Authentication in VPNs and 802.1X networks with Identity Providers

Master's thesis in Cybersecurity

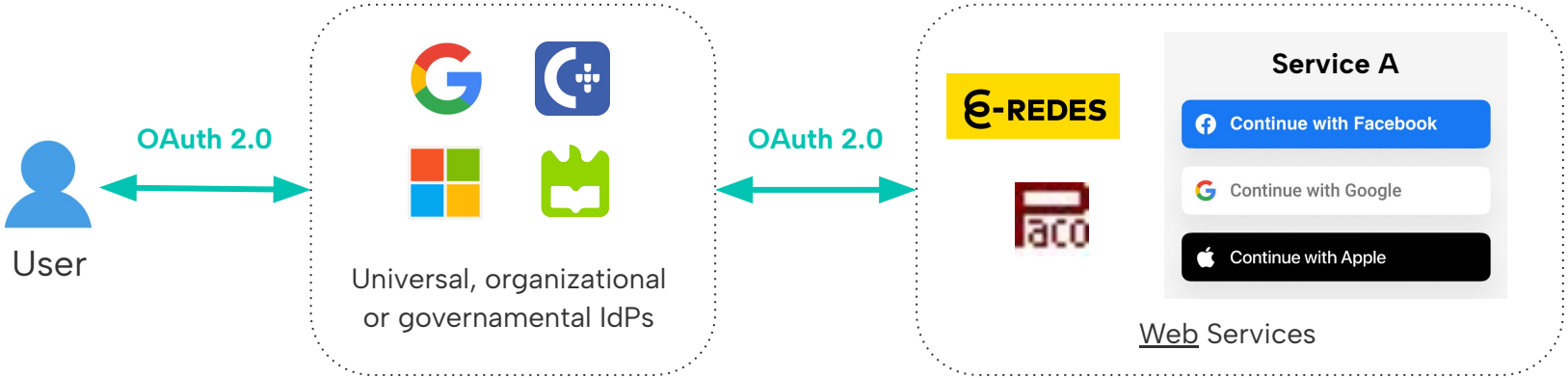
Duarte Mortágua

universidade de aveiro

Contents

Motivation

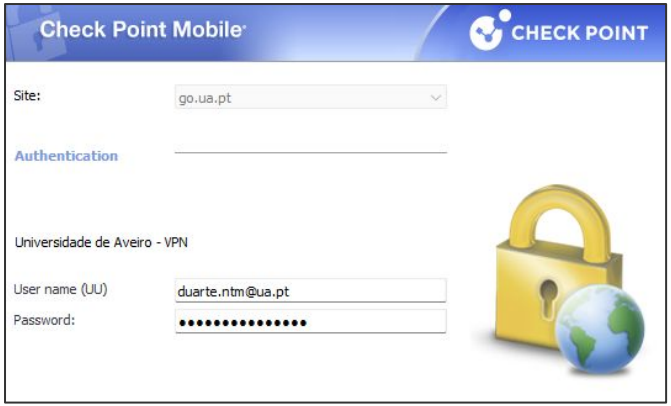
OAuth 2.0 and similar frameworks provide secure authorization policies to federated services for accessing identity resources upon a user authentication.

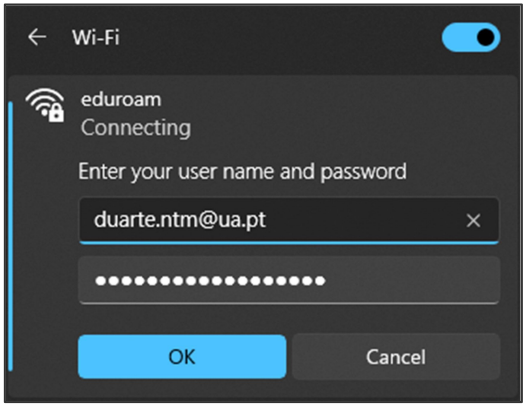


What about authentication outside web?

