MFA for SSH* at Diamond Light Source

James Thorne

* And NoMachine too

Remote access at Diamond

- Fortinet VPNs (have MFA)
  - Corporate
  - BYOD
  - Both staff only
- SSH
  - Staff and Users
- NoMachine ("NX") remote desktop
  - nx-staff
  - nx-user

diamond

Current measures

- Accounts are locked in AD after too many failed attempts
- IP addresses banned after too many attempts in too short a time
- SSH key revocation lists

Why now?

- Several high profile (in photon sciences at least) security incidents
- Because we should
- We **really** should

Options for MFA

- Use a third-party authentication server (e.g. privacyIDEA)
- Use existing MFA provided by Azure AD via RADIUS
- Use the google-authenticator package from EPEL
- Remove SSH / NX access

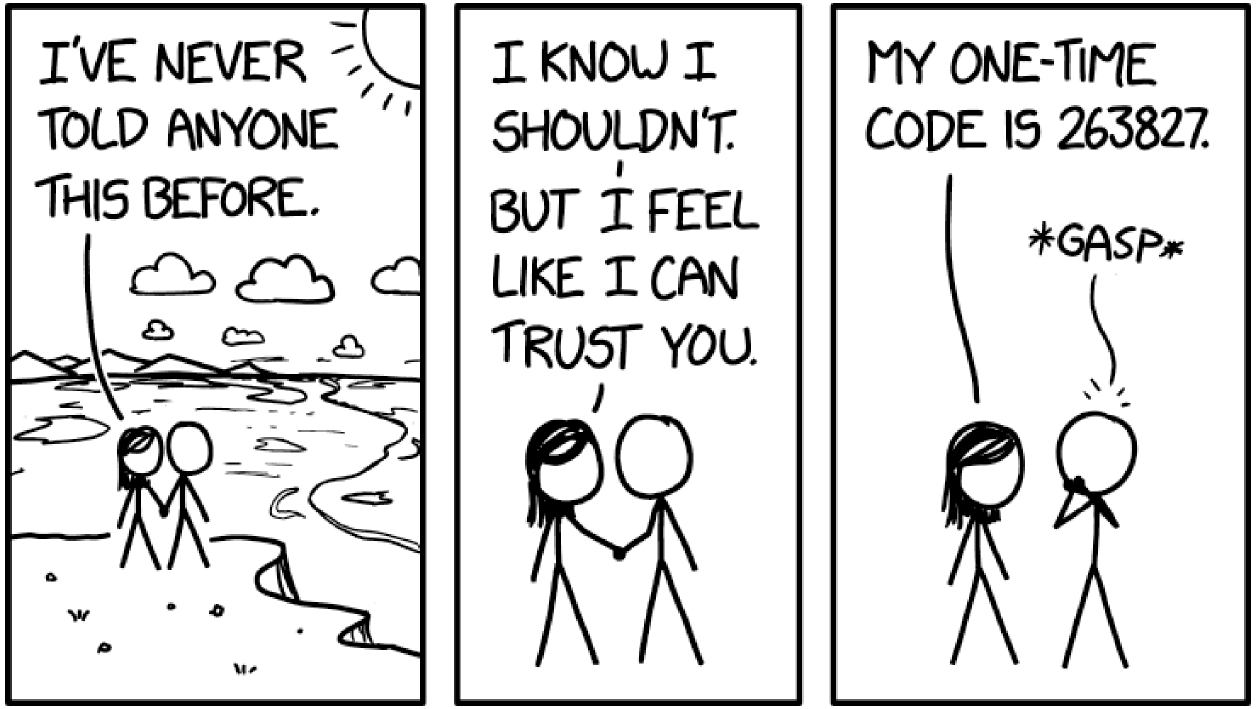
Azure AD via RADIUS

- Preferred solution from Corporate IT
- We already use it for VPN and MS365
- Supports all methods that we have for Azure AD
- Enrolment already set up
- Tested and it works well, mostly
- But…
    - Only available for Diamond staff (needs AD account)
    - What would we do about facility users?

