EAP for Secure Hotspots (EAP-SH)

An EAP authentication protocol to integrate Captive Portals with 802.11i

Nuno Marques - UA
André Zúquete - DETI / IEETA / UA
João Paulo Barraca - DETI / IT / UA

universidade de aveiro
theoria poiesis praxis

ieeta

instituto de telecomunicações

Wi-Fi Security: 802.11i

- Defines most Wi-Fi security mechanisms
  - Network access authentications
  - Payload confidentiality
  - Data frame integrity control
    - 802.11w deals with management frames
- It provides link-layer security
  - Cannot be replaced by security mechanisms provided at different layers

Captive Portals

- Widely used in hotspots in several scenarios
  - Hotels, airports, etc.
- They handle hotspots' network access control
  - Clients' enrolment and authentication
- Require a web-based Man-in-the-Middle hack
  - New clients are redirected to an HTTP Portal
  - The Portal enrolls / authenticates clients
  - Authorized clients stop being redirected

Captive Portals: why?

- Zero configuration
  - Clients do not need to configure anything
    - There are pushed to Captive Portals when needed
    - Browsers maintain session cookies
  - But similar schemes could exist on operating systems for 802.11i
    - They already exist to handle Captive Portals
- Account management
  - Allow the enrolment of people
  - Not possible with 802.11i !!

Captive Portals' security problems

- Do not produce key material for 802.11i/w
  - No link layer protection
  - Frames' payloads are exposed
  - Frame injection is possible
- Sessions can be easily hijacked
- Networks can be abused using tunnels

- WPA3 (Wi-Fi Protected Access 3)
  - Does not tackle this issue

Proposed alternative

- Keep the Captive Portal benefit
  - Enrolment of new users with a web service

- Explore existing Wi-Fi security mechanisms
  - 802.11i/w

- This means dealing at the 802.1X level
  - The 802.11i network authentication framework

EAP-SH: EAP for Secure Hotspots

- The 802.1X is an extensible framework
  - Uses EAP (Extensible Authentication Protocol)
  - There are many different EAP protocols
- EAP-SH is just another EAP protocol
  - One that allows clients to deal with Captive Portals
  - No other allows that

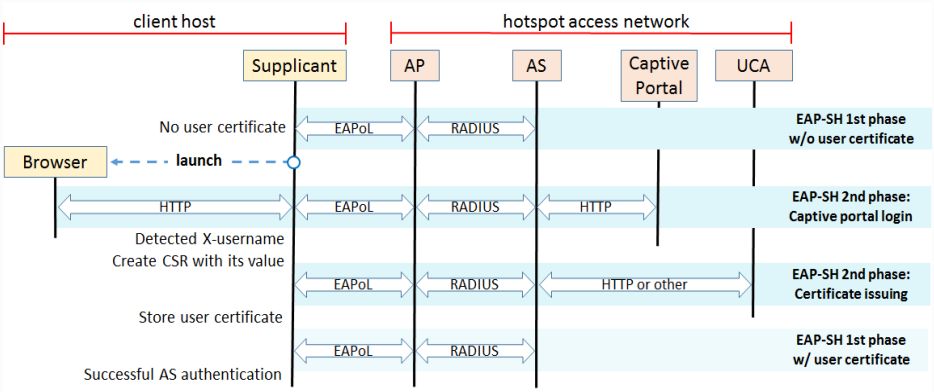
EAP-SH overview

- It combines two authentication types
  - Arbitrary authentication with a web Captive Portal
    - For getting session credentials
  - EAP-TLS authentication
    - With asymmetric key pairs and X.509 certificates
    - Certificates can contain session time limits
- HTTP tunneling
  - Interactions w/ Captive Portals are tunneled by EAP-SH
  - No prior network configuration is required to do that

EAP-SH protocol phases

- 1st phase
  - The client has access credentials
    - Private key and X.509 certificate
    - It uses them as in EAP-TLS
  - Otherwise
    - Creates a TLS tunnel over EAP
    - Jumps to 2nd phase
- 2nd phase
  - Login in the Captive Portal
    - With a browser
    - User participation
  - Request of X.509 certificate
    - Transparently to users
  - Repeat 1st phase

EAP-SH architecture and interactions



Public key certificates

- The only trust anchor is the AS certificate
  - Which is a normal requirement
- Captive Portals do not require a certificate
  - Browsers do not interact directly with them
- Captive Portals' logins do not require HTTPS protection
  - Since HTTP traffic is tunneled over TLS and EAP
- User certificates
  - Can be generated by a Hotspot private CA
  - Only the AS needs to validate them
  - Can establish sessions' time bounds

EAP-SH privacy

- EAP-TLS exposes identities in clients' certificates
  - But client's certificates can have pseudonyms
- Clients request certificates for the identity they get upon a Captive Portal login
  - The Hotspot can use pseudonyms
  - Pseudonyms can change upon each login

EAP-SH security and usability

- Extends 802.11X and generates keys for 802.11i/w
  - Thus enable link security
- Permanent AS certificate configuration
  - No need to check for HTTPS protection
  - There are many ways to securely configure it
- Client software can customize Captive Portals' interfaces
  - To avoid phishing attacks with rogue servers
- Browsers cannot remember users' credentials
  - As they interact directly with the Supplicant's application

EAP-SH performance

- With existing asymmetric credentials
  - Same as an EAP-TLS authentication
- Without those credentials
  - Login with user interaction
  - CSR generation and upload
  - Certificate generation and download
  - EAP-TLS authentication

Conclusion

- EAP-SH integrates Captive Portals with 802.11i
  - Enabling the subsequent link security
- Sessions can be maintained with user certificates
  - Generated on a need basis upon a Captive Portal login
- Supplicants and Authentication Servers need an update
  - But not APs!

Publications

- Marques, N., Zúquete, A., & Barraca, J. P. (2020). EAP-SH: An EAP Authentication Protocol to Integrate Captive Portals in the 802.1 X Security Architecture. *Wireless Personal Communications*, 1-25.
- Marques, N., Zúquete, A., & Barraca, J. P. (2019). Integration of the Captive Portal paradigm with the 802.1 X architecture. *arXiv preprint arXiv:1908.09927*.