Course Introduction; Security mindset

Debdeep Mukhopadhyay
and Mainack Mondal

CS 60065
Autumn 2019

Today's class

- Course structure
- Overview of security

Website / Topics

- https://mainack.github.io/cryptosec2019/

- We would use piazza for regular announcements
  - https://piazza.com/iitkgp.ernet.in/summer2019/cs60065
  - You would need an access code: written on blackboard
  - Use piazza for discussions, shooting questions and more…

Course evaluation

- Internal Assessment (30%)
  - Class test, assignments, tutorial problems
  - To be specified as we go
- Mid semester examination (30%)
  - Closed book
- End semester examination (40%)
  - Closed book

Instructors

- **Debdeep Mukhopadhyay:** Cryptography, hardware/embedded security, side channel attacks
  - Office: CSE Annex 303
  - Also teaching parallel algorithms

Instructors

- **Mainack Mondal:** Web and network security, usable security and privacy, system security and privacy
  - Office: CSE 316
  - Also teaching social computing

Two TAs

Manaar Alam

alam.manaar@gmail.com

Arnab Bag

amiarnabbolchi@gmail.com

Course topics

- Details are in webpage
  - Lets walk through the tentative topics we would cover
  - Not quite in order

Course topics: Overview of security (aka *The starting point*)

- The security mindset
- Threat modelling
- What is security
- A few words on ethics

Course topics: Cryptography (aka *The building blocks*)

- What cryptographic techniques are the building blocks to secure systems?
  - Overview of Cryptography
  - Symmetric key cryptosystems: SPN Ciphers, The Feistel Cipher
  - Modern Block Cipher Standards - AES
  - Cryptanalytic techniques: Linear Cryptanalysis, Differential Cryptanalysis
  - Advanced block cipher design: SBox Design Principles, Modes of Operations
  - Cryptographic Hash functions and Message Authentication Codes
  - Asymmetric Ciphers: The RSA Cryptosystem

Course topics: Network security (aka *internet – the wild west*)

- How the fabric of Internet is often under attack
  - Networking Basics
  - Network threat model
  - Basic Network Attacks
  - DNS, BGP attacks
  - Denial of Service Attacks, smurf attack, Reflection attack
  - Mitigation, IP traceback

Course topics: Web security
(aka *You are online, you will get hacked*)

- How anything/body online can get compromised
  - How the Modern Web Works: Anatomy webpage and http(s) requests
  - SQL injection
  - XSS, CSRF attacks
  - Online tracking
  - Buffer overflow: the curious case of Heartbleed
  - Botnets

Course topics: Usable security (aka *Humans are weak, make them strong*)

- Consider the human factor in security
  - Why usable security
  - A few case studies
  - Qualitative methods to understand humans
  - Usability for developers
  - Phishing attacks and mitigation

Course topics: Privacy and Anonymity (aka *Protect what is yours*)

- How to control your data and protect yourself from prying eyes
  - Definitions of privacy
  - Anonymity: Overview of Tor
  - Attacks on Tor
  - Private information retrieval, differential privacy
  - Anonymous routing

Course topics: Smartphone security (aka *How to make your phone not spy on you*)

- Smartphone can be used to siphon your personal data
  - Permission model in Android
  - Attacks on permission model and mitigation

Course topics: Adversarial ML
(aka *How to attack the skynet*)

- Deep learning is awesome and powerful – but they are not immune to attacks, yet
  - Intro to adversarial machine learning
  - Adversarial Deep Learning

Security: an overview

The security mindset

- Imagine that I have the recipe of Coca Cola in a text file. Naturally, I want to store it securely. You are hired to do that.

- The first task: **Threat modelling**
  - Systematically identifying and enumerating potential threats to the system
  - Who are you protecting against?
  - Rival company? Family member? A nation? …

Step 1: Identify assets and their value

- What is/are the assets in this case?
  - A recipe

- Determine the value of those assets?
  - Can you convert it to a monetary value? (say ₹10 lakh)
  - Factors you need to consider
    - Can others replicate the cola if they have the recipe?
    - Perhaps others already have a “good enough” recipe?
    - How would leaking the recipe affect me, the owner?

Where might the recipe be stored?

- My bank vault
- My laptop
- My Desktop
- My phone
- My email
- My brother’s/ wife's email account or computers
- Github
- The memory of a printer
- My garbage bin

Step 2: Enumerating attack surface

- **Attack surface**: Complete set of points of entry into the system

- E.g.: Attack surface for my email
  - Guessing my password
  - Compromising my email provider
  - Looking over my shoulder when I am working
  - Making friends with my home cleaner (insider threat)
  - ….

Attack surface for laptop

- Physical access to laptop
  - Pick lock of my office
  - Bribe my family members …
- Remote access to laptop
  - “Phish” me (social engineering)
  - Buy a “zero day exploit”…
- Physical proximity to laptop
  - Eavesdrop on the network traffic
  - Point a camera to my screen …

Step 3: Model attackers

- Resource of the attackers
  - Professional thief, Computer expert, A nation state
- How much effort would the attackers put in
  - Would they break a bank vault? Buy a zero day exploit for multi million dollars?
- Finally, what the attackers would not do?
  - E.g., they might not simply guess a 160 digit random passphrase

Step 4: Mitigations

- **Attack vector:** How attacker might gain access to the recipe (attack surface+ resource + effort)
- Mitigation: minimize the likelihood that attack vectors will be used.
- Mitigations can be hard
  - Often a trade-off between usability and security
  - You can keep the recipe out of attackers hand by destroying it – zero usability

What security properties we might want?

- CIA model: Confidentiality, Integrity, Availability
- **Confidentiality:** hide information from entities who are not authorized to view it (e.g., by building mathematical “locks” which you can prove will not be broken without a key)
- **Integrity:** Secure Information should not be altered (or anyone would know/check if its altered)
- **Availability:** Information is always available to the authorized viewer

Ethical considerations

Source: https://myozonelayer.com/2016/11/22/the-4th-monkey-do-no-evil/

Ethical considerations

- Don’t do evil
- If you feel its wrong, it is wrong
- Cyber offenses are punishable by law
  - The case of Mirai Botnet -- five years of probation, 2,500 hours of community service, and $127,000 fine.
  - The case of Swatting – people got killed