Lecture 02: The Security Mindset

Professor Adam Bates

CS 461 / ECE 422

Fall 2019

Goals for Today

- Learning Objective:
  - Take on the perspective of security practitioners
  - Reason about the costs of attacks (and defenses)
- Announcements, etc:
  - **DISCUSSION ROOM CHANGE!!** Section ADJ (4:00-4:50) will take place in 1302 Siebel Center (not 1103).
    - In effect for entire semester! Check website for reminder
  - New to class? Please review course requirements and past materials at https://courses.engr.illinois.edu/cs461/fa2019/
  - Adam has office hours this week (Friday 1-2); TA's do not.

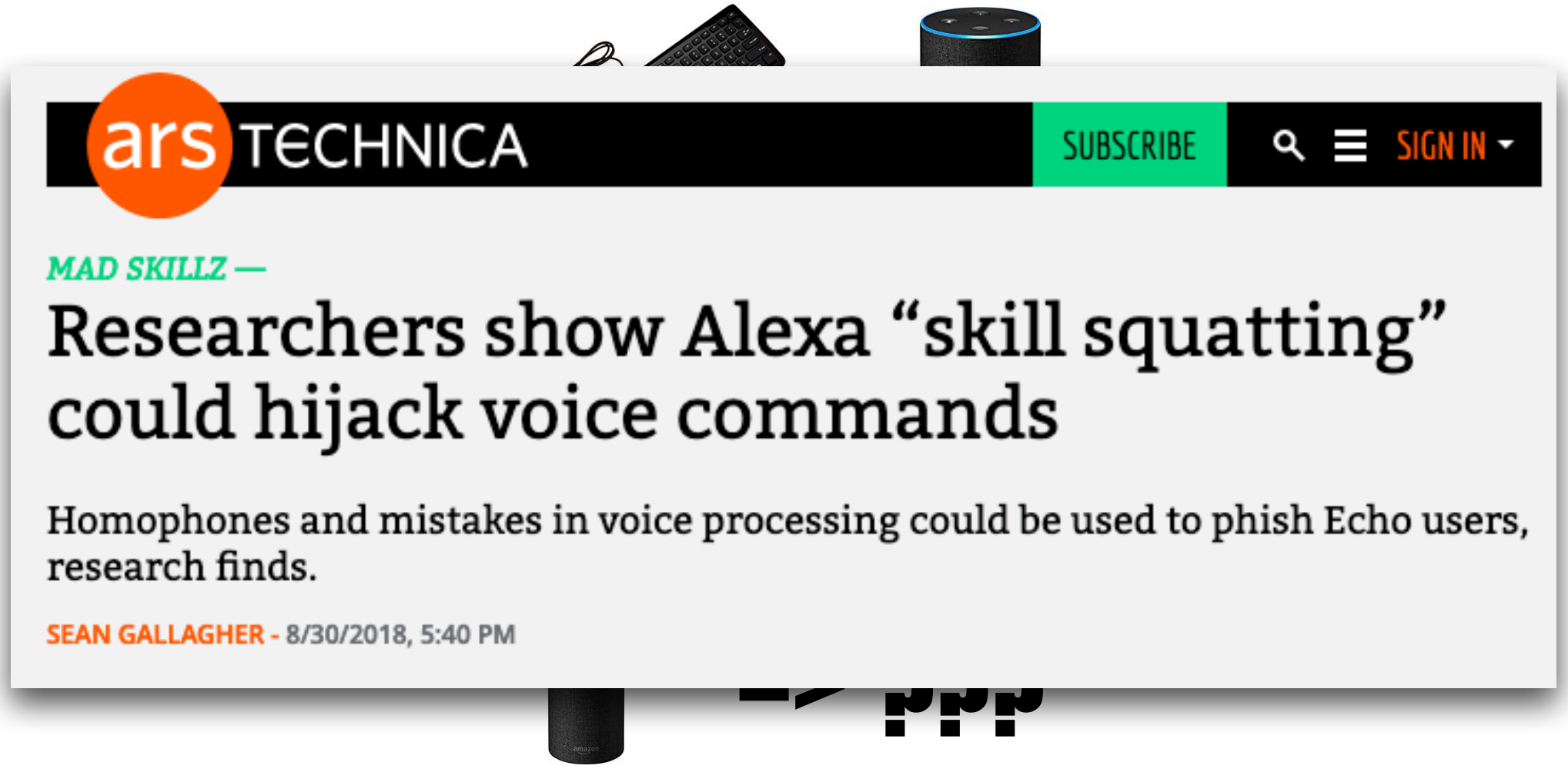
Reminder: Please put away devices at the start of class

More Announcements!

- Announcements, cont'd:
  - *Starting next week,* TA office hours will take place in 4405 Siebel Center (4th floor of Siebel on Goodwin side of bldg.)
  - Today, create your personal Git repository for this course if you haven't already: https://edu.cs.illinois.edu/create-ghe-repo/cs461-fa19/
    - Afterwards your repo will be available at https://github-dev.cs.illinois.edu/cs461-fa19/<NetID>

Reminder: Please put away devices at the start of class

The Security Mindset



ars TECHNICA SUBSCRIBE SIGN IN

MAD SKILLZ —

Researchers show Alexa "skill squatting" could hijack voice commands

Homophones and mistakes in voice processing could be used to phish Echo users, research finds.

