What is Authentication?

The Core Problem of authentication

Authentication vs. Authorization & Access Control

Kinds of Authentication factors (what you know, what you are, and what you have)

- This lecture will focus on passwords, biometrics, and public key authentication.

Password authentication (What you know)

Chosen password requirements/ Measuring Password Strength

people pick their passwords in an insecure way

Learn from the leakage of RockYou

Measuring password strength: Shannon entropy is not a good way, min-entropy is better

How is the password stored?

Never store passwords in plaintext

Storing hashing passwords is a better way, but still has problems

Hashing passwords with salt is the best way

Attacks on Passwords

Online and offline attacks

Multi forms of password authentication

Two-factor authentication

SMS (short message service) Authentication

Time-based One-Time Passwords

Biometric Authentication (What you are)

Fix Biometric Error Rates via fuzzy extractor

Pros and Cons of biometric authentication

Public key Authentication (What you have)

SSH Authentication (https://www.ssh.com/academy/ssh, RFC 4251, 4252)

A simplified version of SSH Authentication

Pros and Cons of SSH authentication

How to use SSH to login Github