Choice: google-authenticator package

- Easily installed from EPEL
- PAM configuration is quite simple
- No RADIUS or other servers to set up.
- Would work for staff **and** facility users
- But...
  - Users must run the enrolment script themselves
  - That script needs to be run somewhere trusted that the user can SSH to (at least for now).
  - Enrolment answers require some IT knowledge

Some problems cannot be fixed


I'VE NEVER TOLD ANYONE THIS BEFORE.
I KNOW I SHOULDN'T. BUT I FEEL LIKE I CAN TRUST YOU.
MY ONE-TIME CODE IS 263827.
GASP

https://xkcd.com/2543/

Challenges

- Considered Azure AD for staff and goolge-authenticator for facility users
  - Too complicated!
  - Likely to need multiple SSH services
- Will need to think hard about enrolment – as simple as possible!
- Communicating change to users and staff. Many are not keen on the idea, even now.
- Soft or hard rollout?

diamond

Enrolment

1. User logs in for first time (either ssh.diamond or a dedicated enrolment machine). We plan to trust user/pass combo on first login.
2. Script is run via pam_exec PAM module that checks for user's MFA config and starts enrolment process if not configured. Most questions pre-answered with DLS defaults.
3. On subsequent logins, user gets MFA prompt.

Some notes on NoMachine ("NX")

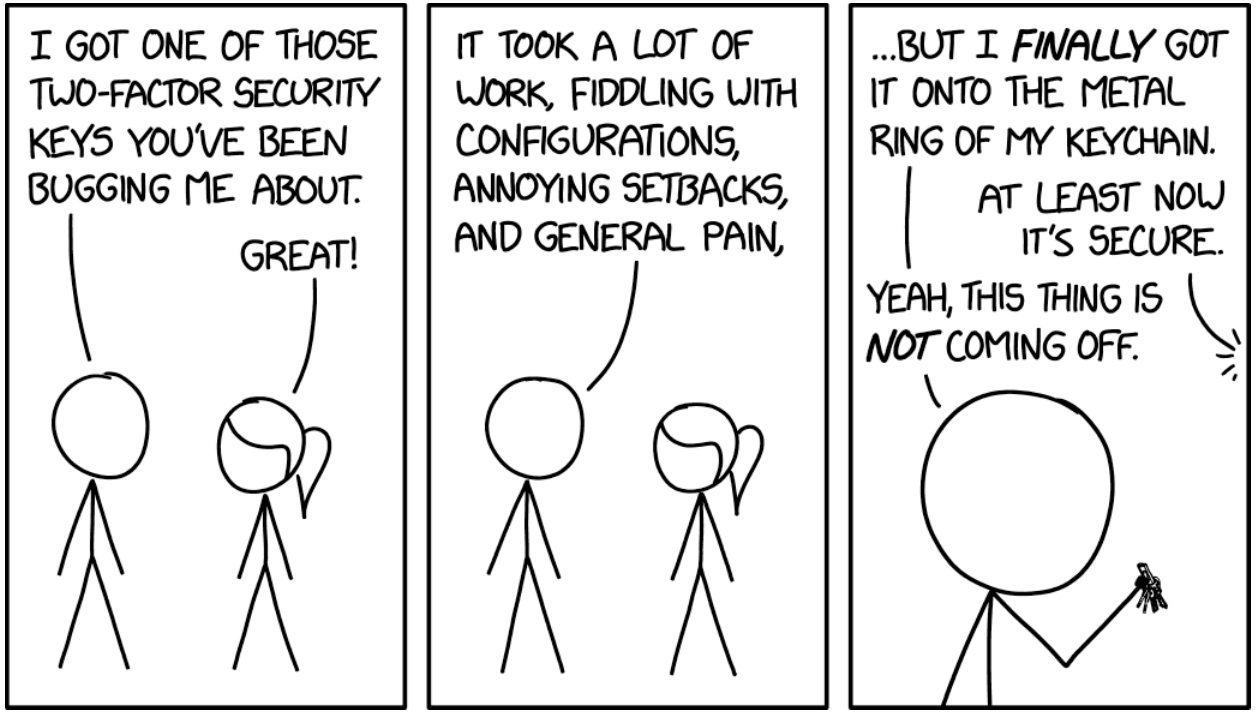
- NoMachine confirmed to pass PAM prompts to user as text input boxes. Work done for SSH "just works" for NX.
- Enrolment would not work via NX so users and staff must login via SSH first.

Summary

- MFA for SSH is hard (at least for us)
- Still need to convince some stakeholders (sigh)
- Enrolment will need some careful development to avoid a large support load.
- Need to consider the future as this proposal is not ideal and may become a "temporary solution".

diamond

Questions?


I GOT ONE OF THOSE TWO-FACTOR SECURITY KEYS YOU'VE BEEN BUGGING ME ABOUT.
GREAT!
IT TOOK A LOT OF WORK, FIDDLING WITH CONFIGURATIONS, ANNOYING SETBACKS, AND GENERAL PAIN,
...BUT I *FINALLY* GOT IT ONTO THE METAL RING OF MY KEYCHAIN.
AT LEAST NOW IT'S SECURE.
YEAH, THIS THING IS *NOT* COMING OFF.

https://xkcd.com/2522/