CSE 127: Introduction to Security

Nadia Heninger and Deian Stefan

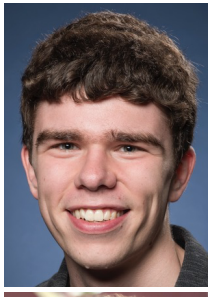
UCSD

Fall 2019 Lecture 1

Instructors

- Instructor: Nadia Heninger nadiah@cs.ucsd.edu
  - Lecture: MW 2-3:20pm 4140 EBU3B
  - Office Hours: W 3:30-4:30pm 3126 or 3138 EBU3B
  - Discussion Section: F4-4:50pm Center 113
- Instructor: Deian Stefan deian@cs.ucsd.edu
  - Lecture: MW 5-6:20pm Center 214
  - Office Hours: W 3:30-4:30pm 3126 or 3138 EBU3B
  - Discussion Section 5-5:50pm Center 113

- TA: Sunjay Cauligi scauligi@eng.ucsd.edu
  - Office Hours: Thursday 2-3pm B260A EBU3B



- TA: Craig Disselkoen cdisselk@eng.ucsd.edu
  - Office Hours: Monday 11am-12pm B270A EBU3B

- TA: John Renner jmrenner@eng.ucsd.edu
  - Office Hours: Friday 1:30-2:30 3148 EBU3B

- TA: Zaki Siddiqui zsiddiqu@ucsd.edu
  - Office Hours: Tuesday 2-3pm B260A EBU3B

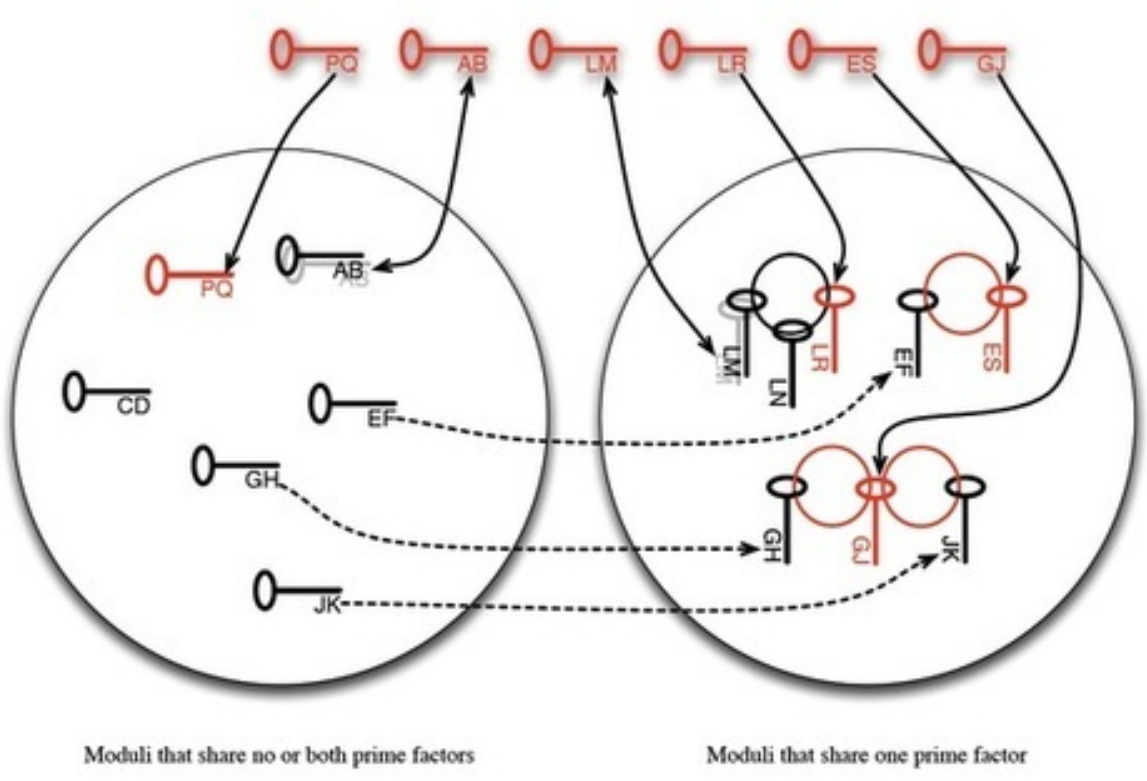
Nadia's work: Cryptographic systems security


4LD

Crypto shocker: four of every 1,000 public keys provide no security (updated)

Almost 27,000 certificates used to protect webmail, e-commerce, and other …

by **Dan Goodin** - Feb 15 2012, 7:00am EST



Keys that share one prime factor are vulnerable to cracking by anyone. Keys that share both prime factors can be broken by the other holder.

