802.1x Networking

tommEE pickles
Moloch Industries

Moloch.org

tommEE.net

Who am I
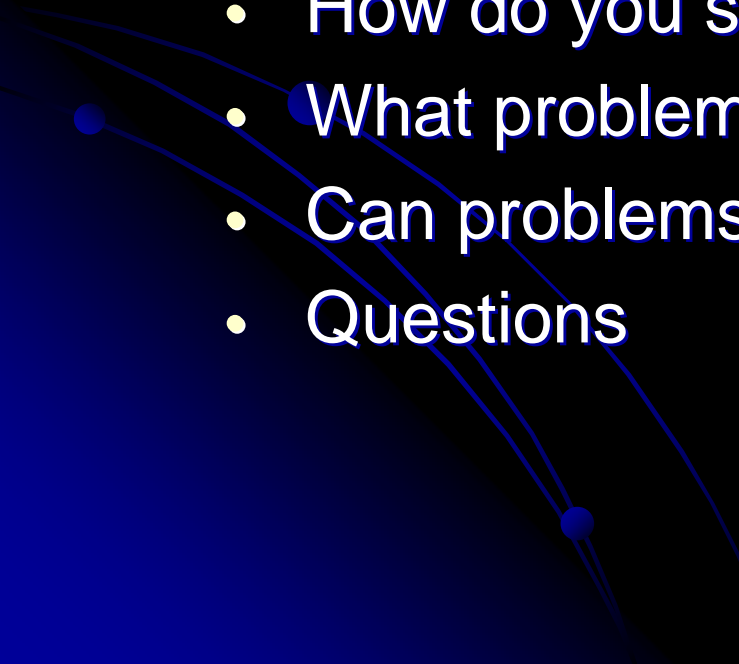
Fun:

Defcon Cannonball Run

Work:

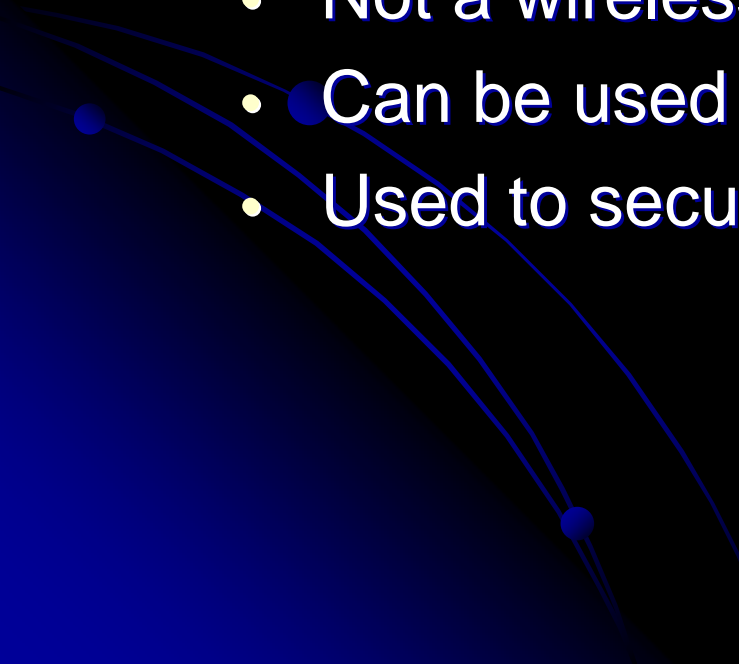15 Years in the grind (MTV, Google, Nature Magazine)

Whore:

TV and Speaking Engagements

Topics

- What is 802.1x?
- Why do we use it?
- How does it work?
- What is required?
- How do you set this up?
- What problems exist?
- Can problems be fixed?
- Questions

What is 802.1x?