SEAN GALLAGHER - 8/30/2018, 5:40 PM

[Kumar et al., USENIX Security'18]

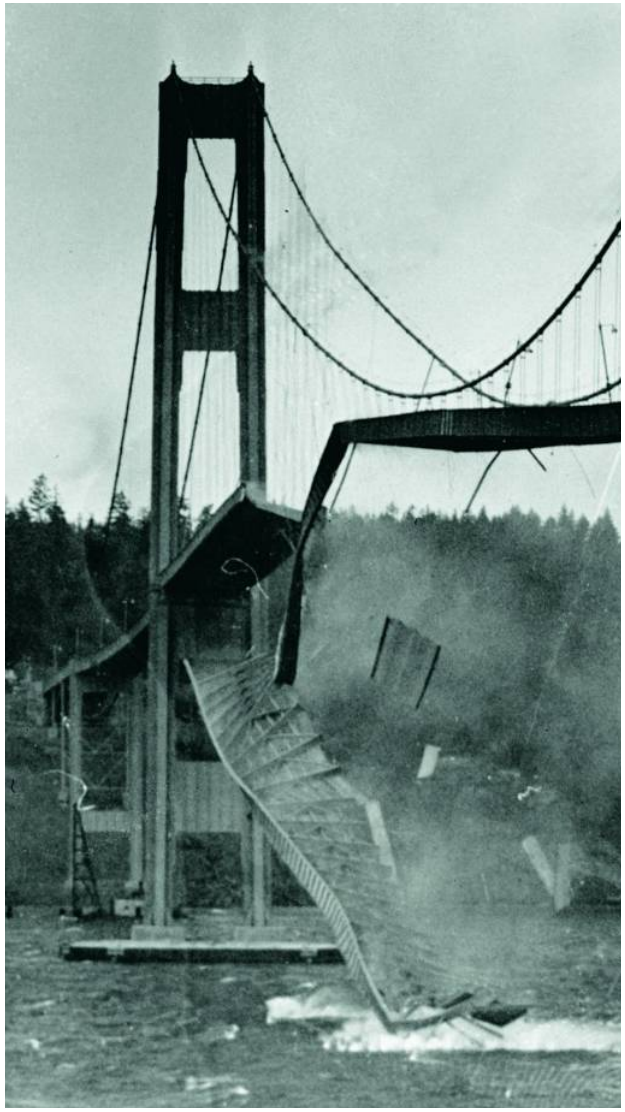
A goal of this course…

- The security mindset, a form of critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
  - How to balance **technology** costs and benefits
    - *Is this technology secure?*
    - *Can it be made secure?*
    - *Is it safe for this technology to exist?*
- Learn to be a security-conscious citizen

What is Computer Security?

- A property (or more accurately a collection of properties) that hold in a given **system** under a given set of **constraints**
  - **system** is anything from hardware, software, firmware, and information being processed, stored, and communicated.
  - **constraints** define an adversary and their capabilities.
- Can also mean the measures and controls that ensure these properties
- Security is weird, requiring a different mindset than other computing properties like correctness or performance…

What's the difference?



Tacoma Narrows Bridge (1940)

New York's World Trade Towers (2001)

Meet the Adversary

- "Computer security studies how systems behave in the presence of an adversary."
  - a.k.a. attacker
  - a.k.a. the bad guy
- The intelligent agent that…
  - actively tries to cause the system to misbehave
  - makes use of legitimate functionality in unexpected ways

"Know your Enemy"

- **Motives & objectives?**
- **Capabilities?**
- **Degrees of access?**

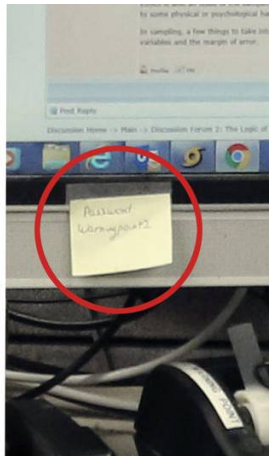
Thinking like an Attacker

To understand or improve the security of a computing system, we need to think like the adversary.

- What are the weak links in the system?
  - *Administrative Gateway? DIY crypto? Physical Access? Weak password?*

Thinking like an Attacker

What's wrong with this picture?



Thinking like an Attacker

To understand or improve the security of a computing system, we need to think like the adversary.

- What are the weak links in the system?
  - *Administrative Gateway? Weak crypto? Physical Access? Weak password?*
- What assumptions does security depend on?
  - *Platform integrity? Trusted Hardware? Proprietary algorithm?*
  - Do the assumptions hold in all cases?
- The attacker is not constrained by the system designer's world view; as defender, you can't be either.

Thinking like an Attacker

To understand or improve the security of a computing system, we need to think like the adversary

- Wh
  - A
- Wh
  - I
  - Do the assumptions hold in all cases?

Practice thinking like an attacker:
For every system you interact with, think about what it means for it to be secure, and image how it could be exploited by an attacker.

- The attacker is not constrained by the system designer's world view; as defender, you can't be either.

Thinking like an Attacker

Exercise

Thinking Like a Defender

- Security Policy
  - What is the intended use of the system?
  - What entities within the system are we trying to protect?
  - What properties are we trying to assure?
  - What components of the system can we trust to enforce these properties?
- Threat Model
  - What are the attackers? What are their capabilities and objectives?
- Risk Assessment
  - What are the weaknesses of the system?
  - How likely are they to be exploited?
- Countermeasures
  - What mitigations are available (technical, non-technical)? What do they cost?
  - Do they satisfy the security policy under the given threat model?