Researchers reveal a method the NSA may use to spy on Web traffic

By Sean Sposito | October 21, 2015 | Updated: October 21, 2015 5:05pm

RISK ASSESSMENT —

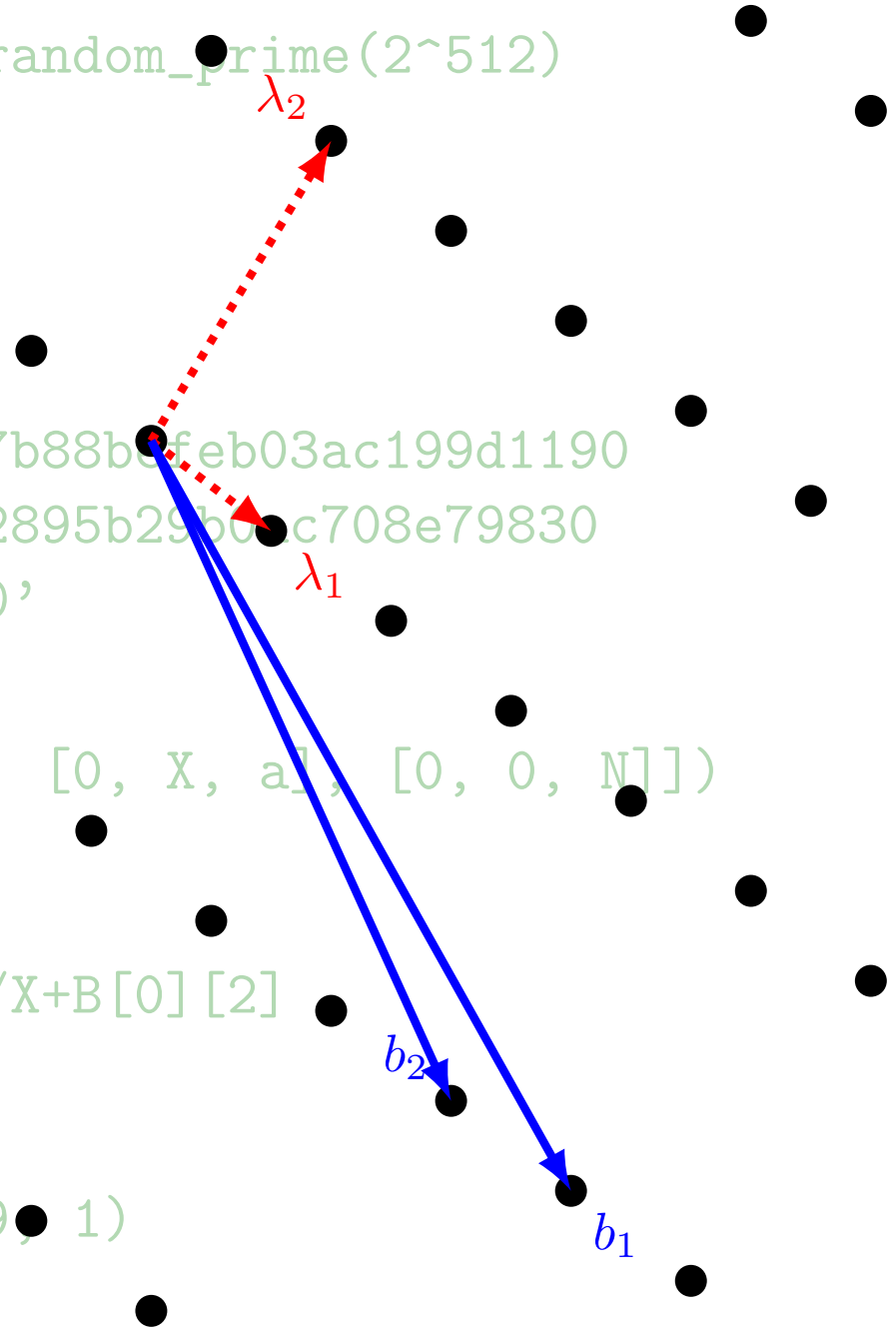
NSA could put undetectable “trapdoors” in millions of crypto keys

Technique allows attackers to passively decrypt Diffie-Hellman protected data.

