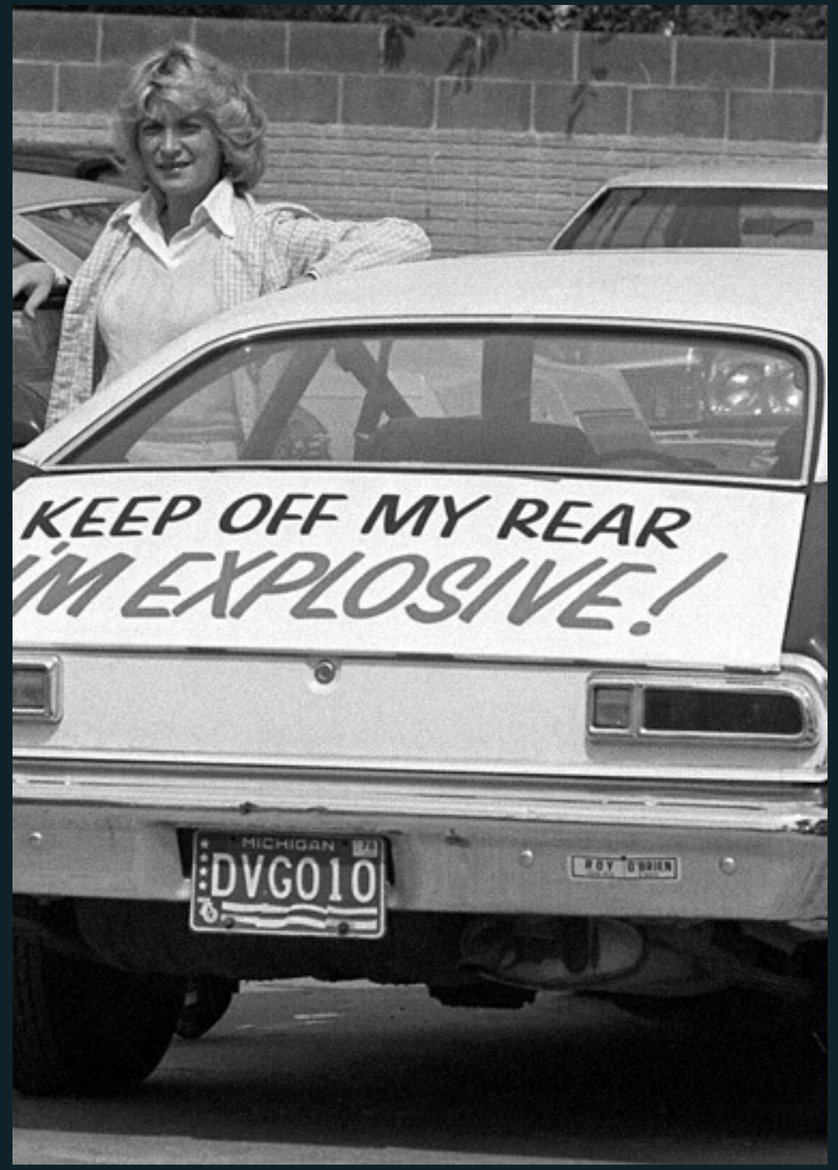
SPOOFI - WIFI SPOOFING MADE EASY

MANUAL ENROLMENT VS AUTOMATIC LIES

RADEXT - IETF 95

WHY IS IT INSECURE?

- MSCHAPv2 is broken, must be wrapped in TLS
- TLS protects data only if peer is not evil
- Ensuring peer is not evil requires a trust relationship
- Trust relationship during bootstrap requires PKI savvy users
- Users are not PKI savvy.

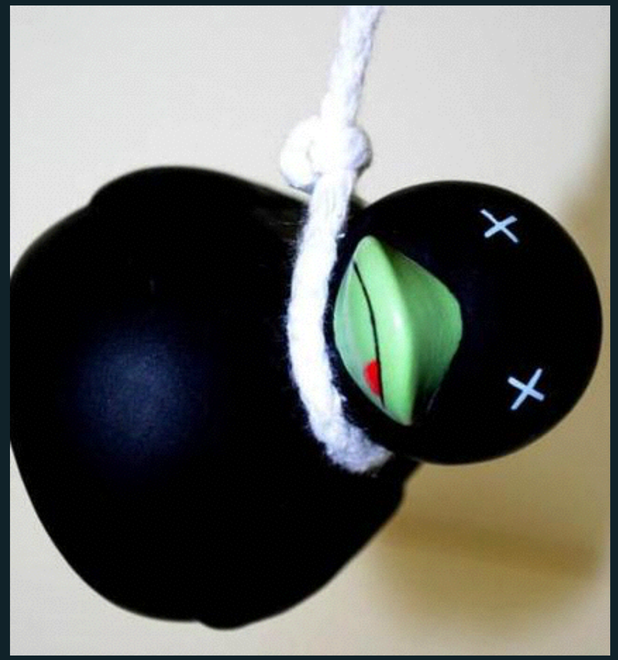


IT'S NOT JUST PEAP

- Any insecure inner method cannot be made secure by using TLS
- Such as:
  - EAP-TTLS-PAP
  - EAP-TTLS-MSCHAPv2
  - EAP-TTLS-GTC
  - PEAP-GTC
- For OSX, IOS, and Windows > 8, it's possible for the server to request TTLS-EAP-GTC or TTLS-PAP and to get the cleartext password
- Oops