- Port Based Network Access Control
  - 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network
- Not a wireless spec, applies to wired too
- Can be used for automatic VLAN assigning
- Used to secure access

Why do we use it?
wireless example

- WEP is insecure (as well as WPA-PSK)

- 802.1x/TKIP not open to replay attacks

- WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security

- WEP is easily broken, meaning the weak encryption standard with WEP is subject to eavesdropping on connections

- Corporate wireless must be secure as wired assets. *man in the van*

Example tools for hacking wireless

- Airsnort - http://airsnort.shmoo.com/
- Aircrack - http://www.wirelessdefence.org/Contents/AircrackMain.htm
- WepCrack - http://wepcrack.sourceforge.net/
- WepWedgie - http://sourceforge.net/projects/wepwedgie/
- There is even a video showing how easy it is to break WEP on a Apple laptop. The video is located at http://tinyurl.com/8w74k
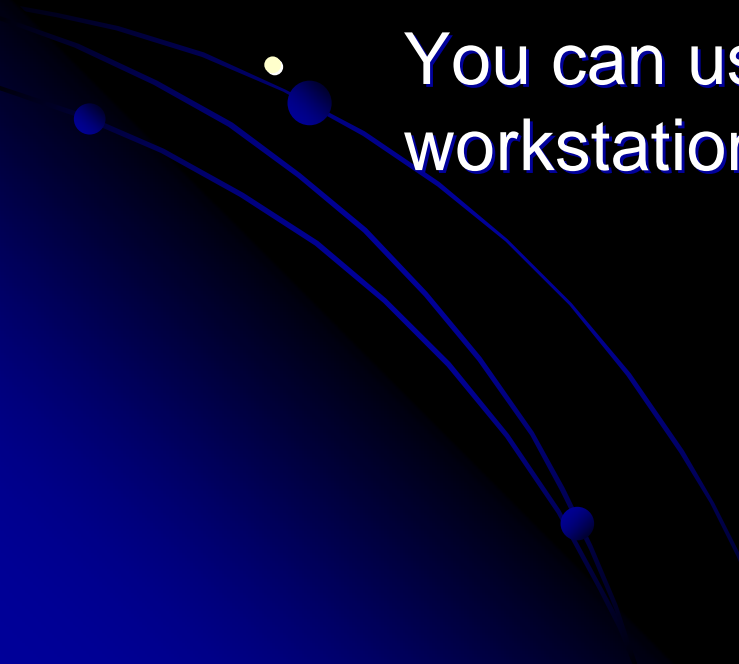
Why do we use it?
wired example

- Force unauthorized users into guest VLANs
- Automatically set network assets for wired employees in conference rooms, etc.
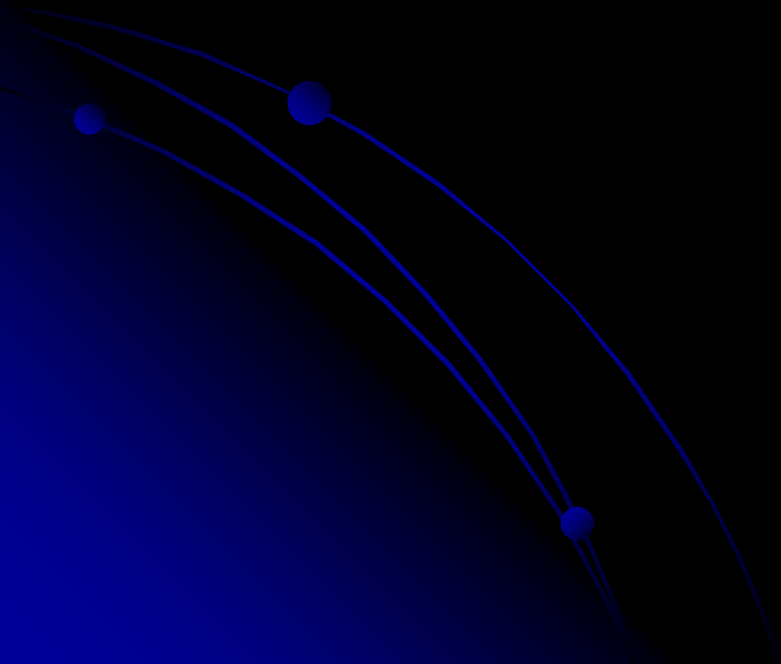
Why do we use it?
wired example cont...