DAN GOODIN - 10/11/2016, 7:30 AM

Nadia's work: Mathematical cryptography

```
p = random_prime(2^512); q = random_prime(2^512)
N = p*q

a = p - (p % 2^86)

sage: hex(a)
'a9759e8c9fba8c0ec3e637d1e26e7b88b0feb03ac199d1190
76e3294d16ffcaef629e2937a03592895b29b0c708e79830
4330240bc00000000000000000'

X = 2^86
M = matrix([[X^2, 2*X*a, a^2], [0, X, a], [0, 0, N]])
B = M.LLL()

f = B[0][0]*x^2/X^2+B[0][1]*x/X+B[0][2]

sage: f.factor()[0]
(x - 27753385000165998643777099) 1)
```



Deian's work: Language-based security

CT-Wasm: Type-Driven Secure Cryptography for the Web Ecosystem

CONRAD WATT, University of Cambridge, UK
JOHN RENNER, University of California San Diego, USA
NATALIE POPESCU, University of California San Diego, USA
SUNJAY CAULIGI, University of California San Diego, USA
DEIAN STEFAN, University of California San Diego, USA

Deian's work: Systems security

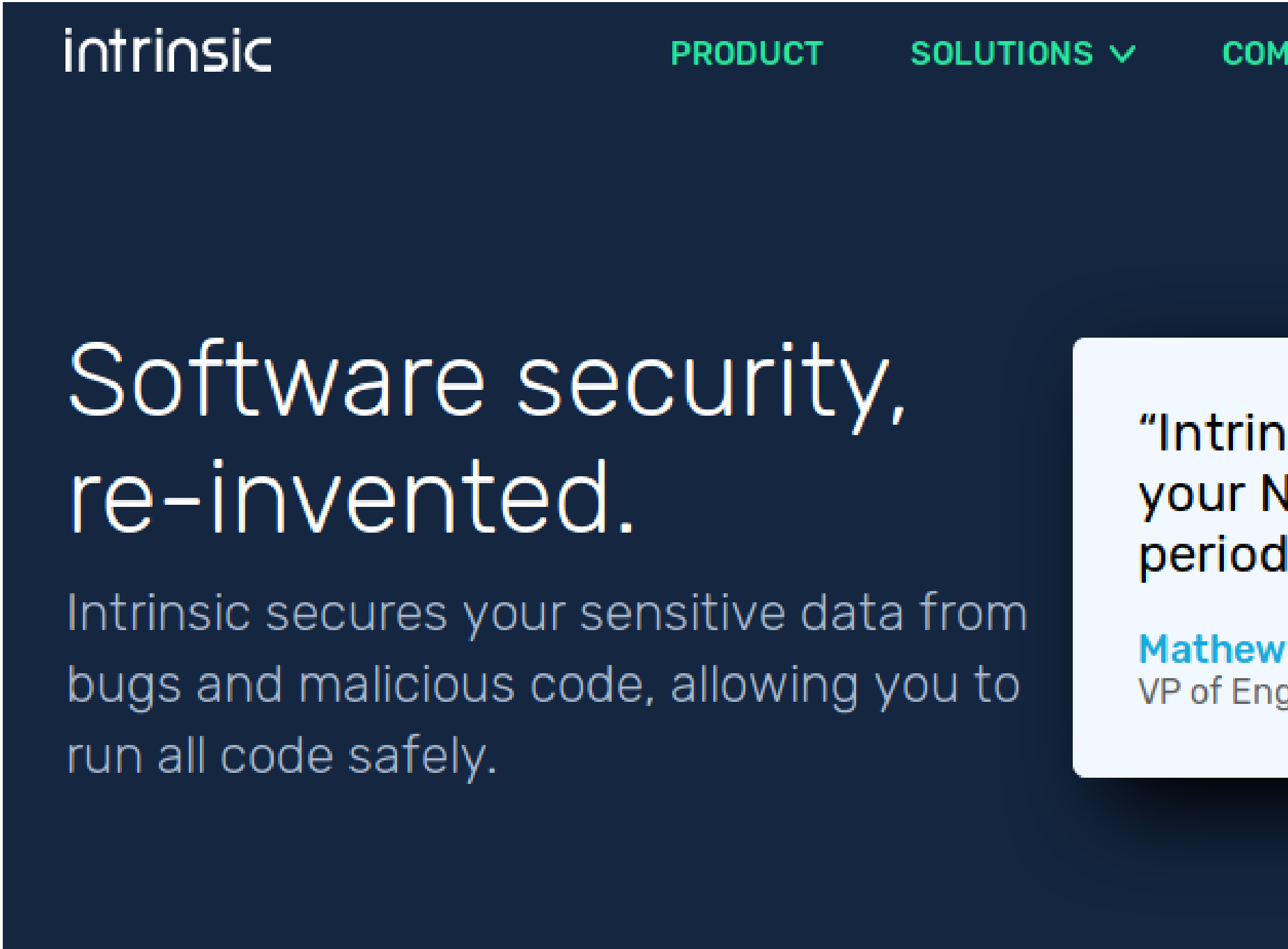
Deian's work: Web security

MOTHERBOARD
TECH BY VICE

Old School 'Sniffing' Attacks Can Reveal Your Browsing History

The way that major browsers store history and structure links leaves them vulnerable to old school 'sniffing' attacks, according to new research from the University of California San Diego.

Deian's work: Web security



Topics Covered

- The Security Mindset
  - Principles, threat modeling...
- Application Security
  - Defensive programming, memory protection, sandboxing, virtual machines, buffer overflows, malware
- Web Security
  - Web architecture, web attacks, web defenses
- Network Security
  - IP, TCP, routing, network protocols, network attacks, network defenses
- Cryptography
  - Public and private-key cryptography, authentication, secure channels, PKI...
- Privacy and Ethics

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 program secure systems
- Learn to be a security-conscious citizen
- Learn to be a `leet h4x0r`, but an ethical one!

Course Mechanics

40% Six projects