Research question

How can an IdP be explored for user authentication or network access, during a VPN or a WiFi network setup?





Contributions

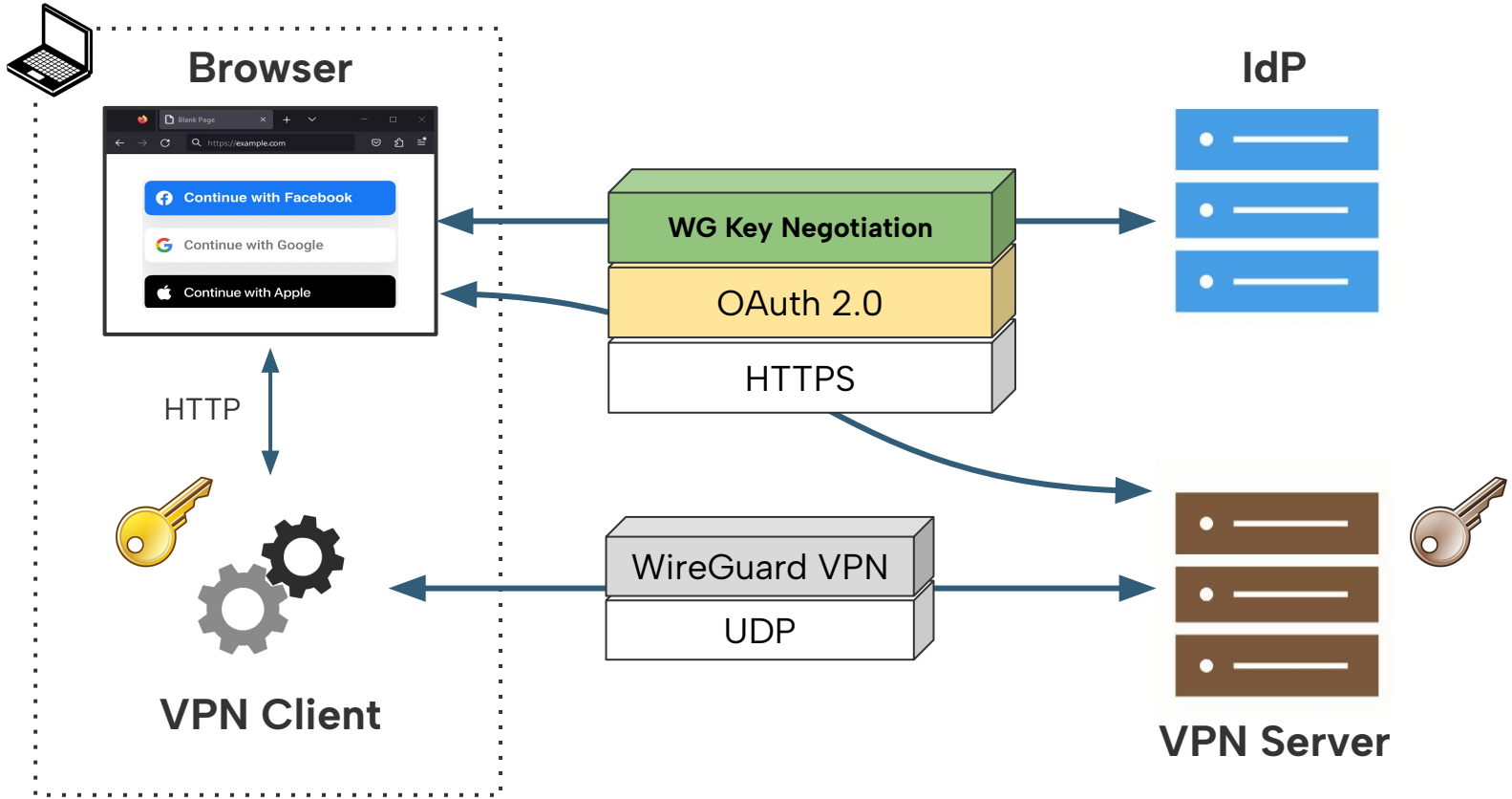
- VPN solution implementing authentication with IdPs (WireGuard negotiation layer)
- 802.1X solution implementing authentication with IdPs (novel EAP method)
- D. Mortágua, A. Zúquete, and P. Salvador, “VPN user authentication using centralized Identity Providers” in *ICNS 2023, The Nineteenth International Conference on Networking and Services*, 2023, pp. 9–18, [Online]. Available: https://www.thinkmind.org/articles/icns_2023_1_30_10016.pdf
- D. Mortágua, A. Zúquete, and P. Salvador, “Enhancing 802.1X Authentication with Identity Providers: Introducing EAP-OAUTH for Secure and Flexible Network Access”, *Computer Networks*, vol. 228, Sept. 2023 (submitted)