- An Example
    - A company (e.g. Moogle) – Large enterprise
    - Has ~5000 employees
    - Sales, HR, IT departments
    - Multiple VLANs for departments
- You can use 802.1x to keep VLANs for workstations when moved.

What is required for an 802.1x network?

- Access Point or switch that supports 802.1x
- RADIUS (Authentication Server)
  - freeradius, Funk, RadiusNT, radiusX
- Client Software (supplicant)
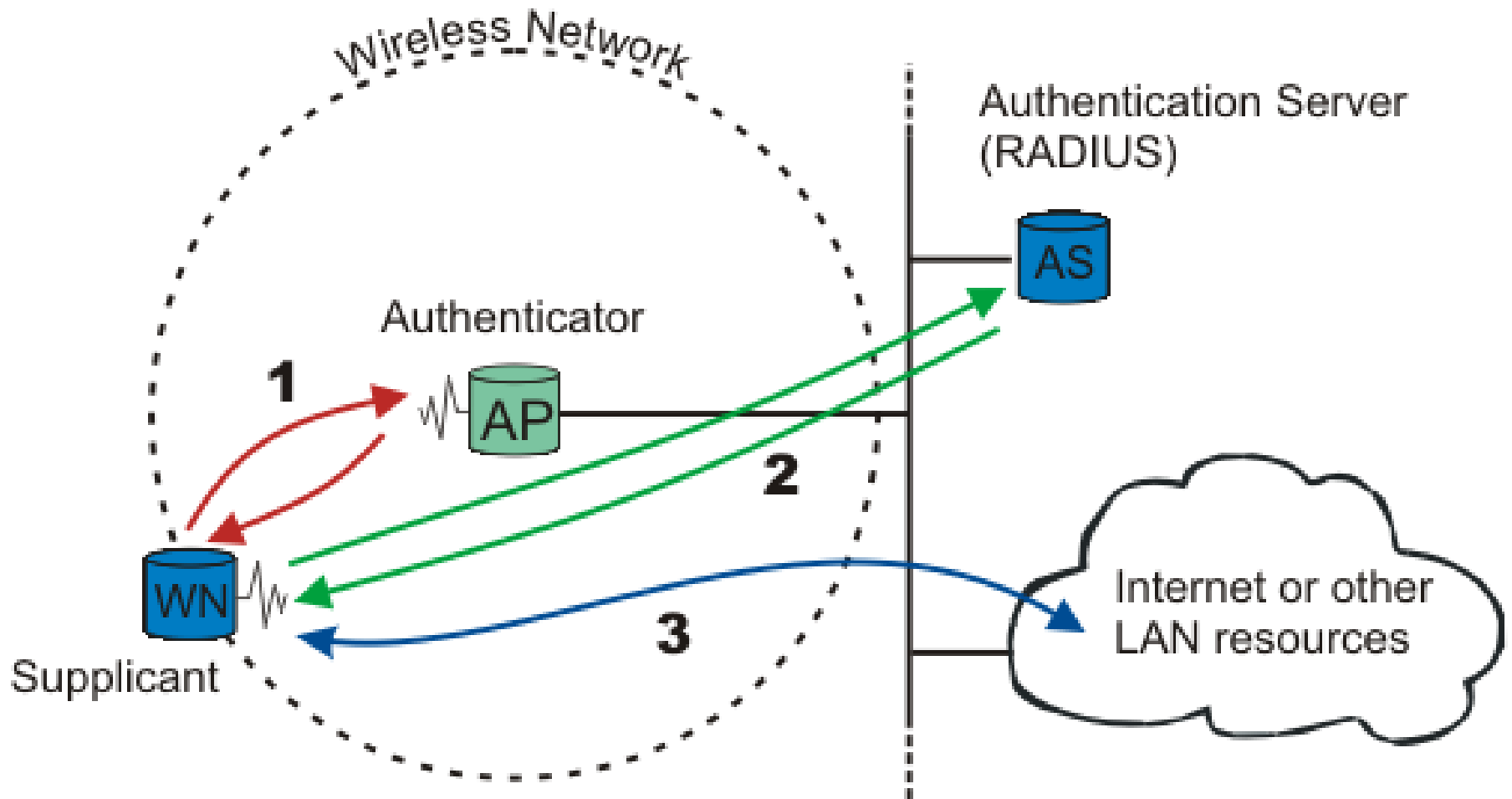 - Odyssey, XP, AEGIS, Xsupplicant, OSX
- Switched Environment

