CS 88: Security and Privacy

01: Introduction

01-23-2024

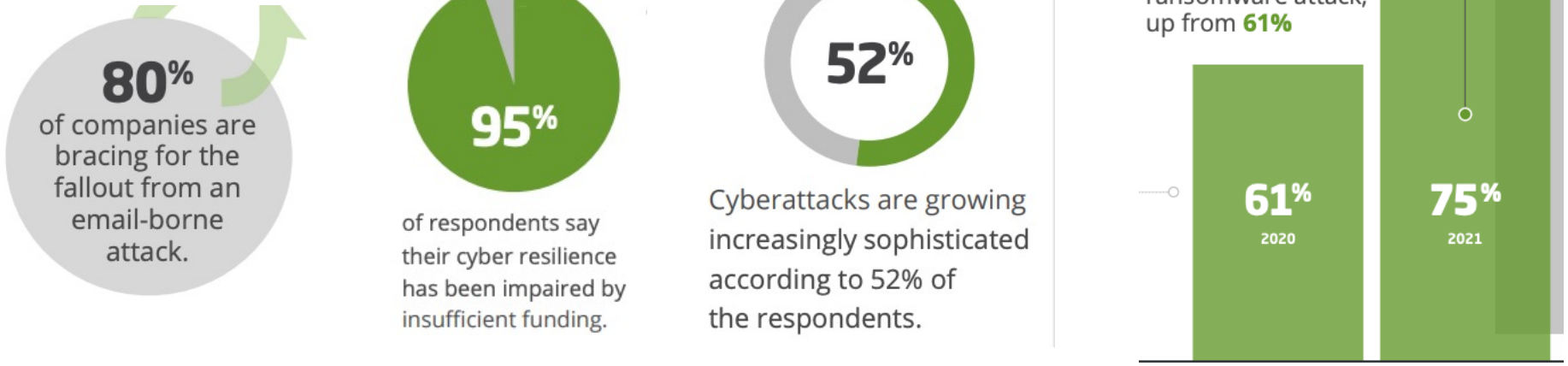
Welcome to CS88!

Today:

- What is this course about?
- Course Structure/logistics
- An Introduction to Security

State of Security & Privacy

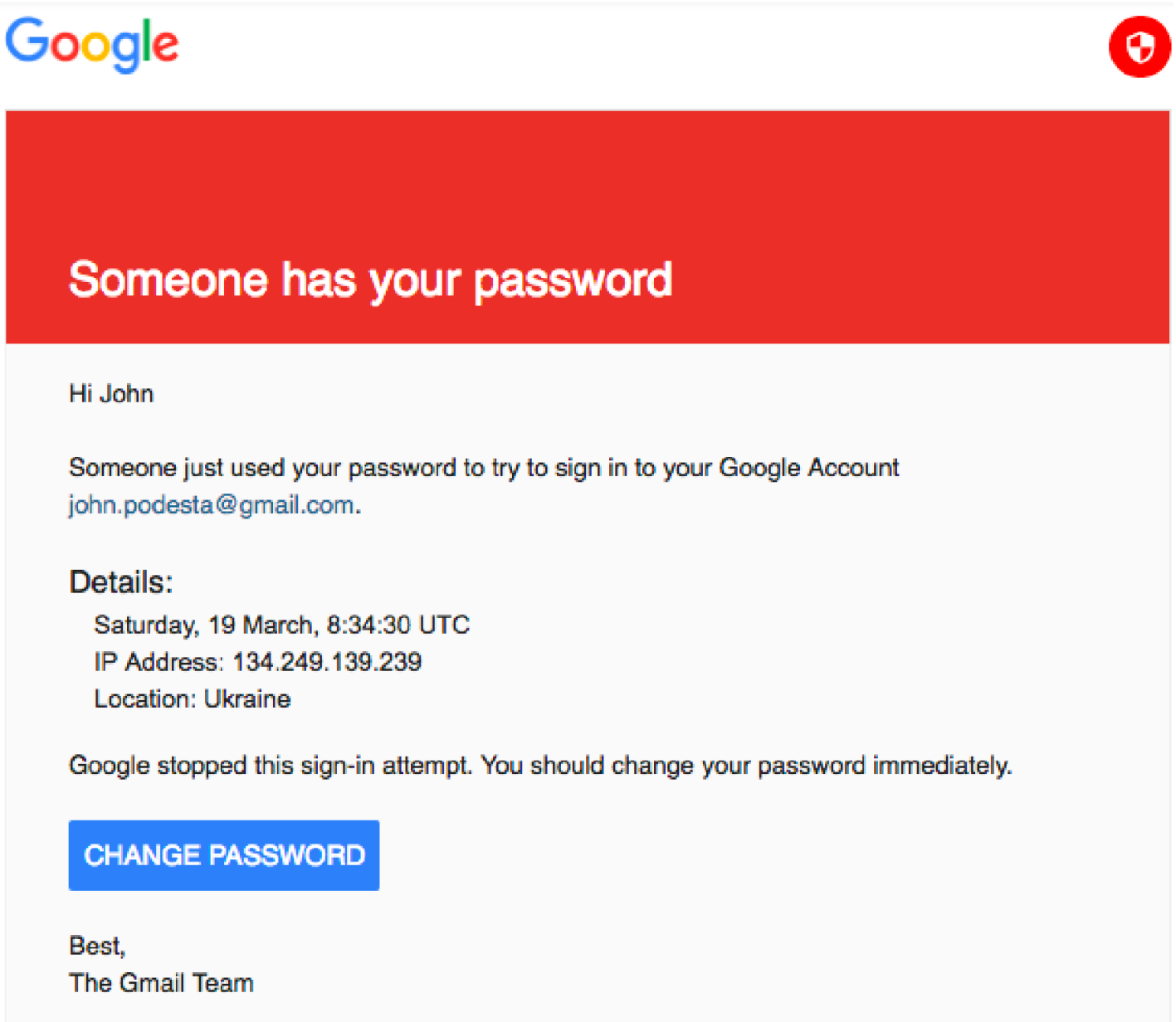
- Nation-state threats and DDoS attacks skyrocket throughout the Russo-Ukrainian War.
- Costa Rican government declared a national emergency in response to ransomware attacks targeting the healthcare and social security systems.
- The Lapsus$ Group: posting source code from Samsung, Microsoft, Nvidia.



https://www.mimecast.com/state-of-email-security/

https://swimlane.com/blog/10-hard-hitting-cyber-security-statistics/

Example threat



What is This Course About?

