CSE 127: Introduction to Computer Security

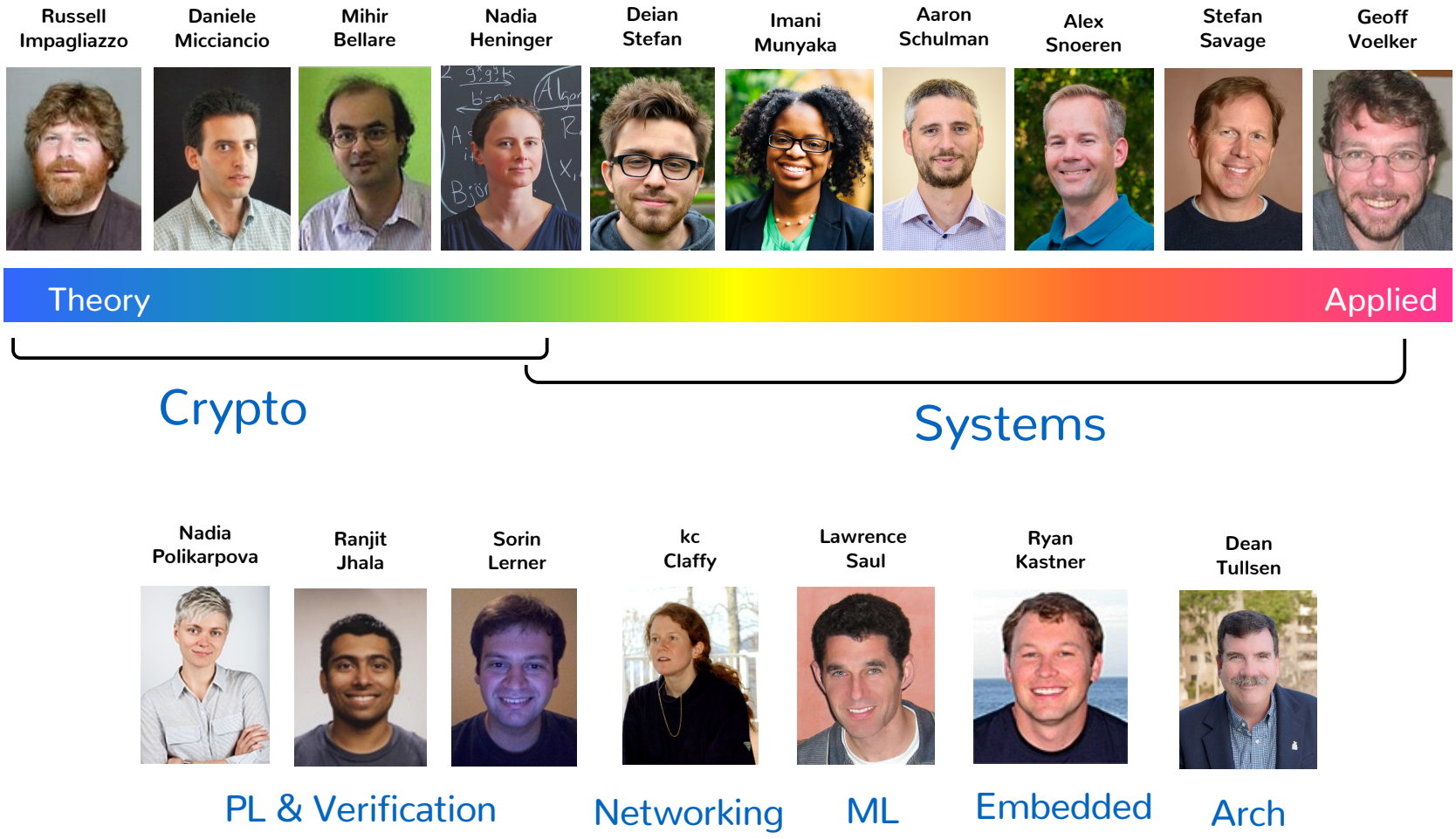
George Obaido, Ph.D.