Literature review

- Tailscale has a WireGuard-based VPN solution
  - The mechanism implementing IdP-based key negotiation is closed-source
- OpenVPN recently integrated SAML IdP authentication
  - It's handled by the closed-source commercial solution "OpenVPN Access Server"
- WarpSpeed (WireGuard based VPN solution) has IdP SAML-based authentication
  - Only under a paid business licence
- *Canyelles Toledano* (2021) combined a VPN with Keycloak
  - The result was unstable
- *Cánovas, Gómez-Skarmeta, López, et al* (2007) proposed a network protocol for adding fine-grained authorization policies in network access
  - It still uses network interface based authentication, and is Eduroam specific
- Marques, Zúquete, and Barraca (2020) proposed an EAP method that integrates Captive Portals in the 802.1X framework

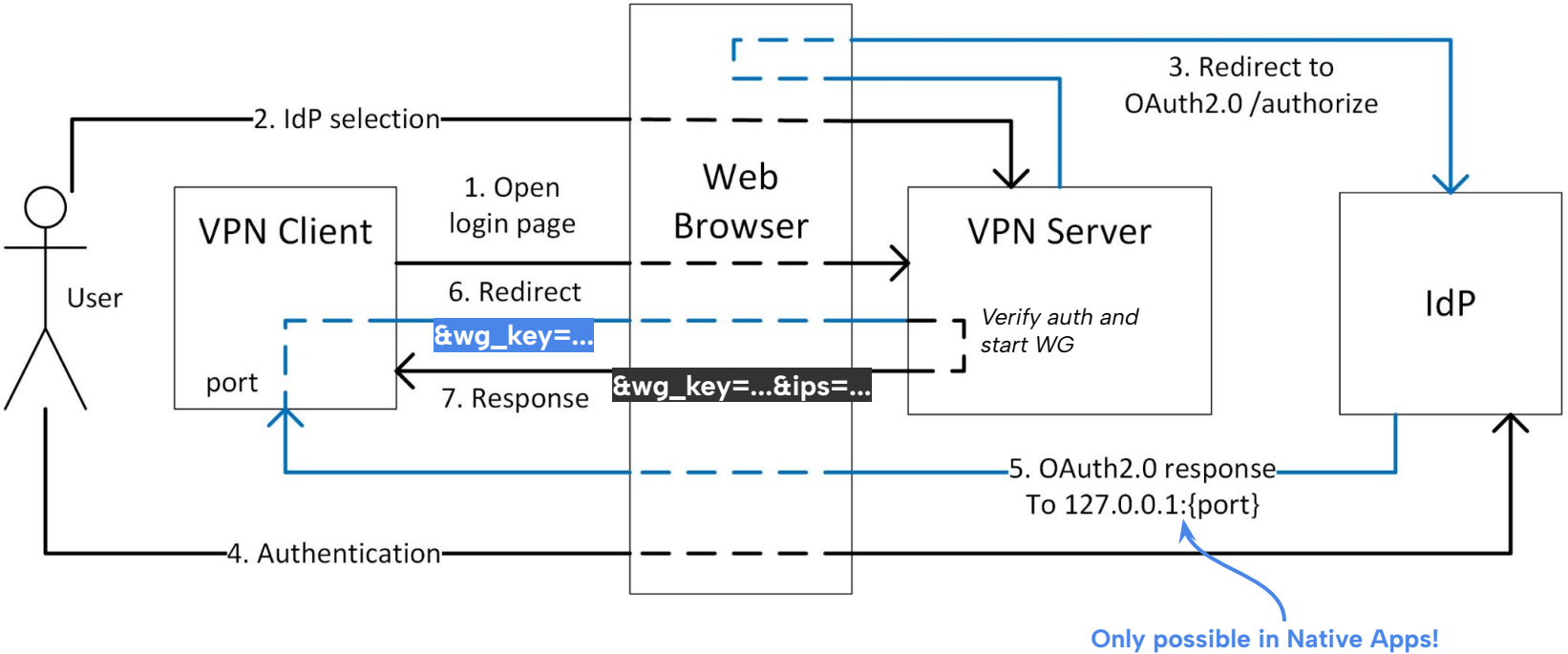
VPN solution using WireGuard

Proposed architecture for VPNs

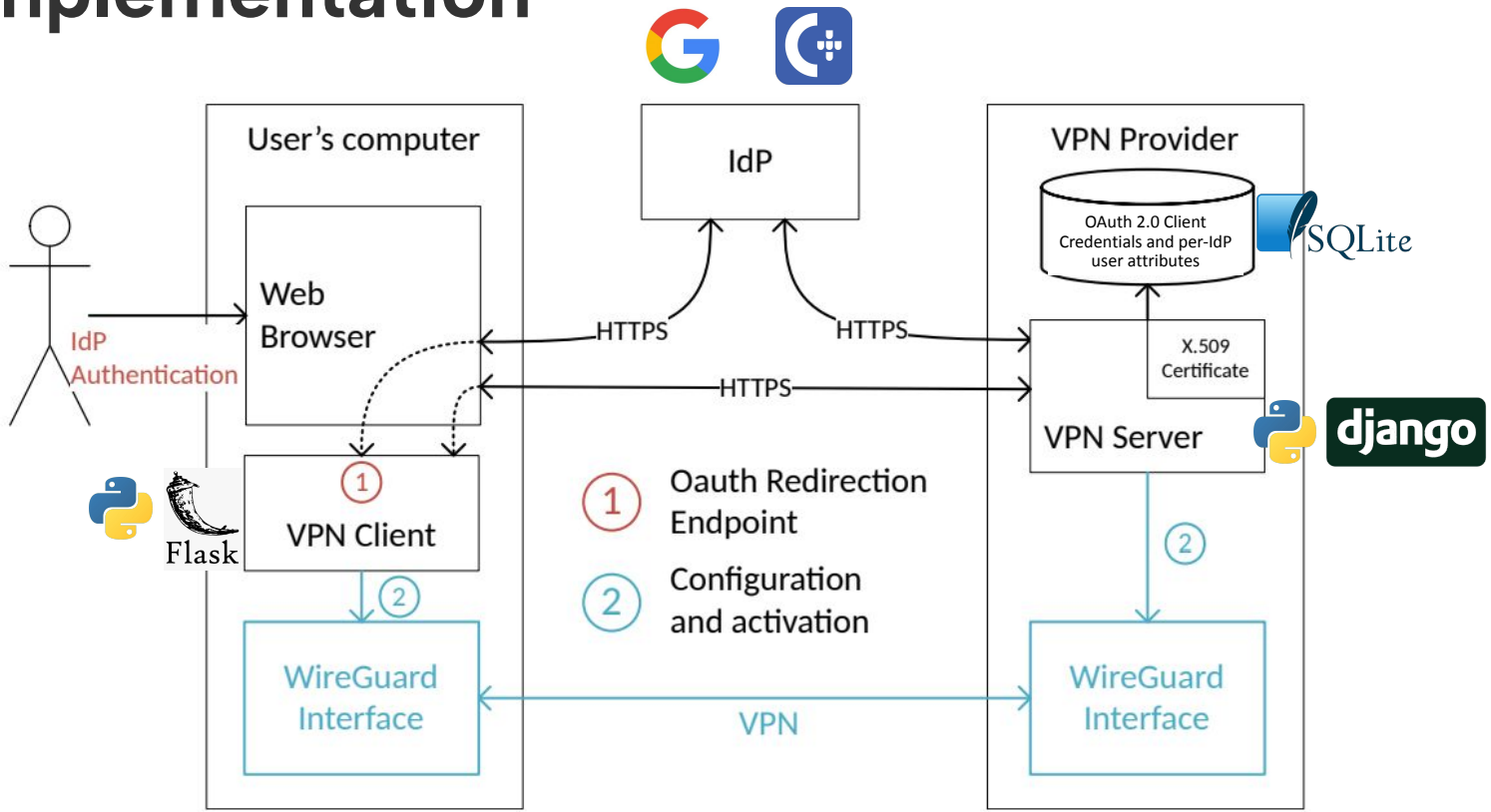


Detailed communication

OAuth 2.0 for Native Apps, where the Client is the VPN Server!



