

CSE 127: Introduction to Security

Deian Stefan

UCSD

Winter 2020 Lecture 1

Course staff



- Instructor: Deian Stefan deian@cs.ucsd.edu
 - Lecture: Mon & Wed 5-6:20pm Center 109
 - Discussion: Fri 2-2:50pm Center 216
 - Office Hours: Wed 3:00-4:00pm in 3126 EBU3B



- TA: Sunjay Cauligi scauligi@eng.ucsd.edu
 - Office Hours: Tue TBA



- TA: Riley Hadden rhadden@eng.ucsd.edu
 - Office Hours: Thu TBA



- TA: Zaki Siddiqui zsiddiqui@ucsd.edu
 - Office Hours: Mon 1:00-2:00pm in B270A EBU3B

My 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

My work: Language-based security

IODINE: Verifying Constant-Time Execution of Hardware

Klaus v. Gleissenthall

University of California, San Diego

Rami Gökhan Kıcı

University of California, San Diego

Deian Stefan

University of California, San Diego

Ranjit Jhala

University of California, San Diego

My work: Systems security

The screenshot shows a Bugzilla bug detail page for bug 1562797. The page has a dark header with the Bugzilla logo and a search bar. Below the header, there's a toolbar with icons for navigating between bugs and sections like Categories, Tracking, and People. The main content area displays the bug details:

Status: Open | **Bug ID:** Bug 1562797 | **Opened:** 3 months ago | **Updated:** 4 days ago

Summary: Use WASM sandboxed libraries in Firefox to reduce attack surface

Categories:

- Product: Core
- Type: task
- Component: ImageLib
- Priority: Not set

Tracking:

- Status: ASSIGNED

People: (Reporter: shravanrn, Assigned: shravanrn)

My work: Systems security

Finding and Preventing Bugs in JavaScript Bindings

Fraser Brown* Shravan Narayan† Riad S. Wahby*
Dawson Engler* Ranjit Jhala† Deian Stefan†

*Stanford University †UC San Diego

My work: Web security



MOTHERBOARD

TECH BY VICE

Old School 'Sniffing' Attacks Can Still 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.

My work: Web security

intrinsic

PRODUCT SOLUTIONS ▾ COMPANY DOCS BLOG Request a Demo

Software security, re-invented.

Intrinsic secures your sensitive data from bugs and malicious code, allowing you to run all code safely.

"Intrinsic is the best way to secure your Node.js Lambda functions, period."

Mathew Self
VP of Engineering, Box



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

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 1eet h4x0r, but an ethical one!

Course Mechanics

40% Six projects

- Assignments will be due at 2pm on Wednesdays.

25% Midterm in class on Feb 10 (or 12)

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

35% Final: Monday (finals week, March 16)

7pm-10pm

\leq 10% Participation

Course Policies

Early policy:

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

Course Policies

Early policy:

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

Regrade policy:

- Regrades should be the exception not the norm.
- Incorrect regrade request \Rightarrow negative points.

Course Policies

Early policy:

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

Regrade policy:

- Regrades should be the exception not the norm.
- Incorrect regrade request \Rightarrow negative points.

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:

<https://cse127.programming.systems>

Collaborative course note wiki on website.
- HW 1 will be up Wednesday. It is due **Wednesday 01/15.**
- Questions? Post to Piazza.

<https://piazza.com/ucsd/winter2020/cse127>

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 assessment infrastructure (e.g., grading system).