Adopting a ``Security Mindset''

What does security mean to you?

What is This Course About?

Adopting a ``Security Mindset''

that new product X sounds awesome! I can't wait to use it!

vs

X sounds cool but I wonder what would happen if someone did Y with it...

Why it's important:

- design better systems/solutions
- security in the broader context: law, policy, ethics, etc.
- technology changes: thinking like a security person more important than learning the specifics of today

What is This Course About?

1. Adopt a ``Security Mindset''
2. Learn how computers/information systems can be attacked.
   - Desirable properties of system X
   - Adversary model (capability of the adversary)
   - Trust assumptions (what I am depending upon for the desirable property to hold against certain adversary)

What is This Course About?

1. Adopt a ``Security Mindset''
2. Learn how computers/information systems can be attacked.
3. Learn to understand and apply security principles when designing/building/analyzing systems
   - principle of least privilege, separation of duty
   - authentication, access control, various crypto tools, sandboxing, isolation
   - No silver bullet; man-made complex systems will have errors; errors may be exploited

Security is Interesting!

The most interesting/challenging threats to security are posed by human/AI adversaries

Security is about cost/benefit tradeoff: *often this tradeoff analysis is not explicit*

Security is not all technological: *Humans are often the weakest link*

Security is Challenging

- Defense is almost always harder than attack.
- Data/Network/Computer Security is much harder than Physical security
  - adversaries can come from anywhere
  - computers enable large-scale automation
  - adversaries can be difficult to identify
  - adversaries can be difficult to punish
  - potential payoff can be much higher

Tools for Security

- Cryptography
- Authentication and Access control
- Hardware/software architecture for separation
- Processes and tools for developing more secure software
- Monitoring and analysis
- Recovery and response

Security is interdisciplinary

- Draws on all areas of CS
  - Theory (especially *cryptography*)
  - Networking
  - Operating systems
  - Databases
  - AI/learning theory
  - Computer architecture/hardware
  - Programming languages/compilers
  - HCI, psychology

Philosophy of this course

- We are not going to be able to cover everything
  - We are not going to be able to even mention everything
- Main goals
  - The security “mindset”
  - Understand and apply security principles to prevent attacks and/or limit their consequences.
  - Become an educated security consumer

You *should* have a better appreciation of security issues after this class

You will *not* be a security expert after this class (after this class, you should realize why it would be dangerous to think you are)

Vasanta Chaganti

Please call me Vasanta or Prof. Chaganti

- PhD: Australian National University & CSIRO Australia
- Post-Doc: UMass, Amherst

Research: What does your network data reveal about you?

Office Hours
SCI 253

- Mondays: 2.00 – 4.00PM
- Tuesdays: 2.00 – 4.00PM

What does your network data reveal about you?

George Washington University apologizes for data project monitoring student and staff locations on campus

Joe Heim • February 12, 2022 at 4:04 p.m. EST

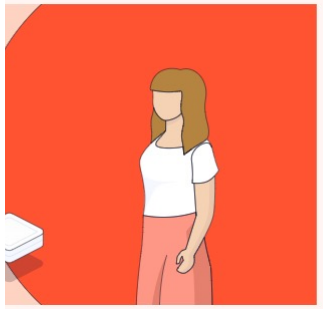
George Washington University apologized for not informing students, faculty and staff about a data analytics project that monitored their location on campus. (Toni L. Sandys/The Washington Post)

-Washington Post, 2022

Spotter

An automated attendance monitoring and early alerting platform.

Get Started Now



SYRACUSE

Opening Lines of Communication

Professors at Syracuse have used Spotter to identify struggling students early.

Read Full Story

ABILENE CHRISTIAN

Opening Cost

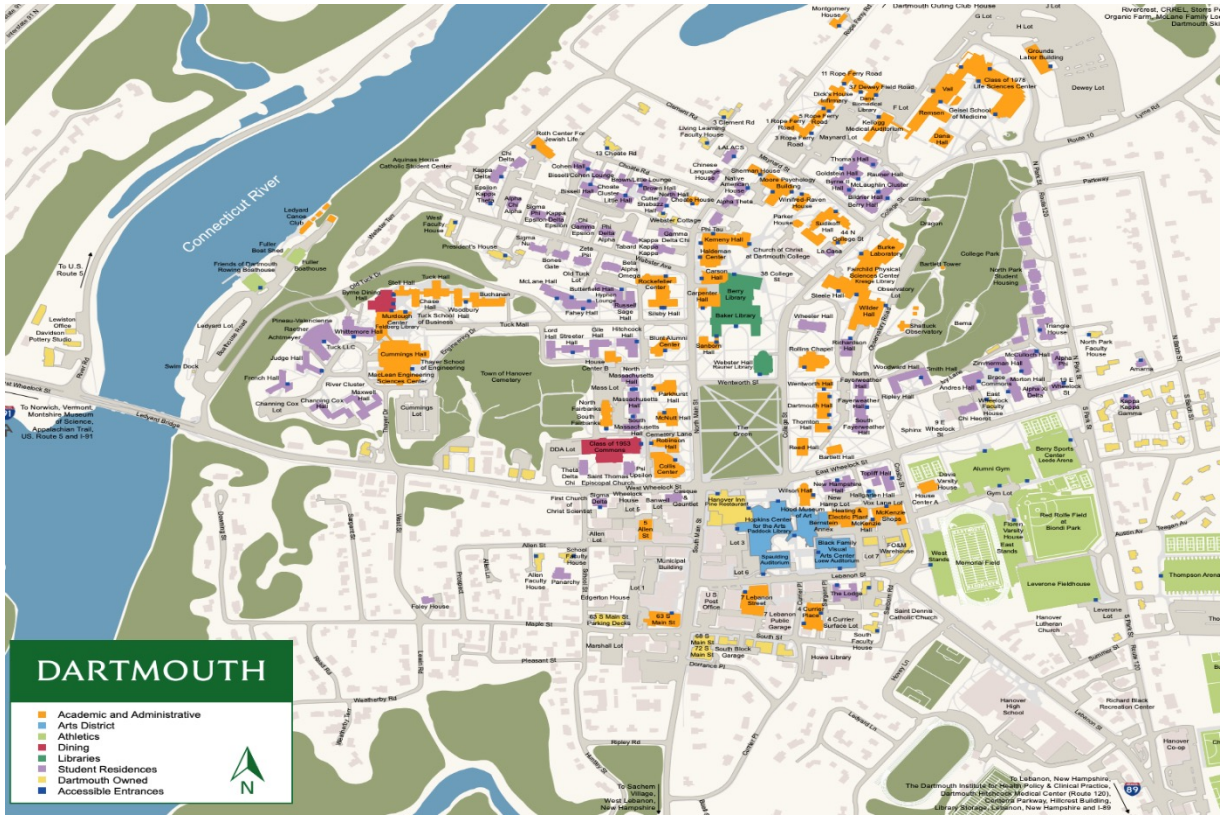
Coaches at Abilene brought Spotter to campus to enable their staff to focus on the students instead of attendance.

