# CSE 523S: Systems Security



Co

Systems

Spring 2018

Jon Shidal

# Plan for Today

- Announcements
  - Always bring your laptop to class
    - anyone without a laptop?
  - HW1 officially assigned today, due 1pm Wednesday
- Questions?
- System Security Fundame
  - Security Principles
  - Security Building Blocks
- Assignment

# SECURITY PRINCIPLES

# Three Natural Questions

- Does it work?
- What will it co
- Is it secure?
- Question: are these 3 questions similar in nature?

# Does it work?  & What will it Cost?

- Functional Requirements
  - Does our system meet them?
  - A lot of the field focuses on this.
- What will it cost?
  - Time?
  - Money?

# What does “Is it secure?” Mean?

- Can anyone else access my data?
- Can I control who uses the device?
- Can anyone use my data and/or the internet connection on the device?
- Can someone spy on my usage of the device?
- Can someone delete or corrupt my data?
- Can anyone see the data I send or receive on a network?

# “Can anyone else access my data?”

- An easy source of trouble: the word “anyone”
- Suppose someone passes this test



- Let’s try to be precise and tie in answering this question

# “Can anyone else access my data?”

- Does the device have authenticated users?
  - Is it a multi-user device?
  - Are data access control mechanisms in place?
  - If users sign-i
    - Is it possible f
    accepting a false user ident



- Can unauthorized users gain access?
  - Has the device been determined to be hack-proof, and impervious to unauthorized access through technical means?

# “Can anyone else access my data?”

- Can authorized users delegate access to their data?
  - If a user can grant data access to another user, does the original user have any control over who else might get access?
- Is there an administrative account that can create and modify user
  - If so, then whoever controls the administrative account can control access to data.
- Can the system be reset to factory defaults without destroying data?
  - Some systems provide a means to reset a system following a lost account credential that keeps the original data intact.

# “Can anyone else access my data?”

- Is the data archived on a backup service or device?
  - If so, how is access to that data managed?
- Do local laws require a ba or access by government authorities?
  - If so, can a user verify either that such an access request is legitimate, or whether such accesses have taken place?

# Have we reached the bottom?

- That was question 1 of 6...
- It seems clear that "Is the system secure?" is a different kind o
- **We need to develop a pe e to manage the seemingly boundless complexity**

# People, Process, Technology

- Security has non-technical aspects
- Our systems a
from many angles.
- To answer “Is it secure?” we need to address each

# Examples

# People

Security measure: Provide training periodically to ensure that users have an understanding of security risks and are aware of common pitfalls



Attack: Fool users into di eir access credentials by sending c g email messages that appear to be legitimate requests. Phishing attacks.

# Process

Security measure: Design rules and procedures for users and systems that are intended to improve security and increase the effort required on the part of the attacker, e.g. a policy locked out after 5 failed logins cannot endlessly attempt passwords.



Attack: Attacker can still disrupt service by attempting multiple logins and forcing accounts to be locked. Then send phishing email with "instructions" for unlocking account.

# Technology

Security Measure: Software systems use a lot of libraries and applications to provide functionality.



Attack: Software with an exploitable weakness is the prime target for attackers find vulnerabilities, exploits get published and attacks spread.

# Sleight of hand?

- Many of these issues seem like apples and oranges.
  - Do they all fit what you thought of as security?
- Unauthorized access is clearly a security violation
- What about obscene?
  - Is it really the same thing?
- How many issues might we dream up?
- What about time?
  - Someone has access, do they keep it forever?
  - Can they make copies of data and keep them?

# Information Security (InfoSec)

- As a field, InfoSec has dealt with these broader issues



- InfoSec enco
  - Network
  - systems security



- "CIA" triad is one contribution of the field

# Confidentiality, Integrity & Availability

- Confidentiality
  - Is it secret?
  - Is it kept secret even while being transmitted to an authorize
  - Is it kept secret even while existence of the data secret?
  - Is the list of authorized users kept secret?



- Integrity
- Availability

# Confidentiality, Integrity & Availability

- Confidentiality

- Integrity
  - Has it been
    - In storage
    - While being transmitt horized user?
- Availability

# Confidentiality, Integrity & Availability

- Confidentiality

- Integrity



- Availability
  - Is it accessible?
  - Is time to access it a factor?
    - What if an attacker just makes it slow and painful for an authorized user to get their data?

# SECURITY BUILDING BLOCKS

# Security Concepts & Building Blocks

- Encryption & Cryptography
  - What most people think of as Security.
  - Its Math so it must be hard and it must be cool.



- Authentication
  - Identifying who or what we are talking to?

# Encryption & Cryptography

- Single-key crypto (aka symmetric crypto)
  - Encrypted data is indistinguishable from random data
  - Use a "shared secret" or "key" to encrypt/decrypt
- Public-key cry
  - I have a pair of keys, pu p private
  - I give you my public key
  - You use the public key to encrypt
  - I use my private key to decrypt

# How do we share and manage keys?

- How do I get your public key?
  - Web, email, USB stick
- How do I get a
- What problems arise?

# Certificates

- We place our trust in “Certificate Authorities”, or CAs
- A certificate contains
  - a public key
  - the name of
  - the name of the attestin
  - and the signature of the CA.
- Which CAs can we trust?
  - Up to Microsoft, Google, Apple, Firefox, etc.

# VeriSign, March 2001

- Issue two Microsoft root/CA certs to a fraudster
- Oops!
- All MSFT up-to-date softw kes" these certificates
  - No public admissions of fraud

# Alternative: Web of Trust

- Use decentralized trust model



- If you know m

ust me

  - Anyone who





  - Anyone who distrusts y w distrust me

# Authentication: Matching Identity with Credentials

- Can be based on
  - Something
  - Something
  - Something you are: ring

# Two-Factor Authentication

- Biometrics are flaky

- A best practice is to rely on two methods to authenticate



cally Maybe not e

- Does anyone here use two-factor authentication?

- Check out:

  https://www.google.com/landing/2step/

# Assignment

- HW1 assigned today, due Wednesday 1/24



- For Wednesd
  - Skim: HTA
  - Read: HTAOE Ch 2. 19