As compared to paranoia?

As compared to paranoia?

Challenge is to think rationally and rigorously about risk. *Rational paranoia.*

Security Policies

- What assets are we trying to protect?
  - We'll need to (efficiently) enumerate the list

- What properties are we trying to assure?
  - Confidentiality
  - Integrity
  - Availability
  - Privacy
  - Authenticity

Security Policies

- What are the intended users of the system?
- What accesses must we authorize within our security policy for the system to perform its intended function?
- What components of the system will we trust to enforce our security policy?
  - i.e., what is our trusted computing base?

Question: What is better, to be trusted or to be trustworthy??

Threat Model

- Who is the adversary?
  - What are their motives and objectives?
  - What are their capabilities?
- What kinds of attacks do we need to prevent?
- Limitations — what kinds of attacks should/must we ignore?

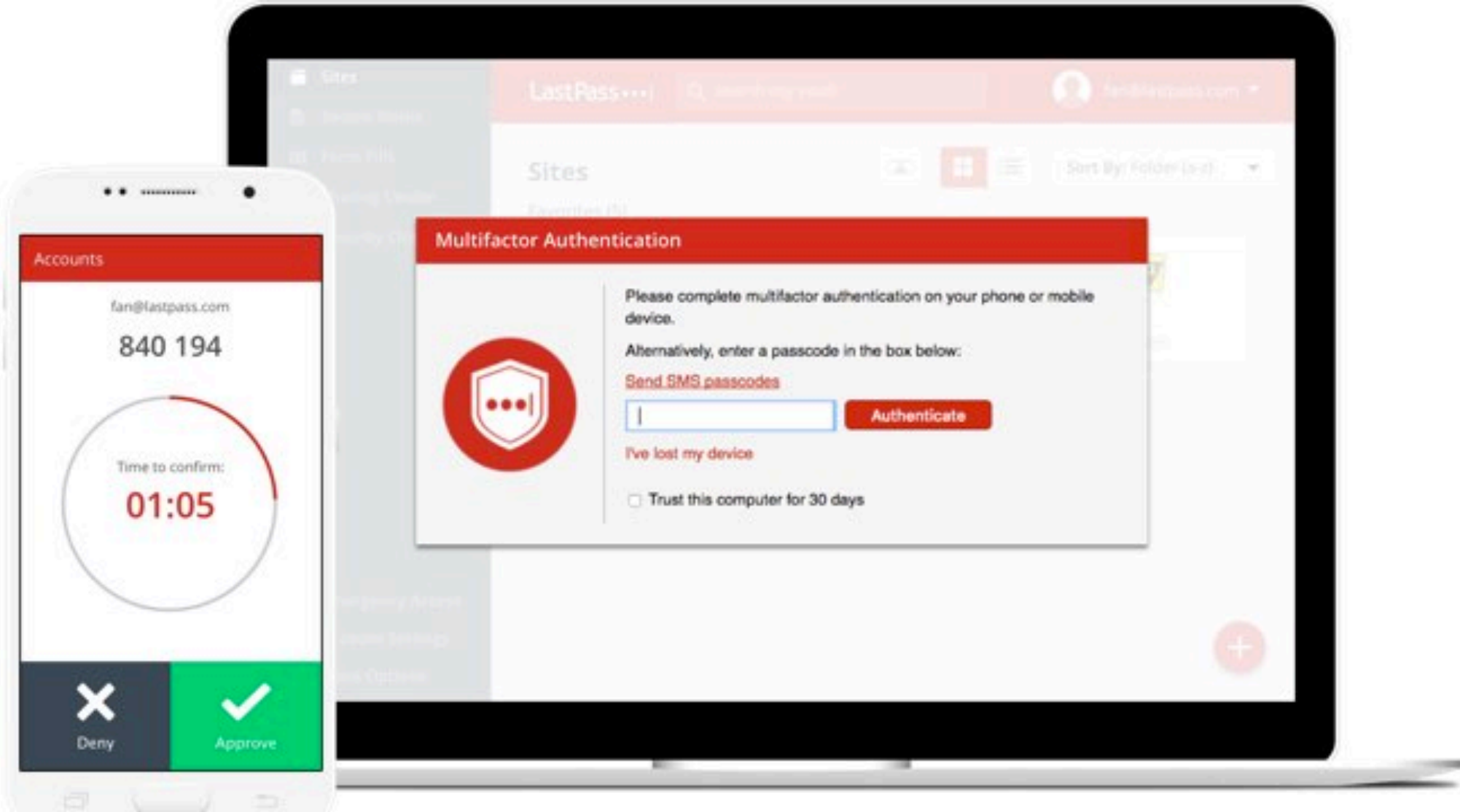
Assessing Risk

- What would a security breach cost us?
  - Direct costs: Money, property, safety, …
  - Indirect costs: Reputation, future business, …
- How likely are we to suffer these costs?
  - Probability of attack?
  - Probability of attack *success*?