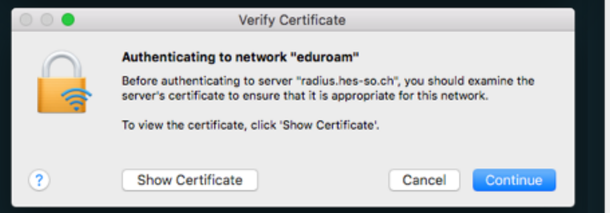
FAILURE OF THE DUCK TEST

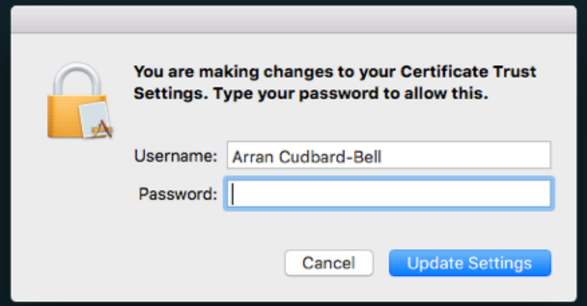
- The only method of identifying wireless network is SSID
  - which isn't really authentication
- The only method of authenticating the EAP server is via the presented certificate
  - fingerprint, CN and signing CA, etc.
- Everyone knows to click through these!
  - just get me online, don’t bother me with certificate warnings
- We can’t trust the users to do the right thing. Administrator intervention is needed.

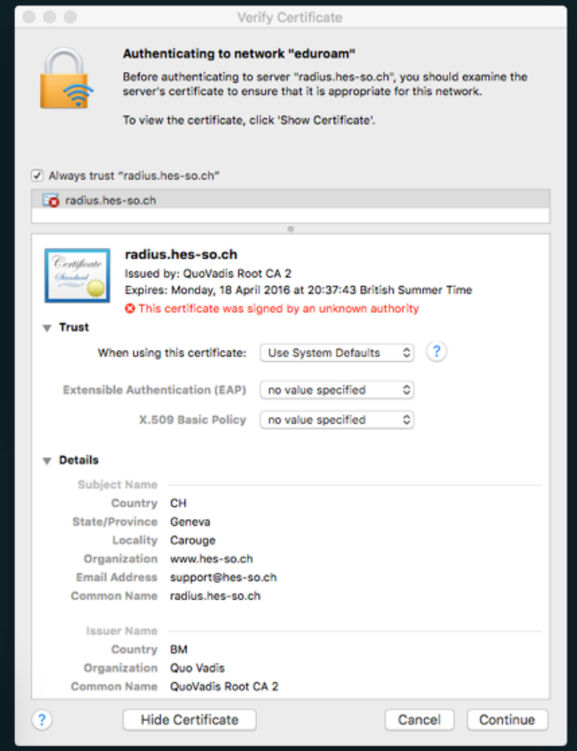


IOS / OS X

- IOS/OSX supplicants prompt for User-Name/Password before negotiating the EAP method
- No option to select personal certificate
- No option to manually configure supplicant profiles
- Only CN of certificate shown in UI (can expand to see full details)
- Trivial to click past certificate verification dialogues, but user at least needs to be able to change trust preferences
- When TTLS is requested, supplicant will send EAP-Identity and trigger EAP negotiation, allowing negotiation of inner EAP-GTC
- Unless network/supplicant settings were defined by a profile, the users cached credentials will be re-used on networks with the same name, but presenting a different cert