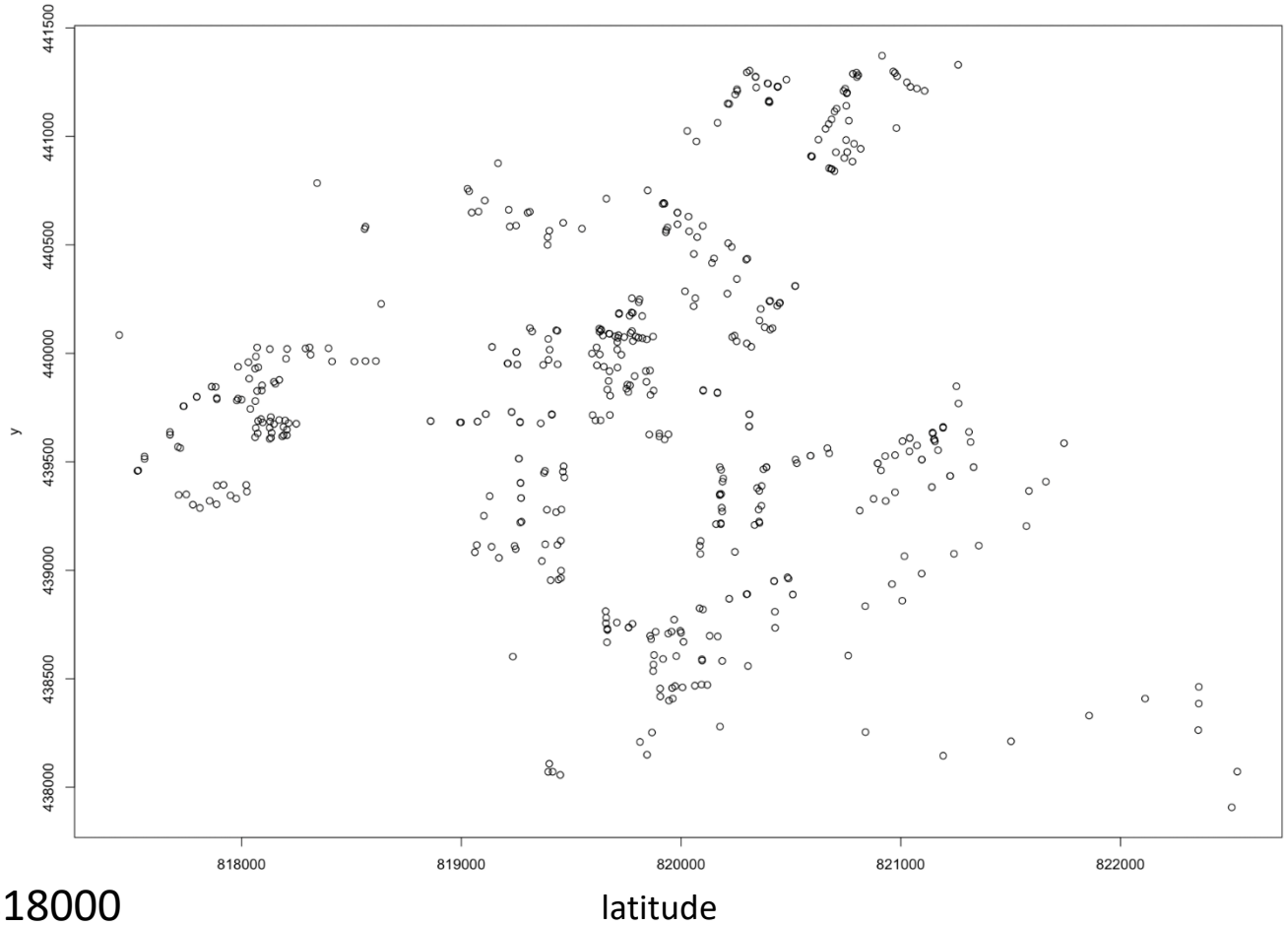
Read Full Story

https://spotteredu.com/

Wireless network data exposes sensitive user information

What does your network data reveal about you?

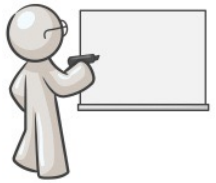




Anonymized network data is susceptible to semantic attacks

Lat-Long coordinates of Access Points Published in CRAWDAD Dartmouth Wireless Traces

Classes: Interactive Classes with Peer Instruction

Readings	Reading Quiz	Instruction	Labs/Exam
			
First Exposure	Gauge understanding	Explore, add context, Provide feedback	Show Knowledge Mastery

- You do the “easy” part before class
- Class is reserved for interactive, customized experiences
- To learn, YOU must actively work with a problem and construct your own understanding of it

Peer Instruction: In-class discussions

- Based on readings for that day
- Individually think about the questions (1 -2 minutes)
- Discuss: Analyze problems with your group
  - (5 – 10 minutes)
  - Practice analyzing, talking about challenging concepts
  - Reach consensus
  - If you have questions, raise your hand and I'll come over
- Class-wide discussions Led by YOU (students) – tell us what you talked about in discussion that everyone should know!

Why Peer Instruction?

- You get a chance to think.
- I get feedback as to what you understand.
- It’s more engaging!
- Research shows it promotes more learning than traditional lecture.

Clickers!

- Lets you vote on questions in real time.
- Like pub trivia, except the subject is always security ☺

Clicker Registration

https://forms.gle/FoVgzx4WVG8Gugqx6

If you don't register your clicker, I can't give you credit for quizzes / participation!