UCSD

Spring 2022 Lecture 1

- Instructor: George Obaido, gobaido@ucsd.edu
  - Office Hours: Wednesday 9:00-10:00am
- TA: Zijie Zhao
  - Office Hours: Tuesday 4:00pm - 5:00pm
- TA: Sumanth Rao
  - Office Hours: Thursday 3:00pm - 4:00pm
- TA: Satish Yerva
  - Office Hours: Wednesday 3:00pm - 4:00pm
- TA: Karthik Mudda
  - Office Hours: Monday 11:00am - Noon

Many amazing folks at UCSD working on security



My Work

- Computer Science Education, Data Science and Data Ethics
- 11+ years in Industry and Academia
- Qualifications: PhD, MSc, and BSc - *all in Computer Science*
- Currently a Postdoctoral Fellow at UCSD.
- Studying CS student attrition – root causes behind drop-outs in CS.

Topics Covered and Course Goals

Topics Covered

- The Security Mindset
  - Principles and threat modeling
- Systems/Software Security
  - Classic attacks and defenses on memory safety, isolation
- Web Security
  - Web architecture, web attacks, web defenses
- Network Security
  - Network protocols, network attacks, network defenses
- Cryptography
  - Public and private-key cryptography, TLS, PKI
- Privacy, Anonymity, Ethics, Legal Issues

Course Goals

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits

Course Goals

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
- Technical skills
  - How to protect yourself
  - How to manage and defend systems
  - How to design and implement secure systems

Course Goals

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
- Technical skills
  - How to protect yourself
  - How to manage and defend systems
  - How to design and implement secure systems
- Learn to be a security-conscious citizen

Course Goals

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
- Technical skills
  - How to protect yourself
  - How to manage and defend systems
  - How to design and implement secure systems
- Learn to be a security-conscious citizen
- Learn to be a `leet h4x0r`

Course Goals

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
- Technical skills
  - How to protect yourself
  - How to manage and defend systems
  - How to design and implement secure systems
- Learn to be a security-conscious citizen
- Learn to be a `leet h4x0r`, but an ethical one!

Course Mechanics

40% (Project 0 to Project 5)

- Work in groups of two
- Do your own programming and writeup
- General discussion is encouraged

Course Mechanics

40% (Project 0 to Project 5)

- Work in groups of two
- Do your own programming and writeup
- General discussion is encouraged

20% Midterm exam 05/04 in class

- On Canvas
- Open-book, independent work

Course Mechanics

40% (Project 0 to Project 5)

- Work in groups of two
- Do your own programming and writeup
- General discussion is encouraged

20% Midterm exam 05/04 in class

- On Canvas
- Open-book, independent work

40% Final exam 06/06 (To confirm time)

- Closed book
- Might be on Canvas too - To advise later

Course Policies

Late days and extensions:

- You have two late days to use as you wish
- Both you and your partner must have late days to use them

Course Policies

Late days and extensions:

- You have two late days to use as you wish
- Both you and your partner must have late days to use them

Regrade policy:

- Regrades should be the exception not the norm
- Incorrect regrade request $\Longrightarrow$ negative points

Course Policies

Late days and extensions:

- You have two late days to use as you wish
- Both you and your partner must have late days to use them

Regrade policy:

- Regrades should be the exception not the norm
- Incorrect regrade request $\Longrightarrow$ negative points

Academic integrity:

- UC San Diego policy:
  `https://academicintegrity.ucsd.edu`
- We have to report suspected cases, don't make it weird
- If you are not sure if something is cheating, ask

Talk to us, it’s a weird time

Course Resources

- No official textbook. Optional books:
  - *Security Engineering* by Ross Anderson
  - *Hacking: The Art of Exploitation* by Jon Erikon

Course Resources

- No official textbook. Optional books:
  - *Security Engineering* by Ross Anderson
  - *Hacking: The Art of Exploitation* by Jon Erikon
- Assignments and readings on course site:

  `https://cseweb.ucsd.edu/classes/sp22/cse127-a/`

Course Resources

- No official textbook. Optional books:
  - *Security Engineering* by Ross Anderson
  - *Hacking: The Art of Exploitation* by Jon Erikon
- Assignments and readings on course site:

  `https://cseweb.ucsd.edu/classes/sp22/cse127-a/`
- Questions? Post to Piazza.