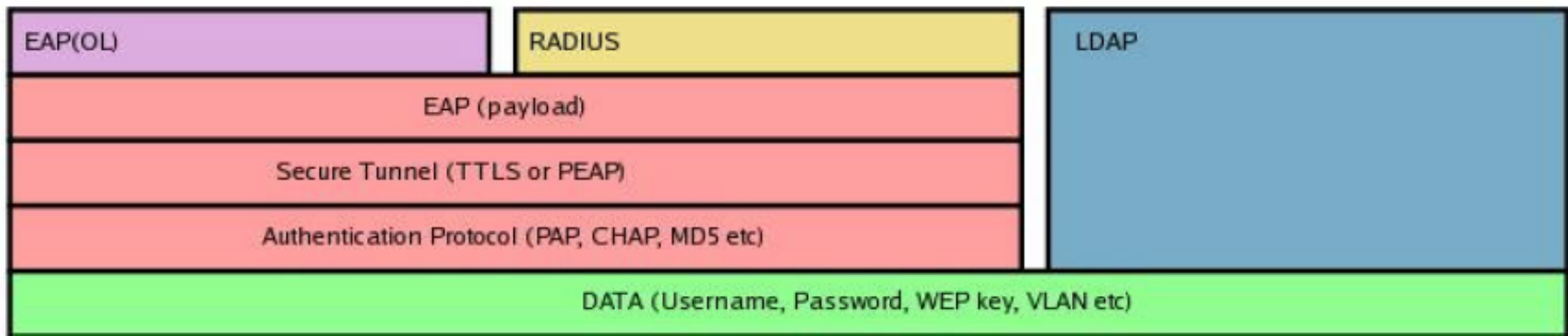# How does it work?
a wireless example

A connection is achieved is by 2 sets of security protocols. 802.1x first uses WPA encryption. This can either be PSK (Pre-shared Key) or TKIP (Temporal Key Integrity Protocol). After association, the AP sends