Participation scores count from week 2 (via paper hand-ins or clickers)

Locating your Clicker ID

iClicker with Hexadecimal ID

Hexadecimal number: numbers 0-9 and letters A – F

ID is also visible when you turn your clicker on.

Schedule

- Tentative Dates:
  - Midterm 1: Feb 23rd
  - Midterm 2: Apr 4th
- Midterm Polls:
  - Select all times that work for you: https://forms.gle/dohk1o6Cjj4srhpB8
  - Respond by the end of week-1!
  - Let me know if these dates are problematic this week!
- Final Project: Presentations during exam week
- Labs @ SCI 254
  - Labs are held on Wednesday: 1:15-2:45PM | 3:00-4:30PM
  - Prev. Lab due on Tuesdays via Github: https://github.swarthmore.edu

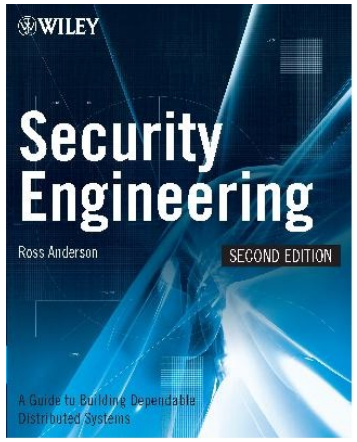
Resources: EdStem

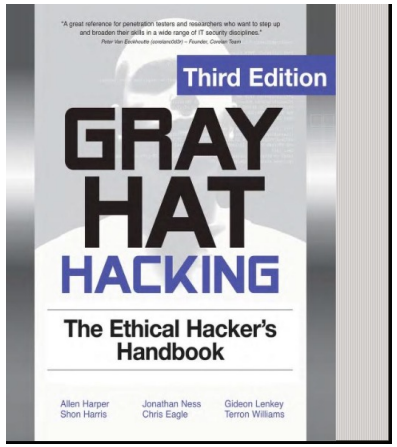
- Edstem Q&A Forum: https://edstem.org/us/join/5f2uet
- All announcements will be on EdStem
- Use Edstem! (counts towards your grade)
  - asking questions (not asked previously)
  - answering questions (you've worked through)
  - when in doubt (e.g., posting code)– leave a private message
  - Response within a day

- Email ***doesn't scale***: course related questions/comments edstem/office hours

Resource: Readings

- No required textbook
- Course readings posted on website
- Optional textbooks:





Course Grade Distribution

- 5% Readings Quizzes (based on assigned readings/videos)
- 5% Class and Lab Attendance
- 5% Edstem participation
- 15% Project
- 35% Midterm Exam-1 (15%) and Midterm Exam-2 (20%)
- 35% Labs (3%, 8%, 8%, 8%, 8%)

Course Grade Distribution

- 5% Readings Quizzes (based on assigned readings/videos)
- 5% Class and Lab Attendance
- 5% Edstem participation
- 15% Project
- 35% Midterm Exam-1 (15%) and Midterm Exam-2 (20%)
- 35% Labs (3%, 8%, 8%, 8%, 8%)

I will drop your three lowest quizzes/no-shows.

Succeeding in Upper-level CS Classes

- Reading comprehension!
- Pre-Reqs: 31 & 35 and ACTUALLY applying material you learnt from those classes
  - remember valgrind and gdb? they'll be your best friends … again!
- Working through code, problem sets, and reading material like you would in the "real-world"
  - making sure you read and understand required readings/videos
  - try/brainstorm different approaches...
  - growth mindset

- It’s been a weird couple of years …and it’s okay to not be on top of everything
- Please reach out to:
  - Me (Vasanta)
  - Your Academic Advisors
  - Student Deans
  - Counseling & Psychological Services

by KC Green

Policies: Late Submissions

Genie (as William F. Buckley Jr)“ There are a few,..provisos, a, a couple of quid pro quos.” - in Aladdin

- Lab Lateness
  - 2 days of extra time for the semester (granularity of days)
  - Email AFTER you are done!
  - No Email: Grade whatever is present at the deadline.

Policies: Academic Dishonesty

- Collaboration
  - **You may discuss approaches, not solutions**
  - You must submit your own work
  - Exams may include questions on programming
- Cheating
  - We take this very seriously. It can have a negative impact on your course grade, your GPA and your record at Swarthmore and beyond.
  - **Don’t do it!**

Policies: Academic Dishonesty

(Few) Examples of plagiarism

- Screen sharing with folks not in your lab partnership
- “Let me read my code out to you, or share the exact API for a particular function”
- Share in words the content in your code: “I first used strncpy to copy the string up to n bytes, and then appended a null character at the end”
- I’m applying a “security mindset” to “think like an attacker” on course assessment infrastructure

Policies: Academic Dishonesty

Examples of how not to plagiarize:

- Behave as though you are a CS ninja
- “What approaches did you try so far?”, “Looks like you have gotten more of the string than you need to, use man pages to look at other string functions”
- Don’t know how to help your friend? Ask them to post to Edstem to the class or send a post privately to me.

Policies: Ethics

- We will be discussing and implementing real-world attacks.
- **Using some of these these techniques in the real world may be unethical, a violation of university policies, or a violation of federal law.**
- This includes the course lab and assessment infrastructure (e.g., unethical use of Virtual Machines, cheating on exams, provided lab/class code, methods, and principles on real-world systems)

- Be an ethical hacker
  - Ethics requires you to refrain from doing harm
  - Always respect human, privacy, property rights
  - There are many legitimate hacking capture-the-flags
- **Sign the ethics form!** https://forms.gle/JZSujVZayiAUpVEJ6

18 U.S. CODE § 1030 - FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS

Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer...

The punishment for an offense...

- a fine under this title or imprisonment for not more than one year, or both...,
- a fine under this title or imprisonment for not more than 5 years, or both... if—
  i. the offense was committed for purposes of commercial advantage or private financial gain;
  ii. the offense was committed in furtherance of any criminal or tortious act...; or
  iii. the value of the information obtained exceeds $5,000

Administrative Questions?

- All of this info is on the class website
- Feel free to ask Q&A on the Edstem discussion board
- This is only the second time we are running this course… so please anticipate
  - changes to the topics we cover
  - scope of lab assignments
  - possible issues with code/VM etc.
- Would be great to get (constructive) feedback!

What is security, anyway?

What makes it different from robustness?