  `https://piazza.com/ucsd/spring2022/cse127_sp22_a00`

Course Resources

- No official textbook. Optional books:
  - *Security Engineering* by Ross Anderson
  - *Hacking: The Art of Exploitation* by Jon Erikon
- Assignments and readings on course site:

  `https://cseweb.ucsd.edu/classes/sp22/cse127-a/`
- Questions? Post to Piazza.

  `https://piazza.com/ucsd/spring2022/cse127_sp22_a00`
- Lectures and office hours:
  - Lectures: In person with a recorded component via Zoom
  - Discussion: This will be held via Zoom (Wednesday 5:00pm-5:50pm)
  - Office hours will not be recorded

Ethics

Ethics

We will be discussing and implementing real-world attacks.

Using some of these techniques in the real world may be unethical, a violation of university policies, or a violation of federal law.

This includes the course assignment infrastructure (e.g., grading system).

Ethics

We will be discussing and implementing real-world attacks.

Using some of these techniques in the real world may be unethical, a violation of university policies, or a violation of federal law.

This includes the course assignment infrastructure (e.g., grading system).

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-flag competitions (mostly for hackers!)

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...

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

Real-World Cases

Computer Fraud and Abuse Act (CFAA) Cases

- In 2011, FBI prosecuted **Andrew Auernheimer**, also known as "Weev" for exposing data of 114K AT&T iPad users
  - Criminal CFAA charge.
  - Found guilty and sent to prison.

Computer Fraud and Abuse Act (CFAA) Cases

- In 2011, FBI prosecuted **Andrew Auernheimer**, also known as "Weev" for exposing data of 114K AT&T iPad users
  - Criminal CFAA charge.
  - Found guilty and sent to prison.
- In 2011, Sony sued **George Hotz**, also known as "Geohot" for jailbreaking PlayStation 3
  - Civil CFAA and DMCA complaints.
  - Settled out of court.

Computer Fraud and Abuse Act (CFAA) Cases

- In 2011, FBI prosecuted **Andrew Auernheimer**, also known as "Weev" for exposing data of 114K AT&T iPad users
  - Criminal CFAA charge.
  - Found guilty and sent to prison.
- In 2011, Sony sued **George Hotz**, also known as "Geohot" for jailbreaking PlayStation 3
  - Civil CFAA and DMCA complaints.
  - Settled out of court.
- In 2011, FBI prosecuted **Aaron Swartz** for downloading academic articles on MIT network from JSTOR
  - Indicted for wire fraud and CFAA.
  - Prosecution continued until his death in 2013.

Computer Fraud and Abuse Act (CFAA) Cases

- In 2011, FBI prosecuted **Andrew Auernheimer**, also known as "Weev" for exposing data of 114K AT&T iPad users
  - Criminal CFAA charge.
  - Found guilty and sent to prison.
- In 2011, Sony sued **George Hotz**, also known as "Geohot" for jailbreaking PlayStation 3
  - Civil CFAA and DMCA complaints.
  - Settled out of court.
- In 2011, FBI prosecuted **Aaron Swartz** for downloading academic articles on MIT network from JSTOR
  - Indicted for wire fraud and CFAA.
  - Prosecution continued until his death in 2013.
- In 2021, **Nathan Van Buren** was charged with "exceeding authorized access" under CFAA
  - A police officer who misused license plate database
  - Supreme court ruled that authorized access for improper purposes is not “exceeding authorized access”

Famous Hackers

Other famour hackers:

- **Kevin Mitnick:** Infiltrated Digital Equipment Corporation (DEC) and copied their software.
- **Gary Mckinnon:** Hacked NASA and US military systems
- **Albert Gonzalez:** Largest credit card heist (170 million credit cards, etc)
- **Jonathan James:** Juvenile, broke into NASA server and stole sensitive information.