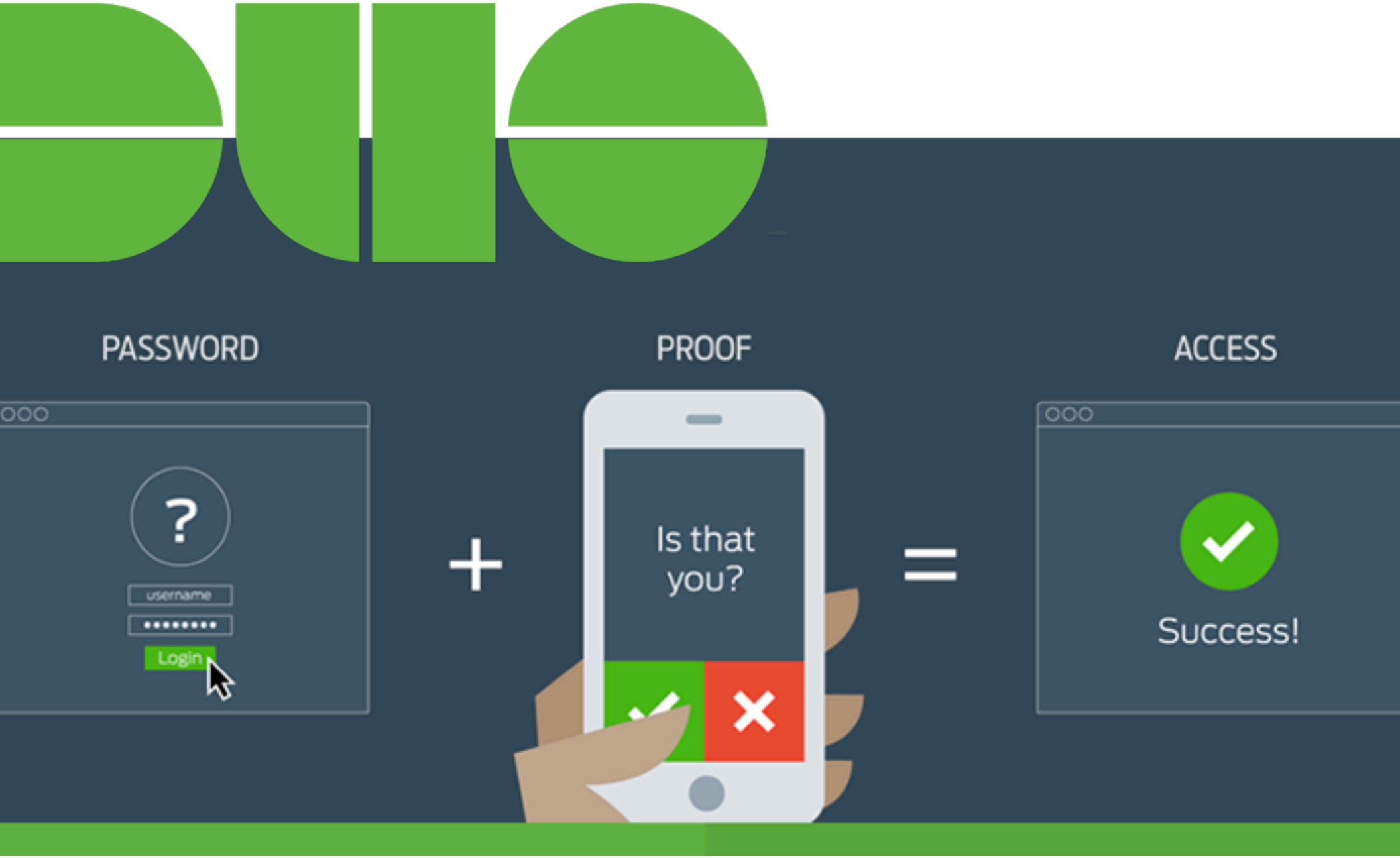
Countermeasures

- No security solution is free…
  - Direct Costs: Design, Implementation, Enforcement, Licenses, Subscriptions, …
  - Indirect Costs: Lost productivity, added complexity, false positives, …
- Challenge is to rationally weigh costs vs. risks
  - Human psychology makes reasoning about high cost/low probability events hard
- Non-Technical Countermeasures?
- Technical countermeasures?

