INTRODUCTION

THEY ARE OUT TO GET YOU
WHAT IS SECURITY?

- A system’s **security policies** describe
  - What the system is **supposed to do**
    - *Store and provide access to a user’s personal files.*
  - What the system is **not supposed to do**
    - *Do not allow other users to access or modify a user’s files, unless explicitly permitted to.*
INTRODUCTION

ATTACKS AND VULNERABILITIES

- An **attack** tries to violate security policies by exploiting vulnerabilities.

- A **vulnerability** is an unintended aspect of a system’s *design, implementation, or configuration*:
  - storing client permissions on the client
  - unchecked array bounds
  - world-writable configuration files
  - initializing pseudorandom generator with a constant seed
INTRODUCTION

ATTACKS REQUIRE RESOURCES

- Some attacks can only be launched by adversaries with significant resources.
  - SHA-1 collision: two PDFs with same hash [1]
    - 6,500 CPU years + 110 GPU years
    - ~$110,000 of cloud time
  - MD5 collision for two Windows Update images: $0.65

- But violating security properties can have great value

INTRODUCTION

RECENT HIGH PROFILE DATA BREACHES

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By TARA SIEGEL BERNARD, TIFFANY HSU, NICOLE PERLROTH and RON LIEBER  SEPTEMBER 7, 2017

Equifax, one of the three major consumer credit reporting agencies, said on Thursday that hackers had gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver’s license numbers.

The attack on the company represents one of the largest risks to personally sensitive information in recent years, and is the third major cybersecurity threat for the agency since 2015.

Equifax, based in Atlanta, is a particularly tempting target for hackers. If identity thieves wanted to hit one place to grab all the data needed to do the...
INTRODUCTION

WHO IS THE ADVERSARY?

- Honest but clumsy (or curious) users
- L33t H@X0rs looking for a challenge
- Disgruntled employees
- Criminals interested in financial gain
- Intelligence agents seeking information
- Militaries intent on overthrowing a government

via Defense Science Board
THE PATH TO SECURITY

- What **threats** are considered?
  - *Who might gain from comprising the system?*

- What **vulnerabilities** are exploitable?
  - *Nation states have bigger budgets than 14-year olds*

- What **assurance** is there that the system is free of vulnerabilities?
HOW DO WE KNOW POLICIES WILL BE ENFORCED?

- Informal (but important)
  - User/developer training and awareness
  - OPSEC-aware business and development processes
  - Trust in the capabilities and reputation of developers
- More formal (focus of this course)
  - Formalization and verification
  - Economic/game theoretical arguments
Policies describe behavior of system *principals*: the people, computers, or other entities involved in a system

A principal may act on its own or on behalf of another principal:

- A program acting on a user’s behalf
- A computer acting on behalf of the program it runs
WHAT SHOULD PRINCIPALS DO? OR NOT DO?

Policies can be described in terms of three properties:

- **Confidentiality**
  - Which principals may learn what information

- **Integrity**
  - What the system ensures, and what changes are permitted

- **Availability**
  - When must inputs be readable or outputs produced
CONFIDENTIALITY

- Protecting secrets as well as *inferences* about them, or even their existence

- For example

  ```plaintext
  public := 0;
  if secret == 1 then
      public := 1
  ```

- The contents of the variable `public` *leaks* the value of the variable `secret` (without requiring direct access)
“Bad things should not happen”

- Correctness criteria
- Absences of crashes or unexpected exits or errors

Also for constraining how data may be modified:

- Only a particular user or program can modify
- Any modification must satisfy X, Y, Z constraints
- Before running code, must pass validation
Access control alone is insufficient

\[
\begin{align*}
\text{public} & := 0; \\
\text{if } \text{secret} == 1 \text{ then} & \hspace{1cm} \text{public} := 1
\end{align*}
\]

\[
\begin{align*}
\text{trusted} & := 0; \\
\text{if } \text{untrusted} == 1 \text{ then} & \hspace{1cm} \text{trusted} := 1
\end{align*}
\]

Controlling how information \textit{flows} is as important as controlling access to it.
“Good things should happen”

A service that is required

- Provide access to cloud backup files
- Continually monitor for evidence of fire
- Process request in the order they are received

Important for critical infrastructure and services that may be subjected to denial-of-service attacks
NAME THAT PROPERTY VIOLATION

- Copying an answer during an exam
- Hacking Equifax and changing your credit score
- Attempting to guess someone’s PIN so many times that it locks the device for five minutes.
- Figuring out a way to run a program that reports whether you have the highest grade in a class.
- Figuring out a way to change someone’s email password and using it to log in and delete an email you sent them.