CSE 127 Computer Security

Alex Gantman, Spring 2018

Lecture 1: Introduction

About me

- Graduated from UCSD
  - 1998 BS Computer Science
  - 2001 MS Computer Science
    (Applied Cryptography and Network Security)
- Lead Product Security team at Qualcomm
  - Joined Qualcomm in 1996 as an intern
  - Still learn something new about how computers work every week

Course Objectives

- A solid foundation of security concepts, backed by concrete examples
- Security mindset
  - How to think like an attacker/ security engineer
  - Looking beyond the system's intended functionality, to what it can be made to do
- Understanding how things work, how they break, and how to fix them
  - Technical details of vulnerabilities, attacks, and defenses

Course Objectives

During your career you will design and build complex systems. With probability asymptotically approaching 1, you will introduce numerous security vulnerabilities in the process.

My goals are to help you:

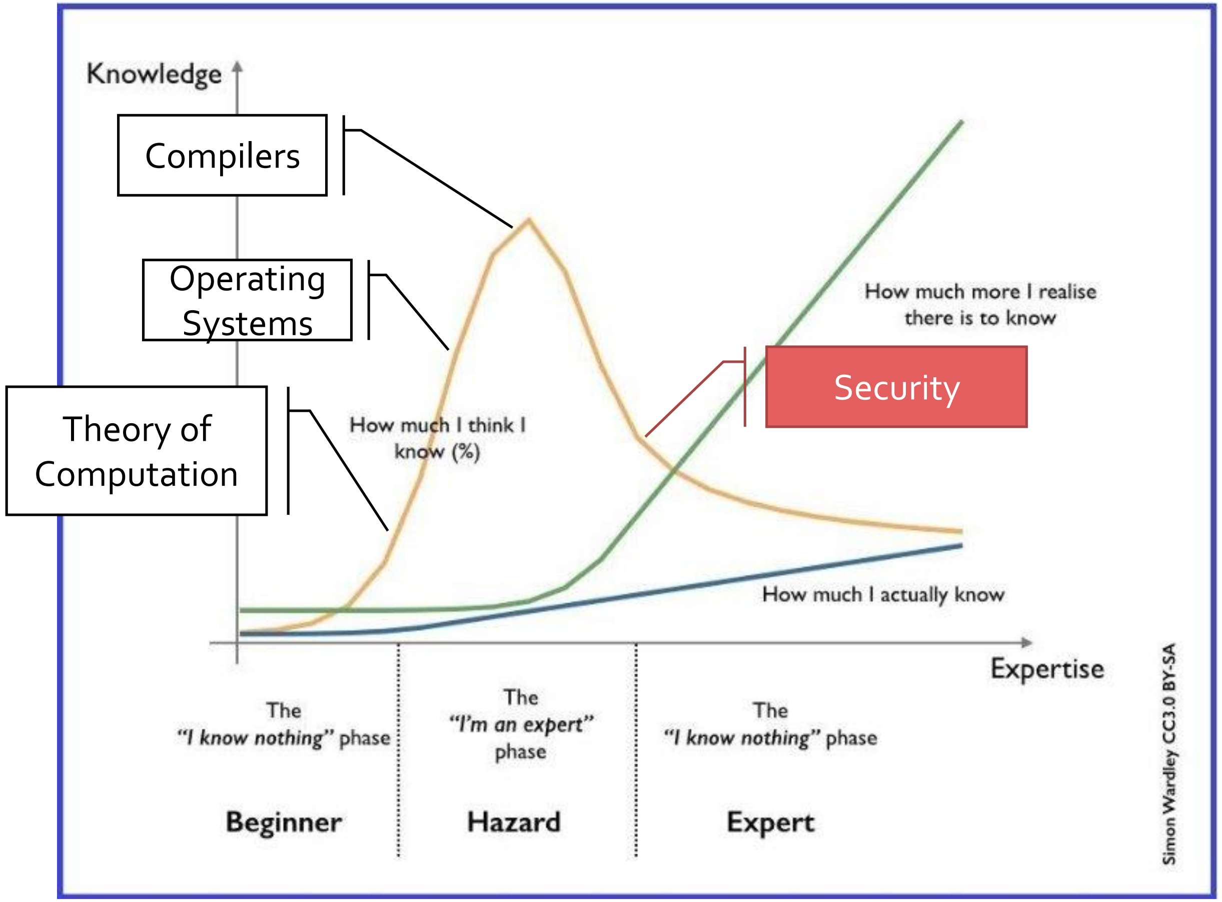
a) Minimize the number and severity of vulnerabilities you will introduce;

b) Better understand the root causes and impact of vulnerabilities that are brought to your attention;

c) Properly address identified vulnerabilities.

