Wireless Network Authentication

Wireless Network Authentication

- We will be talking about the various models of network authentication on wireless network
- We will cover the protocols and mechanisms, as well as the architectures and components to implement it

Overview

- What are we trying to solve
- Protocols & Implementation (mechs) & Layers
- Ways to regulate access to the network (mech)
  - out of scope: MAC filtering, WEP/WPA
  - Captive portal
  - 802.1X (EAPoL and EAP-TLS)
- Architectural components
  - authentication server (Radius)
  - Access Point (authenticator)
  - Supplicant (module to authenticate)
- Non-tech aspects
  - Captive Portal vs 802.1x, Helpdesk, support issues

Basic Terminology

- Some basic terms
  - EAP – Extensible Authentication Protocol
  - PNAC – Port-based Network Access Control
  - Supplicant – a software application, installed on a user's computer, which submits credentials provided by the user, to an ”authenticator”
  - Authenticator – challenges, receives, processes, and replies to authentication requests from a supplicant

What is authentication ?

Let's agree:

Authentication is the process of verifying the claim that an entity is allowed to act on behalf of a given known identity

In plain speak:

- Is this person says who they say they claim to be ?

- Can they prove it (password, signature)

In this case, the entity is the software, acting on behalf of the user controlling the computer

Some core concepts

- Important to distinguish between the following concepts
  - confidentiality
  - access control
  - authentication
  - authorization

Some core concepts (2)

Confidentiality

- Ensure that only those who should have access to information can indeed do so (usually encryption)

Authorization & access control

- Authorization defines what an entity (here, a user, a device) is authorized (allowed), to access or do
- Which networks (ACLs/filters)
- Which systems, which files ? (FS ACLs, permissions)
- When can they log on (time policies) ?
- Can they send email ?
- Can they run this application ?

Access control are the mechanisms by which these rights and restrictions are controlled and enforced

What are we trying to solve

Require authentication so not anyone can access our wireless networks

We want to know WHO, WHERE(*), and WHEN

This is **NOT** the same as using password-based WEP/WPA encryption

- WEP/WPA keys can be shared between users
- No way to identify who has connected, where, and when

We want to know:

- Which user ?
- What area of the wireless network (AP) did they associate with ?
- When did they log on ?

What solutions do we have ?

WEP/WPA

- As explained, they only provide confidentiality at the network level, they do not tell us who is connected

MAC filtering

- Problem: doesn't identify a person
- Easily spoofed, and not a secret information

IP address

- Doesn't restrict physical access to the medium
- Easily spoofed

Captive portals

Captive portals

- Very popular (public areas, airports, hotels, …)
- Very flexible
- Self-explanatory (web page), can enforce AUP (Acceptable Use Policy) validation
- Easy to implement

Downsides:

- Not transparent
- Not standardized (different looks, different credentials, …)
- Requires regular re-authentication (disruptive)
- May require an external authentication server

Captive portals (2)

Many vendors and open source projects

- CoovaChilli, CoovaAP
- WiFidog
- M0n0wall, pfSense
- zeroshell

And many others

Many general networking vendors offer some form of integrated captive portals, e.g.

- Microtik
- HP
- Cisco
- Aruba
- Aptilo

802.1x & EAP

- ”Port-based Network Access Control” (PNAC)
- Originally designed for wired networks (EAPoL), but design accomodated for wireless networks
- RFC5216
- Layer 2 protocol
- 4 states:
    1. initialization (all traffic blocked – no DHCP or anything)
    2. initiation (authenticator sends EAP-Requests, and client responds with EAP-Response-Identity)
    3. negotiation of a method of authentication
    4. authentication if negotiation succeeds
- Traffic is allowed through

802.1x & EAP (2)