- 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

□

#

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

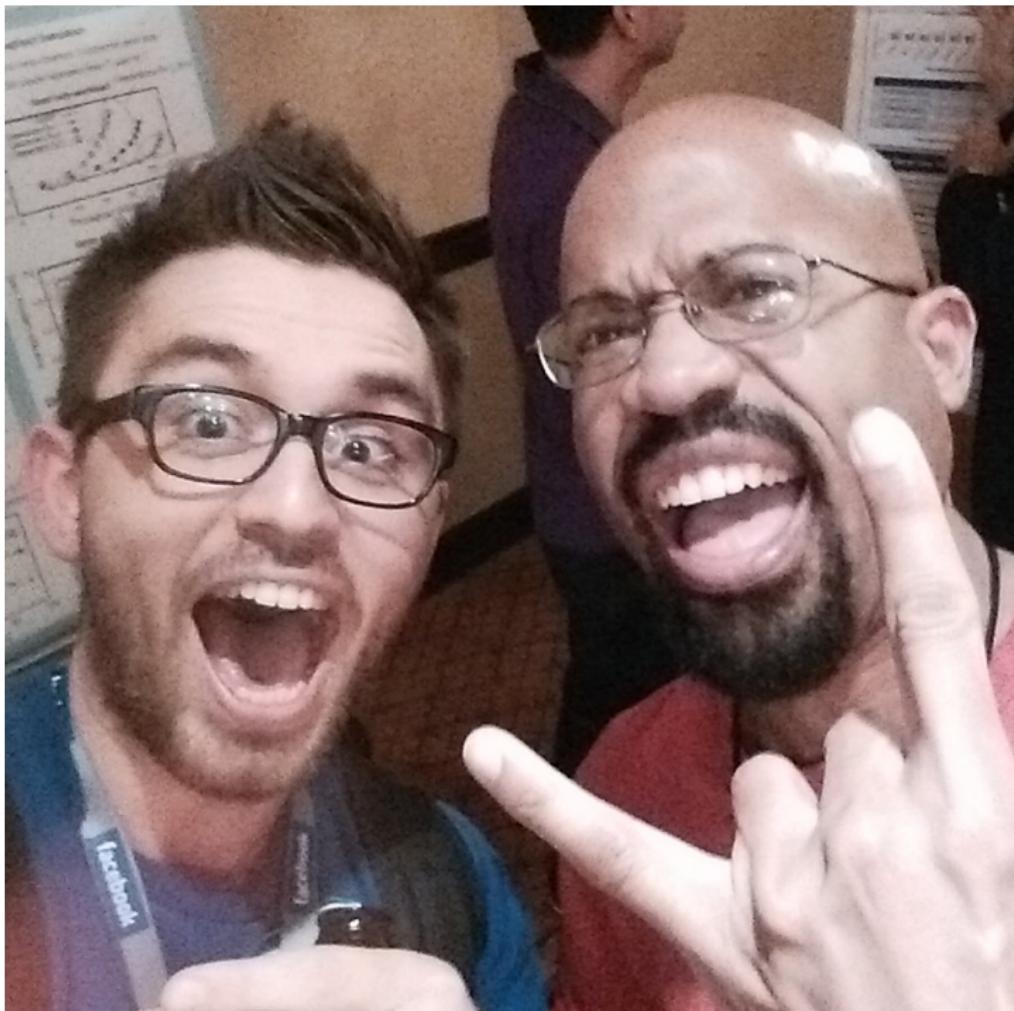
- Who are our adversaries?
 - Motives?
 - Capabilities?
- What kinds of attacks do we need to prevent?
(Think like the attacker!)
- Limits: Kinds of attacks we should ignore?

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"





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

Podesta emails

From Wikipedia, the free encyclopedia

In March 2016, the personal [Gmail](#) account of [John Podesta](#), a former [White House chief of staff](#) and chair of [Hillary Clinton's 2016 U.S. presidential campaign](#), was compromised in a [data breach](#) accomplished via a [spear-phishing](#) attack, and some of his emails, many of which were work-related, were hacked. [Cybersecurity](#) researchers as well as the [United States government](#) attributed responsibility for the breach to the Russian [cyber spying](#) group [Fancy Bear](#), allegedly two units of a [Russian military intelligence agency](#).^[1]

Some or all of the **Podesta emails** were subsequently obtained by [WikiLeaks](#), which published over 20,000 pages of emails, allegedly from Podesta, in October and November 2016.^[2] Podesta and the Clinton campaign have declined to authenticate the emails.^[3]

