Remarks on

Wireless Security and Man-in-the-Middle attacks

Sebastian Büttrich, IT University Copenhagen / NSRC

edit: March 2013, ICTP Trieste

Reminder:
Aspects of IT Security

- Confidentiality
- Integrity
- Availability
- Authenticity

and more ...

“Wireless Security”

- The term “wireless security” is most often used as synonym for “keeping unwanted users out of your network” & “encrypting traffic”
- This addresses to some extent
  - Confidentiality
  - Integrity
  - Availability
- However,
  none of these are fully secured by “wireless security”!

“Wireless Security”

- The idea of “wireless security” seems to be changing: in the old days, it meant: “How do I keep the outsider out”?
- Today, often it means: “How do I keep the insider from taking all my bandwidth?”

“Wireless Security”

- When discussing “wireless security”, dont assume that the wired side is more secure
- Most threats are NOT specifically wireless
- Biggest threats today probably:
  - Windows computers
  - Virus/bots/trojans
  - Uncontrolled file sharing
  - Systems not prepared for high bandwidth connectivity and many dynamic users
  - BYOD

“Wireless Security”

- A healthy way of looking at security on the network level:
  - The network is *the streets and roads*
  - Many people and vehicles travel on these roads
  - Streets and roads are open, or mostly open – we don't lock people into their houses to secure a city
  - If we need to transport money from A to B – we use a protected vehicle (= **“end-to-end security”**)

Security measures you may as well forget

None of these offers any real security:

- Hidden / 'Closed' networks
- WEP encryption
- MAC address lists (though they can be useful in certain situations)

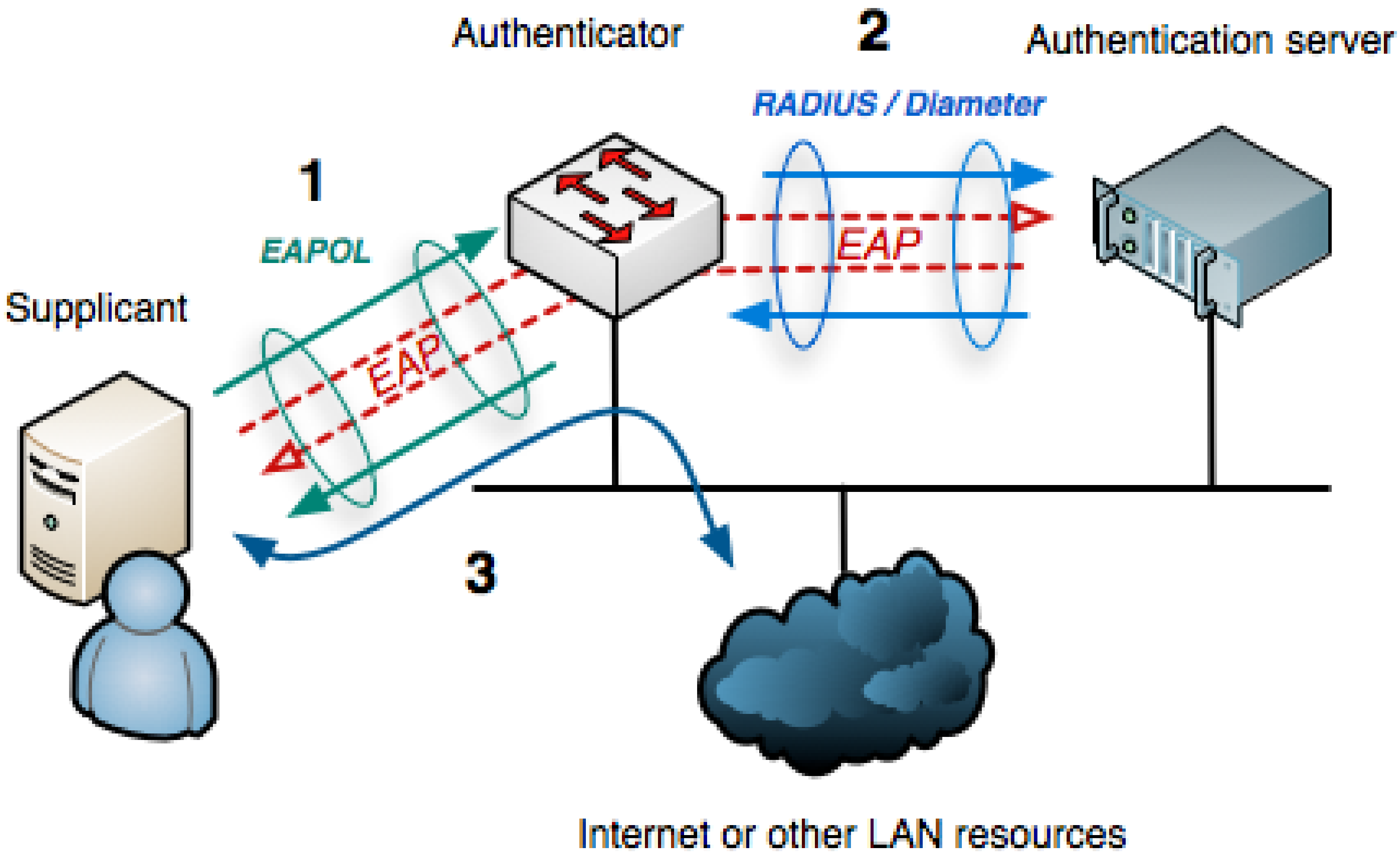
Security measures that work (to some extent)

