Network Security

A Recap Presentation
By Tobias Andersen

Introduction

- **Exam questions within network security are often open-ended**
  - Know your theory well and have good notes for each subject

- **What does the course description say?**
  - ”Ræsonnere omkring enkle sikkerhedsegenskaber for et givent system. ”
  - ”Basal anvendt kryptografi, og operationelle metoder til at sikre styresystemsmekanismer, netværksprotokoller og applikationer.”

- **Today’s program**
  - Explanation of different ways to achieve and threaten some network security properties, as this is what the exam questions will often be about.
  - How to solve a typical network security exam problem

Confidentiality

- **What is it?** The concealment of user's information or resources.

- **To achieve**
  - **Encryption:** by transforming data from plaintext into an unreadable ciphertext using an encryption algorithm and a key. Then only people with the right key can view the data.
  - **Access control:** ensuring that only authorized users can access sensitive data, by having a list of people who can access the data.

- **To threaten**
  - **Eavesdropping:** When attackers intercepts data being transmitted between two parties, if the data is not encrypted, they can easily view the content.
  - **Bruce forcing encryption:** by attempting to systematically guess the encryption key through every possible combination
  - **Leaks:** Employers can leak information, intentionally, or unintentionally.

Confidentiality Exam Example (reexam 2023/24)

We wanna send messages confidentialy in our personal messaging service, so we use encryption to achieve this.

Question 3.4.2: You've decided you've had enough of social media companies and are going to make your own simple messaging service for you and your friends. What IT security mechanisms from the course could you use to achieve confidentiality and integrity in your messages? Explain your choices.

The best choice for confidentiality is to use asymmetric encryption. This however requires that all friends starts by sharing a public key. This can either be used to share the message directly (encrypted with the public key) or staring a shared-secret from which a key for symmetric encryption can be derived. For integrity you could attach a hash of the sent message. This would not need to be hashed according to a cryptographic function so could be done quicker. the reciever can then hash the recieved message and compare the two hashes.

Intergrity

- **What is it?** Ensuring that data has not been altered, during transmission or storage.

- **To achieve**
  - **Checksums :** As you have done in A3 and A4, we can hash our data and send it, so the receiver can verify that their hash matches ours.
  - **Message Authentication Code(MAC) :** Similar to hash checksums but uses a secret key and encryption. The receiver can use the same key, to verify that the MAC matches.
  - **Salt:** add random characters before hashing, to make it harder to for attackers.

- **To threaten**
  - **Data tampering :** When an attacker intercepts data, alters it, and forwards the modified version to the intended recipient.
  - **Man-in-the-middle:** can tamper with the data in transit between two parties.

Confidentiality Exam Example (reexam 2023/24)

We wanna make sure our recieved messages have not been altered, so we make use of hashing to do checksums.

Question 3.4.2: You've decided you've had enough of social media companies and are going to make your own simple messaging service for you and your friends. What IT security mechanisms from the course could you use to achieve confidentiality and integrity in your messages? Explain your choices.

The best choice for confidentiality is to use asymmetric encryption. This however requires that all friends starts by sharing a public key. This can either be used to share the message directly (encrypted with the public key) or staring a shared-secret from which a key for symmetric encryption can be derived. For integrity you could attach a hash of the sent message. This would not need to be hashed according to a cryptographic function so could be done quicker. the reciever can then hash the recieved message and compare the two hashes.

Authenticity

- **What is it?** Identification and assurance of origin of info.

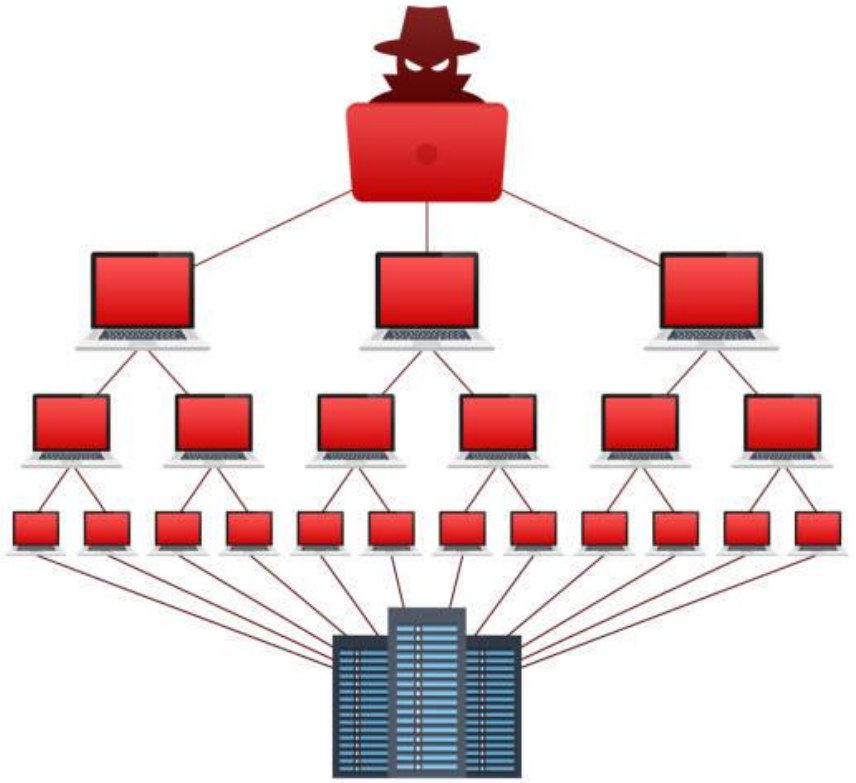
- **To achieve**
  - **Nonce:** Defends against replay attacks by ensuring each message is unique. A randomly generated value sent with the request. The recipient can validate if the nonce has been used before.
  - **Digital signature:** A digital signature uses a sender's private key to create a unique signature for the data. The receiver uses the sender's public key to verify the signature.

