Assignment - PSO 2

Purdue CS426 - Computer Security - Prof. Spafford

Harris Christiansen - February 7, 2018
christih@purdue.edu

Problem 1

Humans are said to be the weakest link in any security system. Give an example for each of the following: (30 pts)

1. a situation in which human failure could lead to a compromise of encrypted data

- Answer

2. a situation in which human failure could lead to a compromise of identification and authentication

- Answer

3. a situation in which human failure could lead to a compromise of access control

- Answer

Problem 2

What is a hash function and what are the 3 properties that make a hash function cryptographically secure? What is a message digest? (10 pts)

What is a hash function and what are the 3 properties that make a hash function cryptographically secure?

- What is it
- What are 3 properties

What is a message digest?

- Answer

Problem 3

Why is it considered a good practice to salt and hash a password before storing it either in a file or database? In a large group of users, what information would be leaked when an attacker obtains access to the database if a password were only hashed and not salted? (20 pts)

Read the following for hints:

- http://blog.moertel.com/posts/2006-12-15-never-store-passwords-in-a-database.html
- https://learncryptography.com/hash-functions/password-salting

Why is it considered a good practice to salt and hash a password before storing it either in a file or database?

- Answer

In a large group of users, what information would be leaked when an attacker obtains access to the database if a password were only hashed and not salted?

- Answer

Problem 4

Describe the difference between a symmetric block cipher and a symmetric stream cipher. What are the strengths and weakness of each when it comes to resistance to cryptanalysis and speed? Explain. (20 pts)

Readings:

RC4 Stream Cipher: https://people.cs.clemson.edu/~jmarty/courses/Spring-2017/CPSC424/papers/RC4ALGORITHM-Stallings.pdf

Prohibiting RC4 Cipher Suites: https://tools.ietf.org/html/rfc7465

Block cipher mode of operation: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

The AES-CBC Cipher Algorithm and Its Use with IPsec: https://tools.ietf.org/html/rfc3602

Understanding Cryptography Lecture Series: https://youtu.be/2aHkqB2-46k

- Answer

Problem 5

(30 pts)

Describe how you can use an asymmetric and symmetric cipher together to efficiently share keys and encrypt a stream of data.

- Answer

Explain how your solution is efficient in eliminating external channels for sharing a secret key and why your solution is optimal for encrypting a large stream of data at high speed.

- Answer

Where is this problem commonly faced in the real world?

- Answer

Problem 6

Read the following:

- Cryptanalysis Attack Models: https://en.wikipedia.org/wiki/Attack_model
- Read Links under Types of cryptographic attacks: http://www.crypto-it.net/eng/attacks/index.html
- (Think of encrypted network traffic for email. What might be some known plaintext that could be used to break encryption?)

In your own words describe the following:

Known Plaintext Attack

- Answer

Chosen Plaintext Attack (CPA)

- Answer

Ciphertext Only Attack (COA)

- Answer

Chosen Ciphertext Attack (CCA)

- Answer

Problem 7

Read the following:

- Side-channel attack: https://en.wikipedia.org/wiki/Side-channel_attack
- TEMPEST: https://en.wikipedia.org/wiki/Tempest_(codename)
- Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses: https://link.springer.com/content/pdf/10.1007%2F3-540-44499-8_24.pdf

Answer the following:

Pick two side channel attacks that can be used against cryptography. Describe how the attacks can be successful and what countermeasures you can use against the attack.

- Answer

From Weingart's article, pick two high technology attacks. Describe how the attacks can be successful and what countermeasures you can use against the attack.

- Answer

Problem 8

Frequency analysis on cipher text to recover plaintext:

Recovered Plaintext
Answer

Output
Answer

Results
Answer

Code
Answer

Problem 9: Extra Credit

Read The Library of Babel: https://web.archive.org/web/20171027213619/https://hyperdiscordia.church/library_of_babel.html

Write a short explanation about how Borge's story is linked to Shannon's perfect security.

- Answer

How many books are in the library (use the author's description to calculate the number, if you can)?

- Answer