Wireless Authentication

Network Startup Resource Center
www.nsrc.org

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

What is Authentication?

Definition:

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

- More simply:
  - Is this person says who they say they claim to be ?
  - Can they prove it (for example, with password, signature)?
  - In our case, the entity is the software, acting on behalf of the user controlling the computer.

Why do we make it so complicated?

It is important to be aware of the differences:

- Just because I am on a certain computer, I am not necessarily its owner -
  the device is not the same as the person.
- Just because I am a certain person, I might not be in the right role to have access to a resource.
  For example:
  user@private.place.net
  is not the same as
  user@at.work.com

Some core concepts, 1

It is 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 do that (time policies) ?
  - Can they run an application or access a service ?
- Access control are the mechanisms by which these rights and restrictions are controlled and enforced

What we are trying to solve

- Require authentication so that
  We know WHO, WHERE(*), and WHEN
- This is NOT the same as using password based encryption (WPA2-PSK)
- 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 IP number did they have?

Solutions

- There are two recommended ways to do this:
  - Captive portal
  - **802.1X (EAPoL and EAP-TLS) – preferred solution**
- Your choice depends on
  - The size of your organization
  - The maturity of your IT systems
    - You will need user stores, databases (e.g. AD/LDAP)
  - Your human resources
    - system admin, helpdesk, support
  - And many other factors

Captive Portal, 1

- Plus
  - Popular (public areas, airports, hotels, …)
  - Flexible
  - Self-explanatory (web page), can enforce AUP (Acceptable Use Policy) validation
  - Relatively easy to implement
- Minus
  - Not transparent
  - Depend on browser
  - Not standardized (different looks, different credentials, …)
  - Requires regular re-authentication (disruptive)
  - Often unreliable and easy to break

Captive Portal, 2

To ”redirect” you to a welcome page,
any one of the following methods may be used:

- HTTP silent redirection
- HTTP 30x redirect
- IP hijacking
- DNS hijacking
- Certain URLs may be allowed
  - e.g Information page, help page, use policies

Captive Portal, 3

- Many vendors and open source projects
  - CoovaChilli, CoovaAP
  - WiFidog
  - M0n0wall, pfSense
  - zeroshell
- Many general networking vendors offer some form of integrated captive portals, e.g.
  - Mikrotik, HP, Cisco, Aruba, Aptilo, Ubiquiti

802.1x/EAP

- Often called WPA2 Enterprise
- Originally designed for wired networks (EAPoL), but design accommodated for wireless networks
- RFC5216
- Layer 2 protocol
  - 4 states:

    1. initialization (all traffic blocked – no DHCP or anything)