Defense: Password Manager



Defense: Two Factor Authentication



Defense: Automatic Updates

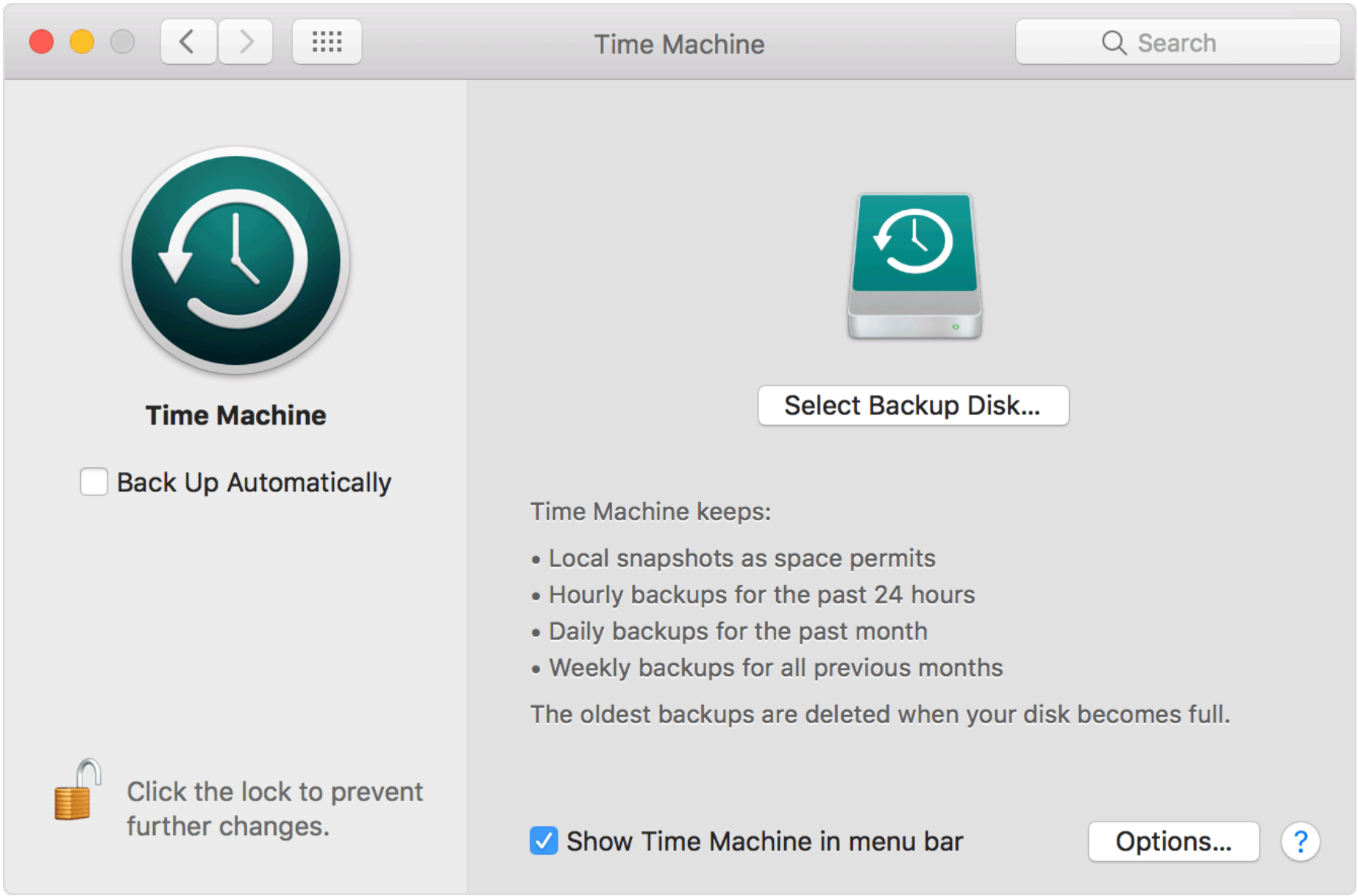
The App Store keeps OS X and apps from the App Store up to date.

- [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

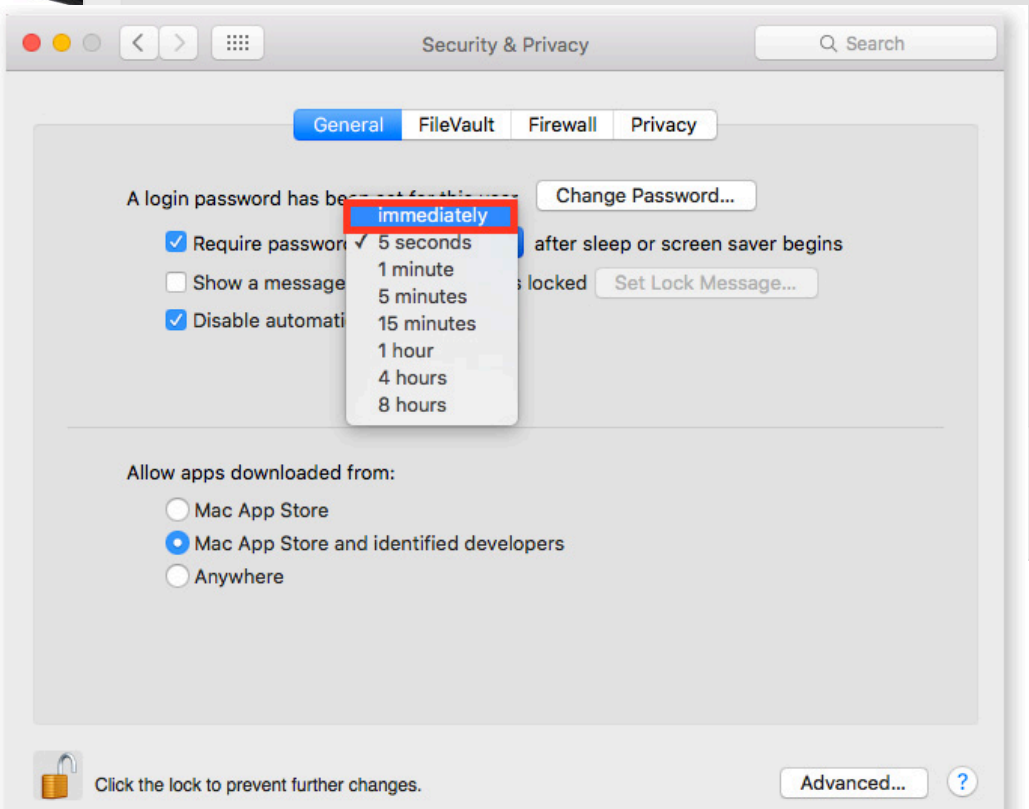
Last check was Thursday, December 1, 2016 Check Now

?

