Lack of automated EAP configuration

A security and privacy threat for network users

IETF 93, Prague, CZ

Stefan Winter <stefan.winter@restena.lu>

Enterprise-Security Networks, Theory

- Wi-Fi: IEEE 802.11i (WPA2/AES with IEEE 802.1X)
- Wired: IEEE 802.1X
- Authentication
  - first, user devices authenticates the network (typically server certificate; PKIX with expected server name)
  - then, presents client credential to the known-good server
  - Protocol to get this done: EAP, the Extensible Authentication Protocol
  - Nothing can possibly go wrong.
- Nice theory.

EAP Overview

- EAP is complex
  - a mere container, carries EAP Methods
  - container needs some configuration itself (e.g. max fragment size)
- Each EAP method has its own set of configuration parameters
  - Authenticate EAP server to the EAP peer (issuing CA, sever name, ...)
  - Authenticate EAP peer to the server
  - Anonymity support
  - … and plenty more
- Multiple methods can be configured ; priority ?

Enterprise-Security Networks, Practice

- Client devices are often configured by **endusers** (argh!)
  - Lengthy PDF instructions are the norm, especially in BYOD
  - UIs typically make it easier to be insecure than secure (« Don't validate server certificate » ; « do you trust this fingerprint ? »)
- **The best auth protocol can't deliver if its users get it wrong.**
  - Main Problem: config is good enough to connect – but with insufficient security
  - Like: username+password correct, but would tell anyone who's asking

How bad is it, really?

- „A Practical Investigation of Identity Theft Vulnerabilities in Eduroam“ (sic)
  (http://syssec.rub.de/media/infsec/veroeffentlichungen/2015/05/07/eduroam_WiSec2015.pdf)
- „a share of **52 %** wrongly configured devices existed in our study,“ […] „ A total 20 % of the vulnerable devices were leaking authentication data in unencrypted form“ [majority of the rest: MSCHAPv2 – easily breakable]
- That's with 'loving and caring admins' – complete setup instructions; educational event explaining the importance
- But then again ...

Automatic Configuration to the Rescue

- „The comparatively small share of **13 %** of wrongly configured **Apple** devices might be due to simplifications of the Wi-Fi configuration by importing **pre-built configuration profiles**.“
- Apple has (proprietary) config format that wraps all EAP config details into one XML file; double-click and be happy
- Difference: getting to a secure config is <u>easy</u> then
- There is no IETF equivalent
  - devices like Android could implement it if it existed!
  - draft-winter-opsawg-eap-metadata-02 is looking for a home :-)

I-D Implementations

- Windows („ArnesLink“)
- Linux
- Android: eduroam CAT app (4.3+)
  - @IETF and using eduroam?
  - Download „eduroam CAT“ from Play Store
  - First, tells you whether your Android eduroam config is fully secure (it's not!)
  - Fed with the config profile of your Identity Provider (from https://cat.eduroam.org), fixes your config