authentication to the authentication server. The supplicant authenticates the user and workstation to network. This can be achieved by smart card, certificates or username-password combinations
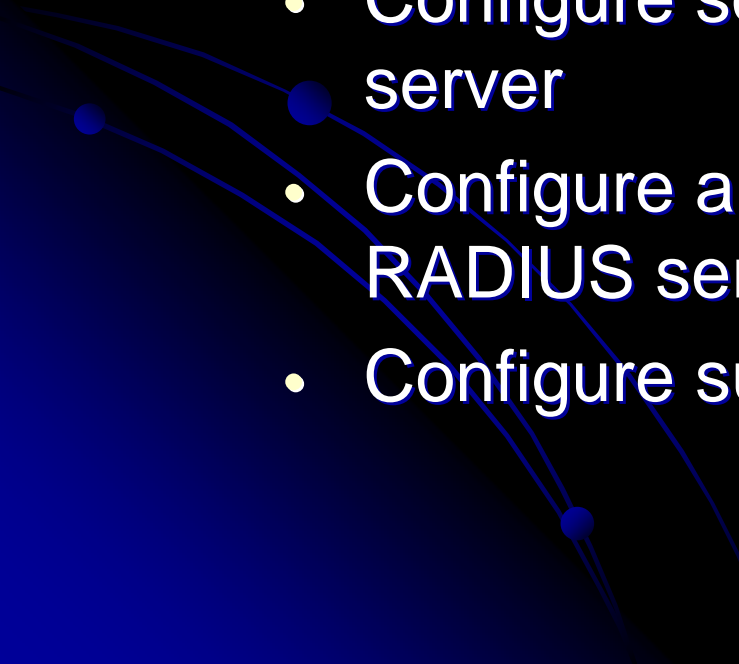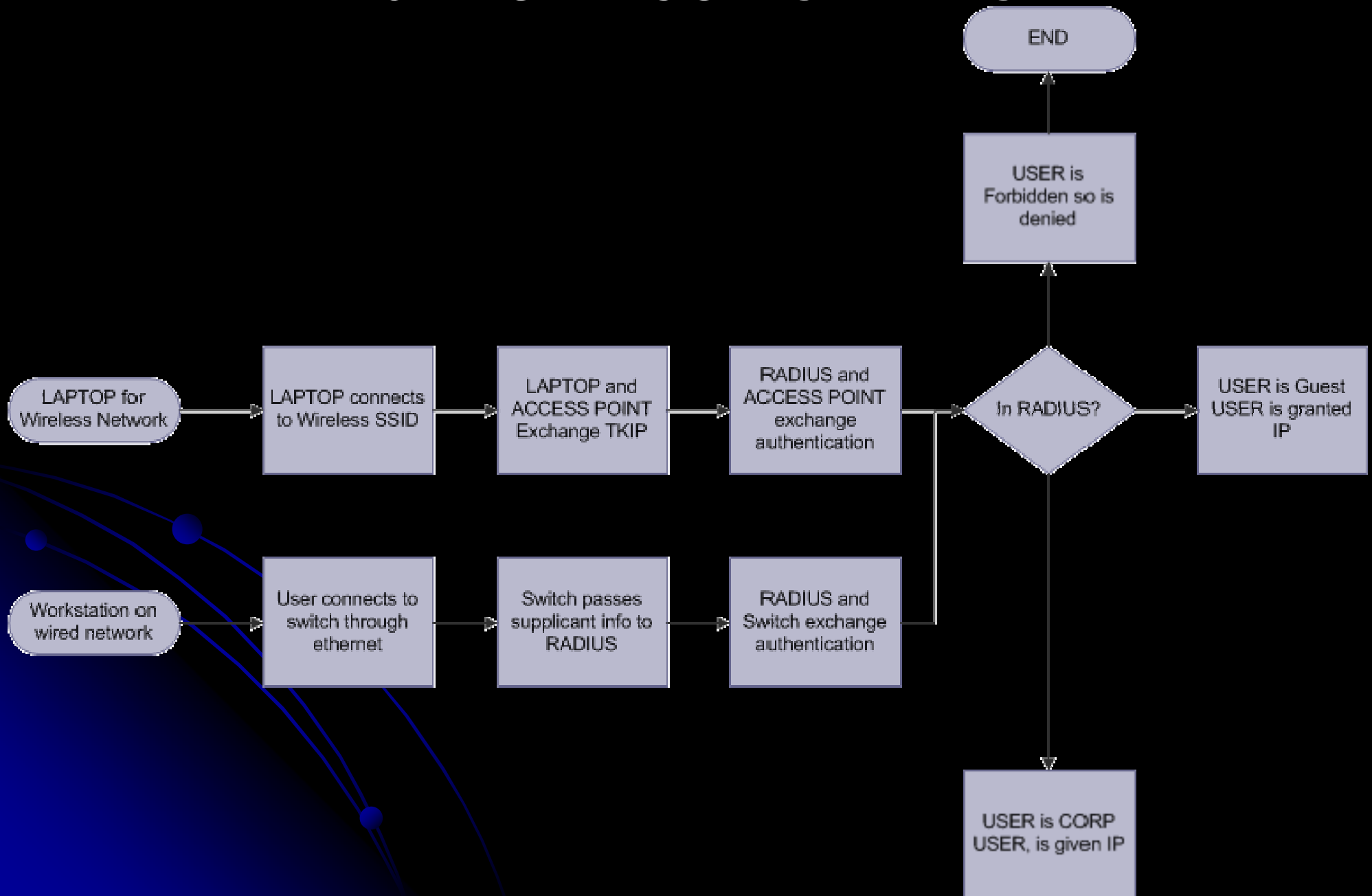
How does it work?