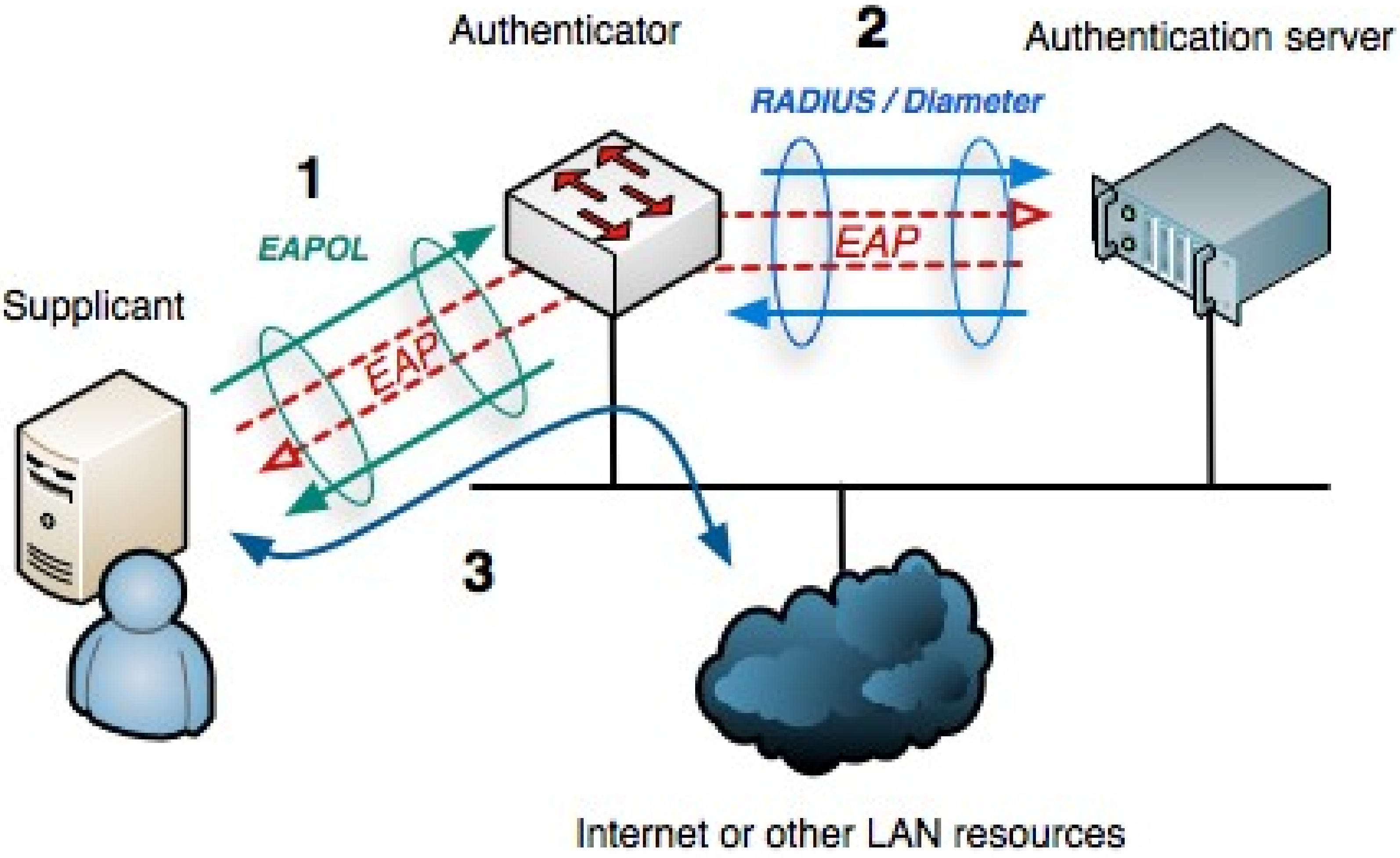
    2. initiation (authenticator sends EAP-Requests, and client responds with EAP-Response-Identity)

    3. negotiation of a method of authentication

    4. authentication if negotiation succeeds

    Traffic is allowed through

802.1x/EAP – How does it work



Source: Wikipedia

802.1x/EAP

- Plus
  - transparent for Applications
  - ”inline” - doesn't require interaction with upper layers like DHCP, IP, HTTP to function
  - standardized for both wired and wireless LANs
- Minus
  - More challenging in deployment
  - requires an external authentication server (Radius)

