CS-457: Introduction to Secure Systems

Introductory Lecture

Papadogiannakis Manos
papamano@csd.uoc.gr

Computer Science Department
University of Crete

Overview

- **What is computer security?**
- **Course Topics**
- **Course Logistics**
  - e.g. Grading

Computer Security

Computer Security

"The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide Confidentiality, Integrity, and Availability."

Not this CIA!

- **Confidentiality: There is information that we want to keep secret**
  - Someone stealing military documents
- **Integrity: We don’t want to allow unauthorized entities to modify information**
  - Someone modifying our bank deposit
- **Availability: We want users to be able to reliably access information when they need to**
  - Someone making 911 drop all calls

https://www.f5.com/labs/learning-center/what-is-the-cia-triad

Computer Security

- **Not as simple as it may sound**
  - Modern systems are complex
- **The Adversarial mindset**
  - You are an engineer with opponents
  - They are intelligent and don't play by the rules
  - They only need to find a single vulnerability
- **In most systems, security is not a priority**
  - Focus on other design criteria (e.g. performance)
  - Comes after the design is complete
  - Often considered not user-hostile

Do you need to be paranoid or sceptical to be cyber-safe online?

https://www.linkedin.com/pulse/do-you-need-paranoid-sceptical-cyber-safe-online-alvin-rodrigues

Course Topics

Topics

- Cryptography
- User Authentication
- Access Control
- Database Security
- Malicious Software
- Denial of Service Attacks
- Intrusion Detection Systems
- Firewalls
- Buffer Overflow
- Software Vulnerabilities
- Operating System Security
- Internet Security Protocols

Cryptography

- Protect information so that only the person a message was intended for can read it

- Back in the old days: Security = Cryptography

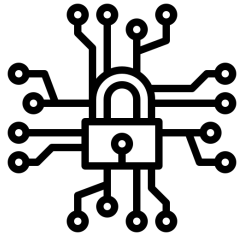
Cryptography

- **Encryption Offers:**
  - Privacy
  - Security
  - Data Integrity
- **Used in:**
  - HTTPS & Certificates
  - Messaging Apps
  - Credit Card Purchases

Your Day with Encryption - Internet Society
https://www.internetsociety.org/blog/2019/10/your-day-with-encryption

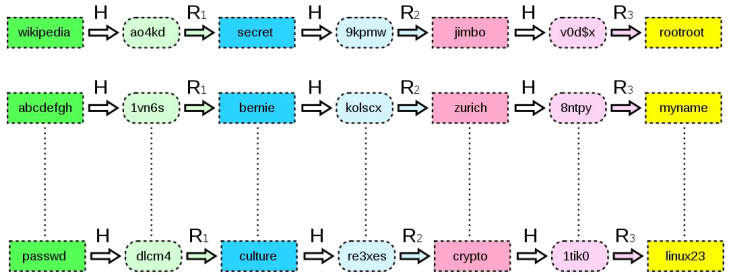
Cryptography

- **Study of building blocks**
  - Feistel Cyphers
- **Attacks against Cryptography**
  - Cryptanalysis, Brute Force
- **Symmetric vs Asymmetric Encryption**
  - Algorithms & Applications



User Authentication

- **How does you verify that the user is who they say they are?**
  - Necessary step for user authorization
- **User Authentication**
  - Something the user knows
  - Something the user possesses
  - Something the user is
  - Something the user does
- **Passwords and attacks**

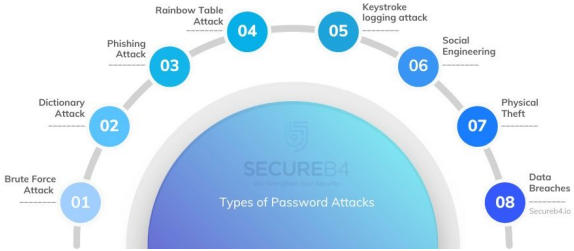


https://cyberhoot.com/cybrary/rainbow-tables/

Passwords

- **Passwords are the most common form of user authentication**

- **Various forms of attacks**
  - Offline dictionary attack
  - Specific account attack (i.e. guessing)
  - Popular password attack
  - Key-loggers
  - Workstation hijacking