Implementation



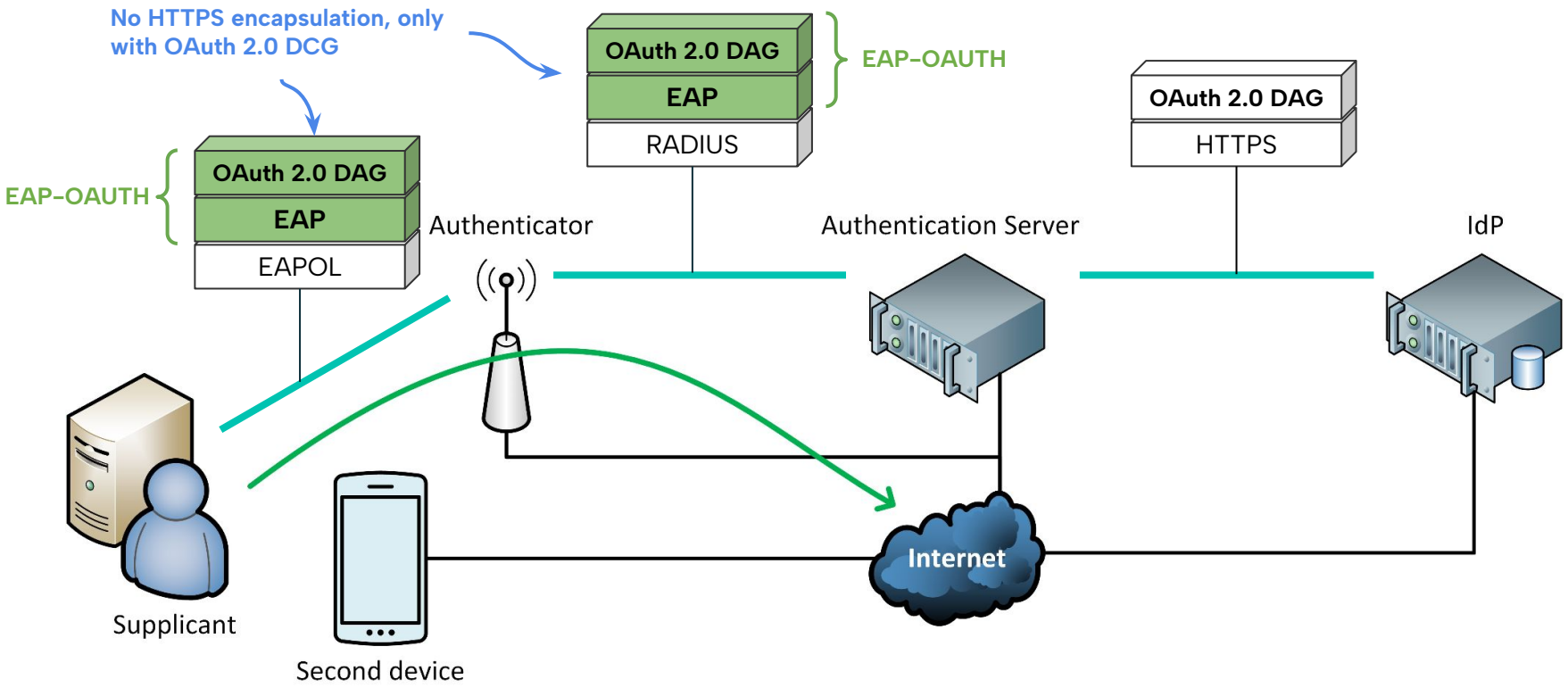
Conclusions for the VPN proposal

- Only attacks against the exchanged messages, the API endpoints and impersonation attacks were considered
- Confidentiality and integrity are assured by HTTPS
- When the Implicit flow is used, the client is not authenticated → inherited problem
- When the Authorization Grant flow is used, the Authorization Code can be stolen inside the user's computer
  - PKCE can mitigate this
