CSE 127: Introduction to Computer Security

George Obaido, Ph.D.

UCSD

Spring 2022 Lecture 1 (Continued)

Continued from Threat Modeling

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)**: Secret code for authentication.
- **Emails:** System for sending and receiving messages electronically.
- **Browsing history**: Pages visited, useful for web marketing and forensics.

Security Policies

What properties are we trying to enforce? (CIA triad)

- **Confidentiality**: Protect sensitive and private information from unauthorized use.
- **Integrity**: Protect data from deletion or modification from any unauthorized party.
- **Availability**: Refers to the actual availability of information.
- **Privacy**: Protect sensitive information, such as personally identifiable information, etc.
- **Authenticity**: Proven fact that something is legitimate or real.

Scenario 1

Rob opens his fitness tracking app to start logging a workout. The app crashes, and Rob was unable to log his workout.

a. Confidentiality
b. Authenticity
c. Availability
d. None of the above

Go to **www.menti.com** and use the code: **35 28 617**

Scenario 2

Kim selected an Easter egg on an XYZ e-commerce platform for $10. At checkout, Kim was asked to pay $1000.

a. Confidentiality
b. Integrity
c. Availability
d. None of the above

Go to **www.menti.com** and use the code: **5219 7835**

Scenario 3

Bob works for a finance company called ABC123. Six months into the position, Bob stole and sold 250,000 customer credit card information on the darkweb.

a. Confidentiality
b. Integrity
c. Availability
d. None of the above

Go to **www.menti.com** and use the code: **8130 7884**

Threat Models

Identifies the types of threat agents that cause harm to computer systems.

- 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?