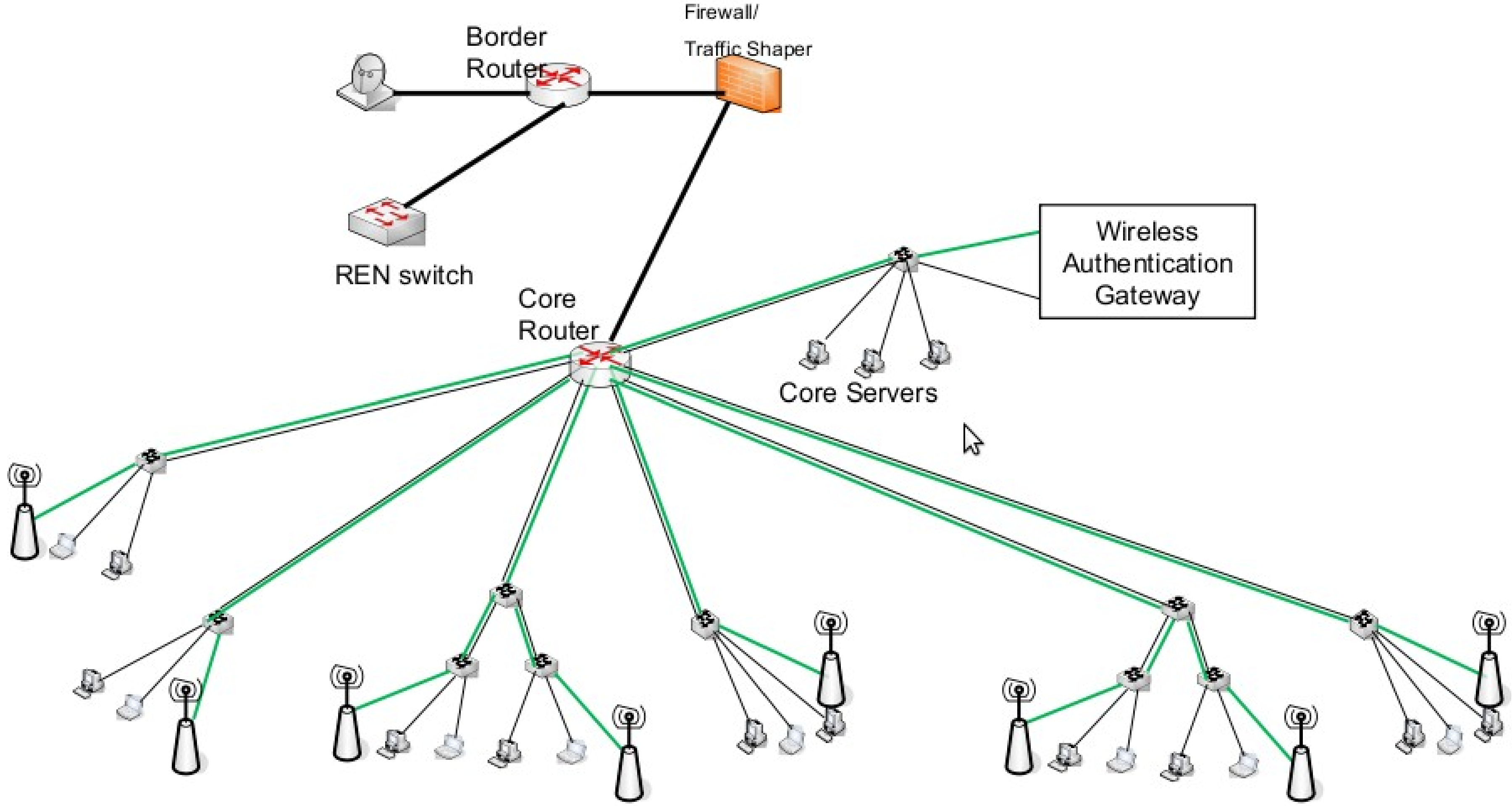
802.1x & EAP vs captive portals, 1

- 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 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 and guests

802.1x & EAP vs captive portals, 2

- 802.1x is layer 2,
  Captive Portals use layers 3 - 7
- Both need authentication backends:
  - SQL or LDAP/Active Directory
  - Can be local flat text file (only advisable for small organizations, or as start/test)
  - Backends can be shared between technologies (captive portal + 802.1x)
- AAA server **Radius -** can use any of the above solutions)

Central authentication backend on core network



Security issues of 802.1x

802.1x or WPA2/EAP is the recommended authentication option, but it has a big security problem too:

- Its outer tunnel security relies on TTLS/SSL certificates
- These are vulnerable to man-in-the-middle attacks – if the client device does not properly check the certificate, then it will give its credentials to ANY AP, e.g. rogue APs
- Its inner tunnel encryption is MSCHAP2, which is known to be broken/crackable

Source and scope of the security problem

The problem is essentially a SSL/TTLS implementation problem

- Clients often do not even check CN (server name that the certificate belongs to), or they trust ANY certificate from a given root (CA)
- Nothing can protect us against client devices with bad certificate check implementations.
- Another part of the problem is the inner tunnel: MSCHAP2 is crackable.