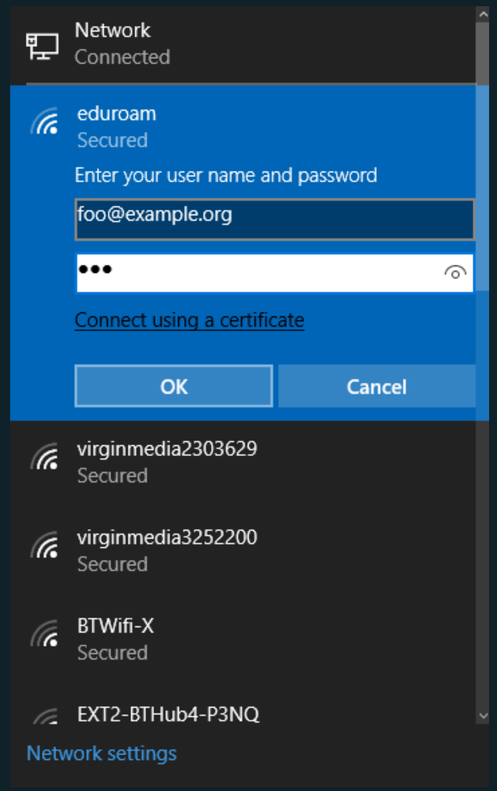


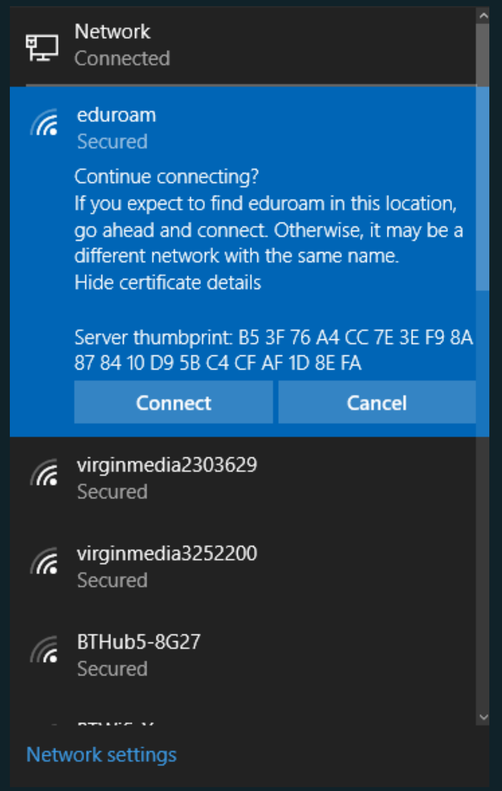


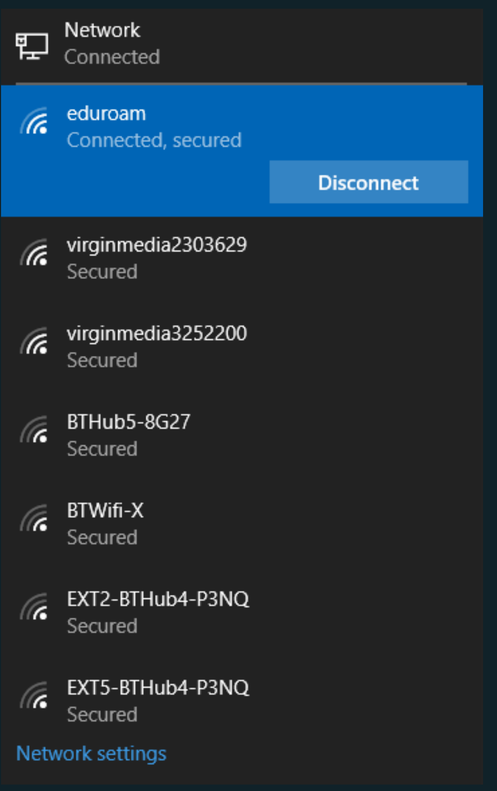


WINDOWS 10

- Windows 10 supplicants prompt for User-Name/Password before negotiating the EAP method
- Allows manual configuration of supplicant, but exceedingly well hidden
- No way to see certificate CN or issuer, the only available detail is the fingerprint
- When TTLS is requested, supplicant will perform EAP-TTLS-PAP by default. EAP won't be negotiated unless explicitly configured.







Spoofi

LEVERAGING INSECURITIES

- You can actually generate a pretty convincing fake certificate on the fly by using public information **provided on the corporate website** (or corporate wifi)
- Supplicant sends EAP Identity of anonymous@example.com
- RADIUS server connects to https://example.com
- Clones fields from HTTPS certificate into a new RADIUS certificate
- Presents the new certificate to the user
  - All the fields are correct
  - New certificate is signed by Verisigm
- User sees a “valid” certificate and clicks through

WHAT THIS MEANS

- Anyone capable of configuring an AP and a RADIUS server can steal User-Name and Password from pretty much all modern devices
  - … but only for manual enrolment in new SSIDs
  - This code exists, and works, today in FreeRADIUS
- SSID names can be spoofed, in order to get users to “sign up” again
  - EDUR0AM
  - UTF-8 SSIDs and IDN homograph attack
- The only work-around is to disable all manual intervention
  - And to rely on administrative configuration for WiFi security

HOW TO FIX IT

- Enterprises, WiFi Roaming groups
  - Use only administrative configurations for EAP. Disallow manual configuration.
  - Use EAP-TLS instead of password-based methods
  - Consider deploying eduroam CAT, 802.1x-config.org, or similar.
  - Adopt HotSpot 2.0 R2. Register interest in OSU (Online Signup Server) certs provided by central authority (GÉANT/Jisc).
- OS/supplicant vendors
  - Remove users from configuration changes and PKI validity checks
  - Verify certificate consistency when re-using cached credentials for AD-Hoc 802.1X profiles.
- IETF/standards bodies
  - Define strongly worded guidelines for supplicant implementors (http://geant3plus.archive.geant.net/Resources/Open_Call_deliverables/Documents/SENSE_final_report.pdf)