Wireless Authentication

Network Startup Resource Center
www.nsrc.org

What is Authentication?

- 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 are?
  - 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 Is It So Complicated?

- I am on a computer. Am I its owner?
  - Device is not the same as person.
- I am a network administrator
  - Should I have access to the finance system?
- I am connecting to the network from home
  - Should I have access to all my work resources?

Authentication Core Concepts

- These are all different concepts:
  - Confidentiality
  - Access Control
  - Authentication
  - Authorization

Confidentiality

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

Authorization

Authorization defines what an entity *(a user, a device)* is authorized *(allowed)*, to access

- 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

Access control is the mechanisms by which rights &restrictions are controlled & enforced

Why Do We Authenticate?

- We want to know: WHO, WHERE(*), WHEN
  - Which user?
  - What AP did they associate with?
  - When did they log on ?
  - What IP number did they have?
- PSK (Pre-Shared Key) cannot tell us this.
  - Keys can be shared between users
  - We can't know who, where, or when.

Authentication Solutions

- We recommended two ways to do this:
  - Captive portal
  - 802.1X (EAPoL and EAP-TLS) (Preferred)
- Your choice depends on
  - The size of your organization
  - The maturity of your IT systems
  - Your human resources
  - Available user stores, databases
    - For example, Active Directory or LDAP

Captive Portals: Positive

- Popular (public areas, airports, hotels…)
- Flexible
- Self-explanatory (web page), can enforce AUP (Acceptable Use Policy) validation
- Relatively easy to implement

Captive Portals: Negative

- Not transparent
- Depend on browser
- Not standardized (different looks, different credentials, …)
- Requires regular re-authentication (disruptive)
- Often unreliable and easy to break

Captive Portals: Redirection

- Any of the following methods can be used:
  - HTTP silent redirection
  - HTTP 30x redirect
  - IP hijacking
  - DNS hijacking
  - Certain URLs may be allowed
    - e.g. Information, help, use policies pages

