CSci 4271W
Development of Secure Software Systems
Day 10: OS security: introduction and authentication

Stephen McCamant (he/him)

University of Minnesota, Computer Science & Engineering

Based in large part on slides originally by Prof. Nick Hopper

Operating systems

- The goal of an operating system is to provide a uniform platform for programs to access system resources.
- The security goal of an operating system is to prevent processes from inappropriately accessing resources used by other processes.
- In order to do this, the OS must also protect itself from the processes it manages.

Operating Systems

An OS broadly provides three kinds of security functions:

- 🛂 Authentication: linking processes to users

Operating Systems

An OS broadly provides three kinds of security functions:

- 🛂 Authentication: linking processes to users
- 🔒 Access Control: making decisions about access to resources

Operating Systems

An OS broadly provides three kinds of security functions:

- 🛂 Authentication: linking processes to users
- 🔒 Access Control: making decisions about access to resources
- 🛡️ Protection: enforcing access control policies

Outline

OS security: overview

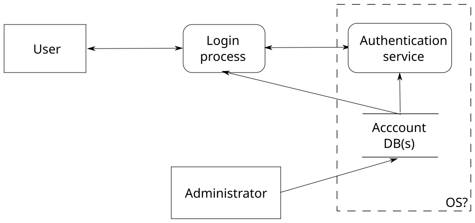
OS security: authentication

Announcements intermission

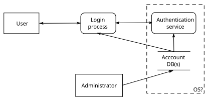
OS security: authentication factors

Authentication

Linking an OS process to an account

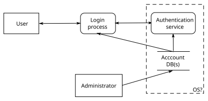


Authentication threats (1/2)



- Spoofing: user ↔ login ↔ auth service
- Tampering: DB, user/login/auth flows
- Repudiation: auth logs

Authentication threats (2/2)



- Information Disclosure: DB, user ↔ login
- Denial of service: user/login/auth flows, login/auth processes
- Elevation of Privilege: login/auth processes

Outline

OS security: overview

OS security: authentication

Announcements intermission

OS security: authentication factors

Upcoming assignments

- Homework 3 now posted, due a week from today
- Section drafts for project 1 due a week from Thursday (updated)
- Are you looking at BCBMC yet?

Outline

OS security: overview

OS security: authentication

Announcements intermission

OS security: authentication factors

Authentication factors

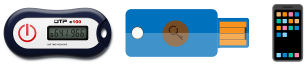
🔑 Something you have

👁 Something you are

Password: ***** Something you know

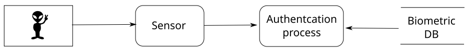
- Someplace (and/or time) you are
- Someone(s) you know

Tokens...(something you have)



- Can be stolen, lost, forgotten, destroyed
- Potentially vulnerable to compromise (e.g. phone)
- Often stored close to what they are protecting
- Inconvenient to users and add cost to system

Biometrics (something you are)



- Examples: face recognition, fingerprint, iris scan, voice recognition, retinal scan, hand geometry
- Sensors experience errors, so authentication is probabilistic
- Possible spoofing of reading to sensor, sensor to system
- Change of measured property
- Information disclosure risks

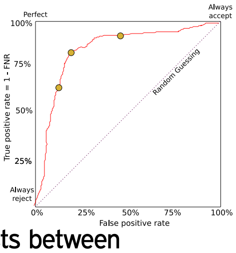
Biometric errors

- Errors can be introduced due to environmental conditions:
  - Lighting, humidity, temperature, etc.
  - Noise (acoustic or E-M)
  - Position of person relative to sensor
  - Normal biological variation, etc.
- Systems produce a confidence level (say, $\in (0, 1)$) and accept if confidence is above some threshold.

Biometric errors, cont'd

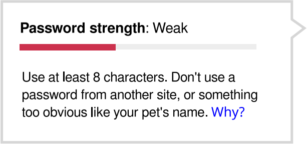
False Positive Rate:
Probability of incorrectly accepting
$FP/(FP + TN)$

False Negative Rate (insult rate):
Probability of incorrectly rejecting
$FN/(FN + TP)$



Tuning the confidence level adjusts between psychological acceptability and safe defaults.

Passwords (something you know)



Password strength: Weak

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?

Hard to remember
vs.
easy to guess

- User-chosen passwords are easy to guess: John-the-ripper-type crackers routinely guess 40%+ of password leaks
- Randomly-generated passwords are hard to remember, so they're written down, stolen, harder to type, forgotten
- Studies show that (well-designed) strength meters can help.

Threats to passwords

- Online attacks
- Offline attacks
- Targeted attacks
- Password reset
- Observation

Protecting passwords

- Cool-down/back-off
  - Online attacks
  - Targeted attacks
- Hashing / salt
  - Offline attacks
- Password expiration?