What makes it different from robustness?

Computer security studies how systems behave in the presence of *an adversary*.

Actively tries to cause the system to misbehave.

Thinking like an attacker

- Look for the weakest links
- Identify assumptions that security depends on. Are they false?
- Think outside the box
  - Not constrained by the system designer's world view!

Start practicing: When you interact with a system, think about what it means to be secure, and how it might be exploited

Example Clicker Question

- Individual vote (think 1-2 minutes)

- Group discussion / group vote (5 minutes)
  - Room should be LOUD

- Class discussion

Discussion Question: Security Mindset

How many of the following activities do you think you can successfully implement? i.e., what vulnerabilities in the system can you find/exploit?

(warning: actively targeting Phineas the Phoenix is against the Swarthmore Honor Code, can be grounds for explusion, and is potentially a federal crime)

1. get access to Phineas the Phoenix's costume
2. get access to Phineas the Phoenix's webpage/facebook page
3. find the exact location of Phineas the Phoenix and all past visit locations

A. successfully accomplish 1 of these attacks

B. successfully accomplish 2 of these attacks

C. successfully accomplish 3 or more attacks

https://www.swarthmore.edu/phoenix/naming-phoenix

Security: Not Just for Computers

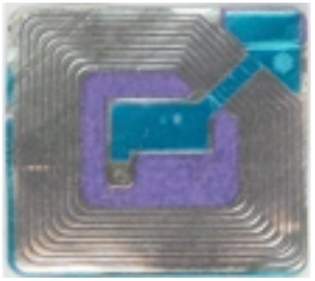
smartphones

voting machines

EEG headsets

medical devices

wearables



RFID

mobile sensing platforms

cars

game platforms

airplanes

So.. what is security?

- Normally, we are concerned with the achieving correctness
  - *e.g., does this software achieve the desired behavior*
- Security is a form of correctness
  - *does this software prevent "undesired" behavior?*
- Security involves an adversary who is active and malicious
  - *Attackers seek to circumvent protective measures*

Correctness vs. Security

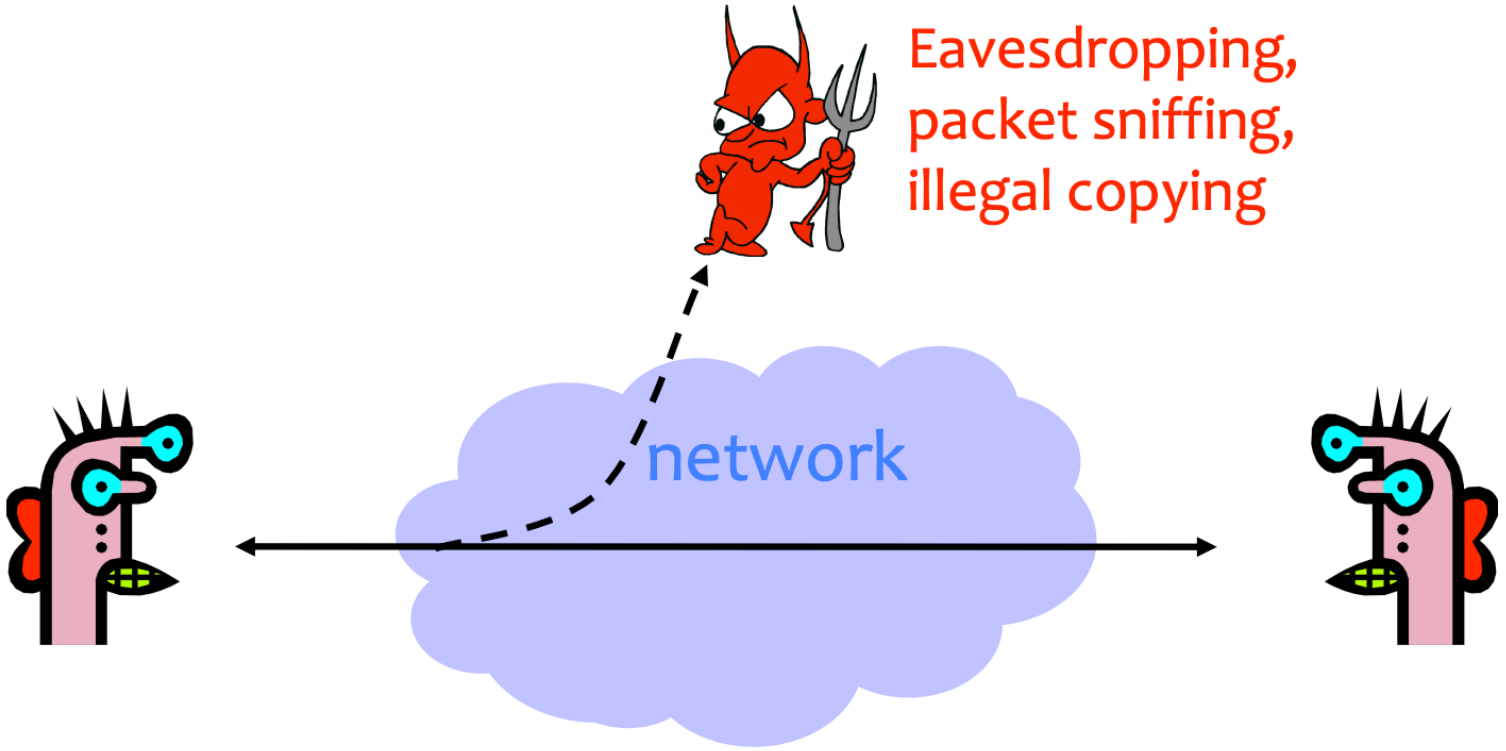
- System correctness: system satisfies specification
  - for reasonable input: get reasonable output
- System security: system properties preserved in the face of attack
  - for unreasonable input: output is not completely disastrous
- Main difference: active interference from an adversary

So.. what is security?