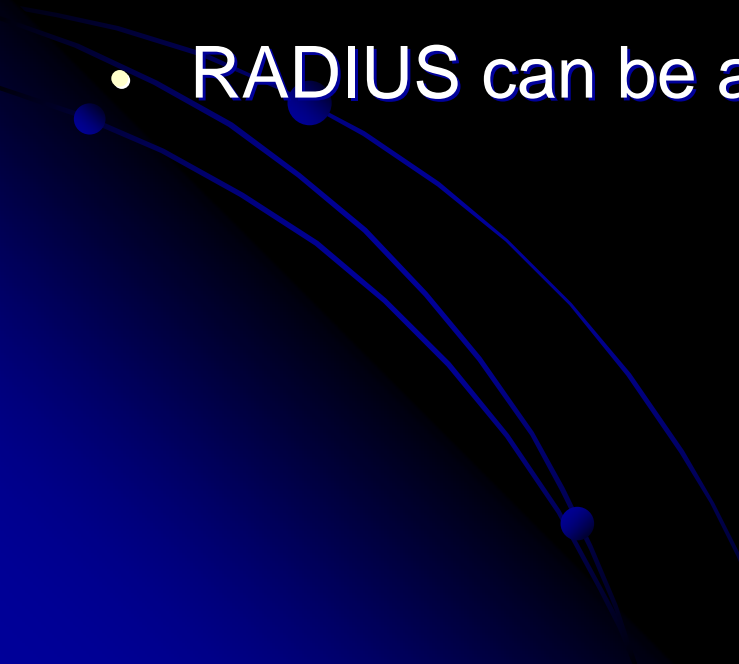Wireless Example

How does it work?

Supplicant — Authenticator — Authentication Server — LDAP Server

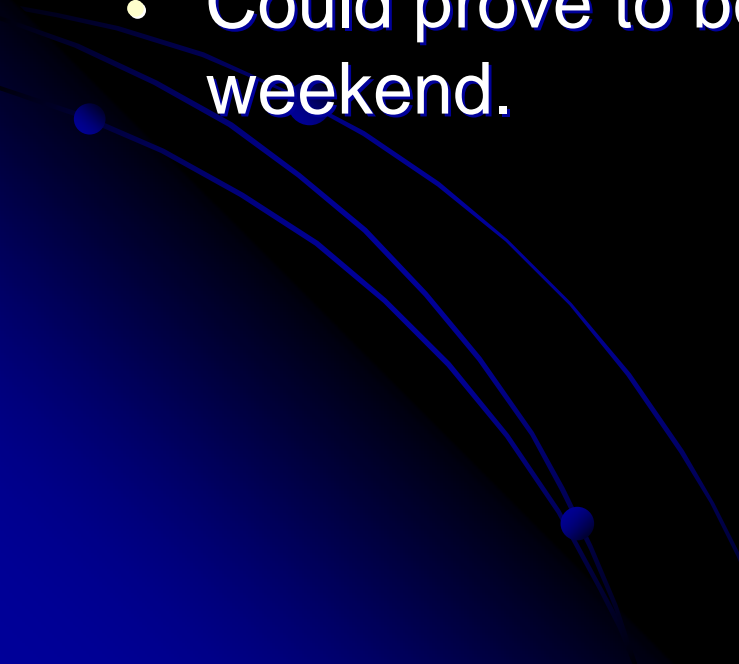| EAP(OL)	RADIUS		LDAP
EAP (payload)			
Secure Tunnel (TTLS or PEAP)			
Authentication Protocol (PAP, CHAP, MD5 etc)			
DATA (Username, Password, WEP key, VLAN etc)			

Authentication Flow

How do you set this up?

- Acquire switch that supports 802.1x
- Build a RADIUS server
- Configure secrets for switch and RADIUS server
- Configure authentication and tunneling on RADIUS server
- Configure supplicant on workstation

What problems exist?