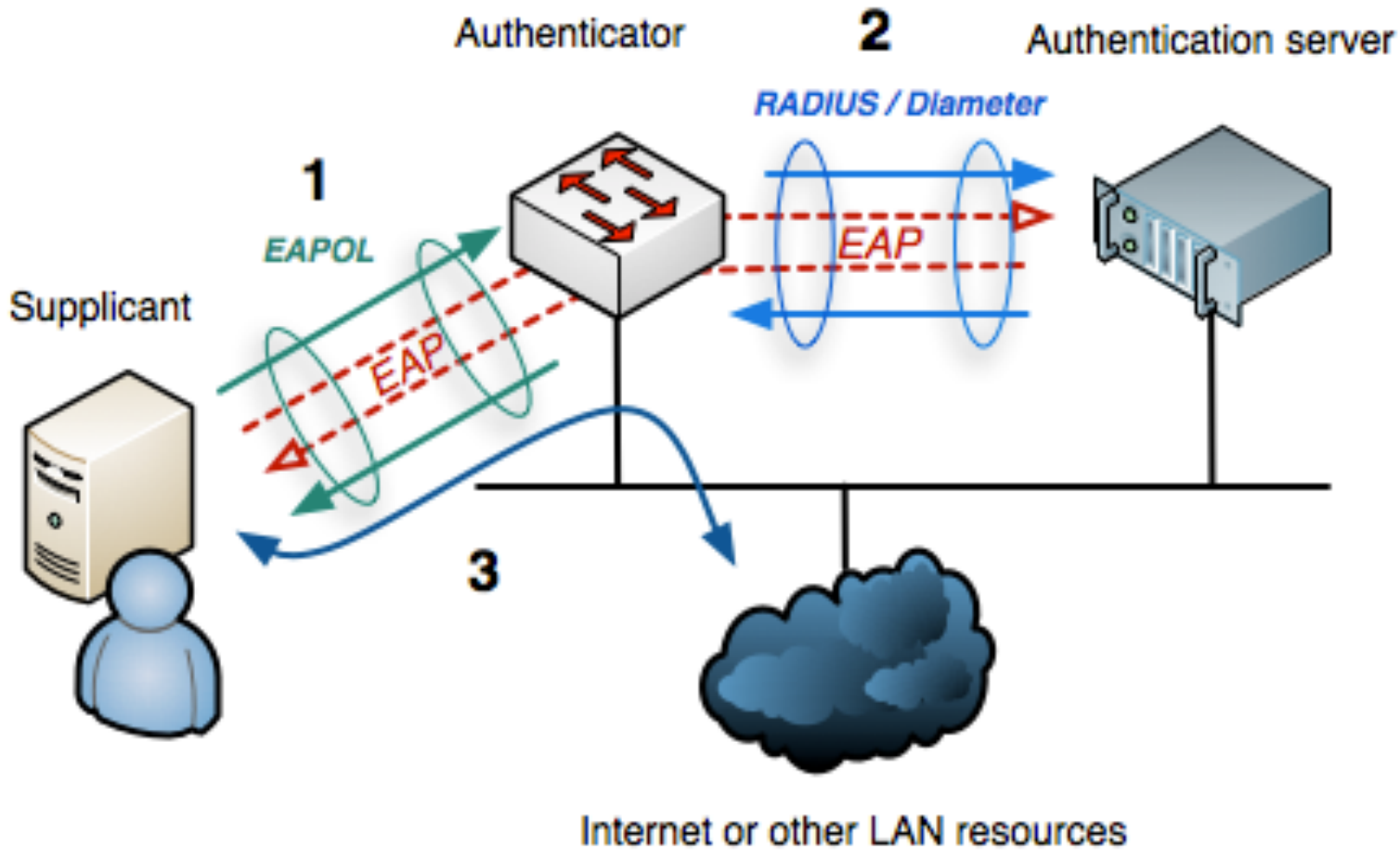
Captive Portals: Vendors

- Many vendors and open source projects
  - CoovaChilli, CoovaAP
  - WiFidog
  - M0n0wall, pfSense
  - zeroshell
- Many networking vendors offer captive portals
  - Aptilo, Aruba, Cisco, HP, Mikrotik, Ubiquiti

802.1x/EAP (WPA2 Enterprise)

- Originally designed for wired networks (EAPoL)
- Modified for wireless networks (RFC5216)
- Layer 2 protocol with 4 states:
  1. Initialization (all traffic including DHCP)
  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

- Positive
  - Transparent for Applications
  - In-line: does not require interaction with upper layers like DHCP, IP, HTTP to function
  - Standardized for both wired and wireless LANs
- Negative
  - More challenging in deployment
  - Requires external authentication server (RADIUS)