- Familiar authentication interface, same set of credentials, simple and scalable implementation, redirect URLs are local, VPN client holds little information

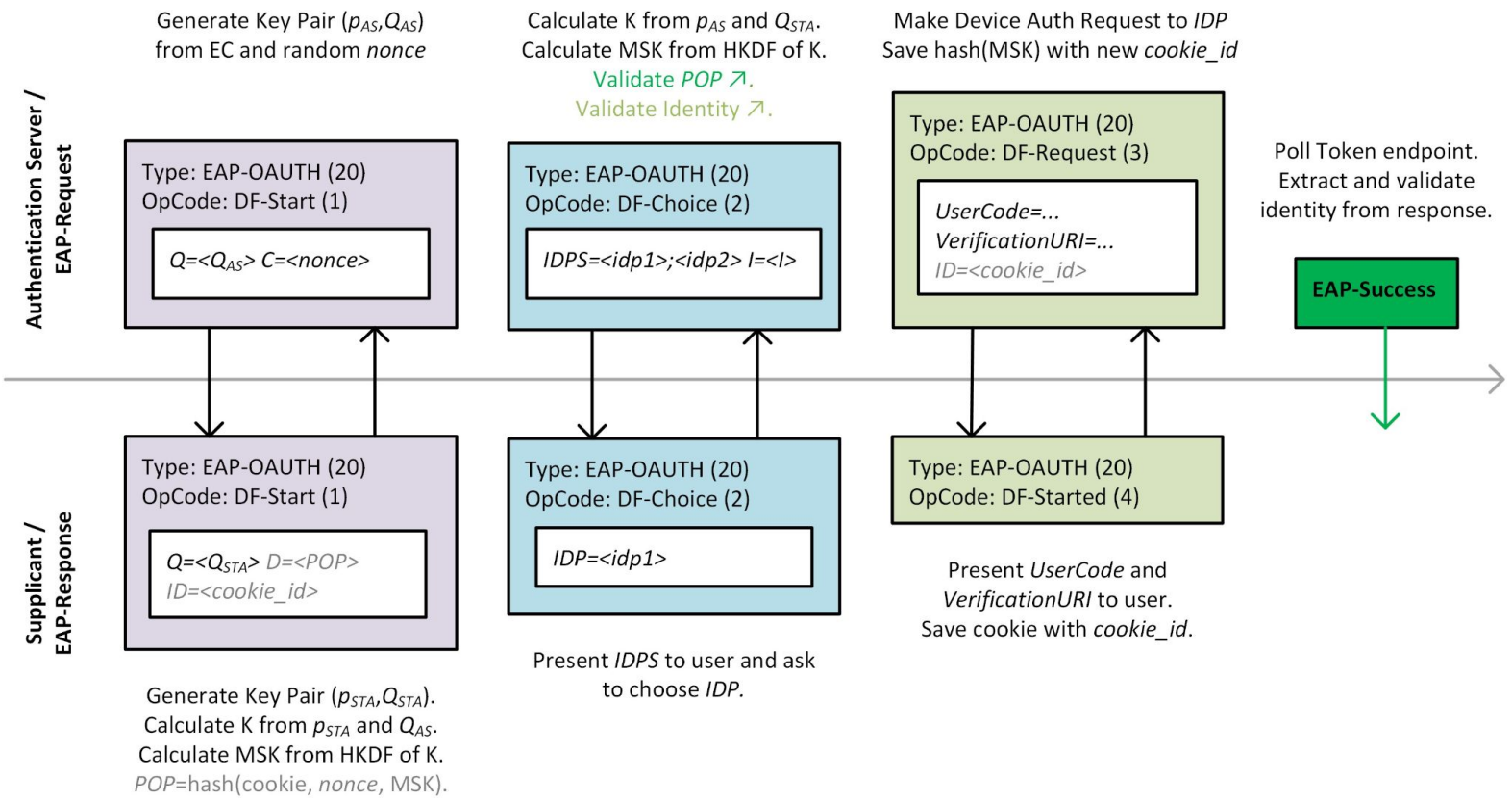
This work presents a streamlined VPN solution that utilizes external IdPs for client user authentication and leverages the OAuth 2.0 authorization process for WireGuard key negotiation, ensuring that only authenticated peers can establish a VPN connection

