

Multi-factor Authentication

Coming to a NERSC near you...

You Have Probably Heard of MFA

Factor == Authentication Method	Password One-time Password (OTP) Certificate Hardware Token Biometric
Multi-factor ::= 2+ factors	password + OTP token + PIN badge + retinal scan
Different attacks for each factor	

As seen on TV

Google

Banking (OTP via SMS, chip and PIN)

Apple Touch-ID and Face ID are technically not multi-factor

What's the point?

Protect against password theft

MFA at NERSC

Current	For ssh Using Google Authenticator Opt-in, can easily opt-out again No password needed between systems
Future	MFA for Web, HPSS, etc. Support for different types of tokens Single-sign-on Automation support

Where it's working

Working	Cori Edison Denovo PDSF Genepool
Testing or In Progress	DTNs NX



any questions?