Course info

● Stefan Savage – Lecturer & taskmaster
  ◆ Web: http://www.cs.ucsd.edu/~savage
  ◆ E-mail: savage@cs.ucsd.edu
  ◆ Office hours: M 4pm (or by appt)
  CSE 3106

● TAs: Aviv Kiss, Edward Sullivan, Louis Dekoven
  ◆ E-mails: akiss@eng.ucsd.edu, elsulliv@eng.ucsd.edu, ldekoven@eng.ucsd.edu, Office hours: TBA

● Course Web pages
  ◆ http://www.cse.ucsd.edu/classes/fa15/cse127-a/ (not much there now)
Course Goals

● How to **think** about security in the real world – **The Security Mindset**
  - Vulnerabilities: threats, capabilities, assumptions
  - Incentives: goals, socio-economic & political

● Technical aspects
  - Software vulnerabilities
  - Attack techniques
  - Defenses
Technical topics

• Basic cryptography & cryptographic protocols
• Access control, authentication and identity management
• Side channels, covert channels and confinement
• Secure code and code exploitation
  ✦ Buffer overflow, format strings, heap spray, race conditions, return-to-libc, etc
• Web vulnerabilities (XSS, CSRF)
• Malware (viruses, worms, rootkits, spyware, etc)
• Network security (protocol attacks, firewalls, NIDS)
• Denial-of-service
• E-crime (spam, phishing, carding, etc)
• Cyberphysical security/Internet of Things
About me...

- I work at the intersection of computer security, networking and operating systems

- **Research**
  - I’m director of the Center for Networked Systems (CNS) on campus and the Center for Evidence Based Security Research (evidencebasedsecurity.org) with UCSD and UCB.
  - Lots of work on security measurement, ecrime, security of cyberphysical systems (esp cars and planes)

- **Policy**
  - National Research Council’s Cybersecurity Research group
  - Institute for Defense Analysis’ ISAT advisory group
  - National Science Foundation CISE Advisory Committee
  - Way too much time on The Hill

- **Industry**
  - Asta Networks (defunct anti-DDoS company)
  - Netsift (UCSD-originated worm defense company) -> Cisco
  - Lots of consulting…
Things we’re known for here at UCSD...

- Taking over automobiles 1,000 miles away
- Copying house/office keys remotely
- Compromising voting machines without adding any code
- Tracking the financial structure of online spam
Prerequisites

- CS 21/Math 15B and CSE120
- In reality, I will not stress the mathematical side of security (take 107… its very good)
- It will help a lot to know about computer architecture, operating systems and networking
  - I’ll do my best to give background, but you’ll be expected to keep up
- You will need to code in C and be comfortable with it. If you don’t know C, expect to learn it quickly
● There is no required textbook for this class
  ○ We’ll read a bunch of Web-based articles
  ○ We may read from Security Engineering by Ross Anderson
    » But its available for free: http://www.cl.cam.ac.uk/~rja14/book.html

● For those who want some “backup”, check out
  ○ *Security in Computing* by Charles Pfleeger
  ○ *Introduction to Computer Security* by Matt Bishop
  ○ *Applied Cryptography* by Bruce Schneier
Grading (approximately)

- Homework/Projects: 35%
- Midterm: 25%
- Final: 35%
- Class participation: 5%
Rules

- Written assignments are due at the *beginning* of class
- Regrades should be the *exception*
  - Addition errors (happy), significant errors in grading (fine), nit picking/grade mongering (death to you)
  - We reserve the right to *completely* regrade your assignments
  - All regrades go first to Aviv, Edward or Louis (our TAs)

- **No Cheating**

- Cheating means not doing the assignment yourself
  - No copying, no Google, etc. If you’re unsure, then ask
  - Ok to *talk* with other students about assignments outside of class
  - Not ok to copy, translate, paraphrase, etc… someone else’s work

- Don’t mess with the professor. **He’s a mean man.**
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 (i.e., you may not attack others)
  - Aside: major legal issues here too
What is security?
What is security?

- Merriam-Webster online dictionary:
  
  **Function:** noun
  
  • **Freedom from danger**
  
  • **Freedom from fear or anxiety**
  
  1: the fulfillment of an obligation  b : SURETY
  
  3: an instrument of investment in the form of a document (as a stock certificate or bond) providing evidence of its ownership
  
  • **Measures taken to guard against espionage or sabotage, crime, attack, or escape**
Computer security?

- Most of computer science is about providing *functionality*:
  - User Interface
  - Software Design
  - Algorithms
  - Operating Systems/Networking
  - Compilers/PL
  - Microarchitecture
  - VLSI/CAD

- Computer security is *not* about functionality

- It is about how the embodiment of functionality behaves *in the presence of an adversary*
History: two competing security philosophies...

● **Binary** model
  - Traditional crypto and trustworthy systems
  - Assume adversary limitations X and define security policy Y
  - If Y cannot be violated without needing X then system is secure, else insecure

● **Risk management** model
  - Most commercial software development (and much real-world security… e.g., terrorism)
  - Try to minimize biggest risks and threats
  - Improve security where most cost effective (expected value)
Classic example (binary): perfect substitution cipher

Invited by combination of Vernam & Mauborgne (~1919)

- Choose a string of random bits the same length as the plaintext, XOR them to obtain the ciphertext.