- WPA2 – shared or personal
- 802.1x = EAP over wireless

  EAP = Extensible Authentication Protocol
- RADIUS (Remote Authentication Dial In User Service) often as manager for centralized Authentication, Authorization, and Accounting (AAA) management – it acts inbetween the user database and wireless Aps
- RADIUS protocol can talk to files, SQL, LDAP etc

How does RADIUS work

source: wikipedia



The reality of 802.1x

- Used in many universities and institutions. e.g. ICTP
- User credentials typically from a user database, e.g. LDAP, Active Directory (AD)
- RADIUS often used for Authentication, Authorization, and Accounting (AAA) management – it acts between the user database and the wireless APs

The reality of 802.1x

- Widely used e.g. in eduroam http://eduroam.org
- Typically used with protocols like

  TTLS or PEAP for the outer tunnel,

  MSCHAP, PAP, CHAP for inner authentication
- Problem: **all inner authentication methods are broken and crackable**

  see: http://wire.less.dk/?p=205

The reality of 802.1x

- Because the inner methods are broken, all **security depends on the outer tunnel** -
  this means, for TTLS a **certificate based approach**
- What is the reality of SSL certificates? Do clients validate them? Typically no!
- This user/client behaviour creates a vulnerability: **Man-in-the-Middle attacks**

Man-in-the-middle attacks

- Advanced attack and analysis tools, e.g. Pineapple
- Pineapple (with “Jasager” software) listens to all probe requests, mimicks the SSID and associates users
- **From there on, all your traffic is belong to me :)**

Demonstration

```
Wireless Access Points (* = current AP)

  ictp-open:        Infra, 00:11:21:ED:B6:C1, Freq 2412 MHz, Rate 54 Mb/s, Strength 35

  ictp-secure:      Infra, 00:11:21:ED:B6:C0, Freq 2412 MHz, Rate 54 Mb/s, Strength 34 WPA WPA2 Enterprise

  ICTP-SDU:         Infra, 00:15:6D:72:48:54, Freq 2437 MHz, Rate 54 Mb/s, Strength 37 WPA2

  *MarconiLab:      Infra, 00:15:6D:18:8F:F8, Freq 2452 MHz, Rate 54 Mb/s, Strength 100 WPA2

  alao:             Infra, 00:27:22:E6:53:2D, Freq 2412 MHz, Rate 54 Mb/s, Strength 98

  Lab_Test_01:      Infra, 00:27:22:E6:54:E6, Freq 2432 MHz, Rate 54 Mb/s, Strength 97 WPA2

  whyme:            Infra, 00:11:24:09:65:F9, Freq 2412 MHz, Rate 54 Mb/s, Strength 97 WPA2

  ictp-secure:      Infra, 00:15:6D:F6:14:0E, Freq 2412 MHz, Rate 54 Mb/s, Strength 100 WPA2 Enterprise
```

Note that we have two different kinds of hardware serving the SSID “ictp-secure” - one of them is in fact an attacker, in this case a harmless one (Sebastian).

It will offer 802.1x authentication, with its own RADIUS server (on Sebastians laptop), and if the client does not validate the certificate, it will willingly send its login to this server, where we can collect the packets, find the handshake dialogue, and crack it.

(rest of this session as live demo)

Questions? Comments?

sebastian@nsrc.org
http://nsrc.org

Sebastian Büttrich, NSRC