Lecture 1 – The Security Mindset

University of Illinois

ECE 422/CS 461

Logistics

- Create your GitHub repository (link on website).
  - You must complete this step before TA can push MP1 to your repository next Tuesday
- First quiz goes out today, due next Friday
- Prof Bates' online 461 now available to both graduate and undergraduate students
- Slides will be uploaded to Canvas before class
  - Poll: How do you use slides if available before class?

Goal of this Lecture

- By the end of this lecture you should:
  - Be able to define security
  - Begin to think like an attacker
  - Begin to think like a defender

Course Objectives

- Common **attacks** and **defenses** in various computer systems (software, hardware, OS, web, network, etc.)

- The security **mindset**, a form of critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance defense costs and benefits
  - Learn to be a security-conscious citizen

The Security Mindset

- Suppose Apple introduces Face ID today. What is your reaction?

- A: I can’t wait to try it!
- B: I wonder if it can be broken by doing X/Y/Z?

What is Computer Security?

- A collection of **properties** that hold in a **system** in the presence of an **adversary** under a set of **constraints**

What is Computer Security?

- A collection of **properties** that hold in a **system** in the presence of an **adversary** under a set of **constraints**

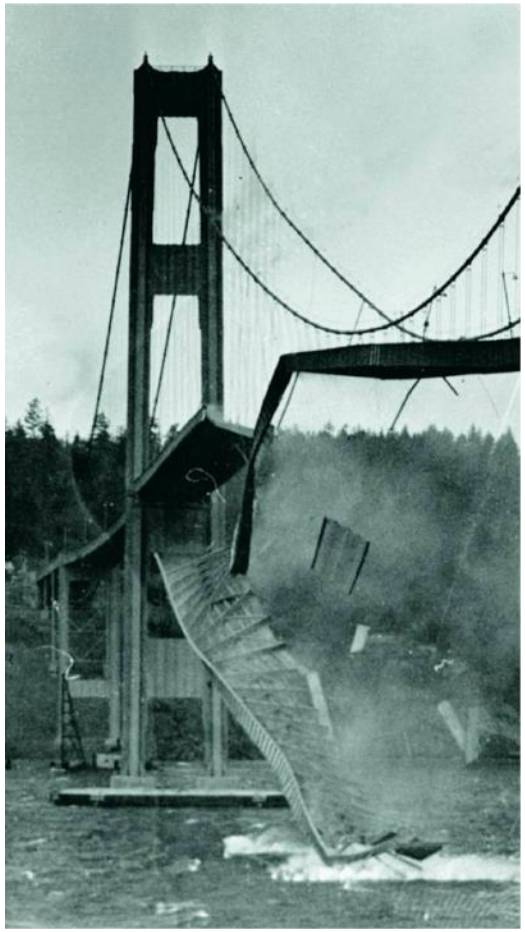
- PC, phones, web servers, data centers, network, IoT devices, smart home, cars, ...
- Hardware, software, data

What is Computer Security?

- A collection of **properties** that hold in a **system** in the presence of an **adversary** under a set of **constraints**

- CIA triad (mostly)
  - **C**onfidentiality
  - **I**ntegrity
  - **A**vailability
  - (Variants: Authenticity, Accountability, Privacy)

What's the difference?



Tacoma Narrows Bridge (1940)

New York's World Trade Towers (2001)

DEPENDABILITY PROBLEM

SECURITY PROBLEM

Meet the Adversary

- Computer security studies how systems behave in the presence of an **adversary**
  - a.k.a. the attacker
  - a.k.a. the bad guy

* An intelligent agent that actively tries to cause the system to misbehave.

What is Computer Security?

- A collection of **properties** that hold in a **system** in the presence of an **adversary** under a set of **constraints**

- Assumptions on the system's & users' behaviors, and adversary's capabilities

“Know your enemy.”

- Motives?
- Capabilities?
- Degrees of access?
- Knowledge?