EAP-OAUTH for 802.1X

Proposed architecture for WLAN authentication

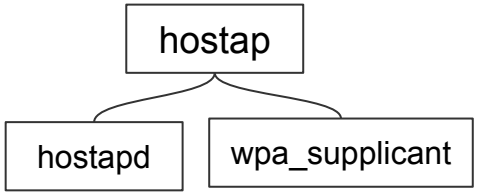


Detailed communication

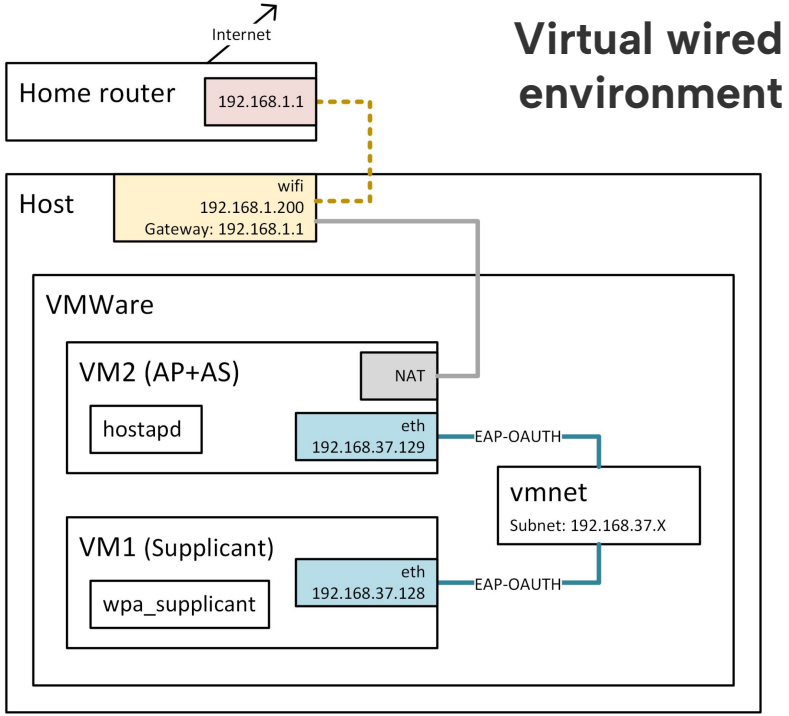


Implementation

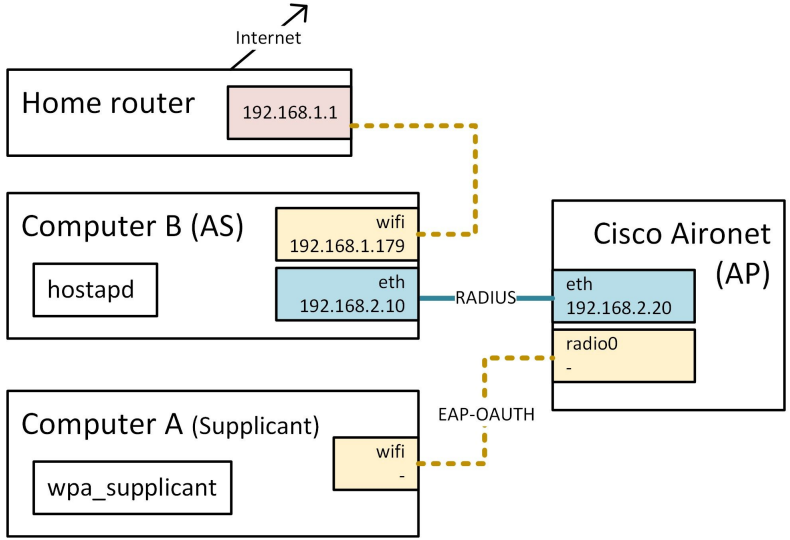
open-source user-space IEEE802.1X



Virtual wired environment



Real WiFi environment



Conclusions for the WiFi proposal

- EAP-OAUTH must always be used with PEAP or EAP-TTLS in order to assure confidentiality and integrity
- The POP mechanism protects leakage to a rogue AS, but does not avoid session hijack
- Fixed IdP URLs and semantic-free attributes can avoid the success of a rogue AS
- Enterprise networks can benefit from SSO experience, enhanced privacy, flexible user authentication, simplified identity management, reduced costs, consistent security policies and easier compliance
- Public hotspot networks can benefit from familiar authentication, enhanced security and support for multiple devices and platforms

This work presents a streamlined network access solution that utilizes external IdPs for client user authentication by integrating OAuth 2.0 directly into the 802.1X network access control process, simplifying authentication and streamlining the user experience.

Final considerations

- Both solutions leverage OAuth 2.0 flows for authentication, providing enhanced security and user experience
- **The VPN solution:**
  - Implements the WireGuard negotiation using OAuth 2.0 with an additional layer
  - Uses OAuth 2.0 Authorization Grant flow or Implicit flow, inserted in the Native Apps approach (localhost with port as redirect URI), and requires a Web browser and a prior Internet connection
- **The 802.1X solution:**
  - Integrates OAuth 2.0 directly into the network access control process, simplifying authentication and streamlining the user experience
  - The non-requirement to have web browser mediation, alongside the possibility of authenticating using a second device, make OAuth 2.0 Device Authorization Grant flow the optimal approach

Future work

- Negotiating the ECDH key agreement protocol within the EAP-OAUTH method
- Agreement between the AS and the Supplicant on the duration of the authentication process with the IdP, and the corresponding polling time by the AS
- Proposal of an evolution of the OAuth 2.0 Device Authorization Grant in order to allow authenticators to provide the totality, or part, of the user code conveyed to the user
- Contribution to the w1.fi open-source repository *hostap* (https://w1.fi/cgit/hostap/), including the new EAP-OAUTH method (TBD very soon)

Thank you

Questions?

Legacy vs IdP authentication

IdPs can provide federated services with user attributes, after they authenticate via a uniform and flexible method.