- Assignments will be due at 2pm on Wednesdays.

25% Midterm in class on 10/30

```
if midterm > 0
   then max(midterm, final)
   else 0
```

35% Final

- Nadia's section: 12/11 3pm-6pm
- Deian's section: 12/12 7pm-10pm

$\leq$ 10% Participation

Course Policies

Early policy:

- Can turn in assigments 3 days early to get 10% of your grade extra credit.
- No late days

Regrades should be the exception not the norm.

No cheating!

- UC San Diego policy:
  `http://academicintegrity.ucsd.edu`
- If you are not sure if something is cheating, ask!
- We will report *all* suspected cheating cases to academic integrity

Resources

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

- Assignments and references will be available on the course web site:

  `http://cseweb.ucsd.edu/classes/fa19/cse127-ab/`

  Collaborative course note wiki on website.

- HW 1 is already up! It is due **Wednesday 10/9**.

- Questions? Post to Piazza.

  `https://piazza.com/ucsd/fall2019/cse127`

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.

- Ethics requires you to refrain from doing harm.
- Always respect privacy and property rights.
- There are many legitimate hacking challenges (CTFs).

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

What is security?

What’s the difference?

What's the difference?

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

** An intelligence that actively tries to cause the system to misbehave.*

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"

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

Breaking into the CSE building.

Exercise

Getting accepted to UCSD.

What other security systems do you interact with?

Thinking like a Defender

- Security policy
  - What assets 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?
- What properties are we trying to enforce?
  - Confidentiality
  - Integrity
  - Availability
  - Privacy
  - Authenticity
  - ⋮