故曰：知彼知己，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆。

Think like an Attacker

- Look for weakest links – easiest to attack
- Think outside the box: not constrained by the system designer's worldview & assumptions

Think like an Attacker

- Look for weakest links – easiest to attack
- Think outside the box: not constrained by the system designer's worldview & assumptions
- Practice: For every system you interact with, think about what it means for it to be secure, and how it could be broken by an attacker.

Exercise

Exercise

- Is Face ID secure?

Spoofing

Think as a Defender

- Security policy (goals)
  - What **properties** are we trying to enforce?
- Threat model (**constraints)**
  - Assumptions on systems, users, environment, and attackers?
- Countermeasures

Security Policy

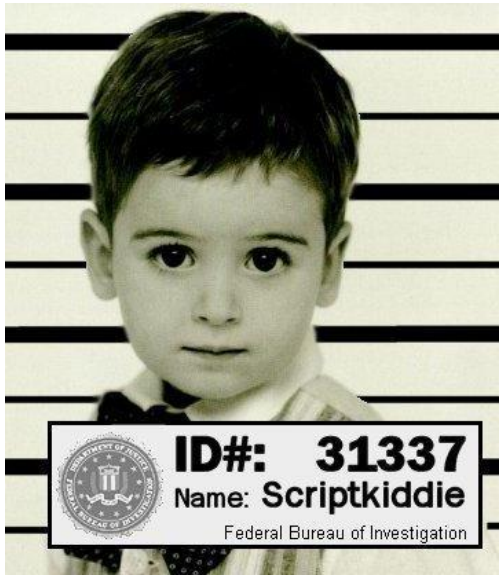
- What **properties** are we trying to enforce?
  - **C**onfidentiality?
  - **I**ntegrity?
  - **A**vailability?
  - Authenticity? Accountability? Privacy?

  - All of these, or a subset of them?

Threat Models

- Who are the attackers? Motives? Capabilities? Degree of access? Knowledge?

  (Know your enemy!)



Threat Models

- Who are the attackers? Motives? Capabilities? Degree of access? Knowledge?

  (Know your enemy!)

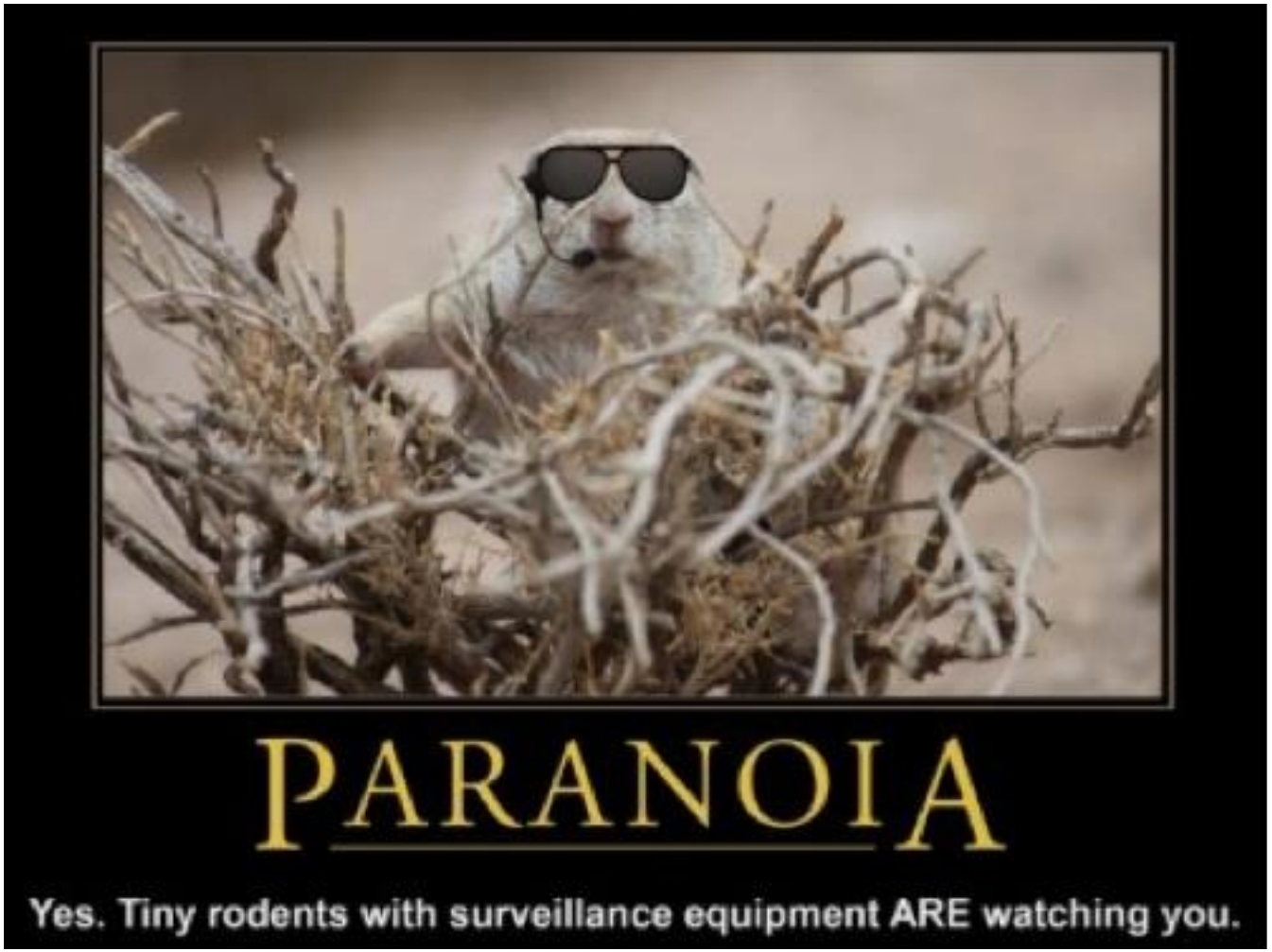
- What kinds of attacks do we need to prevent?