https://secureb4.io/overview-different-types-of-password-attacks/

Database Security

- **(Relational) DataBases are now used over the Internet by numerous users**

- **DBMS Access Control**
  - Access rights (e.g. Role Based)
  - Policies

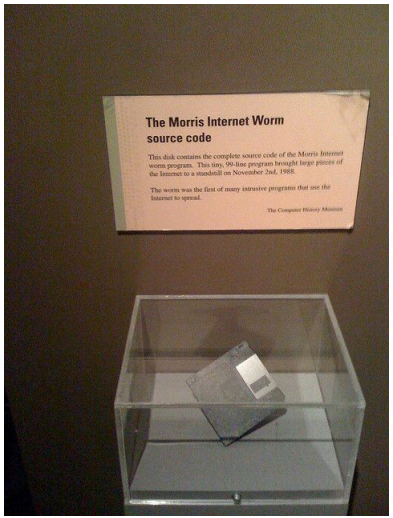
- **Attacks**
  - Inference
  - Injection Attacks

- **Countermeasures**
  - Detection
  - Runtime prevention

Malicious Software

- **Malware: Programs exploiting system vulnerabilities**
  - Virus, Worms, Logic Bombs, Backdoors, Rootkits, Keyloggers, Drive By Downloads, ...

- **How does malware propagate?**
  - Infect other programs
  - Take advantage of vulnerabilities
  - Social Engineering



Malicious Software

- **Advanced Infrastructure**
  - Bots - Command & Control
- **How virus stay hidden?**
  - Polymorphic, Encrypted, etc
- **Countermeasures**
  - Honeypots, AntiVirus, Sandbox

VajraSpy malware: Several espionage apps detected on Google Play Store

After installing malware-laced messenger app, potential victims are directed to visit compromised websites and download more trojanised apps.

https://www.deccanherald.com/technology/gadgets/vajraspy-malware-several-espionage-apps-detected-on-google-play-store-2879885

Denial of Service Attack

- **Prevents legitimate users from accessing a service**

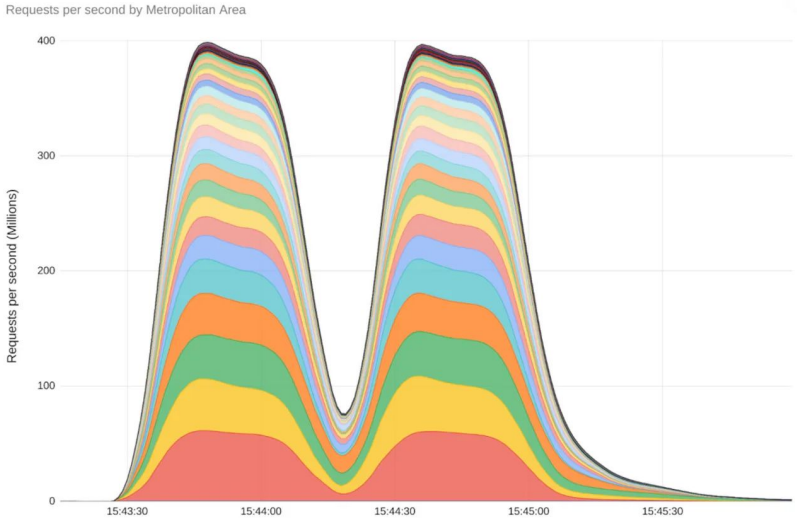
- **Attacks**
  - Network bandwidth
  - System resources
  - Application resources

- **What if there are a lot of attackers?**
  - DDoS

- **Countermeasures**
  - Scale up (?)

