A Configuration File Format for Network Services on Leaf Devices

Preventing security and privacy threats for end users

(draft-winter-opsec-netconfig-metadata-00)

IETF 95, Buenos Aires, AR

Stefan Winter <stefan.winter@restena.lu>

Preface: why at opsec?

- Operational component: configure things on hosts correctly – make things work
- Security component: configure things securely on hosts
  - STARTTLS "if available"?
  - Enable server cert check – unchecked?
- Presented at opsawg (IETF 91) and saag (IETF 93) as draft-winter-opsawg-eap-metadata
- New draft extended significantly
  - Following opsawg and saag recommendations

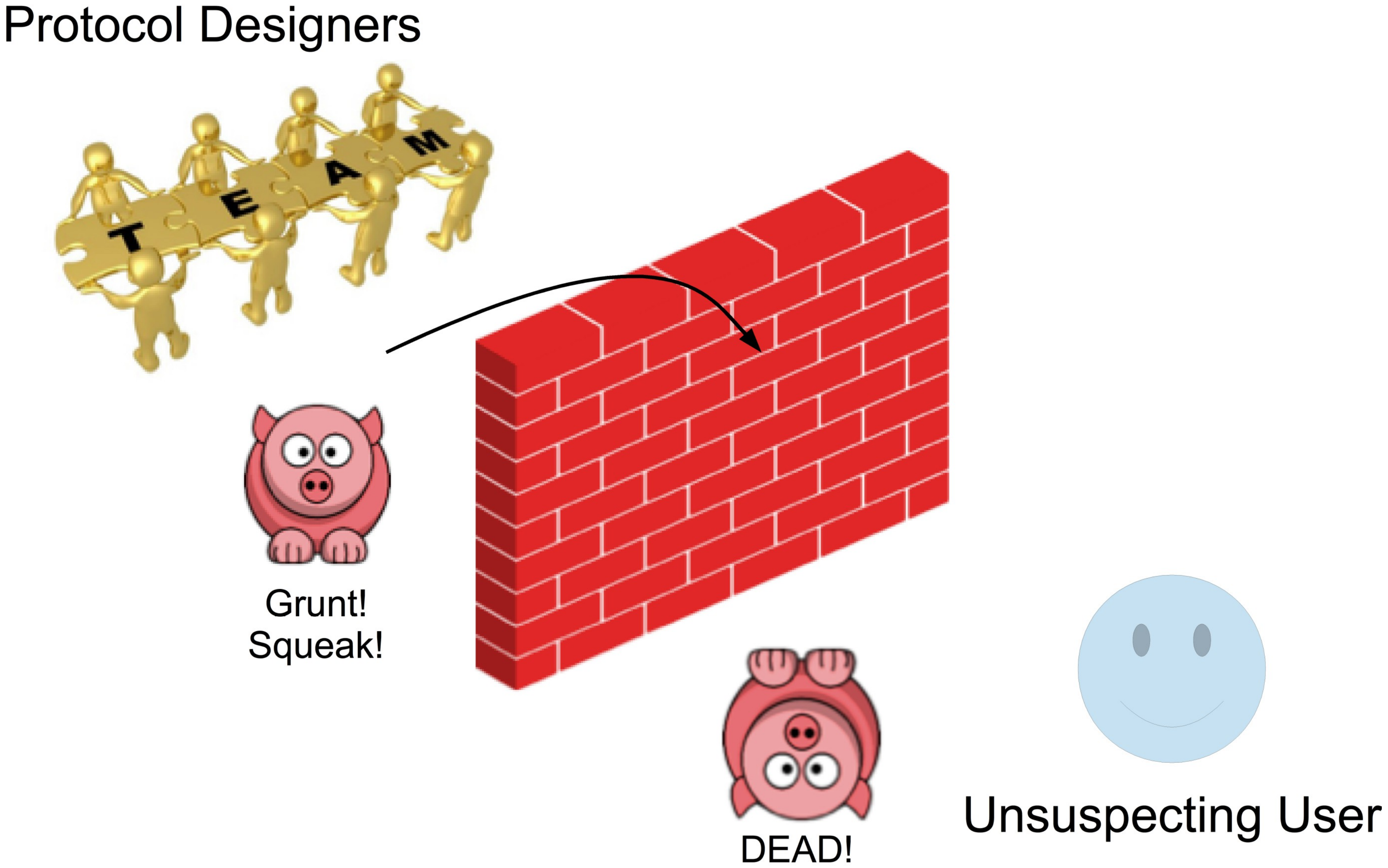
Use Case Enterprise-Security Networks

- 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.

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

Who killed the pig?



Protocol Designers

Grunt!
Squeak!

DEAD!

Unsuspecting User

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!
- Coverage beyond EAP-based Wi-Fi desirable

Coverage of current draft

- draft-winter-opsec-netconfig-metadata-00
  - Follow-up of draft-winter-opsawg-eap-metadata
- Configuration components are re-used between network services → design for that!
  - CA certificate can be trust anchor for Wi-Fi && VPN
  - Same username/password good for Wi-Fi, VPN, IMAP, …
  - Draft assigns UUIDs to all components and allows for cross-references
- Extensible to cover items beyond network config
  - By using YANG
  - I'm a Wi-Fi person → only component that is defined in full detail
  - Plug in more!

Elements covered

NetworkConfiguration

- ProviderInfo (Logo, Terms of Use, Helpdesk Info)
- Certificates (CA or client certificates)
- ClientSideCredenials (usernames, passwords, private keys, ...)
- IPSettingsList (static IP, DHCP, SLAAC, ...)
- EAPIdentityProviderList (EAP methods and their config params)
- WiFiNetwork (Open, EAP, maybe even capport!)

TBD: Signature/Encryption

- YANG produces XML and JSON data formats
- Signing of config files: is the data from a trusted supplier?
  - XMLDSIG? S/MIME signature? JOSE?
- Encryption of config files if they carry private information
  - They don't have to; e.g. could ask for username/password interactively
  - XMLENC? JOSE again?

Next steps?

- More modules for service configs…
- Adoption as WG item?