- **To threaten**
  - **Man-in-the-middle:** The attacker could intercept and replace the digital signature with their own, pretending to be the sender.
  - **Replay attack:** Attacker can capture and resend a legitimate message, impersonating the original sender.

Availability

- **What is it?** Ability to use desired info or resource

- **To achieve**
  - **Rate Limiting:** By limiting the number of requests a user can make in a short period, we can protect against DoS attacks.

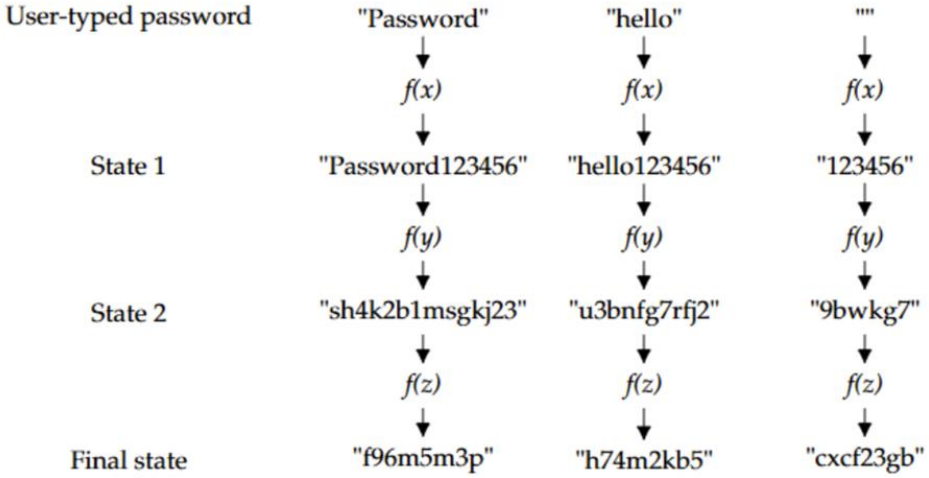


- **To threaten**
  - **Destroy hardware:** Basically destroy the physical aspect that makes the network work, fibers and so on.
  - **Denial of Service(DoS):** Attack overwhelms network resources with excessive traffic, causing systems or services to become slow or unavailable. DDoS does it from many different sources, making it harder to block.

Exam Problem

Example : Exam 2023/2024

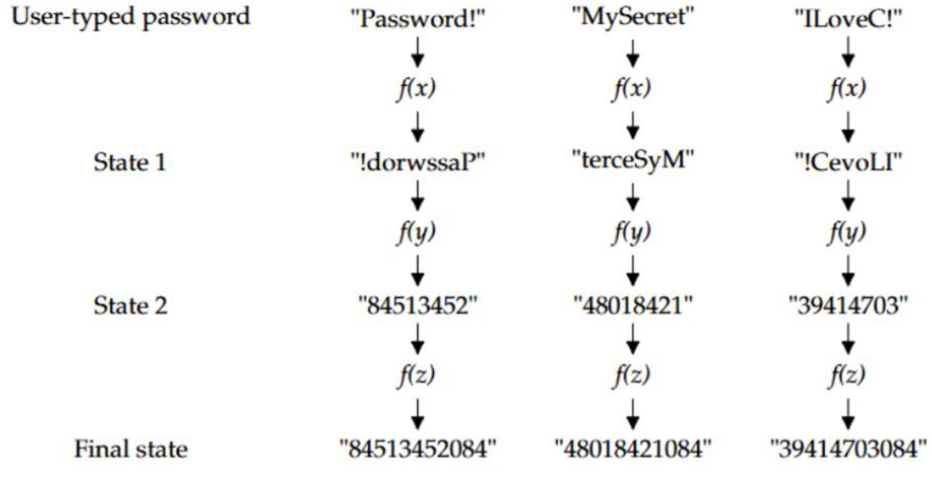
The following diagram shows the state of three user-typed password strings as they are transformed by three functions. So for instance the user-typed password "Password" is transformed by the function *f(x)* into the string "Password123456" as seen in State 1.