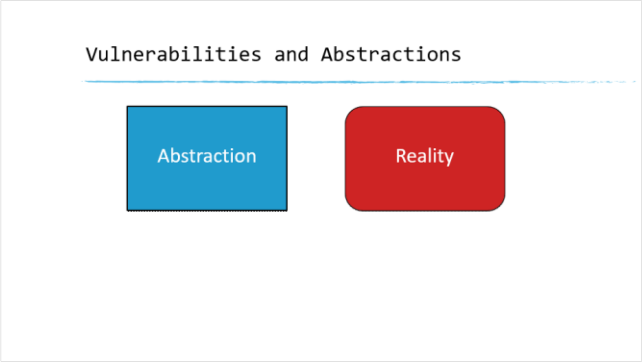
Prerequisites/Expectations

- You are expected to have a basic understanding of
  - C and assembly
  - Operating Systems
  - Computer Architecture
  - Networking



Vulnerabilities and Abstractions

- To build a secure system you must understand what your system is really capable of
  - Not what the requirements said
  - Not what documentation claimed
  - Not what the spec says
  - But what the actual implementation does

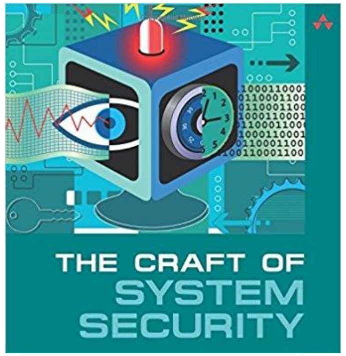


Course Information

- Lecturer: Alex Gantman
  - Lectures: TuTh 5:00-6:20pm, CSE(EBU3B) 4140
  - Office Hours: Th 6:30-7:30pm, CSE(EBU3B) 2106
- TA: Brian Johannesmeyer (and Brown Farinholt)
  - Discussion: Wed 10:00-10:50am, WLH 2113
  - Office Hours: Th 1:00-2:00pm, CSE(EBU3B) B215
- Piazza
  - https://piazza.com/ucsd/spring2018/cse127/home
- Course Web Page
  - https://cseweb.ucsd.edu/classes/sp18/cse127-b/

Course Material

- Textbooks
  - *The Craft of System Security*
    - Authors: Sean W. Smith, John Marchesini
    - ISBN 9780321434838
    - https://www.safaribooksonline.com/library/view/the-craft-of/9780321434838/
    - https://books.google.com/books/about/?id=daZMAAAACAAJ



- Articles & Videos
  - Additional web-hosted content to be assigned
- Slides
  - Based on slides and notes from Kirill Levchenko, Stefan Savage, Alex Dent, Robert Turner, and many others

Grading

- Homework assignments & projects: 35%
- Midterm: 25%
- Final: 30%
- Class participation: 10%
  - Take advantage of the smaller class size
  - I encourage lively in-class discussion
  - I will be calling on people in class

Rules

- Homework and assignments are due on the date and time indicated
  - May work in groups of 2 or individually
- You have seven 24-hour extensions
  - Debited in 24-hour increments when homework is late
  - When you run out extensions, homework will not be accepted
  - No other extensions will be granted
- Regrades should be the exception
  - We reserve the right to completely regrade your assignments

Rules

- No Cheating
  - Read and understand UC San Diego policy: http://academicintegrity.ucsd.edu
  - Cheating means not doing the assignment yourself, providing answers to others, etc.
  - OK to talk with other students about assignments outside of class
  - NOT OK to copy, translate, paraphrase, etc. someone else’s work

Ethics

- In this class you will learn how to attack the security of computer systems (and some physical systems)
- We learn attacks because it is needed to understand how to defend them
- You have an obligation to use this knowledge ethically
  - You may not attack others
  - Many good legitimate hacking challenges.

Vulnerability Disclosure

- Full Disclosure vs Responsible Disclosure vs Coordinated Disclosure
  - Good discussion at:
    - https://blogs.technet.microsoft.com/ecostrat/2010/07/22/coordinated-vulnerability-disclosure-bringing-balance-to-the-force/
- Bug bounties
- Exploit market

- If you discover a previously unpublished security vulnerability, I encourage you to report it to the system developers/maintainers
  - Check following directories or try emailing security@<domain>
    - https://hackerone.com/directory
    - https://www.bugcrowd.com/bug-bounty-list/

Computer Security

- How do we define it?
- How do we measure it?
- How do we achieve it?

Defining Security

- What is security?
  - “Security is the comfort in the freedom to take action” – Jim Hutchison
- What is a secure system?
  - “System that remains dependable in the face of malice” – Ross Anderson

Defining Security

- Security is not a functionality feature
  - Most of computer science is about providing functionality:
    - User Interface, Software Design, Algorithms, Operating Systems/Networking, Compilers/PL, Microarchitecture
  - Computer security is not about functionality
    - It is about how the embodiment of functionality behaves in the presence of an adversary.
    - Making sure the system does what it was supposed to do and only what it was supposed to do.
- Holistic property
  - "Software security is about integrating security practices into the way you build software, not integrating security features into your code" – Gary McGraw

Measuring Security

- How do we measure security?
- First, think of how we measure car safety
  - Are cars safer to drive today than they were 40 years ago?
  - How can we tell?
    - Safety tests?
    - What is the ultimate measure of car safety?
  - What are our units of measure?
    - Do we normalize per car, per person, per mile driven, etc.?
  - What if we did not have cars? Would more people stay alive?
- Back to computers
  - Are computers more secure today than they were 20 years ago?
  - How can we tell?
    - What is the ultimate measure of computer security?
  - What are our units of measure?
    - Do we normalize per computer, per person, per transistor, per byte processed, etc?
  - Would we be safer overall without computers?