- General security goals: “CIA”
  1. Confidentiality
  2. Integrity
  3. Availability

Confidentiality (Privacy)

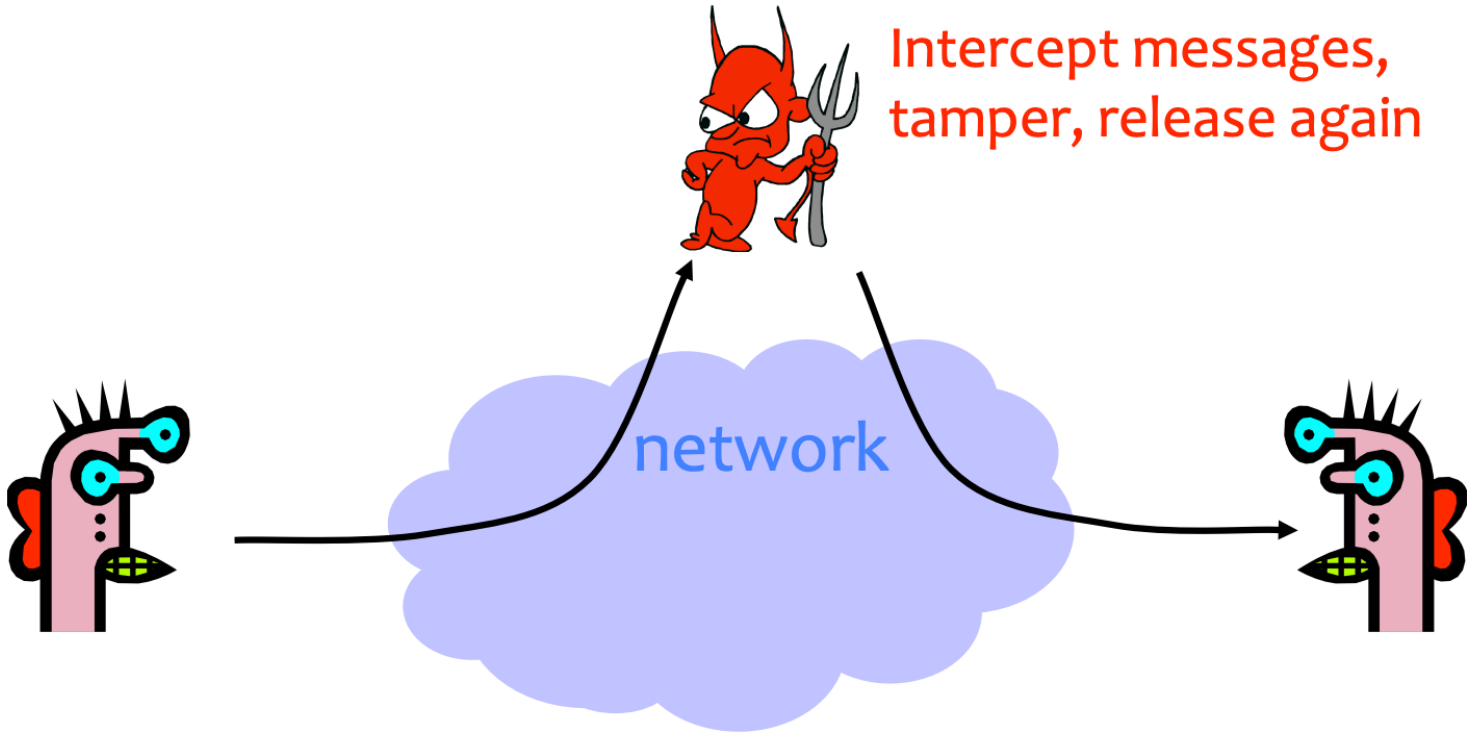
Confidentiality is concealment of information



Adapted from Franzi Roesner, Yoshi Kohno

Integrity

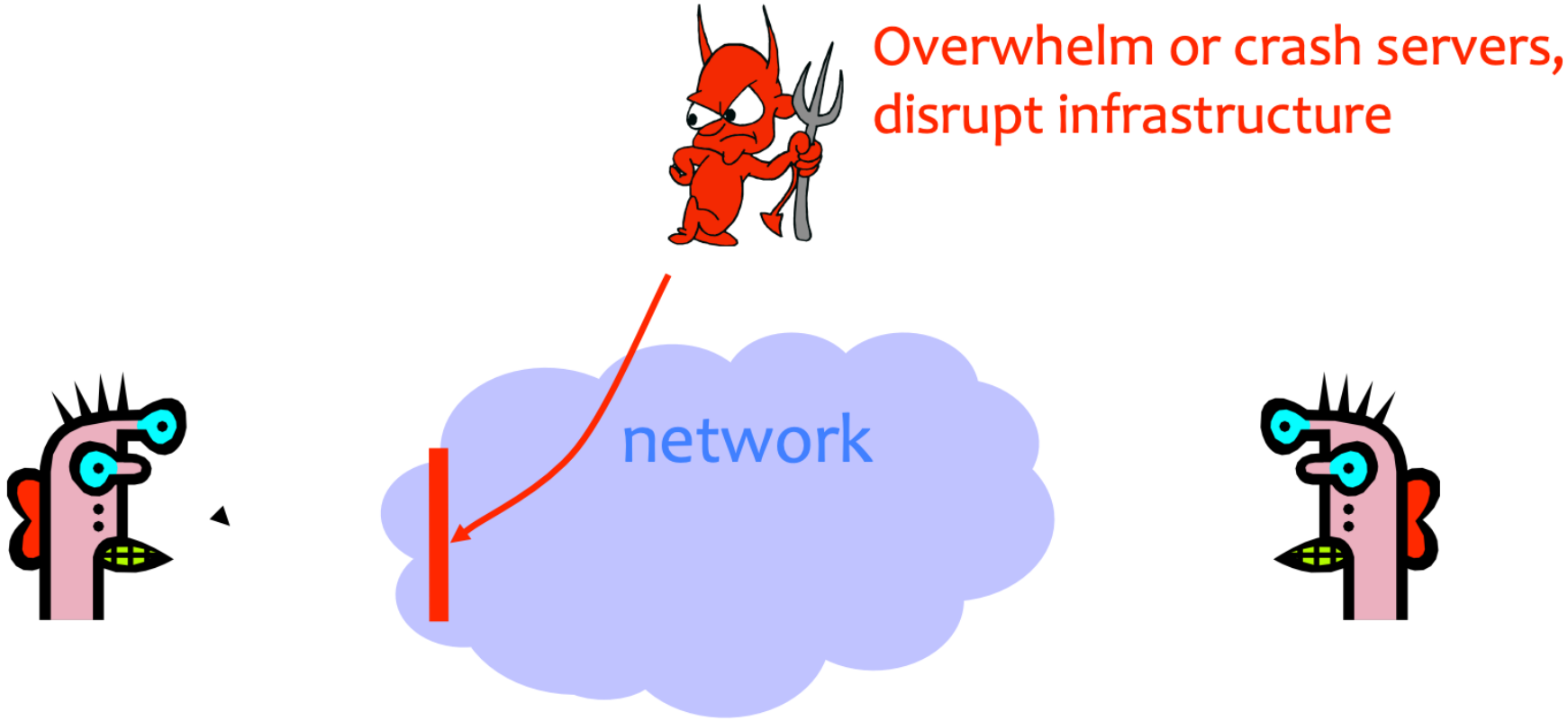
Integrity is prevention of unauthorized changes



Adapted from Franzi Roesner, Yoshi Kohno

Availability

Availability is the ability to use information or resources



Adapted from Franzi Roesner, Yoshi Kohno

So.. what is security?