- Laptop theft
- Supplicant configs are in clear text in some client software
- RADIUS can be attacked

Laptop theft?

- If you laptop gets stolen the 802.1x Username/Password/Certs will be stolen too.

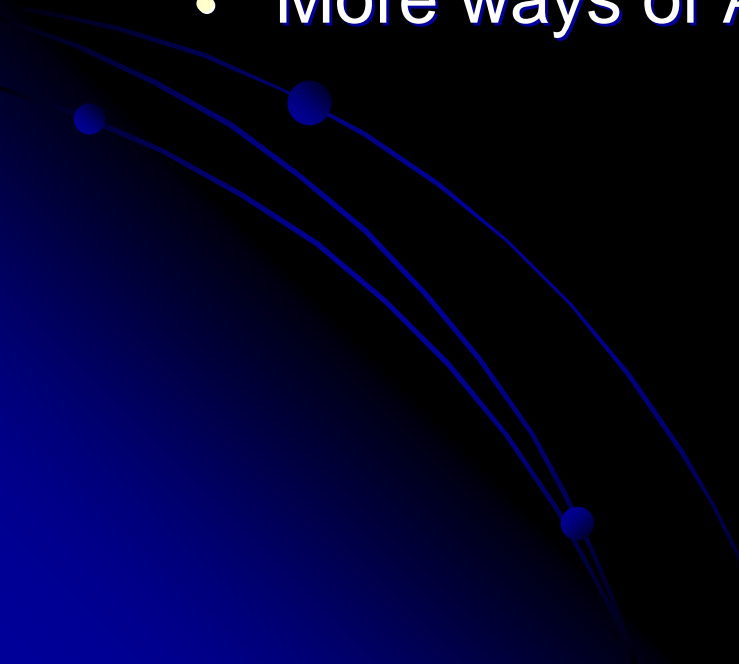- Could prove to be a huge hole if it happened on a weekend.

Supplicant configs are in clear text.

- Xsupplicant is the Linux client and linux config is in clear text
- OSX supplicant client is in clear text
- This contains the username/password.

RADIUS can be attacked

- It's easy to DOS a RADIUS server
- If RADIUS dies, many authenticated services will too. RADIUS utilizes UDP
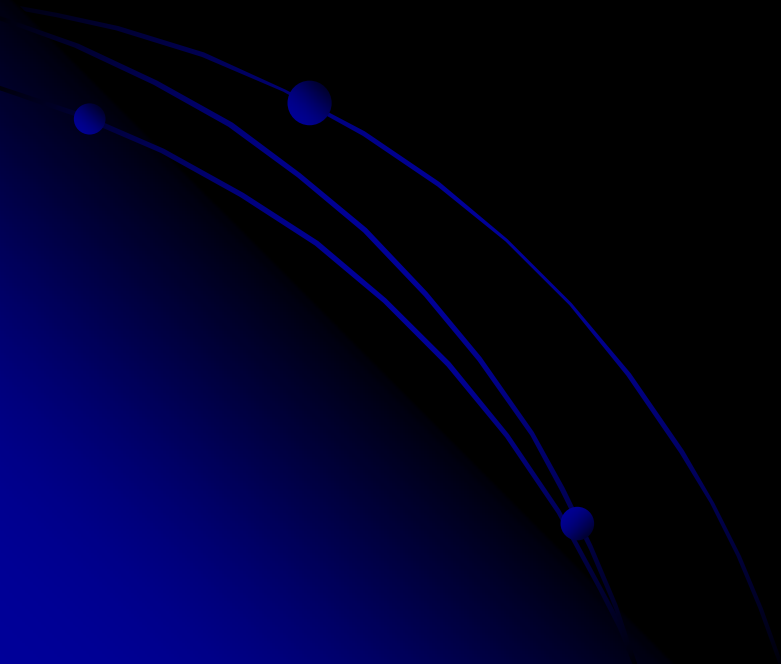
Can problems be fixed?

