2FA + SSH: A Creative Solution for Secure, User-friendly HPC Authentication

Fabian Lingenhöl
Motivation

- **Goal:** Prevent unauthorized login with stolen credentials
- **Common solution:** Multi-factor authentication
- **Problem:** How to integrate with SSH?
  - SSH certificates
  - Local OTP service (e.g. pam_oath)
- **Our solution:** Remote OTP service
Integrate 2FA and SSH

Service Portal (bwIDM)

- LDAP
- LinOTP

reg-app
Integrate 2FA and SSH

Service Registration

Token Registration

Service Portal (bwIDM)

LDAP

LinOTP

Browser

reg-app
Integrate 2FA and SSH

Service Registration
Token Registration

Browser

Service Portal (bwIDM)

LDAP
LinOTP

HPC System

SSH Client

User name

SSH Server

LDAP
reg-app

2FA + SSH: A creative solution for secure, user-friendly HPC authentication
Integrate 2FA and SSH

- Browser
  - Service Registration
  - Token Registration

- SSH Client
  - User name
  - OTP
  - Service PW

- HPC System
  - SSH Server

- Service Portal (bwIDM)
  - LDAP
  - LinOTP

- reg-app
  - LDAP
  - LDAP
  - LinOTP

- 2FA + SSH: A creative solution for secure, user-friendly HPC authentication

May 24, 2023
What about automated workflows?

- So far:
  - Successfully integrated 2FA
  - Separated cluster operation and identity management
- But: Automated workflows often rely on SSH keys
- Dynamic (de-)activation of keys
  - E.g. we unlock „interactive“ SSH keys only if user logged in with 2FA in the past hour
  - Enables automated workflows
User Adoption

Login method by number of users
- 2FA only: 89%
- 2FA + Key: 10%
- Command Key: 1%

Login method by number of logins
- 2FA only: 48%
- 2FA + Key: 36%
- Command Key: 16%

Numbers are for March 2023 on HoreKa