- What kinds of attacks should we ignore?

Risk Assessment

- What would security breaches cost us?
  - Direct costs: Money, property, safety, ...
  - Indirect costs: Reputation, future business, …
- How likely are the breaches?
  - Probability of attacks?
  - Probability of attack success?

Rational Paranoia



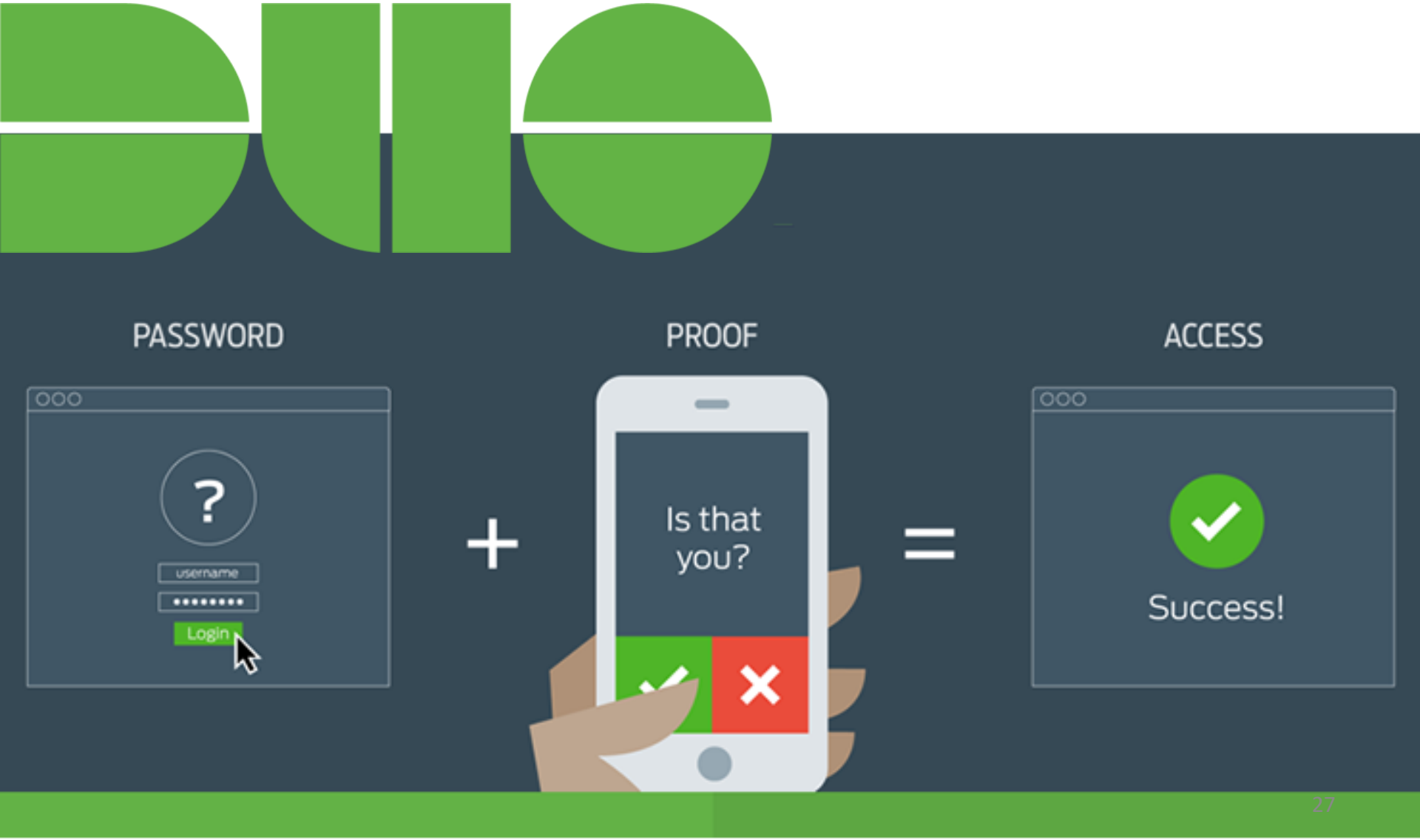
Countermeasures

- No security mechanism is perfectly secure
  - What assumptions are we relying on?
  - Terminology: trusted vs. trustworthy component
- No security mechanism is free
  - Direct costs: implementation, performance, …
  - Indirect costs: lost productivity/convenience, added complexity, …

Countermeasures

- No security mechanism is perfectly secure
- No security mechanism is free
- No system is ever completely secure. Challenge is to rationally weigh costs vs. risks.
  - Human psychology makes reasoning about high cost/low probability events hard