Source: https://www.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

What is security?

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.*

Good engineering involves thinking about how things can be made to work; the security mindset involves thinking about how things can be made to fail.

- Bruce Schneier

The Security Mindset

- Thinking like an attacker
  - Understand techniques for circumventing security
  - Look for ways security can break, not why it won't

The Security Mindset

- Thinking like an attacker
  - Understand techniques for circumventing security
  - Look for ways security can break, not 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**.

Thinking like an Attacker

- Look for weakest links
- Identify assumptions that security depends on
  Are they false?

Thinking like an Attacker

- Look for weakest links
- Identify assumptions that security depends on
  Are they false?
- Think outside the box

Thinking like an Attacker

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

Thinking like an Attacker

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

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


1
2
3
4
5
6
7
8
9
*
0
#

Exercise

How would you break into the CSE building?

Exercise

How would you steal my email password?

Exercise

What security systems do you interact with?

Thinking like a Defender

- Security policy
  - What are we trying to protect?
  - What properties are we trying to enforce?
- Threat model
  - Who are the attackers? Capabilities? Motivation?
  - What kind of attack are we trying to prevent?
- Risk assessment
  - What are the weaknesses of the system?
  - What will successful attacks cost us?
  - How likely?
- Countermeasures
  - Costs vs. benefits?
  - Technical vs. nontechnical?

Security Policies

- What *assets* are we trying to protect?
  - Password (hashes)
  - Emails
  - Browsing history
- What properties are we trying to enforce?
  - Confidentiality
  - Integrity
  - Availability
  - Privacy
  - Authenticity

Threat Models

- Who are our adversaries?
  - Motives?
  - Capabilities?
- What kinds of attacks do we need to prevent? (Think like the attacker!)
- Limits: What kinds of attacks should we ignore?

