Lesson 9 – Review and lab

MidTerm Review

Midterm questions 1/2

- Describe the CIA model and its importance.
- Describe at least one security schema used by hardware.
- What is a replay attack? Provide an example.
- What is a zombie computer?
- What is asymmetric encryption?

Midterm questions 2/2

- What is the difference between virus and malware?
- What are the differences between a password and a key?
- What is the difference between a passive attack an active attack?
- Define:
  - Authorization
  - non-repudiation
  - Authentication
  - Identity

Bonus

Should they (Eddy and Linda) trust the email from Tom? Why? Should they open the gift? Why?

Terms used in midTerm

- Key (cryptography)
- Passive attack
- Active attack
- Authentication
- Authorization
- Non-repudiation
- Identity (digital identity)
- CIA (confidentiality, integrity, and availability)
- Hardware security scheme
- Replay attack
- Zombie computer (attack)
- Asymmetric encryption
- Computer virus
- Password

Find definitions in:
- Text books
- Class material
- www.google.com or www.wikipedia.org

Midterm average

Name	Current points	Midterm	Extra	Quizzes	Assignments	Missing points	Potential grade	Current grade
Max points value is 10								
Class Average	4.37	6.47	1.15	7.04	6.98	4.50	81.29	65.32
Median	4.81	6.50	1.00	7.00	8.00	4.50	84.06	70.20
Standard Deviation	1.50	2.58	0.49	1.86	3.06	0.00	12.12	21.89
Class Average %	43.69%	64.74%	11.50%	70.36%	69.79%	45.00%	81.29%	65.32%
Median %	48.06%	65.00%	10.00%	70.00%	80.00%	45.00%	84.06%	70.20%
Standard Deviation %	14.99%	25.83%	4.89%	18.64%	30.62%	0.00%	12.12%	21.89%

Midterm grades

2 A
4 A-
4 B
6 …
13 F

D is the average

Improving midterm grade (optional activity)

- Oral test (15 to 20min interview)
  - Questions will be similar to the midterm questions
    - Questions on slides 3 and 4 of this slide deck
  - Will ask only the same terms used in the midterm
    - Terms in slide 6 of this slide deck
  - Be prepare to explain the terms, give examples, compare with other terms (in the same list), and defend your answers
  - Strict grading
- Your midterm grade cannot go down
  - It can stay the same or go up
- Week 12
  - Saturday afternoon (starting after class)
  - Schedule in advance

Second half of the semester

Second half of the semester 1/2

- Week 9 (3/19)
  - Review midterm and encryption/signature lab
  - initial project discussion
- Week 10 (3/26)
  - Intro to VPN, DMZ, Firewalls
- Week 12 (4/09)
  - Network organization, Attack and Defense.
  - MidTerm interviews (Saturday afternoon)
- Week 13 (4/16)
  - Security Management Practices, Processes and Policies.

Second half of the semester 2/2

- Week 14 (4/23)
  - Quiz and Incident Investigation.
  - Project discussions
- Week 15 (4/30)
  - Regulations, Standards, Legal, Ethical, & Professional Issues
- Week 16 (5/07)
  - Project presentations
- Week 17 (5/14)
  - Final Examination

Lab

Lab

- Team up based on laptops
  - Each laptop will constitute a team
- Use “GNU Privacy Guard” (GPG)
  - Download from “www.gnupg.org”
  - Install GPG
- Every email sent on this exercise must start with: Lab1
  - This to facilitate identification
- Each team writes a lab report
  - List team members
  - Describe the steps taken during the ab
  - Describe any problem and its resolution

Generate keys

- Generate a private and a public key for each person in the team
  - Expire the key in one day (we only need it for this exercise)
  - Each member should remember his or her passphase
  - Select something easy
- Email the public keys to the instructor and the other teams
- For each of the following exercises use a different pair of keys

Send an asymmetric encrypted message

- Compose a message with the name of your team members, the current weather conditions, and the current date and time. Fell free to add more information to the message.
- Encrypt the message with the public key of the receiver
  - Send one message to the instructor, and one to each other team

Decrypt an asymmetric encrypted message

- Decrypt the message that your team receives
- Include those decrypted messages in the lab report indicating where they came from (from which team)

Sign a message

- Compose a new message containing your original plaintext message and one of the received messages from another team.
- Sign that message only (do not encrypt it).
- Make a copy of the signed message and modify it. Now you have two messages (original and modified).
- Send the two messages to the instructor and other teams

Verify a signed message

- Your team will receive two messages from the other teams, and you must verify the signature and decide which message was modified after it was signed

Encrypt using symmetric keys

- So far we have been using asymmetric keys. Now we will use symmetric keys for this exercise.
- Use the -c (--symmetric) option to encrypt a message
- Send that message to the instructor and each other team

Decrypt a symmetric encrypted message

- Decrypt the symmetric messages you have received and include them in the report

Summary

- We have done three exercises
  - Signed messages
  - Asymmetric encrypted messages
  - Symmetric encrypted messages
- Describe in the lab report the differences between them

The End