General security goals: “CIA”: Confidentiality, Integrity, Availability

- How about if you receive data from an unknown person? what principle does it fall under?
- How about if a college student subverts DRM protections and creates a unprotected MP3 of a Beatles album?
- Internet connected machine with the latest updates and software installed. Privacy violations?
- ..How about accountability, non-repudiation, usability?

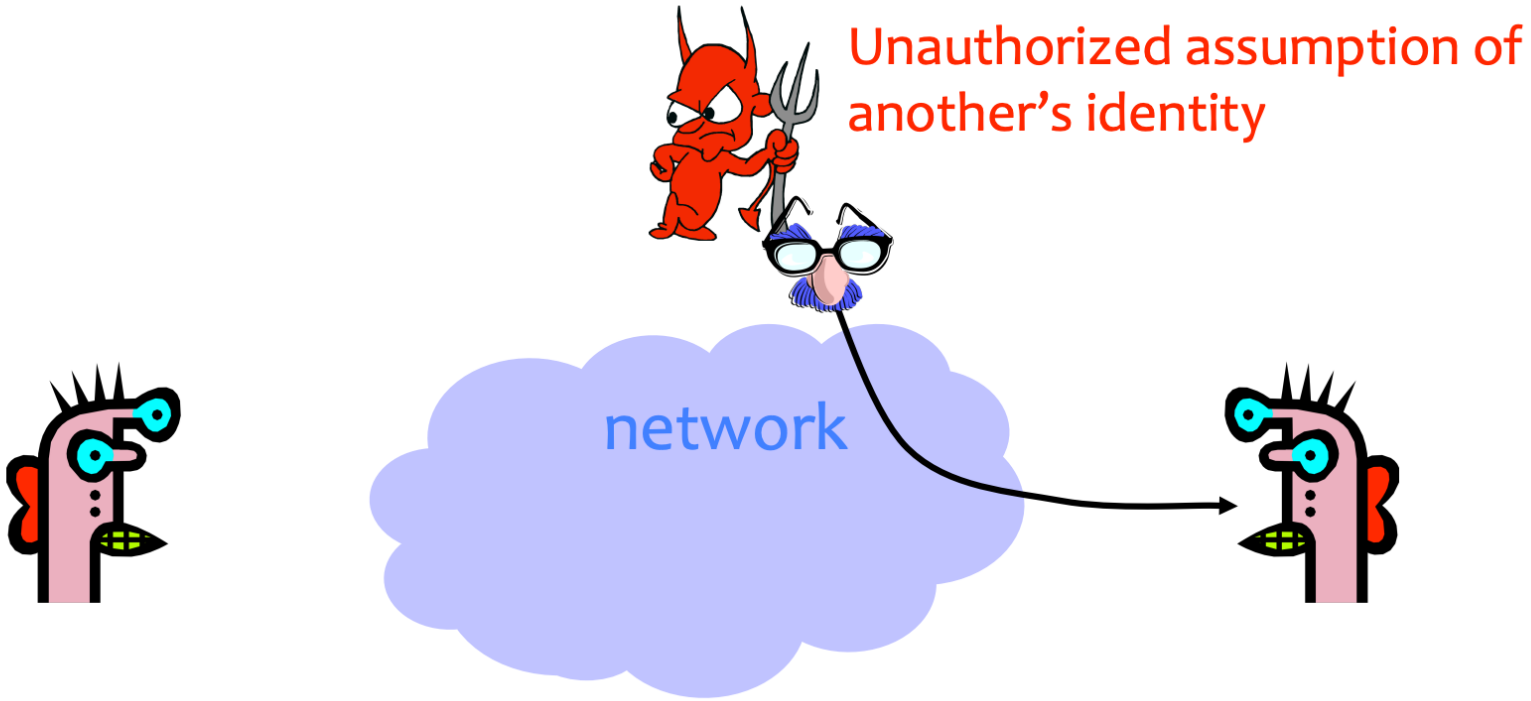
So.. what is security?

General security goals: “CIA”: Confidentiality, Integrity, Availability

- How about if you receive data from an unknown person? what principle does it fall under?
- How about if a college student subverts DRM protections and creates a unprotected MP3 of a Beatles album?
  - POV of RIAA: bad thing
  - POV of end users: technology prevents legitimate “fair use”
- Internet connected machine with the latest updates and software installed. Privacy violations?
- ..How about accountability, non-repudiation, usability?