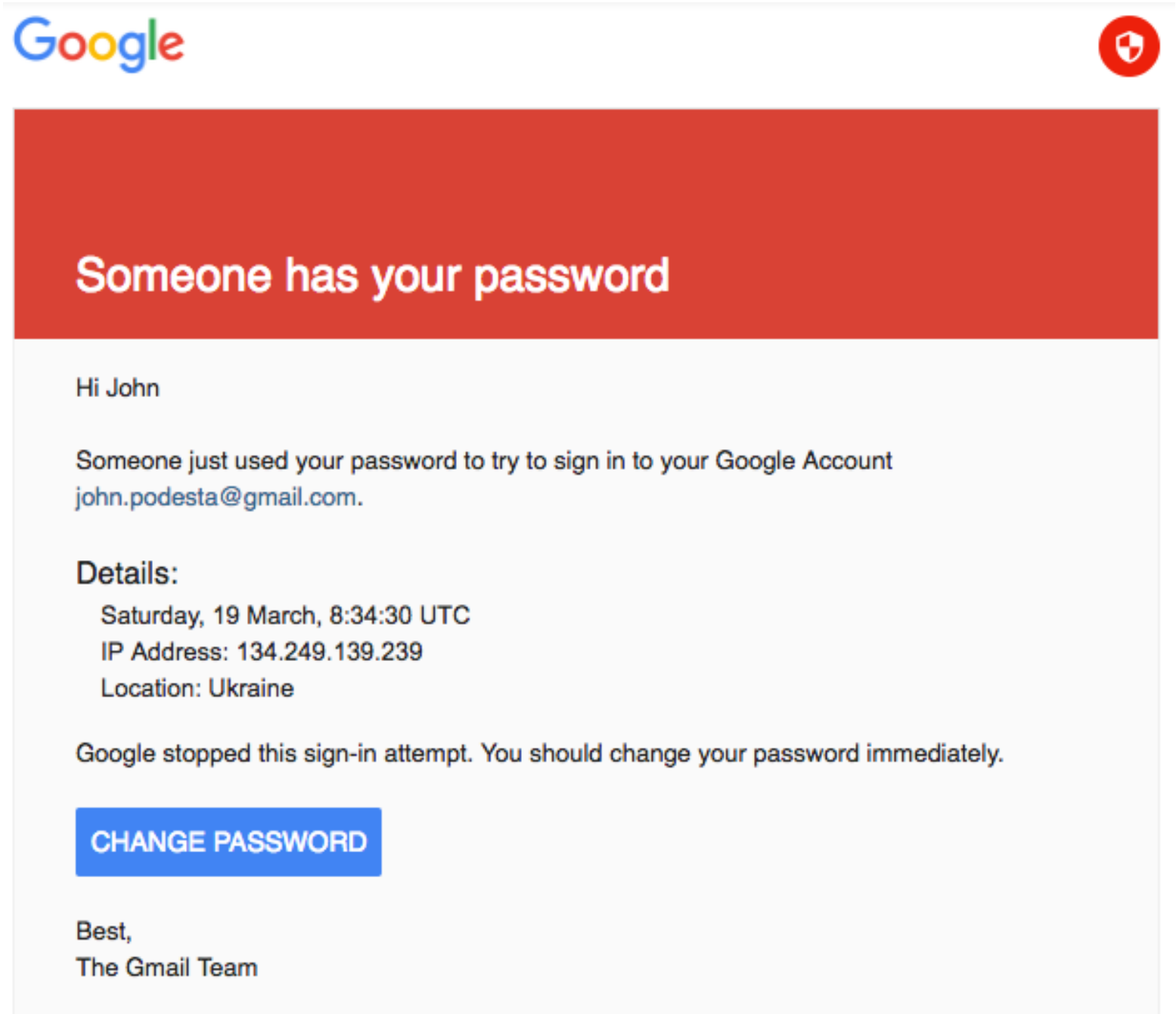
Example of Threat Modeling

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	Magical amulets? Fake your own death, move into a submarine? YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

James Mickens "This World of Ours"

Example of Threat Modeling



Who is John Podesta?