**Perfect Secrecy** (proved by Claude Shannon)

- Probability that a given message is encoded in the ciphertext is unaltered by knowledge of the ciphertext
- Proof: Give me any plaintext message and any ciphertext and I can construct a key that will produce the ciphertext from the plaintext. Zero information in ciphertext
Classic example (risk mgmt): Concrete barricades

- Prevent incursion by car bombers
Some problems with the binary model of security

- Many assumptions are brittle in real systems
  - Real artifacts fragile, imperfect, have bugs/limitations
  - Implicit dependencies with exposed layers
    » Example: reading secret bits off current draw on a chip

From Paul Kocher
Some problems with the binary model of security

- Hard to know what security policy should be?
  - What are the dangers?

- Finally: \textit{hugely expensive}... how many fully formally verified systems are out there?
Some problems with the risk management model of security

But I only need to win once, you fool!
Some problems with the risk management model of security

- Creates arms race – forced co-evolution

Adversary invents new attack

Defender creates new defense
Some problem with the risk management model of security

- It's fine to say security is a spectrum, but how to *evaluate* risk or reward?
  - How many units of security does your anti-virus product give you?

- And the best you can hope for is *stalemate*
  - And we’re losing stalemate in a number of situations (e.g., SPAM, Malware)
Key meta issues in Security

- Policy
- Risks
- Threats
- Value
- Protection
- Identity & Reputation
Policy

- What **is** a bad thing?

- Remarkably tricky to define for known threats
  - The software on your computer likely has 100s of security options... How should you set them?
  - What might be a good security policy for who gets to access faculty salary data?

- Even harder for unknown threats
  - SPAM

- Can be non-intuitive
  - Should a **highly privileged** user have more rights on a system or less?
Risks & threats

- Risk
  - What bad things are possible?
  - How bad are they and how likely are they?

- Threats
  - Who is targeting the risk?
  - What are their capabilities?
  - What are their motivations?

- These tend to be well formalized in some communities (e.g. finance sector) and less in others (e.g. energy sector)
The Threat Landscape
(courtesy David Aucsmith, Microsoft)

- National Interest
- Personal Gain
- Personal Fame
- Curiosity

- Script-Kiddy
- Hobbyist Hacker
- Expert
- Specialist
- Vandal
- Thief
- Trespasser
- Author
- Spy
The Threat Landscape
(courtesy David Aucsmith, Microsoft)

National Interest

Personal Gain

Personal Fame

Curiosity

Script-Kiddy  Hobbyist Hacker  Expert  Specialist

Spy

Tools created by experts now used by less skilled attackers and criminals
Value

- What is the cost if the bad thing happens?
- What is the cost of preventing the bad thing?

- Example: credit card fraud
  - Who pays if someone steals your credit card # and buys a TV with it?

- Example: Permissive Action Links for nuclear weapons
Protection

- The mechanisms used to protect resources against threats
  - This is most of academic and industrial computer security

- Many classes of protections
  - Cryptographic protection of data
  - Software guards
  - Communication guards
  - User interface design (protect user against own limitations)

- Can be either proactive or reactive
Deterrence

- There is some non-zero expectation that there is a future cost to doing a bad thing
  - i.e. going to jail, having a missile hit your house, having your assets seized, etc
  - Criminal cost-benefit: $M_b + P_b > O_{cp} + O_{cm}P_aP_c$ [Clark&Davis 95]
    - $M_b$: Monetary benefit
    - $P_b$: Psychological benefit
    - $O_{cp}$: Cost of committing crime
    - $O_{cm}$: Monetary cost of conviction
    - $P_a$: Probability of getting caught
    - $P_c$: Probability of conviction

- Need meaningful forensic capabilities
  - Audit actions, assign identity to evidence, etc
  - Must be cost effective relative to positive incentives
Switching gears: Identity

- Identity is implicit in virtually all security questions…. but we rarely think about it much

- We have strong intuitions however
  - How do you feel about “Black Unicorn” the cypherpunk?
  - How about A.S.L. von Bernhardi the investment banker?
Identity

- What is it?
  - One def: *The distinct personality of an individual regarded as a persisting entity; individuality* (courtesy Black Unicorn)
  - Another: *A unique identifier – distinguishing mark* (courtesy A.S.L. von Bernhardi)

- What’s the difference between an **identity** and an **identifier**?
  - Allows naming; to establish an assertion about reputation

- Reputation?
  - A specific characteristic or trait ascribed to a person or thing: e.g., “a reputation for paying promptly”
  - Potentially a predictor of behavior, a means of valuation and as a means for third-party assessment

- Value comes from binding reputation and identifiers
- But how to make this binding?
Due diligence and trust

- **Due diligence**
  - Work to acquire multiple independent pieces of evidence establishing identity/reputation linkage; particularly via direct experience
  - Expensive

- **Trust**
  - *Reliance on something in the future; hope*
  - *Allows cheap form of due-diligence: third-party attestation*
  - Economics of third-party attestation? Cost vs limited liability
  - What is a third-party qualified to attest to?
  - Culturally informed/biased?
That’s it for today

- Any questions?
- For next time go watch Johnny Long’s “No Tech Hacking” video (on web site)
- Next time we’ll talk about basic security principles
  - Confidentiality, authentication, integrity
  - Authorization
- No section this Monday