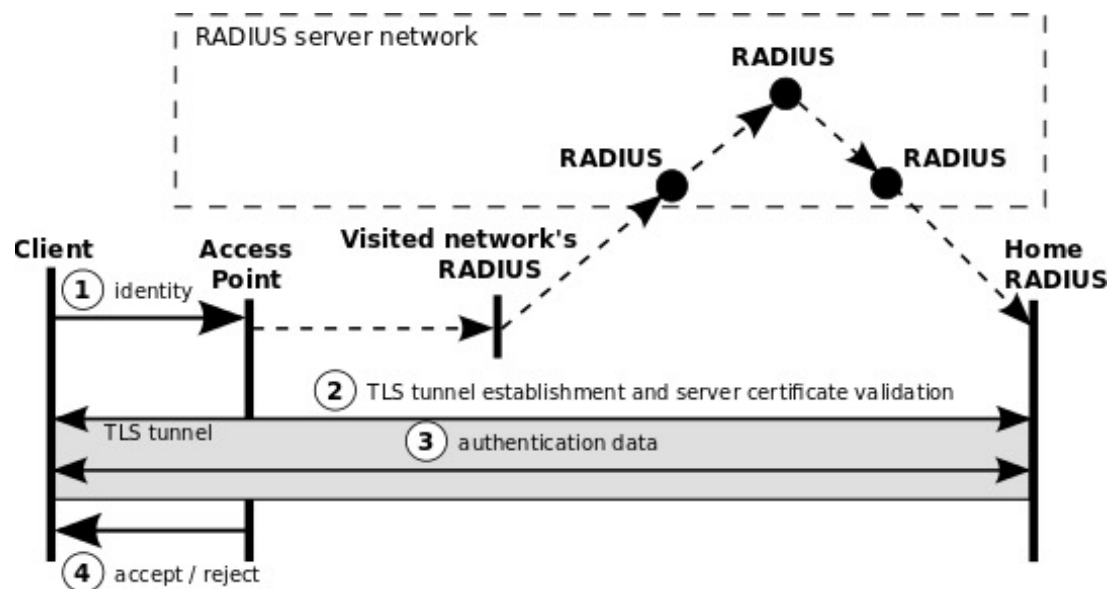
EAP Authentication



(from Stallings, Crypto and Net Security)

Eduroam

- Many campuses have started deploying Eduroam for WiFi (UVA, Vtech has it, we may get it soon:
<https://www.eduroam.us/node/3489>)
 - Better than MAC address-based authentication (based on 802.1x protocol)
 - Allows you to access WiFi at other universities



(<https://web.syssec.ruhr-uni-bochum.de/eduroam/>)

Eduroam Config Woes

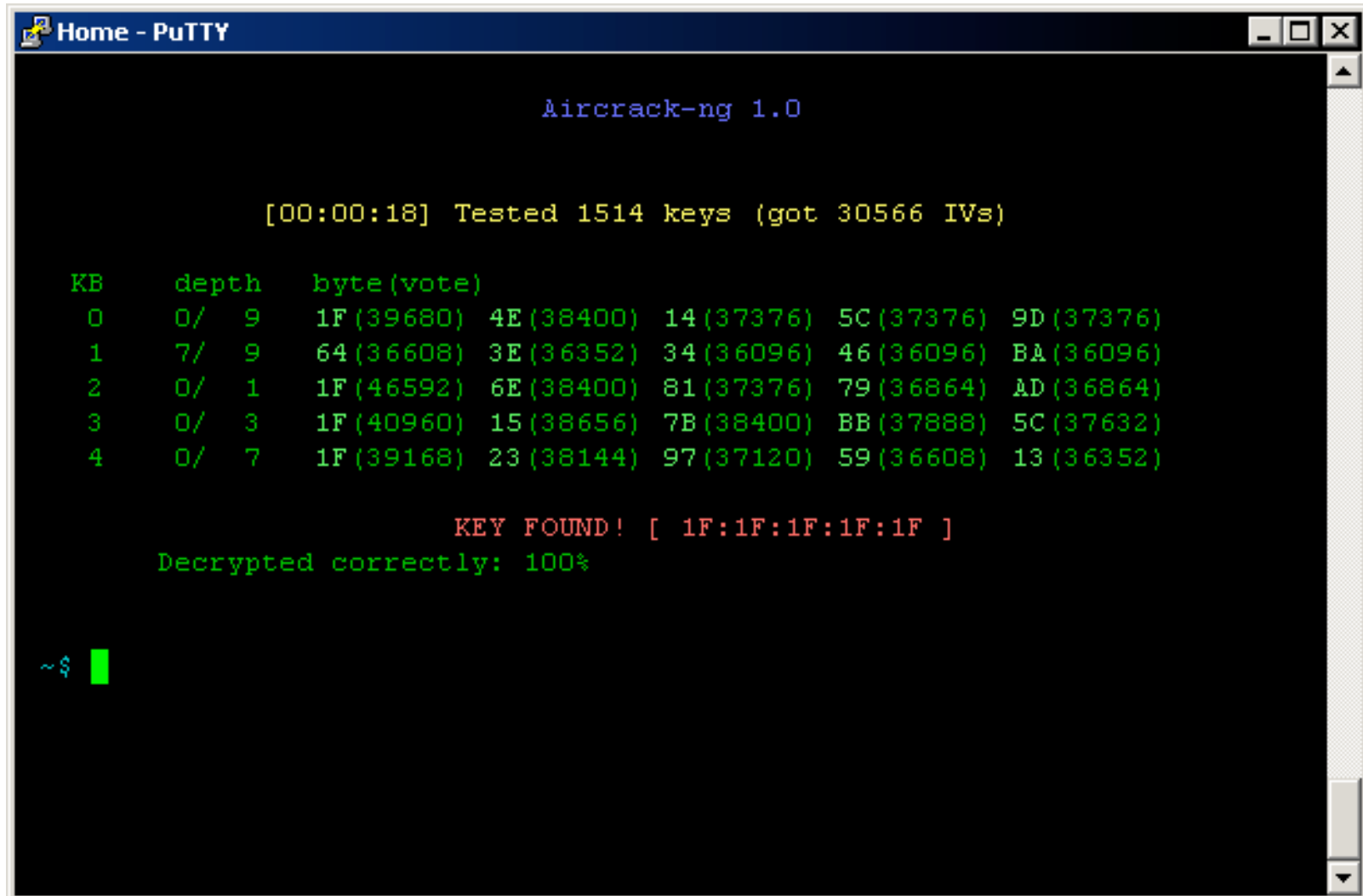
- Brenza et al. “A Practical Investigation of Identity Theft Vulnerabilities in Eduroam.” WiSec 2015.
- <https://web.syssec.ruhr-uni-bochum.de/eduroam/>
- Found that many Eduroam clients contain configuration errors
 - Root CA not set, so any certificate pushed by the AP will be valid. (Configure your root CA!)
 - Deficient certificate validation / Missing server name check / common name check
 - Often problem with the platform
- Enables Evil Twin attack (associating with rogue AP), which can result in
 - Eavesdropping or modifying traffic
 - Exposure of passwords (arguably more severe)