Threat Models

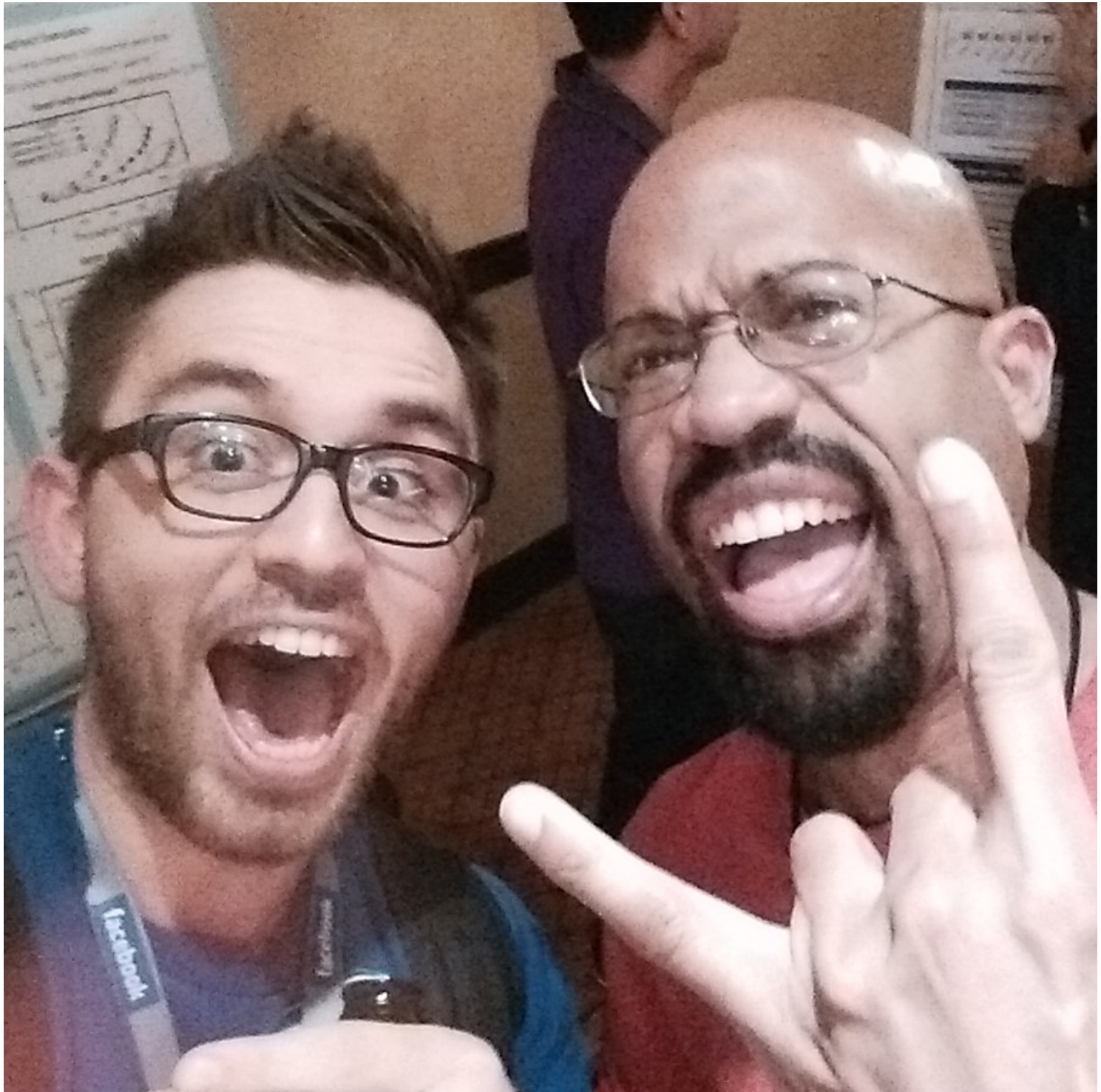
- Who are our adversaries?
  - Motives?
  - Capabilities?
- What kinds of attacks do we need to prevent? (Think like the attacker!)
- Limits: Kinds of attacks we should ignore?

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"


facebook

Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:

Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

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?

Donald J. Trump ✔ @realDonaldTrump · 2h

Only reason the hacking of the poorly defended DNC is discussed is that the loss by the Dems was so big that they are totally embarrassed!

8,852 5,672 20.5K

Donald J. Trump ✔ @realDonaldTrump · 2h

Intelligence stated very strongly there was absolutely no evidence that hacking affected the election results. Voting machines not touched!