- Laptop Theft? Maybe
- Supplicant configs in clear text? Yes
- RADIUS protected from attacks? Yes
- More ways of Authorizing users? Yes

Laptop Theft?

- Let me tell you a story...
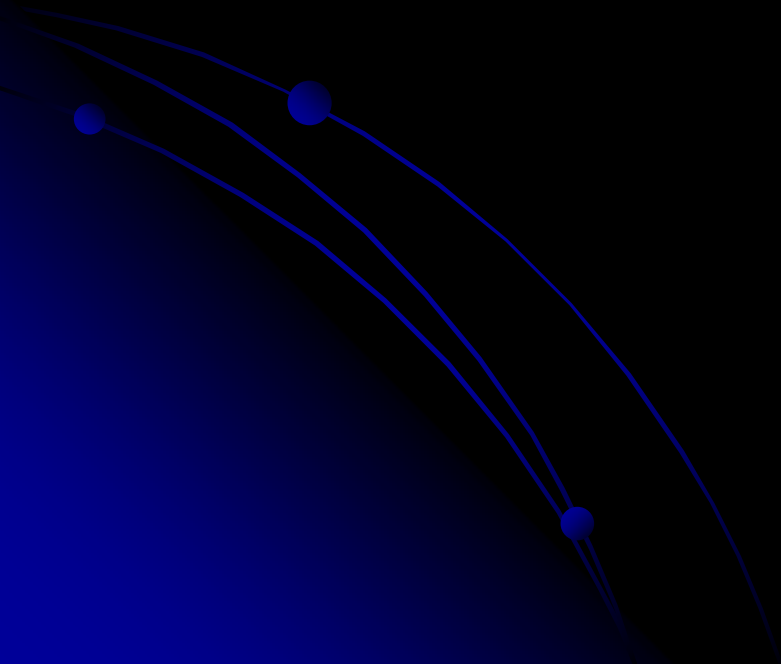
Supplicant configs in clear text?

- Ideas to fix it
    - File Vault on OSX
    - Maybe GPG configs and require password
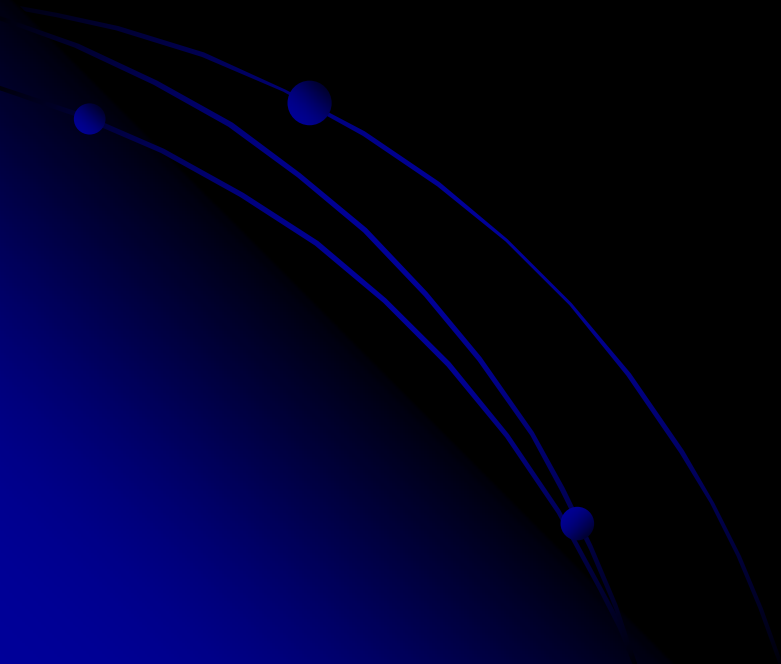
RADIUS protected from attacks?

- Firewall
- ACL
- Private VLAN

More ways of Authorizing users?

- Captive Portal
  - Captive Portal connecting to LDAP or Active Directory

Questions

Contact

tommEE pickles

tommEE@gmail.com

tommEE.net

moloch.org