- **Detect & React**

Denial of Service Attack

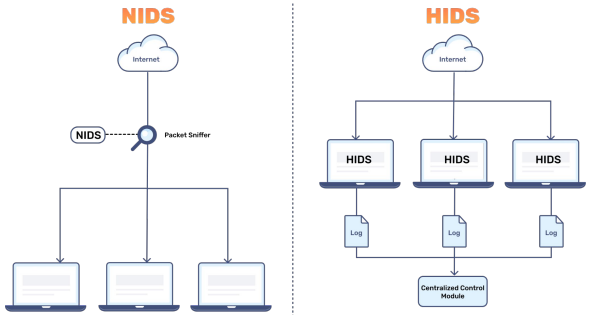


Google Cloud, AWS, and Cloudflare report largest DDoS attacks ever
https://www.zdnet.com/article/google-cloud-aws-and-cloudflare-report-largest-ddos-attacks-ever/

DDoS attack on Pennsylvania court system knocks out filing systems, bail payment site
https://therecord.media/ddos-attack-knocks-pennsylvania-court-system-services-offline

Intrusion Detection Systems

- **Detect intruders**
  - Remote root compromise, Server Defacement, Password Cracking, Sensitive Data Access, etc..
- **Heuristic Detection vs Anomaly Detection**
  - Fast and Accurate
- **Host Based vs Network Based**
  - Classify traffic as benign/malicious



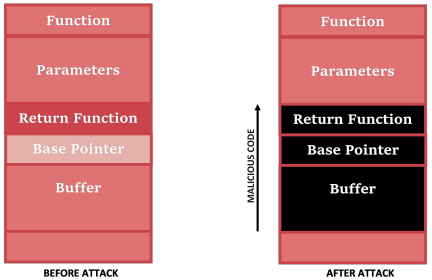
https://bunny.net/academy/security/what-is-network-intrusion-detection-nids/

Firewalls and IPS

- **We detected an attack, why not stop it?**
  - Intrusion Prevention Systems
- **Utilize advanced algorithms to detect attacks and try to stop them (e.g. Drop packets)**
  - No room for false positives
- **Firewall creates a perimeter defence**
  - Protects our network from “others”
  - All network traffic goes through it

Buffer Overflow

- **Try to go out of bounds, inject code and then execute it**

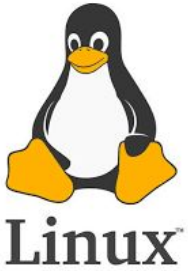


https://www.hackingarticles.in/a-beginners-guide-to-buffer-overflow/

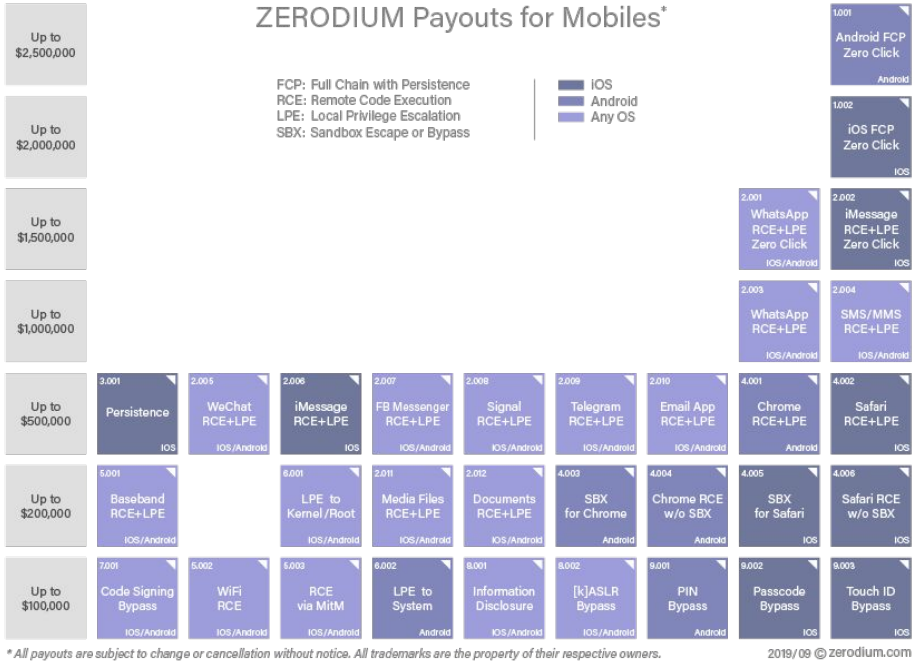
- **Old attack mechanism**
  - But still relevant, why?
- **Attacks**
  - Return to libc
  - NOP Sled
- **Defences**
  - Compile-time
  - Run-time