Motor vehicle deaths in U.S. by year [edit]

Year	Deaths	Vehicle miles travelled (billions)	Fatalities per 100 million VMT	Population	Fatalities per 100,000 population	Change (in percent)
2016	37,461		1.18	323,121,000	11.59	
2015	35,485	3,095	1.15	321,370,000	11.06	▲10.5%
2014	32,744	3,026	1.08	318,860,000	10.28	▼-0.9%
2013	32,893	2,988	1.10	316,129,000	10.40	▼-3.3%
2012[7]	33,782	2,969	1.14	313,914,000	10.75	▲2.6%
2011[6]	32,479	2,950	1.10	311,588,000	10.42	▼-2.3%
2010[2]	32,999	2,967	1.11	309,326,000	10.668	▼-3.5%
2009	33,883	2,957	1.15	306,700,000	11.048	▼-9.7%
2008	37,423	2,977	1.26	303,824,640	12.317	▼-11.0%
2007	41,259	3,031	1.36	301,139,947	13.701	▼-3.85%
2006	42,708	3,014	1.42	299,398,484	14.265	▼-2.79%
1978	50,331	1,544.70	3.26	222,584,545	22.612	▲4.02%
1977	47,878	1,467.03	3.26	220,239,425	21.739	▲4.12%
1976	45,523	1,402.38	3.25	218,035,164	20.879	▲1.27%
1975	44,525	1,327.66	3.35	215,973,199	20.616	▼-2.45%
1974	45,196	1,280.54	3.53	213,853,928	21.134	▼-17.14%
1973	54,052	1,313.11	4.12	211,908,788	25.507	▼-1.92%
1972	54,589	1,259.79	4.33	209,896,021	26.008	▲2.79%

https://en.wikipedia.org/wiki/List_of_motor_vehicle_deaths_in_U.S._by_year

Measuring Security

- Automotive safety engineers have NHTSA data to provide feedback on what works and what doesn’t.
- Healthcare professionals have FDA and CDC data to provide feedback on what works and what doesn’t.
- Security engineers have thought leaders.
  - What we lack in data on what works, we more than make up with fanatical beliefs in what should work.

Measuring Security

- Thought exercises
  - The government plans to invest 100 billion dollars to improve computer security over the next decade. How do you measure the impact of this initiative?
  - Activists are calling for greater legislative regulation of computer security. How do you measure the effectiveness of such regulation?
  - A vendor claims their product is more secure than the competition's. How do you evaluate the relative security of two products?

Security of Consumer Systems

- What physical items do you have in your home that stand a chance to "remain dependable in the face of malice"?
- Consumer goods tend to require careful handling
  - Nothing in my house can survive a three-year-old armed with scissors
- Objects for public spaces are designed for moderate abuse
  - Uglier, poorer functionality, more expensive

- Unique problem for electronic devices
  - Must offer price, functionality, and aesthetics of a consumer product…
  - …but be designed for abuse
- Systems that you design and implement will need to withstand not just casual abuse from bored teenagers, but targeted attacks by trained professionals.

Security Evolution

- As engineers, we often delude ourselves into thinking that we understand our own creations
  - or that we can create complex systems to do only what we meant them to do
- But … Nobody knows how these systems really work
  - Complexity of computer systems is approaching complexity of biological organisms
    - 3 billion base pairs in human genome
    - 10+ billion transistors in modern CPUs
- Complex systems co-evolve with attacks against them
  - Resiliency is developed in response to encountered threats
  - Systems deemed secure today may not be resilient to new threats

“Meltdown” and “Spectre”: Every modern processor has unfixable security flaws

Immediate concern is for Intel chips, but everyone is at risk.

Review

- What is a secure system?
  - “System that remains dependable in the face of malice” – Ross Anderson
- Building secure systems requires understanding how things ***really*** work
  - Attackers exploit the delta between perception of how systems work and how they really work
- Security engineering is still very nascent
  - A lot of craft and lore
  - Not enough science
  - Difficult to measure

Additional Resources

- *The Market For Silver Bullets* by Ian Grigg
  - http://iang.org/papers/market_for_silver_bullets.html
  - “Security can be viewed as a market where neither buyer nor seller has sufficient information to be able to make a rational buying decision. … these characteristics lead to the arisal of a market in *silver bullets* as participants *herd* in search of *best practices*, a common set of goods that arises more to reduce the costs of externalities rather than achieve benefits in security itself.”

Homework

- Read *Reflections on Trusting Trust* by Ken Thompson
  - https://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf
- Read Chapter 1 from *The Craft of System Security*
- First project is due next week (4/9 @ 10pm)
  - Getting comfortable with the debugger and project submission system

Next Lecture…

Security Foundations: Threat Models and Risk Analysis