Federated SSH with Moonshot

Alex Perez-Mendez

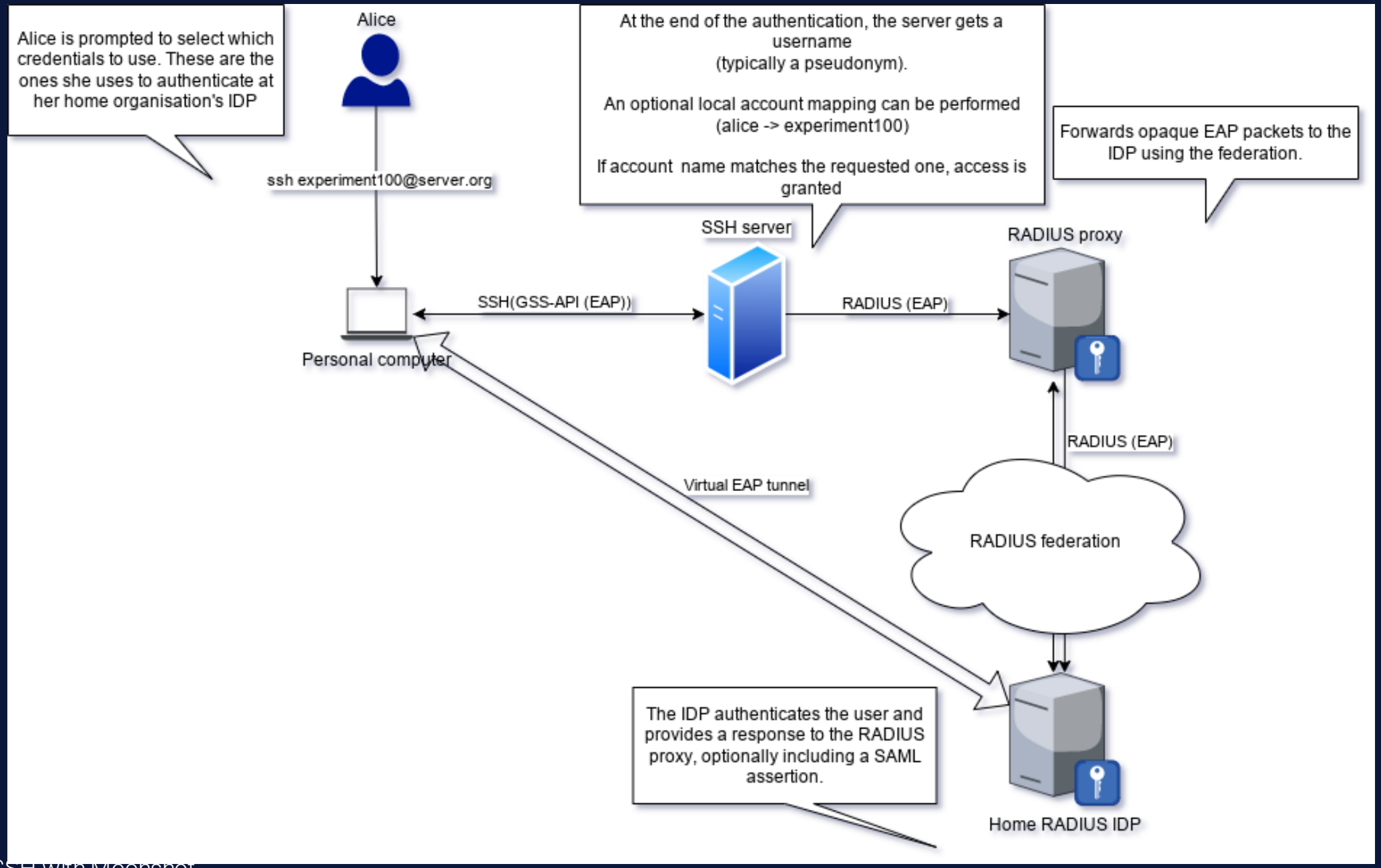
alex.perez-mendez@jisc.ac.uk

Moonshot in a nutshell

- Technology, based on the IETF ABFAB open standards (RFCs 7055, 7056, 7057, 7831, 7832, and 7833), that aims to enable federated access to virtually any application or service.
  - Strong authentication as used by eduroam (EAP/RADIUS/RadSec);
  - Strong authorisation as used by many national federations (SAML); and
  - Strong service/application integration as used by many major applications (GSS-API)
- In simpler words:
  - Apply the federation model that worked well for eduroam
    - To provide application-level access control
    - With authorisation improvements