Defense: Two Factor Authentication



Defense: Automatic Updates

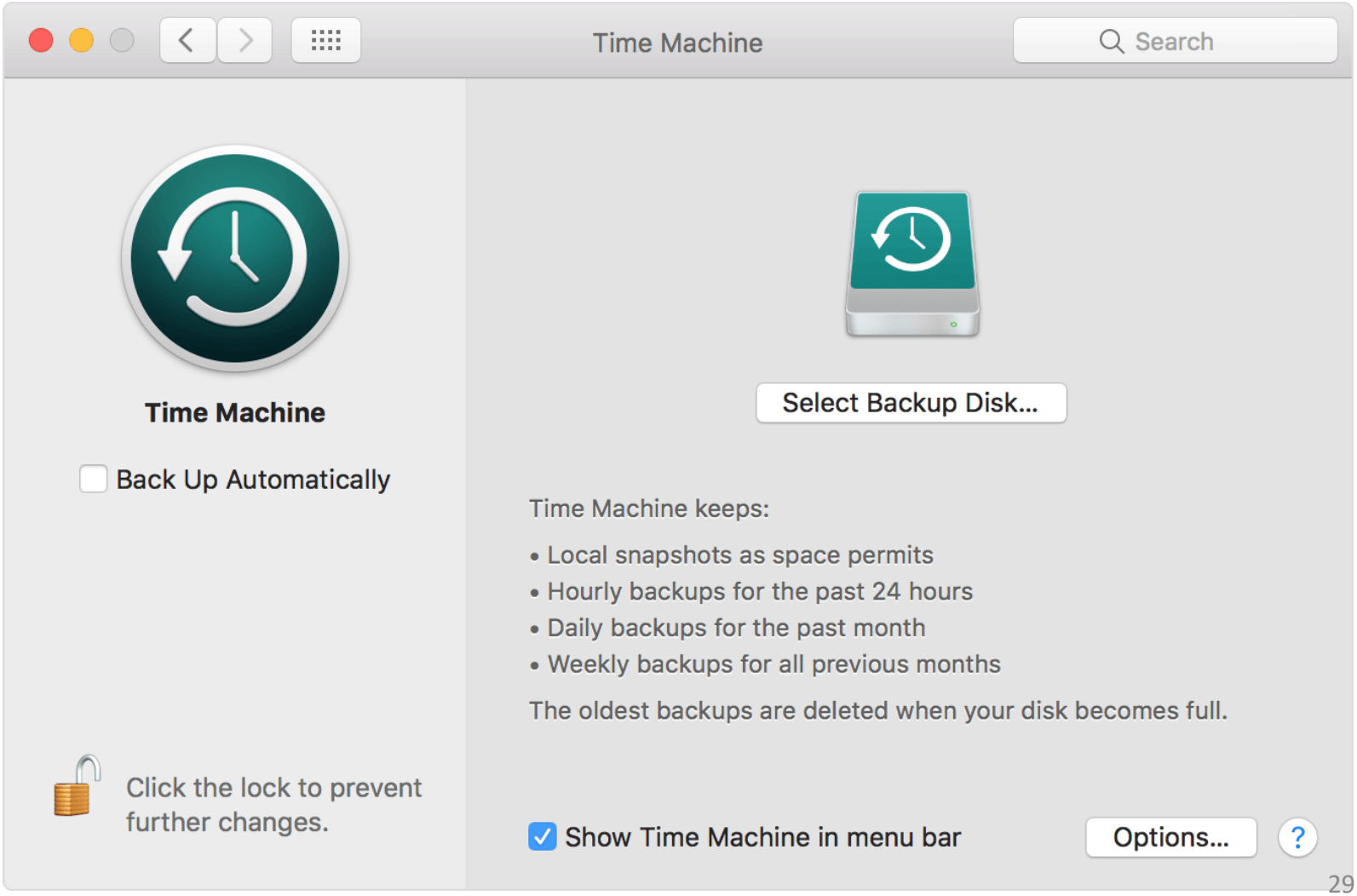
The App Store keeps OS X and apps from the App Store up to date.

- [x] Automatically check for updates
  - [x] Download newly available updates in the background
    You will be notified when the updates are ready to be installed
  - [x] Install app updates
  - [ ] Install OS X updates
  - [x] Install system data files and security updates
- [-] Automatically download apps purchased on other Macs
  Can't determine if automatic downloads are enabled due to a network problem

