# Accessing SSH resources using IRIS IAM

Will Furnell

STFC

Science and Technology Facilities Council

# Context

- SSH keys
- x509 Certificates
- Managed by LDAP/custom solutions
- AD/LDAP authentication

# SSH access via IAM

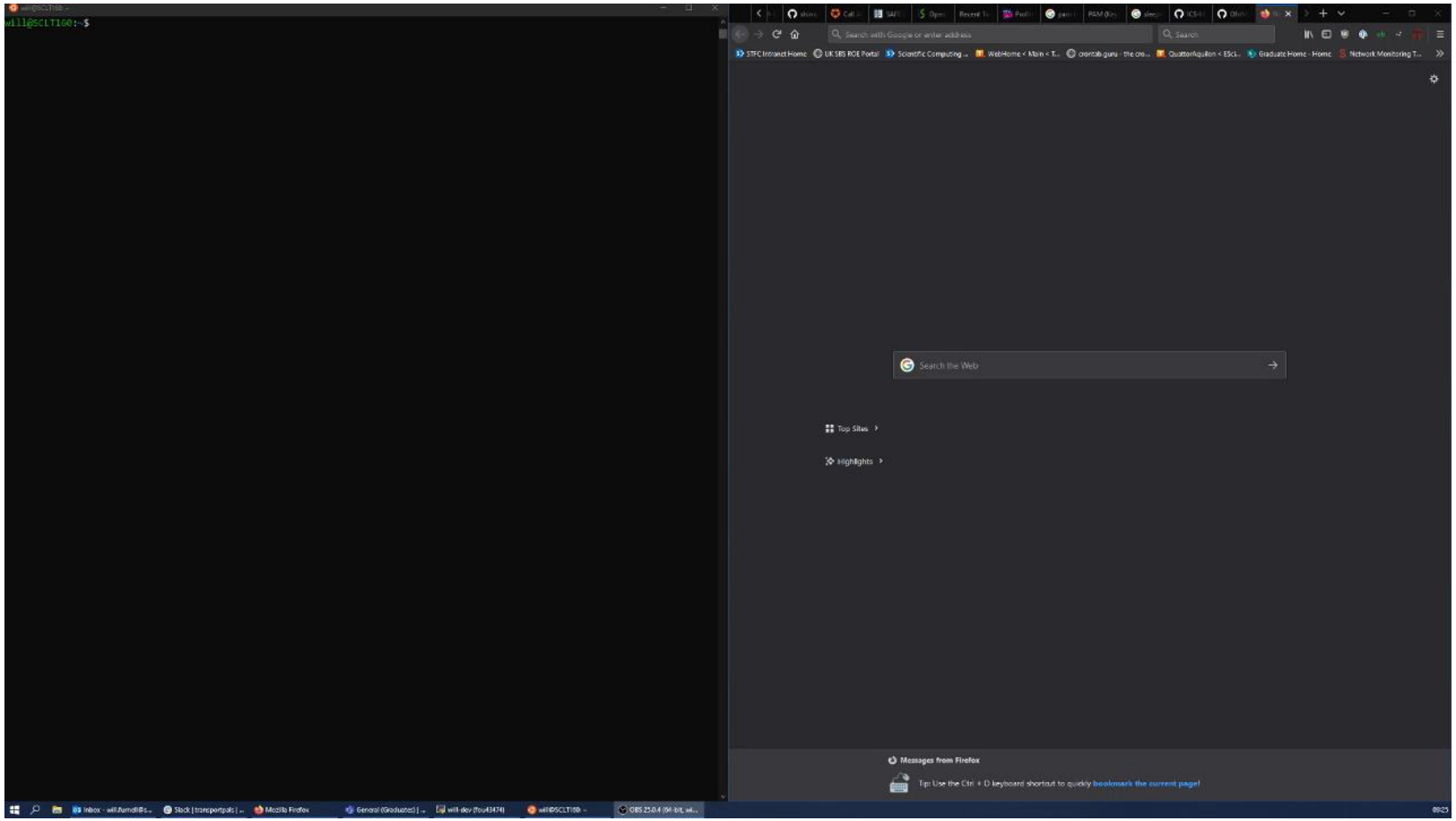
- PAM Module
  - https://github.com/stfc/pam_oauth2_device
    - Fork of https://github.com/ICS-MU/pam_oauth2_device
- No client side software needed
- Integrates well with IRIS IAM & Openstack
- No special/custom SSH server required
- Not just SSH!

Science and Technology Facilities Council

# OpenStack

- Get context metadata to retrieve OpenStack project instance is in
- Get IAM groups for this OpenStack project
- Check if users IAM group is in this list
- Check if the username the user is trying to log in as (which could be shared, e.g. *root*) is the same as the one in the pam_oauth2_device configuration file
- Let them in!

# Demo video




Science and Technology Facilities Council

# Alternative software

- Other options considered, but…
- Moonshot
  - Needs client software, which is no longer supported on Windows
  - All institutions need to deploy a RADIUS server with Moonshot support
  - We've now decommissioned our instances
- Vault
  - Needs client side software/scripts (which does work on Windows)
  - More management involved (just IAM UI is better for us)
  - Otherwise an interesting option!

will.furnell@stfc.ac.uk

Science and Technology Facilities Council