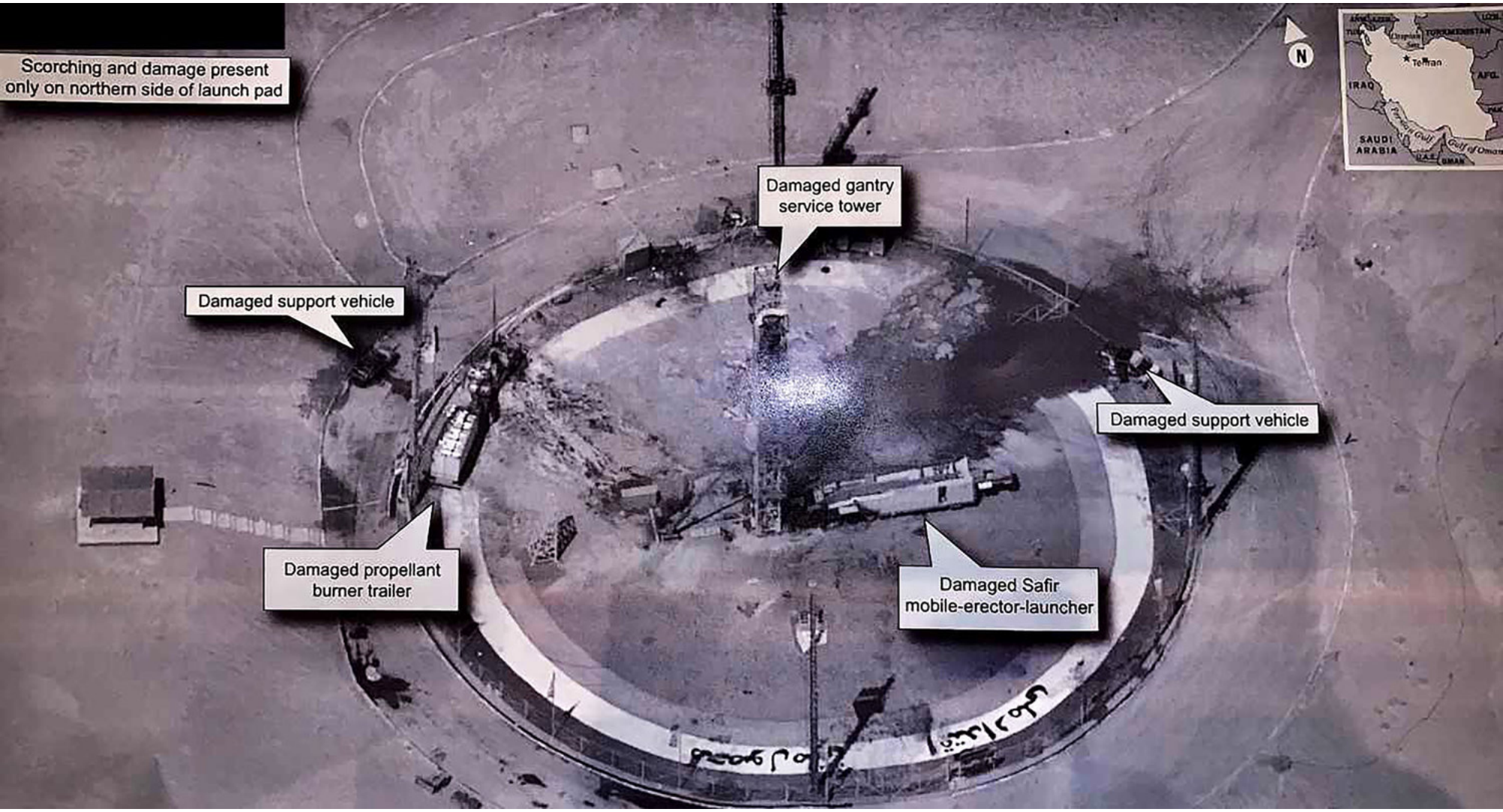
6,118 6,154 18.9K

Donald J. Trump ✔ @realDonaldTrump · 10h

Gross negligence by the Democratic National Committee allowed hacking to take place.The Republican National Committee had strong defense!

Countermeasures

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


Scorching and damage present only on northern side of launch pad
Damaged gantry service tower
Damaged support vehicle
Damaged support vehicle
Damaged propellant burner trailer
Damaged Safir mobile-erector-launcher
N
Tehran
IRAQ
SAUDI ARABIA
TURKMENISTAN
AFG.
UAE
OMAN

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 accept a software update?

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

Exercise

Protecting the CSE bear?

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

Secure Design

- Common mistake:
  Trying to convince yourself that the system is secure
- Better approach:
  Identify the *weaknesses* of your design and focus on correcting them
- Secure design is a **process**
  Must be practiced continuously; can’t be retrofitted

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

- Complexity vs. security?

Security Principles

- Defense-in-depth
- Diversity
- Maintainability

Exercise

Preventing cheating on an exam?

Exercise

Preventing you from stealing my password?

Reminder: Assignment 1 is due Wednesday October 9 at 2pm.

Next lecture: Buffer overflows!