Assessing Risk

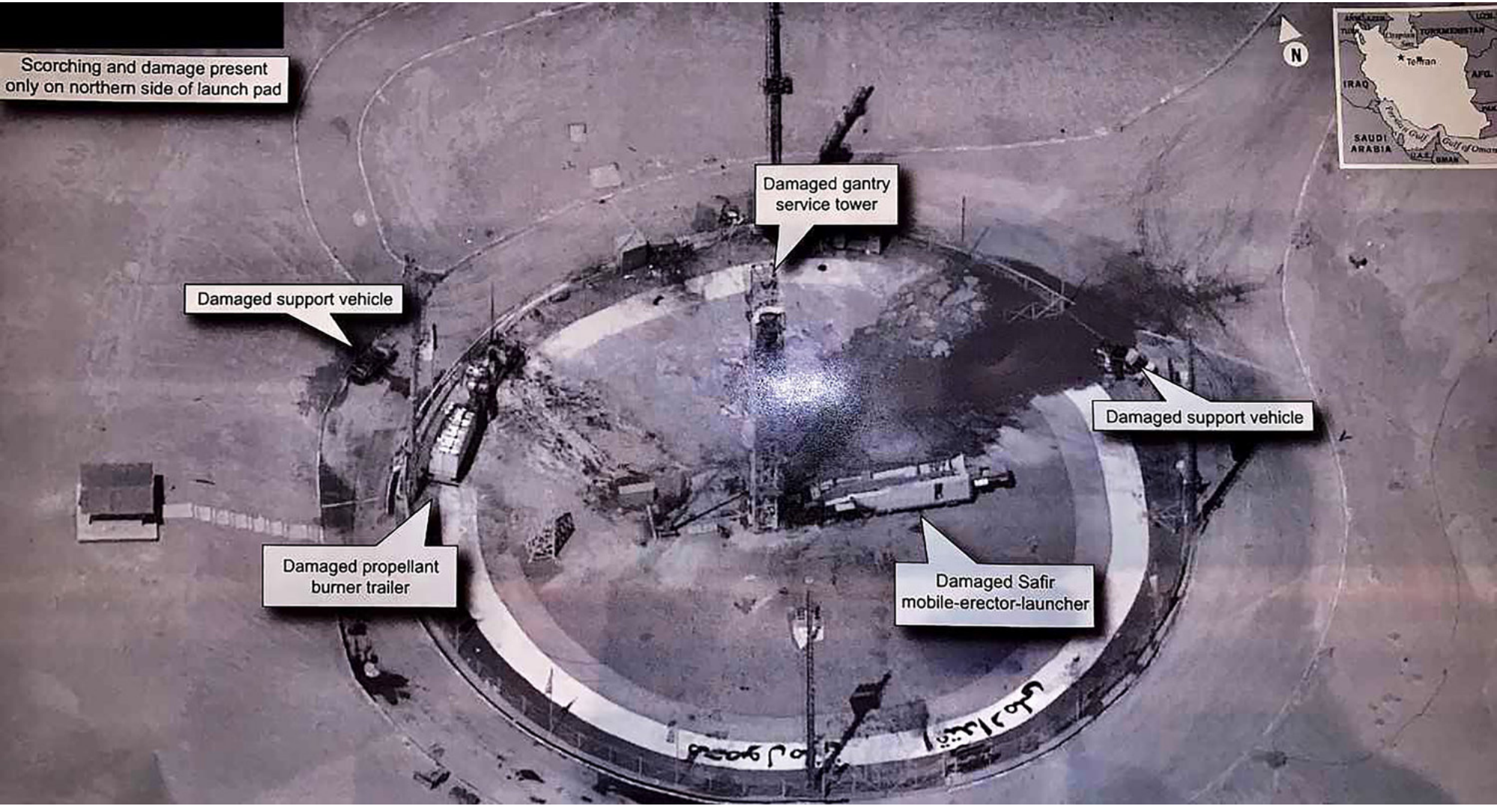
Remember: *Controlled paranoia*

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

Countermeasures

- Technical countermeasures
- Nontechnical countermeasures
  Law, policy (government, institutional), procedures, training, auditing, incentives, etc.

How do we protect classified satellites?



Security Costs

- No security mechanism is free
  - Direct costs:
    Design, implementation, enforcement, false positives
  - Indirect costs:
    Lost productivity, added complexity
- Challenge is to rationally weigh costs vs. risk
  - Human psychology makes reasoning about high cost/low probability events hard

Exercise

Should you lock your door?

- Assets?
- Adversaries?
- Risk assessment?
- Countermeasures?
- Costs/benefits?

Exercise

Should you use automatic software updates?

- Assets?
- Adversaries?
- Risk assessment?
- Countermeasures?
- Costs/benefits?

Exercise

Should we protect the CSE bear?

- Assets?
- Adversaries?
- Risk assessment?
- Countermeasures?
- Costs/benefits?

Secure Design

- Common mistake:
  Convince yourself that the system is secure

- Better approach:
  Identify *weaknesses* of design, focus on correcting them
  Formally prove that design is secure (soon)

- Secure design is a **process**
  Must be practiced continuously
  Retrofitting security is super hard

Where to focus defenses

- *Trusted components*
  Parts that must function correctly for the system to be secure.

- *Attack surface*
  Parts of the system exposed to the attacker

Security Principles

- Simplicity, open design, and maintainability
- Privilege separation and least privilege
- Defense-in-depth and diversity
- Complete mediation and fail-safe

Exercise

Preventing cheating on an online exam?

Exercise

Preventing you from stealing my password?

Next lecture: Buffer overflows!