Software Security

- **Programmers make mistakes**
  - This leads to vulnerabilities
- **Defensive programming**
  - Detect and gracefully handle abnormalities
- **Operating Systems Security**
  - Techniques & Design



Software Security

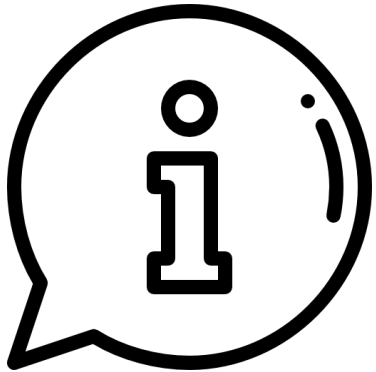


https://zerodium.com/program.html

Course Logistics

Information

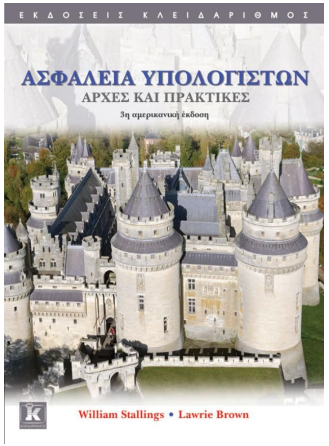
- **Course Credits**
  - 6 ECTS
  - (E5) Software Systems and Applications
- **Prerequisites:**
  - CS-150: Programming
- **Recommended:**
  - CS-345: Operating Systems
  - CS-335: Computer Networks



Book

- **"Computer Security Principles and Practice"**
  - William Stallings & Lawrie Brown, 3rd edition

- **Final Exam Curriculum:**
  - Chapters: 1, 2, 3, 5, 6, 7, 8, 9, 10, 11, and 12



Grading

The final grade is calculated as follows:

- **40% Assignments:**
  - Assignment 1: 15%
  - Assignment 2: 25%
- **60% Final Exam**

Notes:

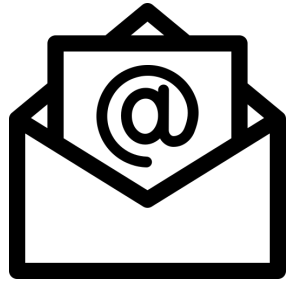
- **Code review for each assignment**
- **During final exams you are not allowed to use any kind of notes, books or communications devices**

Mailing List

- **Subscribe by sending an email to** `majordomo@csd.uoc.gr`
  - No subject
  - `subscribe hy457-list`

- **Send to** `hy457-list@csd.uoc.gr` **to reach the teaching assistants and fellow course classmates**
  - Most mails should go there

- **Send to** `hy457@csd.uoc.gr` **to reach the instructors and teaching assistants only**
  - Do not abuse it!



Teaching Assistants

- **Office Hours for each assignment**
  - Room: B210

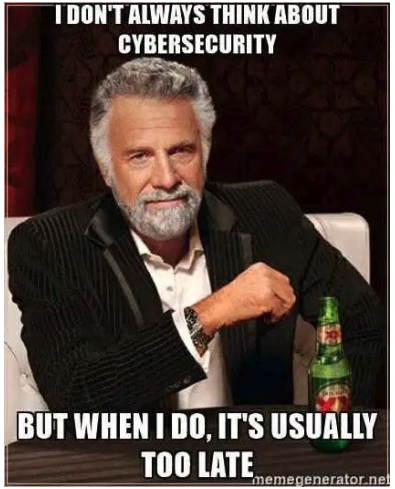
- **Teaching Assistants**
  - Papadogiannakis Emmanouil
  - Vlachogiannakis Giannis
  - Papafragaki Konstantina

Lectures

- **Lectures:**
  - Tuesday 14:00 - 16:00
  - Thursday 14:00 - 16:00
  - Friday 14:00 - 16:00 (Lab)

- **Always check the website for the latest schedule**
  - Things change...

- **Next class: 13 Feb**
  - Prof. Evangelos Markatos



Credit

- Icons from FlatIcon, made by:
  - Freepik
  - surang

Thank You!

papamano@csd.uoc.gr

Questions?