Advantages

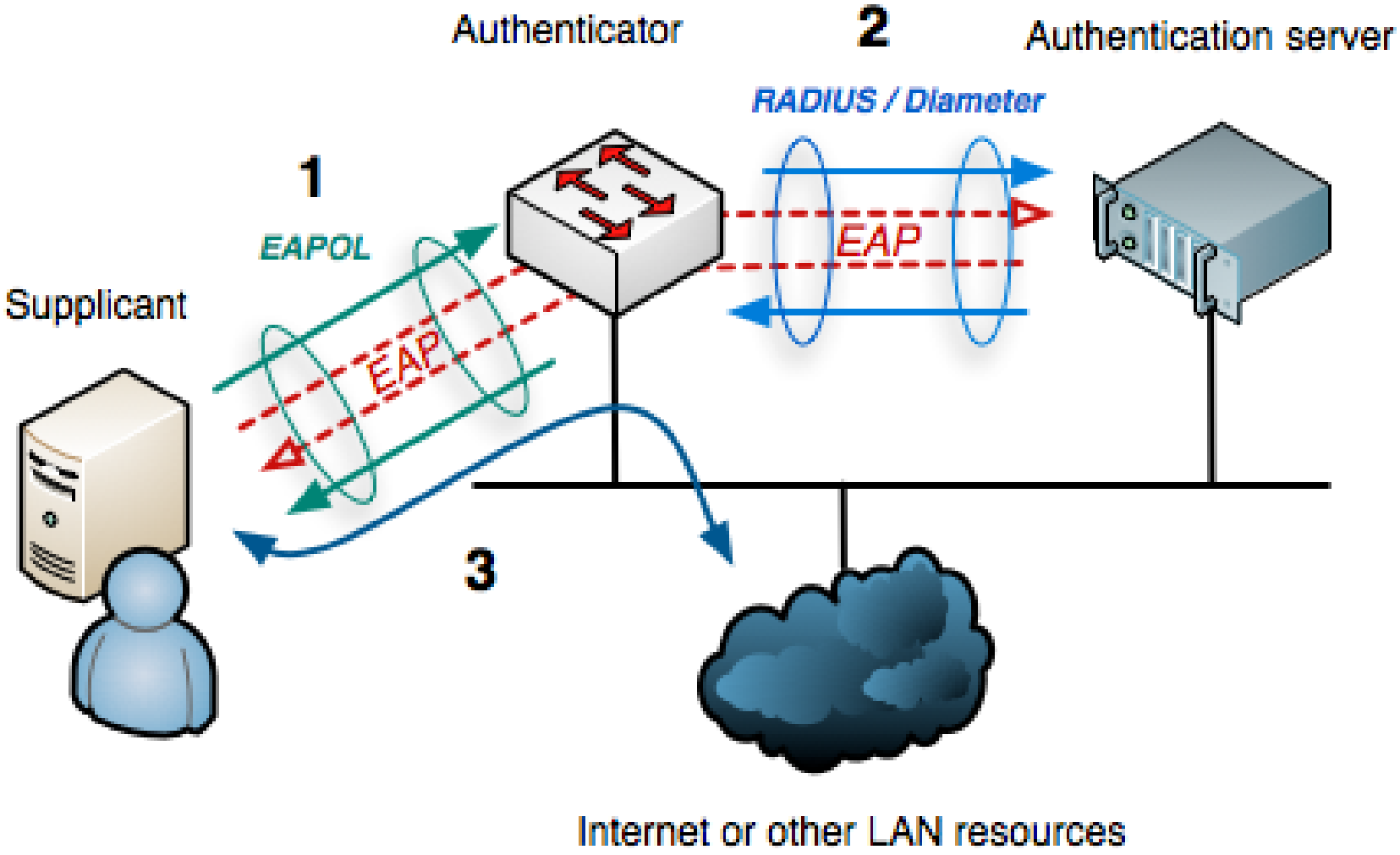
- transparent for Applications
- ”inline” - doesn't require interaction with upper layers like DHCP, IP, HTTP to function
- standardized for both wired and wireless LANs
- authentication mechanism is well known (MS-CHAP or PAP, from PPP/PPPoE)

Downsides

- may require new network equipment and/or firmware upgrade
- may require an external authentication server

How does it work

source: wikipedia



802.1x & EAP vs captive portals

They are complementary:

Captive portals may be preferable for networks, or parts of the network, where there are many non-regular, guest users

Captive portals can guide users, provide helpdesk contact information

802.1x is more streamlined – and standardized – making it preferable for known, pre-configured users

A combination of both may be useful

- 802.1x everywhere is possible, on LAN/WLAN (dedicated SSID)
- ”Guest”-style captive portal for the rest (different SSID)
- Captive portal remains more intuitive for first time users

… **if** it is your policy to have guests! (may not be the case)

802.1x & EAP vs captive portals - 2

Function at different levels

- 802.1x is layer 2 (0x888E frame type)
- Captive Portals use layers 3 - 7

Authentication backends & components

- SQL or LDAP
- Local flat text file
- Radius (which can use any of the above solutions)
- Backends can be shared between technologies (captive portal + 802.1x)

Wireless Network Authentication

Wireless Network Authentication

- We will be talking about the various models of network authentication on wireless network
- We will cover the protocols and mechanisms, as well as the architectures and components to implement it

Overview

- What are we trying to solve
- Protocols & Implementation (mechs) & Layers
- Ways to regulate access to the network (mech)
  - out of scope: MAC filtering, WEP/WPA
  - Captive portal
  - 802.1X (EAPoL and EAP-TLS)
- Architectural components
  - authentication server (Radius)
  - Access Point (authenticator)
  - Supplicant (module to authenticate)
- Non-tech aspects
  - Captive Portal vs 802.1x, Helpdesk, support issues

Basic Terminology

- Some basic terms
  - EAP – Extensible Authentication Protocol
  - PNAC – Port-based Network Access Control
  - Supplicant – a software application, installed on a user's computer, which submits credentials provided by the user, to an ”authenticator”
  - Authenticator – challenges, receives, processes, and replies to authentication requests from a supplicant

What is authentication ?