How does Moonshot work with SSH

- SSH allows access control to be performed via GSS-API
- GSS-API allows interchangeable authentication methods.
- Moonshot implements GSS-EAP, which performs this authentication with EAP and RADIUS/RadSec.
- When a user tries to access an SSH server, they are prompted to select their identity from an identity selector.
    - Then, GSS-API + EAP + RADIUS authentication happens
    - If authentication succeeds and the federated identity matches the requested resource, access is granted.


Alice is prompted to select which credentials to use. These are the ones she uses to authenticate at her home organisation's IDP
Alice
ssh experiment100@server.org
At the end of the authentication, the server gets a username
(typically a pseudonym).
An optional local account mapping can be performed
(alice -> experiment100)
If account name matches the requested one, access is granted
Forwards opaque EAP packets to the IDP using the federation.
SSH server
RADIUS proxy
SSH(GSS-API (EAP))
RADIUS (EAP)
Personal computer
RADIUS (EAP)
Virtual EAP tunnel
RADIUS federation
The IDP authenticates the user and provides a response to the RADIUS proxy, optionally including a SAML assertion.
Home RADIUS IDP

Can Moonshot connect to the existing SAML federations?

- No, it requires a RADIUS-based federation infrastructure, similar to the one used for eduroam.

Can Moonshot connect to the existing eduroam federation?

- No. While technically possible, the SLA of eduroam indicates it is only usable for network access control.

What federation alternatives are there?

- Building a dedicated RADIUS/RadSec federation.
- Best approach is using the *Trust Router* protocol to improve the security
    - End-to-End connections between RADIUS proxies and RADIUS IDPs

How does the solution mitigate sharing of SSH keys?

- SSH keys are not used in this solution, since GSS-API is an alternative authentication path in SSH.

Does the solution allow for delegation?

- Yes, using OpenSSH ProxyCommand option together with either the `netcat` utility or the `-W option`
- https://moonshot-wiki.atlassian.net/wiki/spaces/Moonshot/pages/159187668/OpenSSH+Client

What are the client requirements and supported platforms?

- Clients need to install Moonshot software
  - Currently available for Linux (AMD64 and ARM64)
  - and MacOS (AMD64)
  - Missing support for mobile platforms (Android and iOS) and MS Windows >= 10
- Vanilla OpenSSH client works well

What are the SSH server requirements and does the solution require additional software beyond SSH server?

1. Install Moonshot software
2. Install a patched version of OpenSSH
   - In order to accept other GSS mechanisms beyond Kerberos

Does the solution allow for non-interactive client logins?

- Yes
- Moonshot credentials can be installed in the system, describing what services they are applicable for (list of regular expressions).
  - For example, `host/*.hpc.jisc.ac.uk`
- If a matching credential is found for the service, the user is not prompted

What requirements are put on the incoming federated identity?

- It needs to match the requested resource (eg. `account` in `account@server.org`)
- A local account mapping can be performed:
  - In the RADIUS proxy (the mapping is applied to all Moonshot services in the visited organisation)
  - In the SSH server (mapping only valid in the SSH server)

How is provisioning towards the SSH server set up?

- Not needed.
- SSH server will trust the RADIUS answer coming from the RADIUS proxy.
- The requested resource (eg. `experiment100`) needs to exist in the server
  - There are ways in which this can provisioned Just-in-time.

How does revocation work?

- By disabling the account at the home IDP
- If authentication at the home RADIUS IDP fails, access is not granted
- No need to communicate with the visited organisation

Does the setup allow for MFA?

- Yes, Moonshot allows using OATH-TOTP
- Works by appending the OTP code at the end of the password

Demo

- We will use a docker-based testbed that you can easily use:
- https://github.com/janetuk/moonshot_docker

Questions welcome

alex.perez-mendez@jisc.ac.uk