Addressing security issues of 802.1x

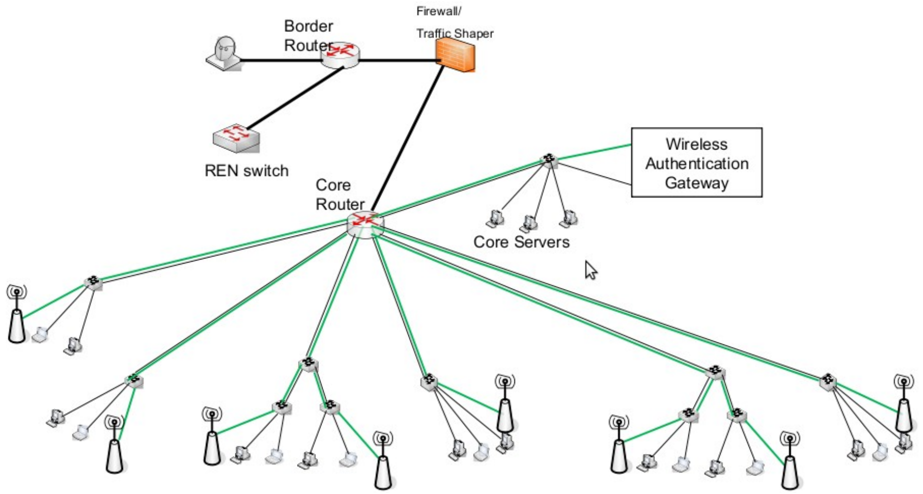
- We can enforce the best possible client configuration, for example by using the **eduroam CAT tool**, see https:/cat.eduroam.org
- See also security recommendations on https://wiki.geant.org/

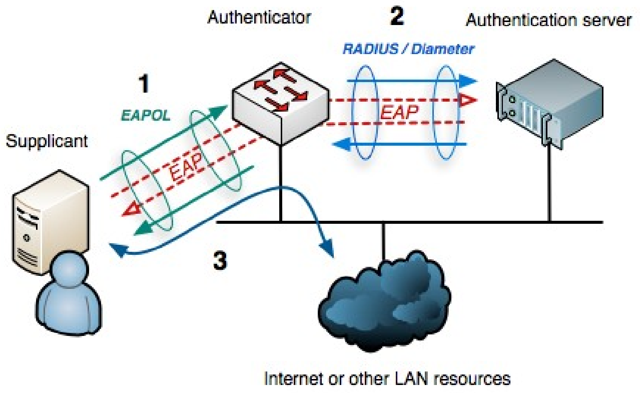
Demonstration of man-in-the-middle attacks on 802.1x

- Get user to associate to rogue AP and start handshake,
- Authentication process
- Packet dump everything
- Analyze the traffic, isolate the handshake
- The outer tunnel is easy – as the attacker owns certificate and keys
- The inner tunnel (typically MSCHAP2) can be cracked (via offline or online services)

NSRC recommendation for authentication

- User store in LDAP/AD, e.g. OpenLDAP
- RADIUS, e.g. freeradius
- Despite the security problems, **802.1x remains the best option** – with Captive Portal as a second option



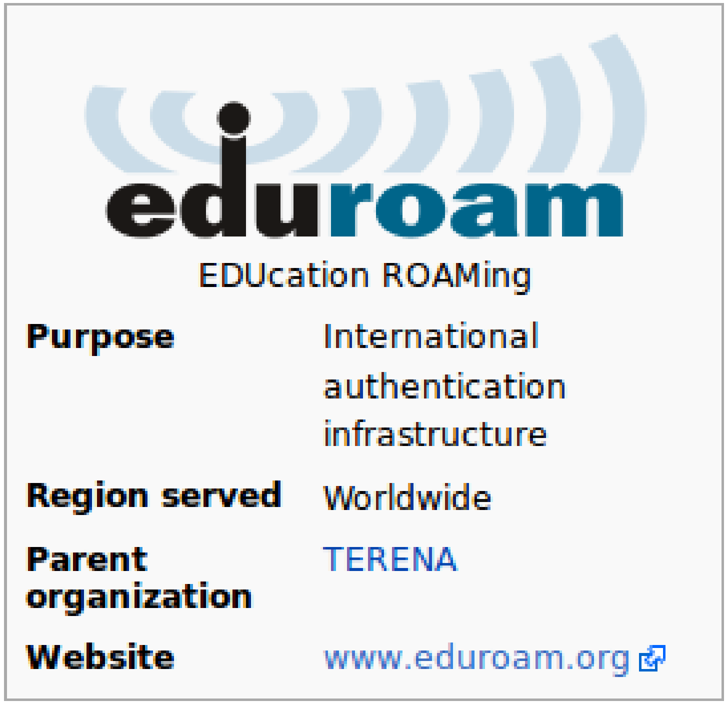


eduroam

- A recommended addition to your campus networks authentication is **eduroam,**

  an international roaming service
  for users in research,
  higher education
  and further education.

  Learn more at:



eduroam

EDUcation ROAMing

Purpose	International authentication infrastructure
Region served	Worldwide
Parent organization	TERENA
Website	www.eduroam.org