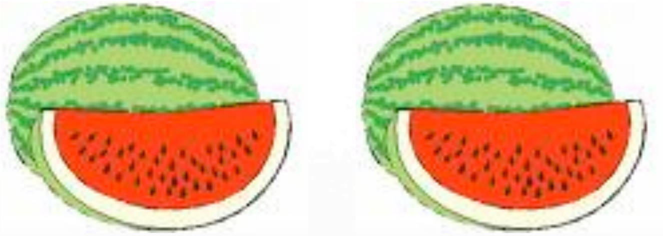
Computer Security

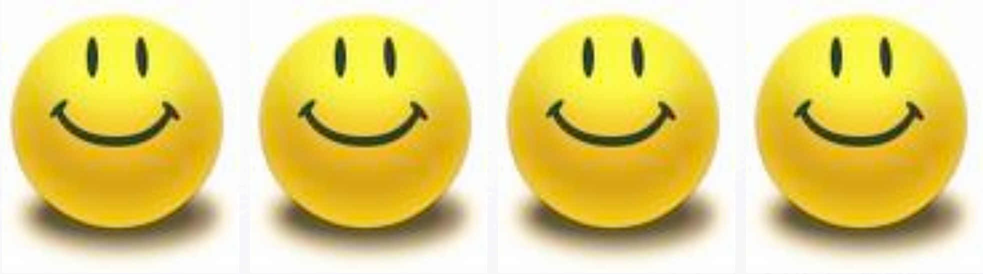
Class Introduction

Aggelos Kiayias

Security

- Asset(s)
- User(s)
- Adversary





Goals

- Confidentiality: Access of assets (viewing/printing/copying/listing) is restricted to entities that are authorized to do so.
- Integrity: Assets are processed (modified/altered/created/deleted etc.) only in authorized ways by authorized parties.
- Availability: Assets are accessible to authorized parties at the appropriate times.

How to achieve such goals?

- Understand the adversary.
  - what are the resources available?
  - what is the goal of the attack?
- Understand the modes of attack.
  - in what ways can the attack be launched?
  - what are the vulnerabilities?
- Understand the security/usability tradeoff.
  - “A turned-off system is a secure system.” (Is it?)

Points to consider, I

- Security is not an "add-on" feature.
- Computer system design must be transfused with security design.

Points to consider, II

- A system is as secure as its weakest component.
  - There is nothing that you can add to your system (firewalls, antivirus, encryption, biometrics, etc.) that can make it secure just by itself.
- Be wary of snake-oil security products.
  - "Unbreakable ciphers"
  - "No key cryptosystems"
  - "Secret cipher"
  - "1-million bit length"
  - etc.

Points to consider, III

- Thinking like an adversary is essential for building secure systems.
  - in fact you have to think like any possible adversary!
- Always keep in mind the questions
  - Who is the adversary?
  - What are the attack possibilities?
  - What is at stake?

Points to consider, IV

- Security holes and vulnerabilities are invariably discovered constantly.
  - the absolute transparency principle:
    - publicize all attacks and reveal all details of security components.
    - A discovered attack that is publicized forces positive changes (patching, upgrading, reevaluations of assets).
    - A discovered attack that is kept muffled is a time-bomb.
  - Security cannot be attained through obscure design.

This class

- Investigates how security can be achieved in
  - Software
  - Networks
  - Operating Systems
  - Databases
- Introduces the toolbox for building secure systems: ciphers, hash functions, signatures…
- Puts security into perspective w.r.t. legal, ethical and business aspects.

Software

- Programming & Security.
  - Vulnerabilities in Software
  - and how they can be exploited.
- Software with malicious/questionable intent
  - Viruses, Worms, Trojan Horses, etc.
  - Spyware
  - Web bugs.
  - Cryptoviruses
  - How to protect against the above, write better code, test whether they are present etc.

O/S

- Operating System Security.
  - Object protection and separation.
  - Memory protection.
  - Authentication of users.
- Trusted O/S platforms
  - Security models
  - Required features
  - Debate

Databases

- Integrity.
- Auditability.
- Access control.
- Learning through queries and Inference.
- Privacy.

Networks

- Network protocols - flaws and vulnerabilities.
- Threats.
- Authentication.
- Denial of service attacks.
- Intrusion Detection and honeypots
- Authentication.
- Packet sniffing.
- Firewalls and malware protection.
- Secure protocols: Kerberos, SSL, IPSec.

Business & Ethics

- Risk analysis.
- Security Policies.
- Estimating the cost of attacks.
- Laws and rights pertaining to Computer Systems.
- Computer Crime.
- Ethical issues.

Cryptography

- Encryption.
  - symmetric, public-key.
- Digital signatures.
- Message authentication codes.
- Hash functions.

Case studies

- Digital rights management.
  - How to distribute digital content while protecting intellectual property rights.
- Browsing the Internet anonymously.
- Electronic Voting.
- Electronic Payments.
- Electronic Identities.

Attacks

Authentication attacks.
Session high-jacking.
Cipher cryptanalysis.
Collision attacks
Exploiting buffer overflows.
Routing attacks.
Man-in the middle attacks.
Denial of service.
Side-channel attacks.
Phishing
Viruses.

Authentication attacks
Trojan horses
Worms
Cryptoviruses
Kleptographic attacks
Reverse-engineering
Social engineering

Class Administration

- Projects. (50%)
  - There will be 5 projects. some of them in groups.
- Exams. (50%)
- There will be 2 exams: midterm/final.

Student Conduct

- The class will touch on sensitive issues (including advanced attack ideas, vulnerabilities and so forth)
- If a student is found to employ acquired knowledge with the purpose of launching an attack (beyond the ones that will be asked as a homework :-) he/she will be immediately given an 'F' and possibly disciplinary action will follow.

Student Conduct, II

- No: cheating!
- No: plagiarizing!
- Yes: class participation!
- Yes: critical thinking!

Class Bulletin Board

http://kiayias.com/smf

- What you should do:
  - Register during this week.
  - Check the board frequently for announcements.
  - Post questions, ideas, subjects for discussion.
  - Participate in discussions.
- Important: Your shown name in the system must be your FULL NAME. Any other registrations will be deleted.

Web-site of Class

http://kiayias.com/compsec

- What you will find there:
  - the syllabus.
  - slides from class presentations.
  - project and homework material.