Let's agree:

Authentication is the process of verifying the claim that an entity is allowed to act on behalf of a given known identity

In plain speak:

- Is this person says who they say they claim to be ?
- Can they prove it (password, signature)

In this case, the entity is the software, acting on behalf of the user controlling the computer

Some core concepts

- Important to distinguish between the following concepts
  - confidentiality
  - access control
  - authentication
  - authorization

Some core concepts (2)

Confidentiality

- Ensure that only those who should have access to information can indeed do so (usually encryption)

Authorization & access control

- Authorization defines what an entity (here, a user, a device) is authorized (allowed), to access or do
- Which networks (ACLs/filters)
- Which systems, which files ? (FS ACLs, permissions)
- When can they log on (time policies) ?
- Can they send email ?
- Can they run this application ?

Access control are the mechanisms by which these rights and restrictions are controlled and enforced

What are we trying to solve

- Require authentication so not anyone can access our wireless networks
- We want to know WHO, WHERE(*), and WHEN
- This is **NOT** the same as using password-based WEP/WPA encryption
  - WEP/WPA keys can be shared between users
  - No way to identify who has connected, where, and when
- We want to know:
  - Which user ?
  - What area of the wireless network (AP) did they associate with ?
  - When did they log on ?

What solutions do we have ?

WEP/WPA

- As explained, they only provide confidentiality at the network level, they do not tell us who is connected

MAC filtering

- Problem: doesn't identify a person
- Easily spoofed, and not a secret information

IP address

- Doesn't restrict physical access to the medium
- Easily spoofed

Captive portals

Captive portals

- Very popular (public areas, airports, hotels, …)
- Very flexible
- Self-explanatory (web page), can enforce AUP (Acceptable Use Policy) validation
- Easy to implement

Downsides:

- Not transparent
- Not standardized (different looks, different credentials, …)
- Requires regular re-authentication (disruptive)
- May require an external authentication server

Captive portals (2)

Many vendors and open source projects

- CoovaChilli, CoovaAP
- WiFidog
- M0n0wall, pfSense
- zeroshell

And many others

Many general networking vendors offer some form of integrated captive portals, e.g.

- Microtik
- HP
- Cisco
- Aruba
- Aptilo

802.1x & EAP

- ”Port-based Network Access Control” (PNAC)
- Originally designed for wired networks (EAPoL), but design accomodated for wireless networks
- RFC5216
- Layer 2 protocol
- 4 states:
    1. initialization (all traffic blocked – no DHCP or anything)
    2. initiation (authenticator sends EAP-Requests, and client responds with EAP-Response-Identity)
    3. negotiation of a method of authentication
    4. authentication if negotiation succeeds
- Traffic is allowed through

802.1x & EAP (2)

Advantages

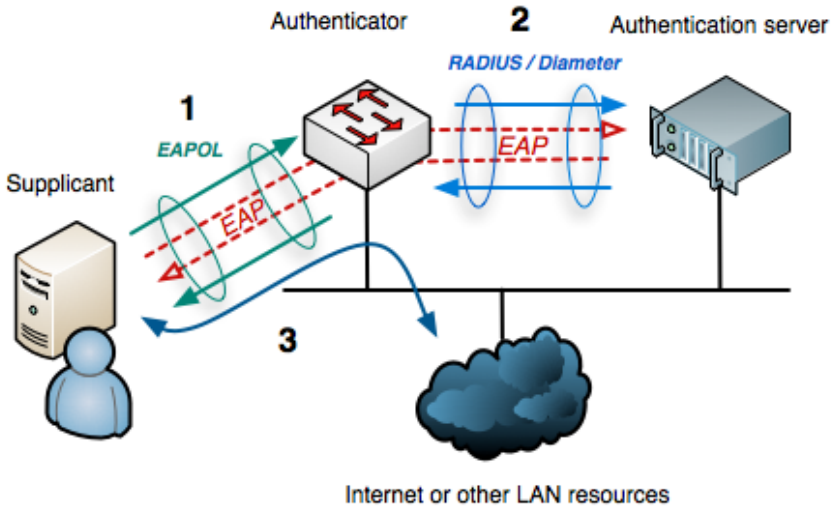
- transparent for Applications
- ”inline” - doesn't require interaction with upper layers like DHCP, IP, HTTP to function
- standardized for both wired and wireless LANs
- authentication mechanism is well known (MS-CHAP or PAP, from PPP/PPPoE)

Downsides

- may require new network equipment and/or firmware upgrade
- may require an external authentication server

How does it work

source: wikipedia



802.1x & EAP vs captive portals

They are complementary:

Captive portals may be preferable for networks, or parts of the network, where there are many non-regular, guest users

Captive portals can guide users, provide helpdesk contact information

802.1x is more streamlined – and standardized – making it preferable for known, pre-configured users

A combination of both may be useful

- 802.1x everywhere is possible, on LAN/WLAN (dedicated SSID)
- ”Guest”-style captive portal for the rest (different SSID)
- Captive portal remains more intuitive for first time users

… **if** it is your policy to have guests! (may not be the case)

802.1x & EAP vs captive portals - 2

Function at different levels

- 802.1x is layer 2 (0x888E frame type)
- Captive Portals use layers 3 - 7

Authentication backends & components

- SQL or LDAP
- Local flat text file
- Radius (which can use any of the above solutions)
- Backends can be shared between technologies (captive portal + 802.1x)