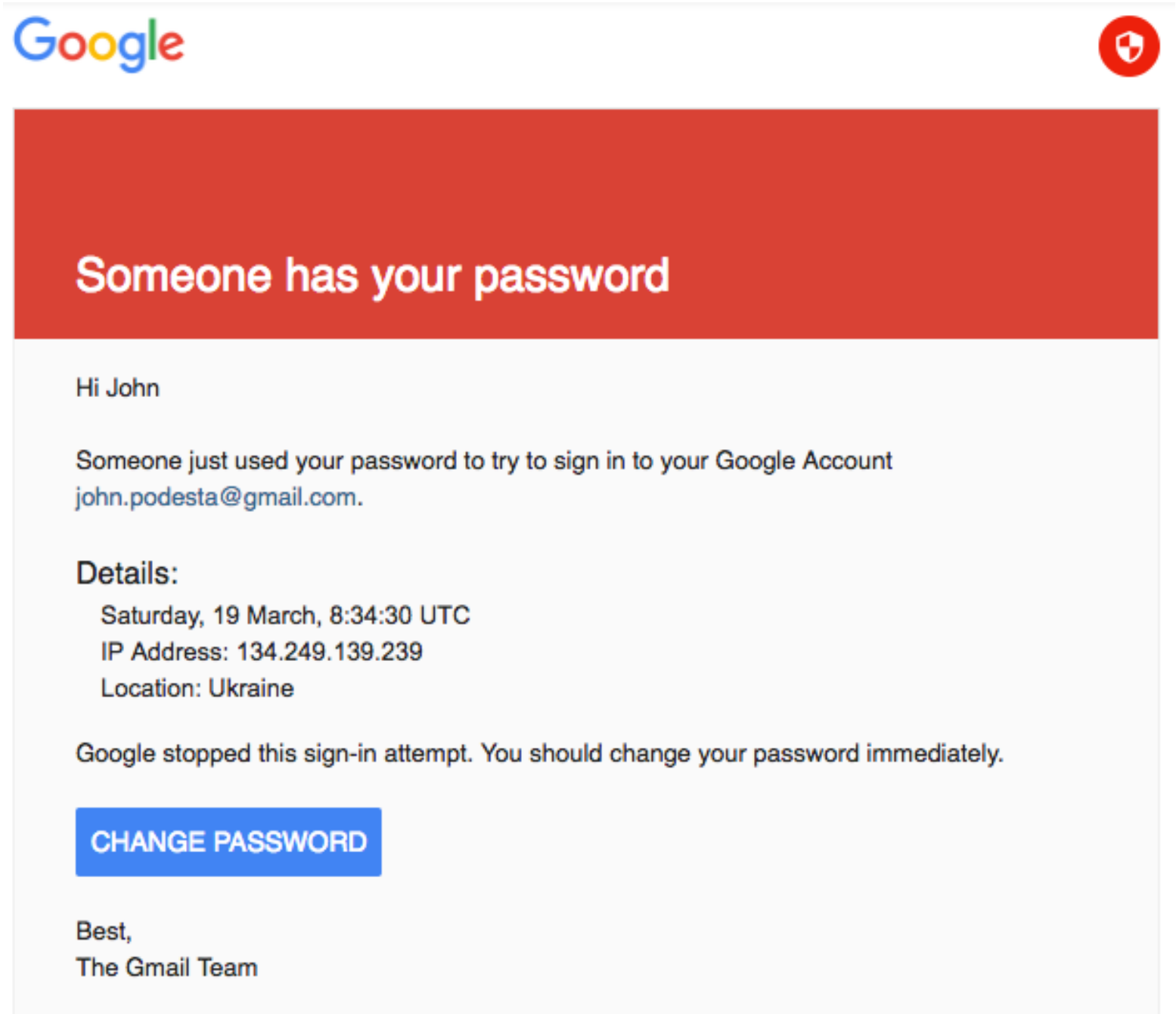
Example of Threat Modeling

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*

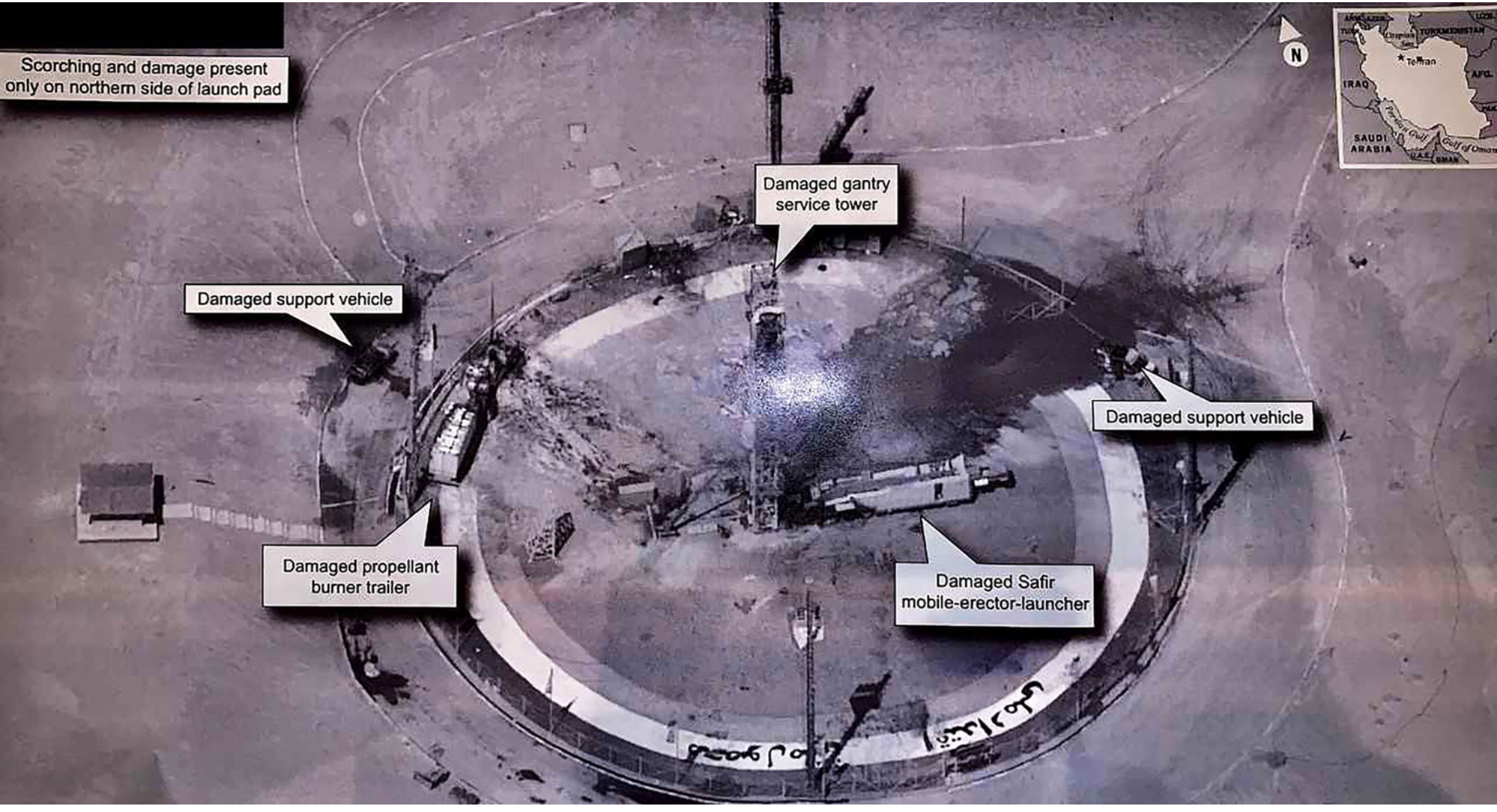
- What would security breaches cost us?
  - Direct costs: Money, property, safety, . . .
  - Indirect costs: Reputation, future business, well being, . . .
- How likely are these costs?
  - Probability of attacks?
  - Probability of success?

Countermeasures

- Technical countermeasures
  * Firewalls, Anti-virus programs, IDS programs, etc.

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

How do we protect classified satellites?



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?

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

Group Discussion

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?

Next lecture: Buffer overflows!