Ethical Student Hackers

Enterprise Wifi

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

Glossary of Acronyms

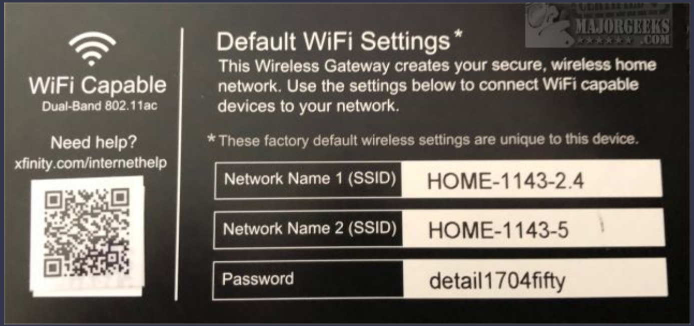
- SSID: the visible name of the network
- ESSID: SSID which could apply to multiple access points
- BSSID: access point MAC address
- WPA2-PSK: WiFi networks that have the same password for everyone who wants to connect to them
- WPA2-EAP: WiFi networks that demand a username and a password, which are sent to a RADIUS server
- RADIUS: a server for client authentication

Personal Wifi

Password authentication

4 way handshake

Covered in a previous session



WiFi Capable
Dual-Band 802.11ac

Need help?
xfinity.com/internethelp

Default WiFi Settings*
This Wireless Gateway creates your secure, wireless home network. Use the settings below to connect WiFi capable devices to your network.

*These factory default wireless settings are unique to this device.

Network Name 1 (SSID)	HOME-1143-2.4
Network Name 2 (SSID)	HOME-1143-5
Password	detail1704fifty

Authentication Options

PSK - Pre-Shared Key

- Device and Router have a key they both know

WPA2

- Personal wifi

GSM

- Global System for Mobile communication
- What we call mobile data

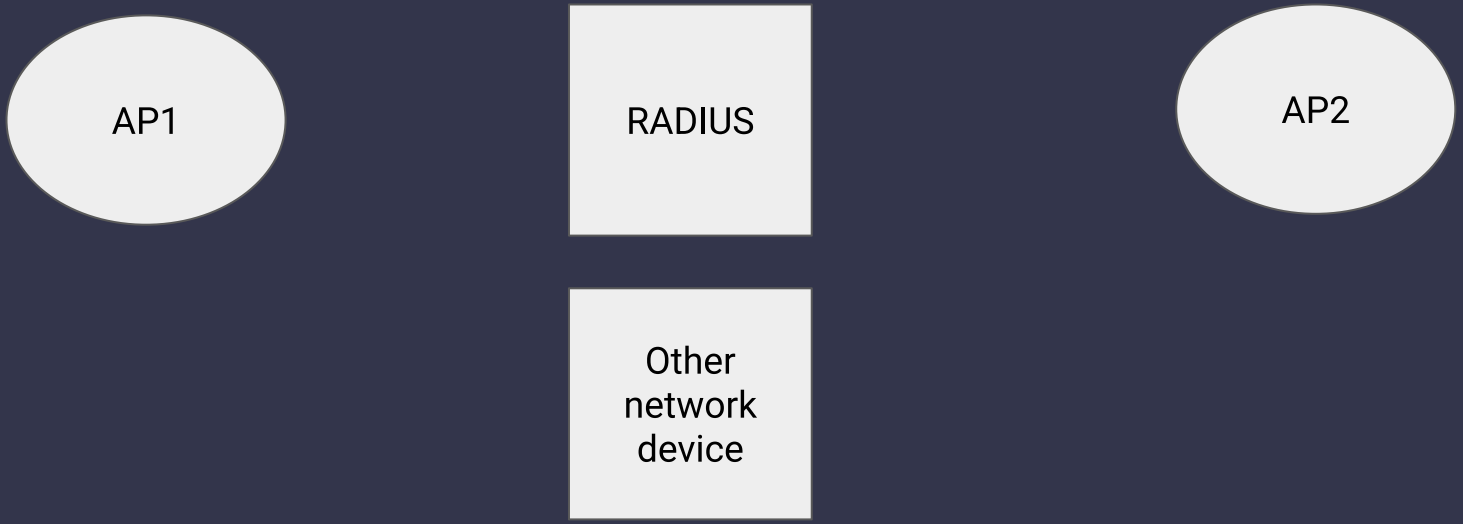
Certificate

- A private key is used to generate a certificate which is then signed by an authority.
- The certificate is then used as proof that you are a trusted user

