Security procedures and MFA

IRIS security workshop

10th Feb 2021

Current access procedures

- Some variation between sites
  - Where these differ, the our procedures are presented here…
  - Not all security tools are mentioned...
- Firewalls
  - Some login nodes bypass firewalls for performance reasons
    - Rely on OS firewall (IP tables)
  - Other services are behind firewalls
- Access generally only ssh
  - With ssh keys
    - Passphrases mandated, but cannot be enforced

Security tools used

- Fail2ban
  - Blocks repeated failed access attempts using iptables
- rkhunter
  - Looks for unexpected changes to files
    - Including inode changes

Regular patching

- Critical updates applied ASAP
  - Most systems use CentOS
- Regular scheduled downtime periods
  - For other updates

ssh-related

- Host-based authentication internally
  - No internal ssh keys to be compromised
  - No use of authorized_keys file
- Known compromised keys revoked
- Known hosts keys hashed

User lifecycles

- Annual renewal of accounts
- Moribund accounts (4 months) disabled

Vulnerability Mitigation

- e.g. recent hyperthreading bugs

Multifactor authentication trial

-
- Motivation: May 2020 HPC cyber attack
  - And others
  - MFA being rolled out at universities
  - TWG recommends adoption
- Password + TOTP solution
  - Currently opt-in
    - Trial period being used to iron out issues
  - Will be enforced for all users shortly
    - Trust on first use approach: Secret generated at first login (time limited)

Anticipated MFA issues

- Automated workflows
  - Now largely worked out
  - Multiplexed ssh connections
  - Trusted IP as 2nd factor
- Lost secret
  - Video conference with PI to generate new code
  - time limited trust on first use

Potential weaknesses

- Non-ssh services
  - e.g. ports open for web services
- User weaknesses
  - Compromised ssh keys/accounts

Security items

- Standing item on fortnightly TWG meeting
- 2 members of security council
- -security mail list

Future plans

- MFA rollout likely
- User account creation updates
- Ongoing hardening