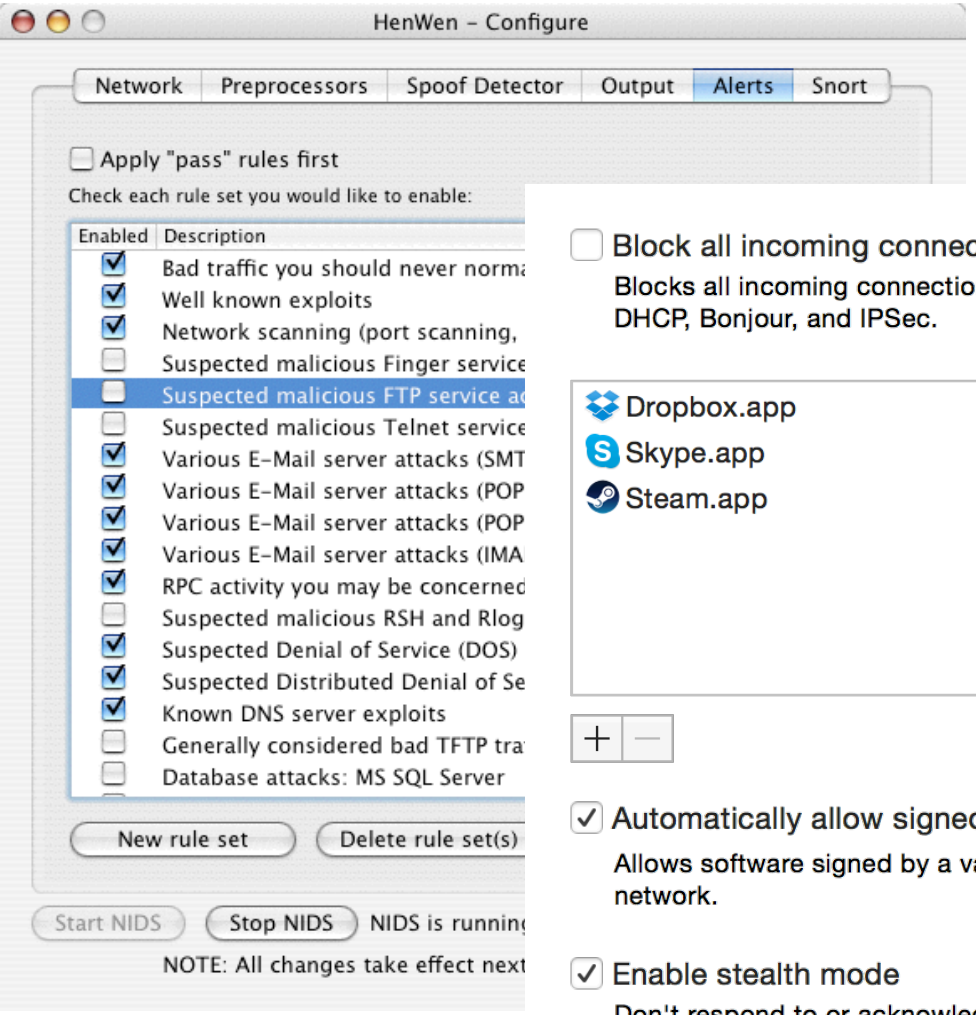
Defense: Backups

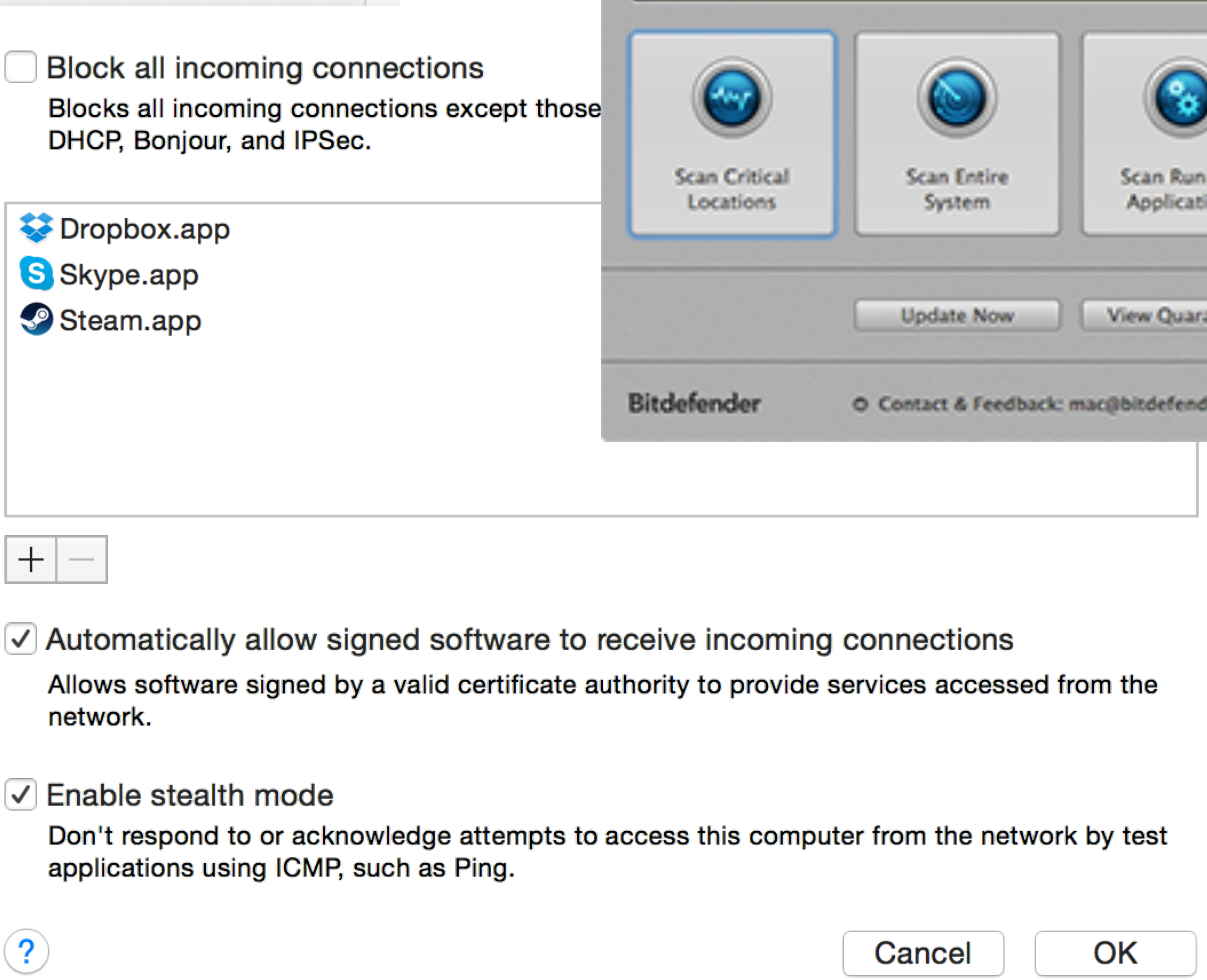


Defense: Disk Encryption, Physical Security

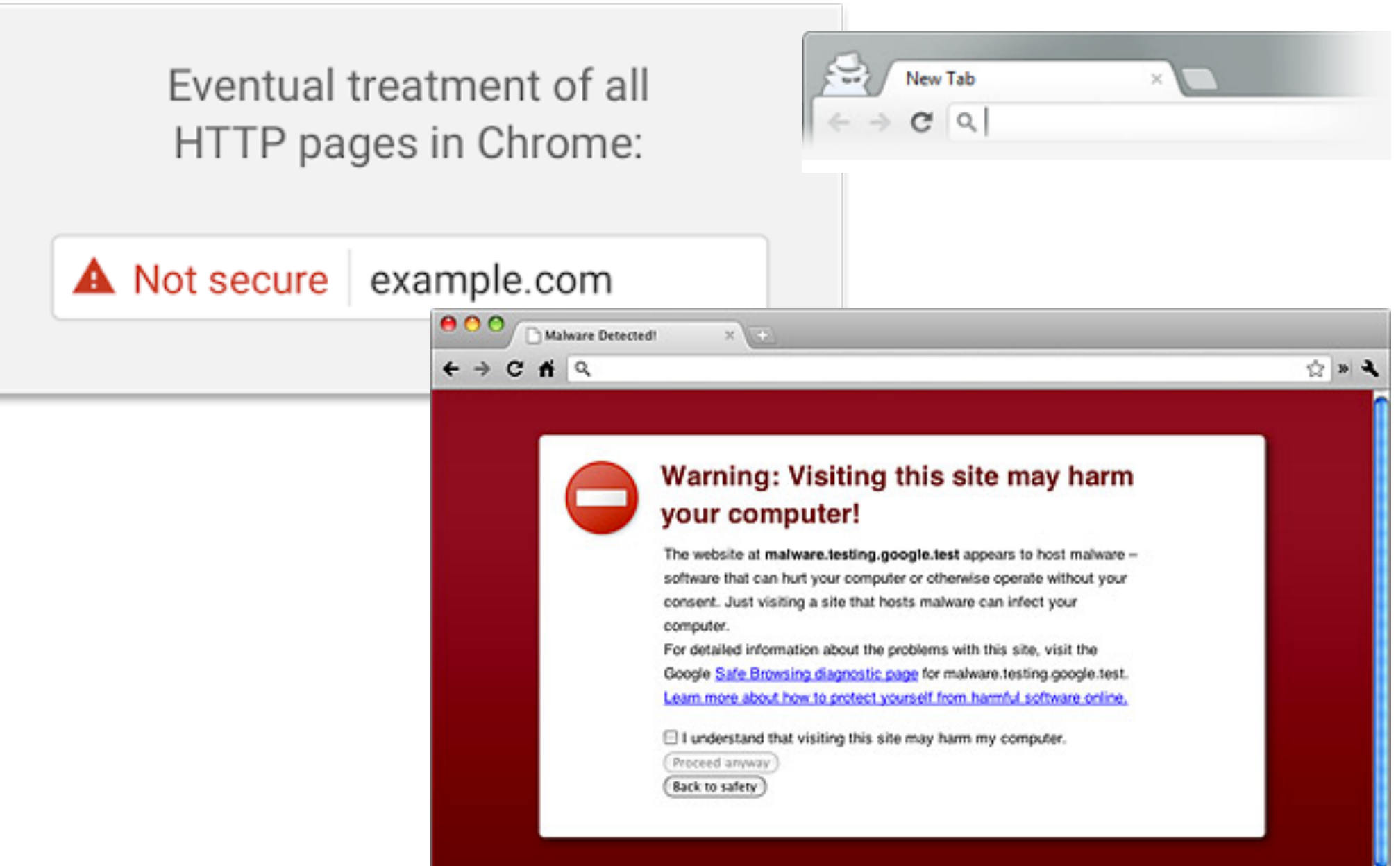


Defense: Firewall, IDS, AV

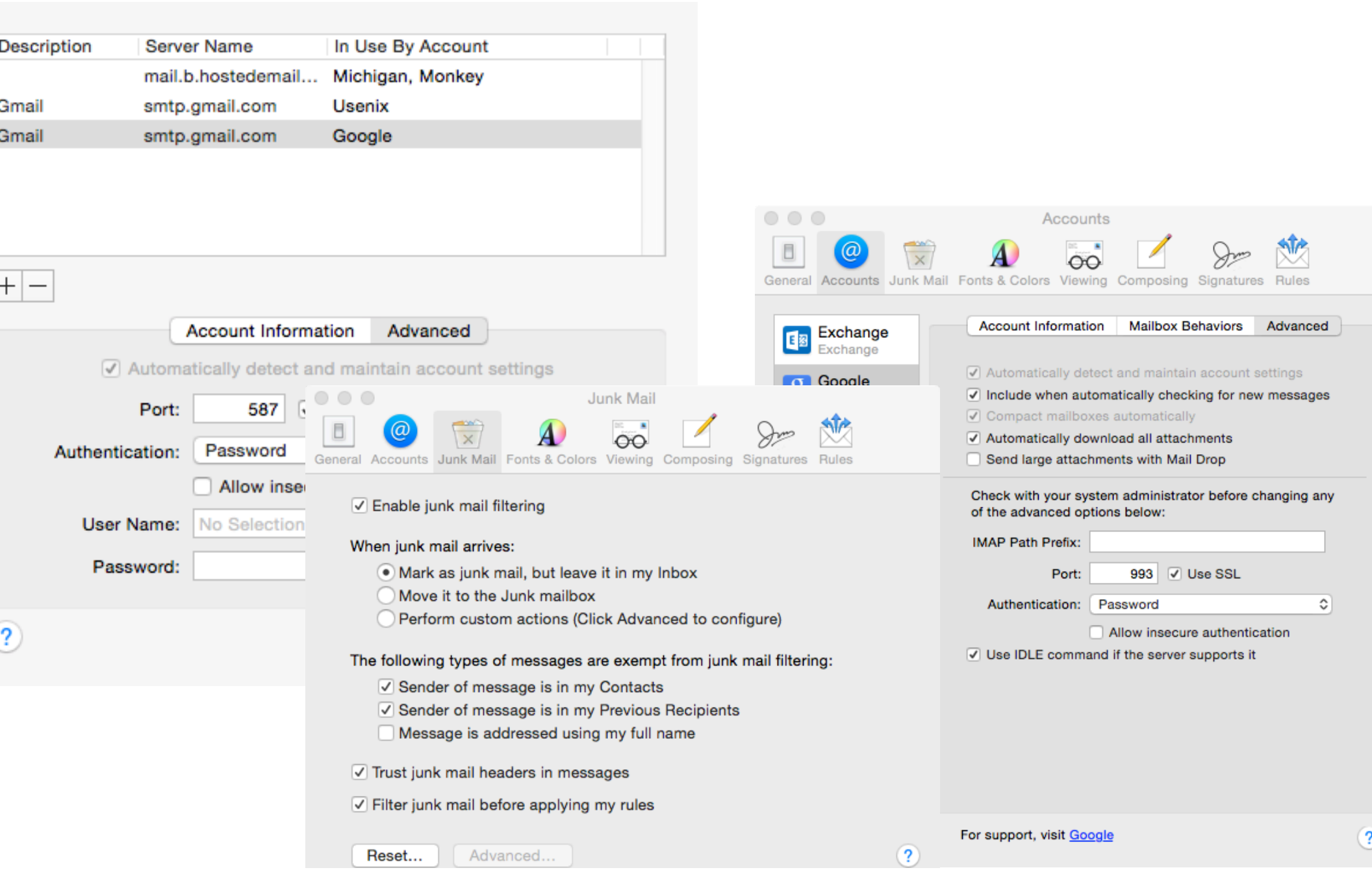




Defense: Safe Browsing



Defense: Secure E-mail



Exercise


Proposed changes to Siebel's security policy? threat model? countermeasures?

Exercise Too

- Should you lock your bike?
  - Adversaries?
  - Risk assessment?
  - Countermeasures?
  - Costs/benefits?

The Security Mindset

- Thinking like an attacker
  - Understand techniques for circumventing security.
  - Look for ways security can break, not reasons why it won't.
- Thinking like a defender
  - Know what you're defending, and against whom.
  - Weigh benefits vs. costs: No system is ever completely secure.
- "Rational paranoia!"

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/

Questions?