Enterprise WiFi

802.1X

Radius servers are used for authentication

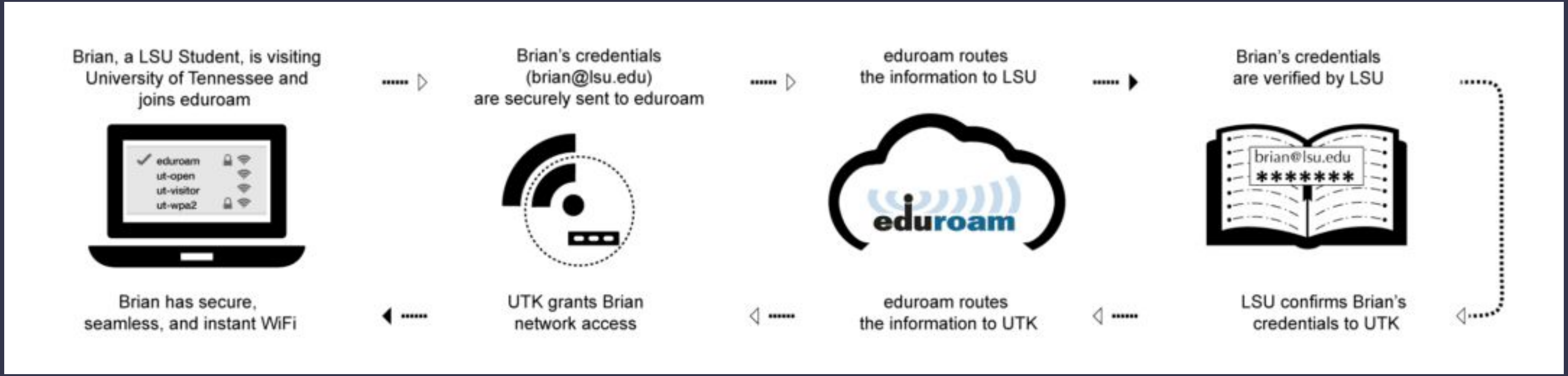


Eduroam

How it works

Eduroam CAT

What weaknesses



Brian, a LSU Student, is visiting University of Tennessee and joins eduroam

Brian's credentials (brian@lsu.edu) are securely sent to eduroam

eduroam routes the information to LSU

Brian's credentials are verified by LSU

LSU confirms Brian's credentials to UTK

eduroam routes the information to UTK

UTK grants Brian network access

Brian has secure, seamless, and instant WiFi

Impersonation

- Set up RADIUS server
- Have an AP link to it
- Call the AP ‘eduroam’
- User connects to our network
- Enters username and password
- Refuse the connection - our RADIUS server stores the info

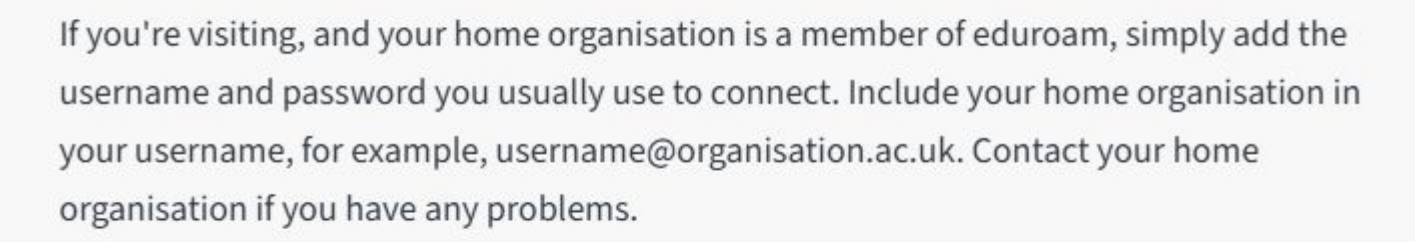
Prevention

- Certificates !!! Eduroam CAT

Signal strength

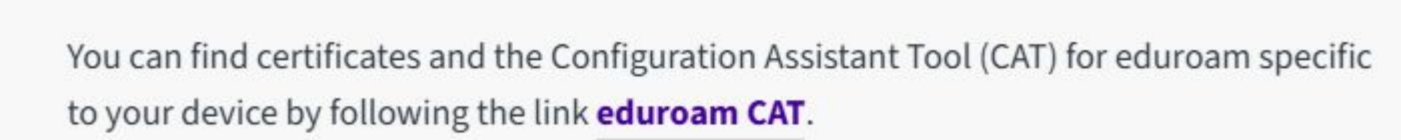
Our Uni

This is taken from the uni website on eduroam



If you're visiting, and your home organisation is a member of eduroam, simply add the username and password you usually use to connect. Include your home organisation in your username, for example, username@organisation.ac.uk. Contact your home organisation if you have any problems.

And a while below that is this small, easily missed line …



You can find certificates and the Configuration Assistant Tool (CAT) for eduroam specific to your device by following the link **eduroam CAT**.

https://www.sheffield.ac.uk/it-services/eduroam

Practical

Requirements: hostapd-wpe and hashcat, wifi adapter that supports AP mode

Use instructions here to help: https://www.kali.org/tools/hostapd-wpe/#hostapd-wpe

hashcat -a 0 (output from hostapd-wpe) (wordlist)

If you need to use the internet again after killing network: systemctl start NetworkManager

Installing Kali tools on Ubuntu

```
apt-key adv --keyserver keyserver.ubuntu.com --recv-keys ED444FF07D8D0BF6
```

```
echo '# Kali linux repositories | Added by Katoolin\ndeb http://http.kali.org/kali kali-rolling main contrib non-free' >> /etc/apt/sources.list
```

```
apt-get update -m
```

Upcoming Sessions

What’s up next?

www.shefesh.com/sessions

Next week:

TOR and anonymity

Any Questions?

www.shefesh.com

Thanks for coming!