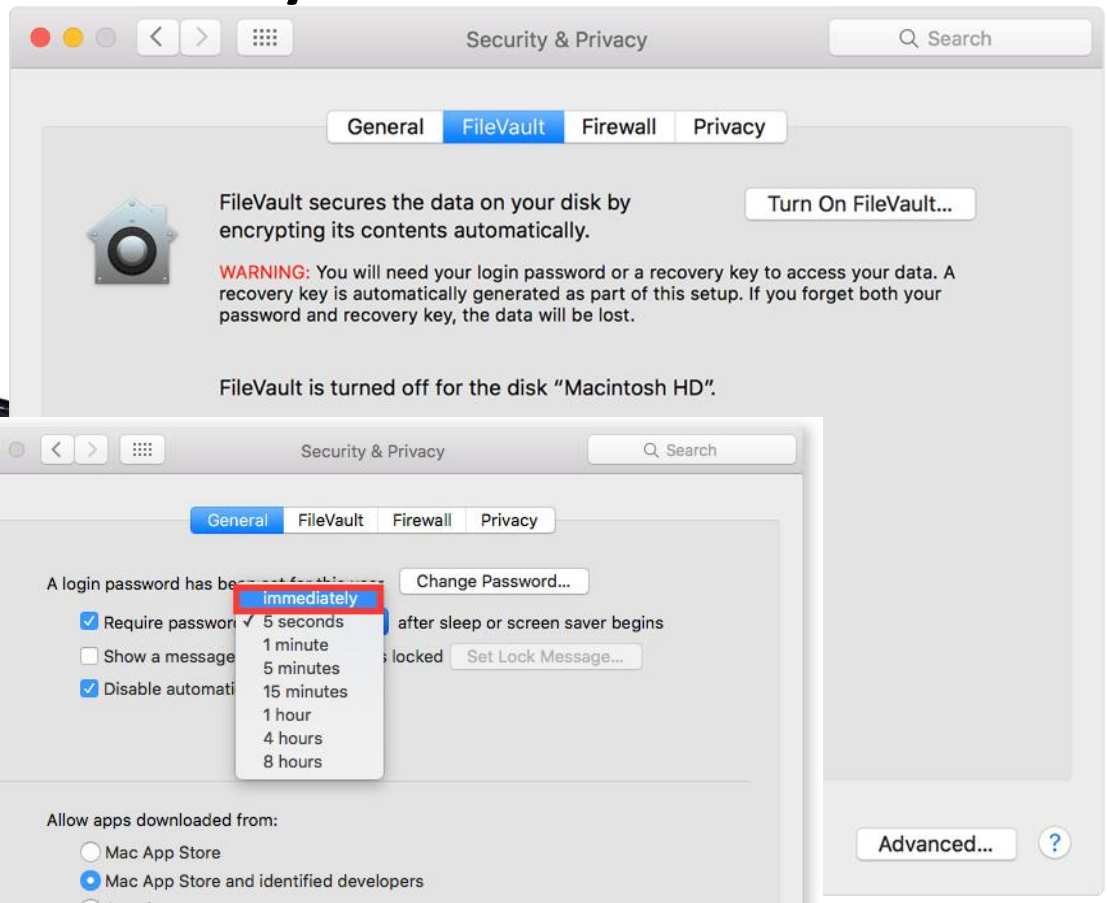
Last check was Thursday, December 1, 2016 Check Now

?

Defense: Backups

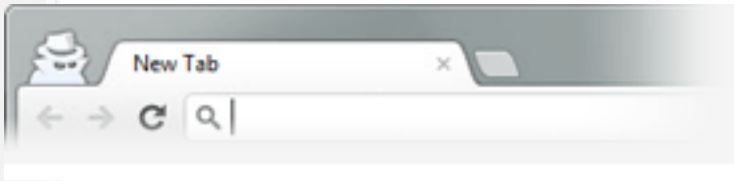


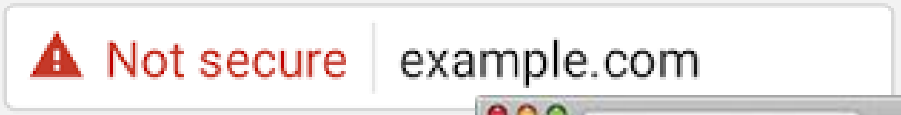
Defense: Disk Encryption, Physical Security



Defense: HTTPS, Safe Browsing

Eventual treatment of all HTTP pages in Chrome:





Summary: Computer Security

- A collection of **properties** that hold in a **system** in the presence of an **adversary** under a set of **constraints**

Summary: Security Mindset

- Think like an attacker
  - Look for ways to break a system
- Think like a defender
  - Know what you're defending, against whom
  - Assess risks and set reasonable threat model
  - Weigh benefits vs. costs of countermeasures

To Learn More …

- The Security Mindset. https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html
- https://freedom-to-tinker.com/blog/felten/security-mindset-and-harmless-failures/
- https://cubist.cs.washington.edu/Security/2007/11/22/why-a-computer-security-course-blog/