Password Exposure

- The most common authentication method in Eduroam uses TLS to create a secure tunnel for password authentication
 - PEAP or EAP-TTLS for the tunnel
 - Password authentication via
 - EAP-PAP: cleartext password
 - EAP-MSCHAPv2: challenge response, but can still brute-force passwords (known to be a weak protocol)
 - *However, we have misconfigured clients*
- Use EAP-TLS
 - **Why does this help?**
 - MITM, but no threat of password exposure.

Practical Attacks

Plenty of tools available (usually exploit RC4 weakness)



```
Home - PuTTY

Aircrack-ng 1.0

[00:00:18] Tested 1514 keys (got 30566 IVs)

KB    depth  byte(vote)
0      0/   9   1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376)
1      7/   9   64(36608) 3E(36352) 34(36096) 46(36096) BA(36096)
2      0/   1   1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864)
3      0/   3   1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632)
4      0/   7   1F(39168) 23(38144) 97(37120) 59(36608) 13(36352)

KEY FOUND! [ 1F:1F:1F:1F:1F ]
Decrypted correctly: 100%

~$
```

MitM with airbase-ng

```
AIRBASE-NG(1) 1. sh AIRBASE-NG(1)

NAME
airbase-ng - multi-purpose tool aimed at attacking clients as opposed to the Access
Point (AP) itself

SYNOPSIS
airbase-ng [options] <interface name>

DESCRIPTION
airbase-ng is multi-purpose tool aimed at attacking clients as opposed to the Access
Point (AP) itself. Since it is so versatile and flexible, summarizing it is a chal-
lenge. Here are some of the feature highlights:
- Implements the Caffe Latte WEP client attack
- Implements the Hirte WEP client attack
- Ability to cause the WPA/WPA2 handshake to be captured
- Ability to act as an ad-hoc Access Point
- Ability to act as a full Access Point
- Ability to filter by SSID or client MAC addresses
- Ability to manipulate and resend packets
- Ability to encrypt sent packets and decrypt received packets

The main idea is of the implementation is that it should encourage clients to associate
with the fake AP, not prevent them from accessing the real AP.

A tap interface (atX) is created when airbase-ng is run. This can be used to receive
decrypted packets or to send encrypted packets.

As real clients will most probably send probe requests for common/configured networks,
```



Roll over image to zoom in



GL.iNet GL-MT300N-V2(Mango)

**Portable Mini Travel Wireless Pocket
VPN Router - WiFi Router/Access
Point/Extender/WDS | OpenWrt | 2 x
Ethernet Ports | OpenVPN/Wireguard
VPN | USB 2.0 Port | 128MB RAM**

[Visit the GL.iNet Store](#)

4.2 ★★★★★ 9,911 ratings

| 539 answered questions

13 Price Changes

-23% \$30⁹⁰

List Price: \$39.90

✓prime

FREE Returns

With **Amazon Business**, you would have **saved \$178.89** in the last year. [Create a free account](#) and **save up to 15%** today.

May be available at a lower price from [other sellers](#), potentially without free Prime shipping.

Brand	GL.iNet
Model Name	GL-MT300N-V2
Special Feature	Access Point Mode
Frequency	Dual-Band

https://www.amazon.com/GL-iNET-GL-MT300N-V2-Repeater-300Mbps-Performance/dp/B073TSK26W/ref=psdc_300189_t1_B01AL7P1FU

Jamming

- Wireless signals are subject to jamming
- **Analog Jamming:** decrease signal-to-noise ratio by flooding with radio waves
 - basic techniques easy to detect -- just listen for jamming signals
 - more advanced techniques leverage features of the communication system (e.g., FM) to undetectably jam
 - standard defense: spread spectrum
- **Digital Jamming:** exploit multiplexing scheme to consume all channel bandwidth