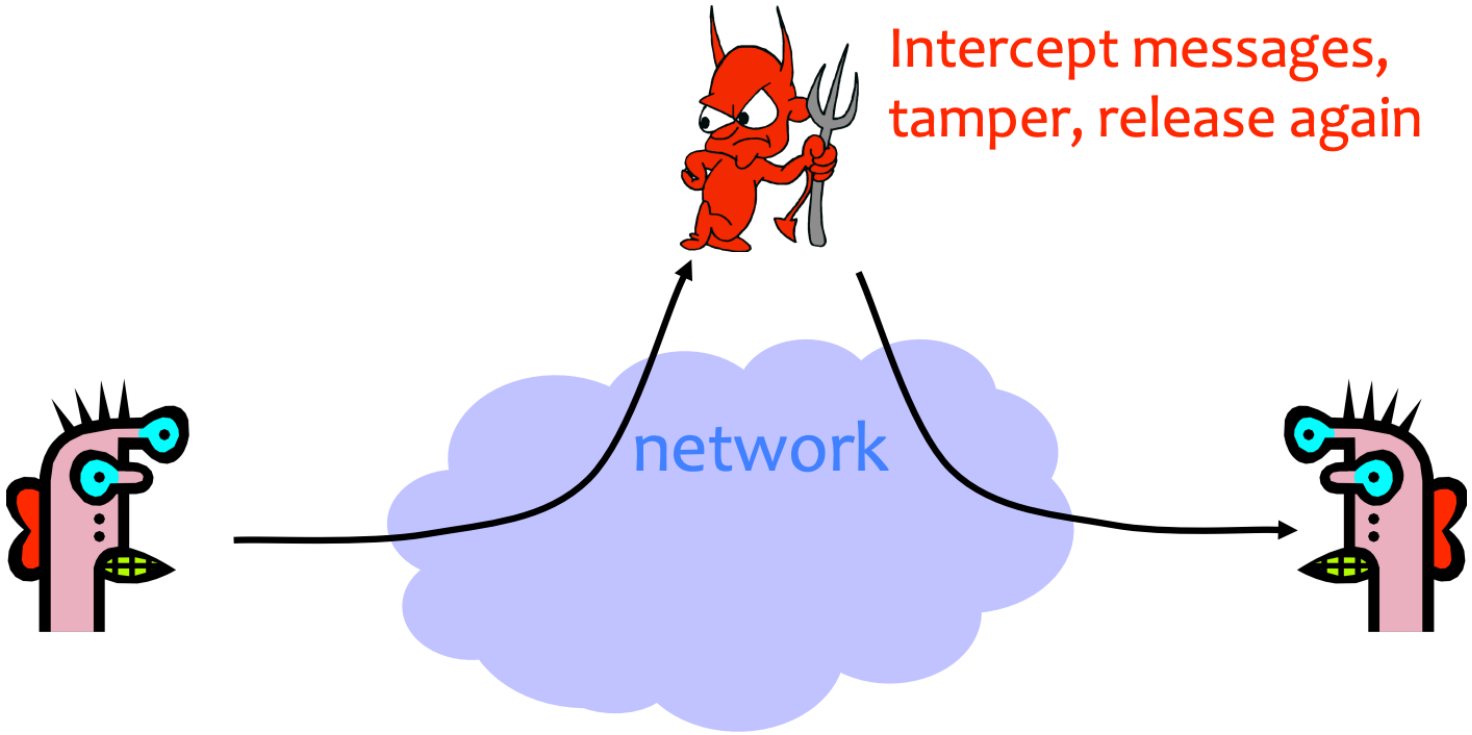
Authenticity

Authenticity is knowing who you're talking to



Accountability and Non-Repudiation

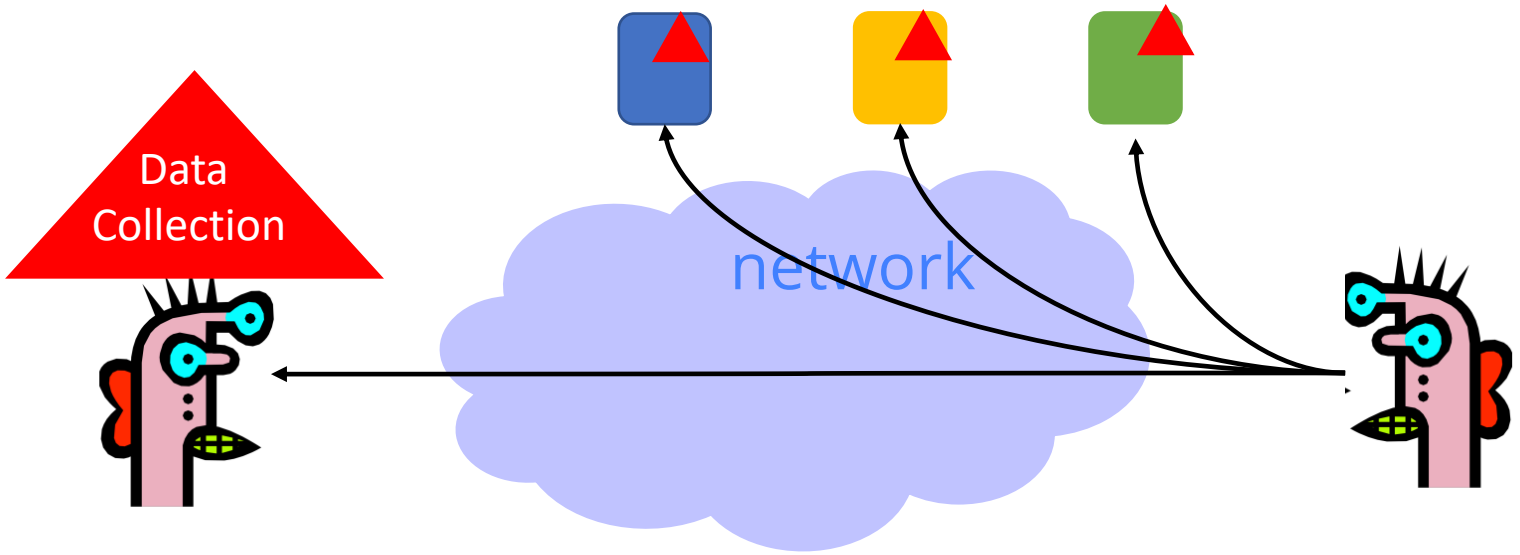
Provide evidence that a specific action occurred



Audit Log: Timestamp: Source IP, Dest IP, Data transferred

Adapted from Franzi Roesner, Yoshi Kohno

Privacy of collected information



Adapted from Franzi Roesner, Yoshi Kohno

So.. what is security?

General security goals: “CIA”

- Confidentiality
- Integrity
- Availability

- …
- Authenticity
- Accountability and non-repudiation
- Access Control
- Privacy of collected information

Threat Modeling:

- Assets: What are we trying to protect? How valuable are those assets?
- Adversaries: Who might try to attack, and why?
- Vulnerabilities: How might the system be weak?
- Threats: What actions might an adversary take to exploit vulnerabilities?
- Risk: How important are assets? How likely is an exploit?
- Possible Defenses

Threat Modeling

- Perfect security? No such thing!
- BUT..
  - attackers have limited resources
  - make attackers pay unacceptable costs to succeed!
- Defining security per context:
  - identify assets, adversaries, motivations
  - threats, vulnerabilities, risk,
  - possible defenses...

Next class..

- The security mindset
- Software Security