Cybersecurity experts interviewed by [PolitiFact](#) believe the majority of emails are probably unaltered, while stating it is possible that the hackers inserted at least some doctored or fabricated emails. The article then attests that the Clinton campaign, however, has yet to produce any evidence that any specific emails in the latest leak were fraudulent.^[4] A subsequent investigation by U.S. intelligence agencies also reported that the files obtained by WikiLeaks during the U.S. election contained no "evident forgeries".^[5]

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

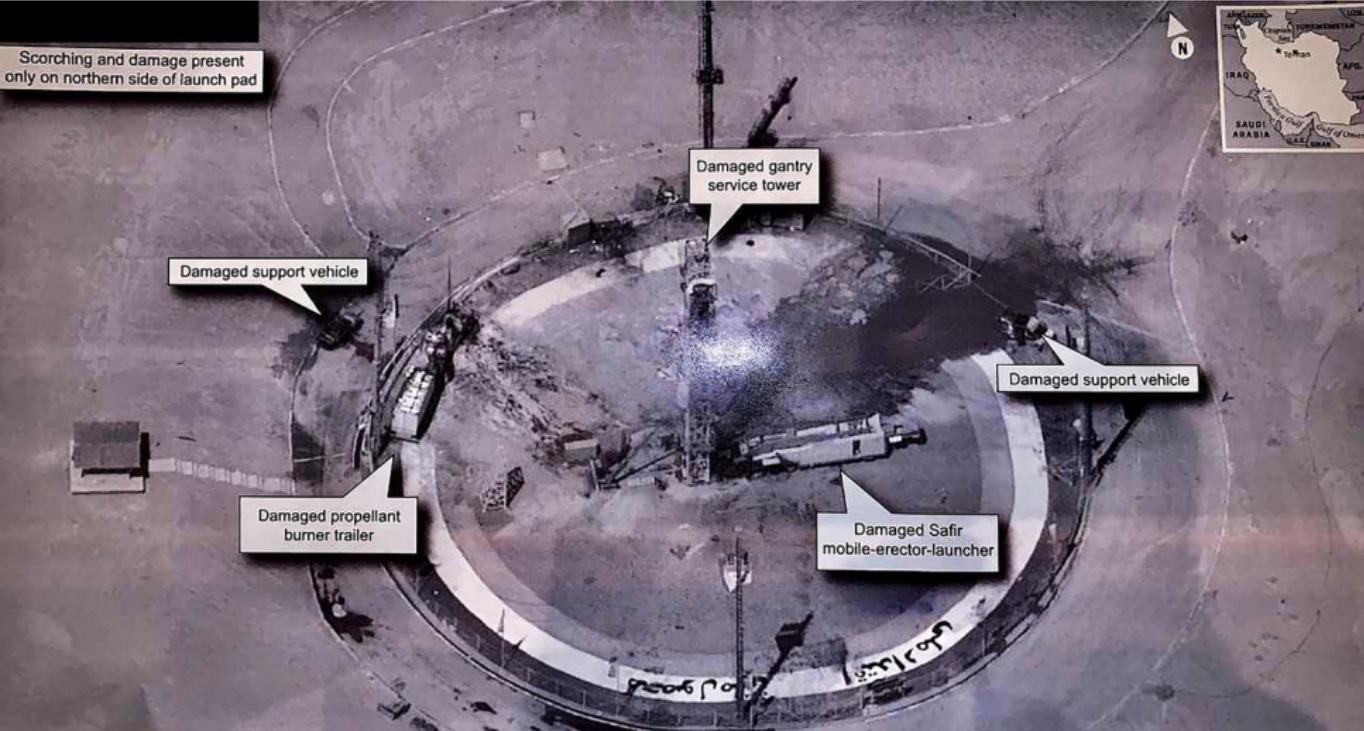


Donald J. Trump @realDonaldTrump · 10h

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.



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?

Next lecture: Buffer overflows!