Multifactor Authentication in DiRAC

Jon Wakelin, University of Leicester

Multifactor Authentication

- Verify a user's identity using multiple credentials
  - Credentials could be: password, fingerprint, face, SSH key, SSL cert, One-Time-Password, usb key, etc, etc

- Different classes of authentication factors:
  - Things you know (knowledge): Password, PIN
  - Things you have (possession): Swipe-card, Yubikey, smartphone (receive SMS), smartphone (TOTP), SSH Key
  - Things you are (inheritance): biometrics, fingerprints, face or voice recognition
  - Location: Could be indicated by IP range

- Prefer factors from different classes
  - Often "Something you have" + "Something you know"

Multifactor Authentication

- In theory any combination of factors counts as MFA

- In practice some combinations are better than others, e.g.

  - Swipecards, Hardware token, and biometric scanners can be expensive
  - And it's difficult to distribute them securely to remote users

  - SMS requires more complicated infrastructure. Not secure either.

  - SSH key less secure because it's typically stored on same device that you use to enter your password
  - So both could be stolen at the same time.

Motivation -> Security

- 2020 Cyberattack against HPC sites
  - International, multisite and apparently targeted attacks against HPC
  - Stolen/compromised credentials use to step between systems
  - Several UK sites compromised

- Security incident at Newcastle U and Northumbria U
  - Assumed to be ransomware attack

- MFA being rolled out at pace across all UK Universities

- DiRAC TWG recommended adoption of MFA across its services

MFA across DiRAC

- Leicester (DIaL and ARM)
  - Password + TOTP
  - Cost effective, well understood and wide-range of free OTP apps available

- EPCC
  - Already introduced multifactor with Password + SSH key
  - Note: Cannot enforce passwords on private SSH keys (this is a user education issue)
  - Note: SSH key typically stored on same device that is used to enter password

  - SAFE has MFA as an option

- Cambridge
  - Currently using Password + TOTP for administrative access
  - Situation for end-users is complicated because CSD3 provides services for DiRAC, EPSRC Tiers, and local users.

- Durham/Cambridge
  - Both intend to introduce MFA for end-users in mid-term

MFA across DiRAC

- At this stage we cannot provide a single federate MFA across DiRAC
  - Each host site has its own constraints
  - Local security policies, complexity of system and user-base, existing MFA mechanisms

- The goal is to improve our security stance
  - Where we can
  - In a timely and cost-effective fashion

DIaL MFA – Basics

- Password + TOTP
  - Cost effective, well understood and a wide-range of free OTP apps are available
- Introduced in two phases
- Phase 1: Opt-in (23/Sep/2020)
  - But we strongly suggest that at least one user from every project tries it
  - And everyone sends us their feedback
- Phase 2: Compulsory (TBC)
  - Depends on outcome of Phase 1

DIaL MFA – What do I need to do?

- Install an OTP app on your phone before you start
  - Authy, Google Authenticator, MS Authenticator, FreeOTP, LastPass, etc, etc
  - Do not need internet connection.
  - No information is sent over network.

- If you do not have a smartphone
  - Standalone OTP apps are available
  - But note …
  - you will be keeping the “thing you have” (i.e. your OTP secret)
  - On the same device that you will enter the “thing you know” (i.e. your password)

DIaL MFA – Phase 1

- People wishing to opt-in will need to create a secret
  - Instructions will be provided

- The secret will be displayed in the SSH terminal as a QR code
  - Secret is also displayed as a string (should you need it)
  - Rescue codes will also be displayed

- Take a screenshot of the QR code using your OTP app.
  - Do not share this with others.
  - Close your terminal once you have imported secret.

- Store the rescue codes somewhere safe
  - Don’t write down passwords or secret.
  - Rescue codes can only be used once – for instance if you lose your phone.

DIaL MFA – Phase 2

- MFA becomes compulsory
  - Timescale for implementation depends on outcomes from Phase 1

- Secret will be created automatically on first entry
  - You should import into your OTP app immediately.

- We are using a trust-on-first-use (TOFU) approach
  - I.e. you can login **once** using just a single factor
  - It is likely we will time-limit this (e.g. 24 hours from the point your account is created).

DIaL MFA – Anticipated issues

- Automating workflows
  - One of the main uses of passwordless SSH keys
  - EPCC have already had to address this and have looked different solutions
  - Multiplexed SSH connections
  - IP address could act as second factor for “trusted” systems

- Lost phone / lost secret
  - Email is insecure we cannot just send you a new secret or rescue code
  - DiRAC Host sites do not keep personal details for users – so we cannot call you or ask you security questions
  - Current solution
    - Web-conf with PI (who should be known to us) and project member (who should be known to PI)
    - PI should confirm identity of member to in order to establish a chain of trust.
    - Once identity is confirmed – we revert to time-limit TOFU or else issue a one-time Rescue Code.

Questions?