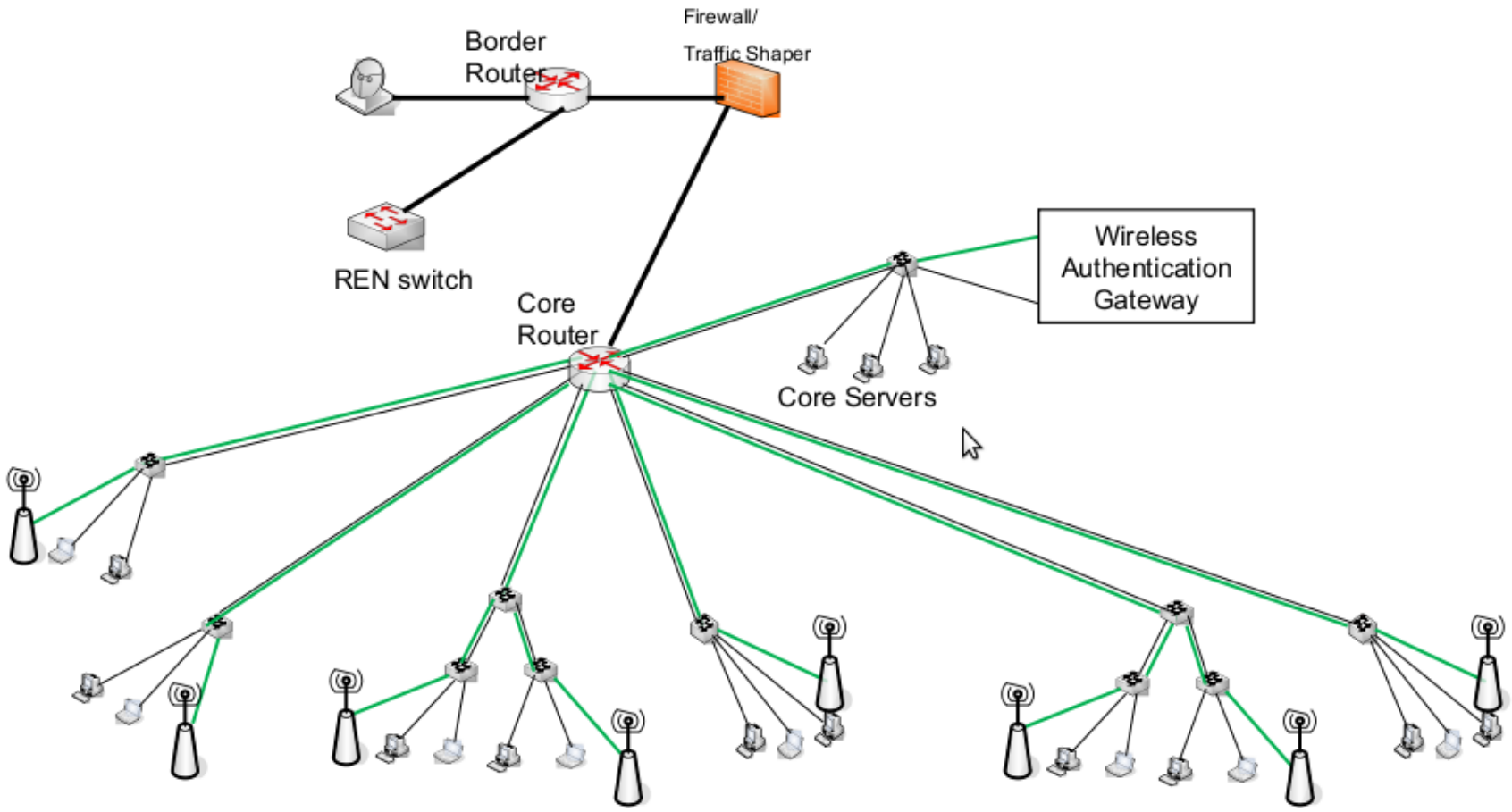
802.1x & EAP vs Captive Portals

- **Captive Portals**
  - Intuitive & easy for first time users and guests
  - Can guide guests, provide information & help
- **802.1x**
  - Is streamlined & standardized for regular access
    - Making it preferable for known users
  - But there's overhead for first-time users
- **Combining both may be useful**
  - 802.1x can be used on all LAN/WLAN
  - Captive portals can be used on guest Wi-Fi SSIDs

802.1x & EAP vs Captive Portals

- 802.1x operates at Layer 2
- Captive Portals operate at Layers 3-7
- Both need authentication back-ends:
  - SQL or LDAP/Active Directory
  - Can be local flat text file
    - (only for small organizations, or as start/test)
- Back-ends can be shared between technologies
  - (captive portal + 802.1x)
- **RADIUS** can use any of the above solutions

Authentication in the Core Network



802.1x Security Problems

- 802.1x or WPA2/EAP is the recommended authentication option, but has security problems
- Outer tunnels rely 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
- Inner tunnel authentication is MSCHAP2
  - MSCHAP2 is known to be compromised

802.1x Security Problems

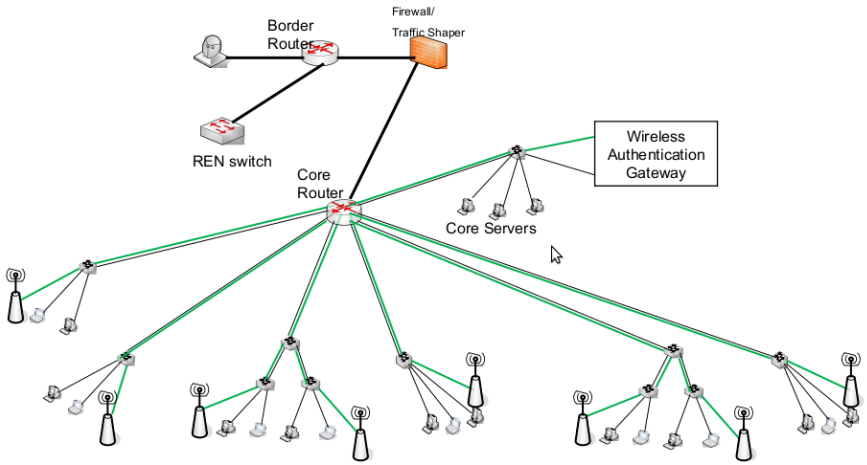
- Client devices that do not check certificates…
  - Will give their credentials to any AP, even a rogue one!
  - Are vulnerable to man-in-the-middle attacks.
- Nothing can protect clients that don't check…
  - CN (Common Name) or CA (Certificate Authority)
- However we can protect our networks
  - We can enforce the best possible client configuration, for example using the eduroam CAT tool. https://cat.eduroam.org
  - See also security recommendations on https://wiki.geant.org/

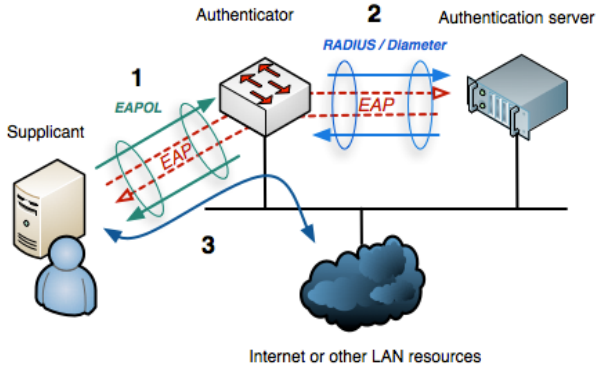
802.1x MITM Attack

- 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 Recommends

- User store in LDAP/AD, e.g. OpenLDAP
- RADIUS, e.g. FreeRADIUS
- Despite the security problems…
- **802.1x remains the best option**
- Captive Portal is a valid 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.org