Question 3.4.1: Each of the three functions *f(x)*, *f(y)*, and *f(z)* are performing either encryption, hashing or salting. From the inputs and outputs, what do you deduce each function is doing? State your reasons for your conclusions. Note that *f(x)* is the same function in all three columns, as is *f(y)* and *f(z)*, and that encryption, hashing, and salting are all used.

Example : Rereexam 2023/2024

The following diagram shows the state of three user-typed password strings as they are transformed by three functions. So for instance the user-typed password "Password!" is transformed by the function *f(x)* into the string "!dorwssaP" as seen in State 1.



Question 3.4.1: Each of the three functions *f(x)*, *f(y)*, and *f(z)* are performing either encryption, hashing or salting. From the inputs and outputs, what do you deduce each function is doing? State your reasons for your conclusions. Note that *f(x)* is the same function in all three columns, as is *f(y)* and *f(z)*, and that encryption, hashing, and salting are all used.

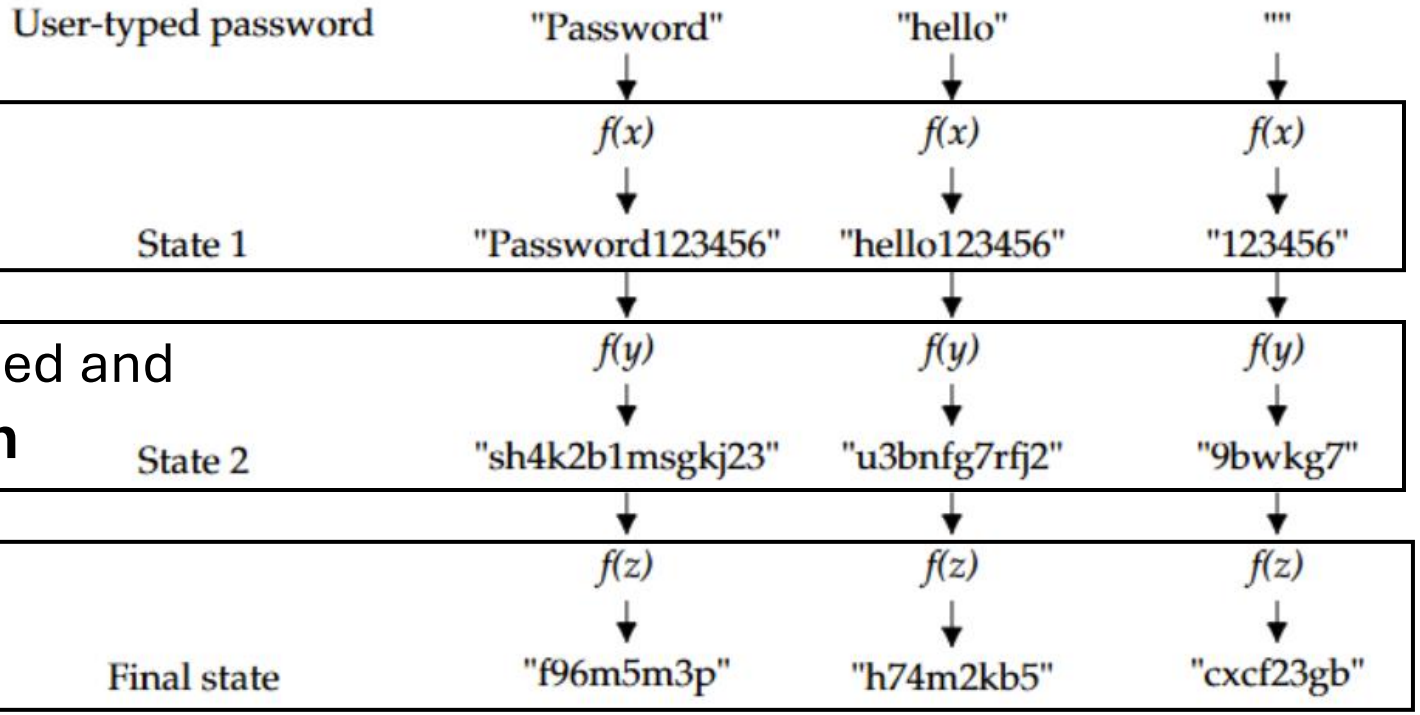
How To Solve

- **Salting :**
  - Will add characters to the output.
  - Check if the only difference between previous states, and new states is extra characters.
- **Hashing :**
  - Produces a fixed length output.
  - Check if all the new states are of equal length.
- **Encryption :**
  - Produces output of varied length.
  - Check if the length varies between new states.
  - Sometimes has a recognizable pattern, but don’t expect it.

- **Process of elimination :**
  - Do whichever two you find easiest first, to isolate the last one
  - (Only applies if exam text states all three are used, as it often does)

Example : Exam 2023/2024

The following diagram shows the state of three user-typed password strings as they are transformed by three functions. So for instance the user-typed password "Password" is transformed by the function *f(x)* into the string "Password123456" as seen in State 1.



We add "123456" at the end of all passwords, so **f(x) is salting**

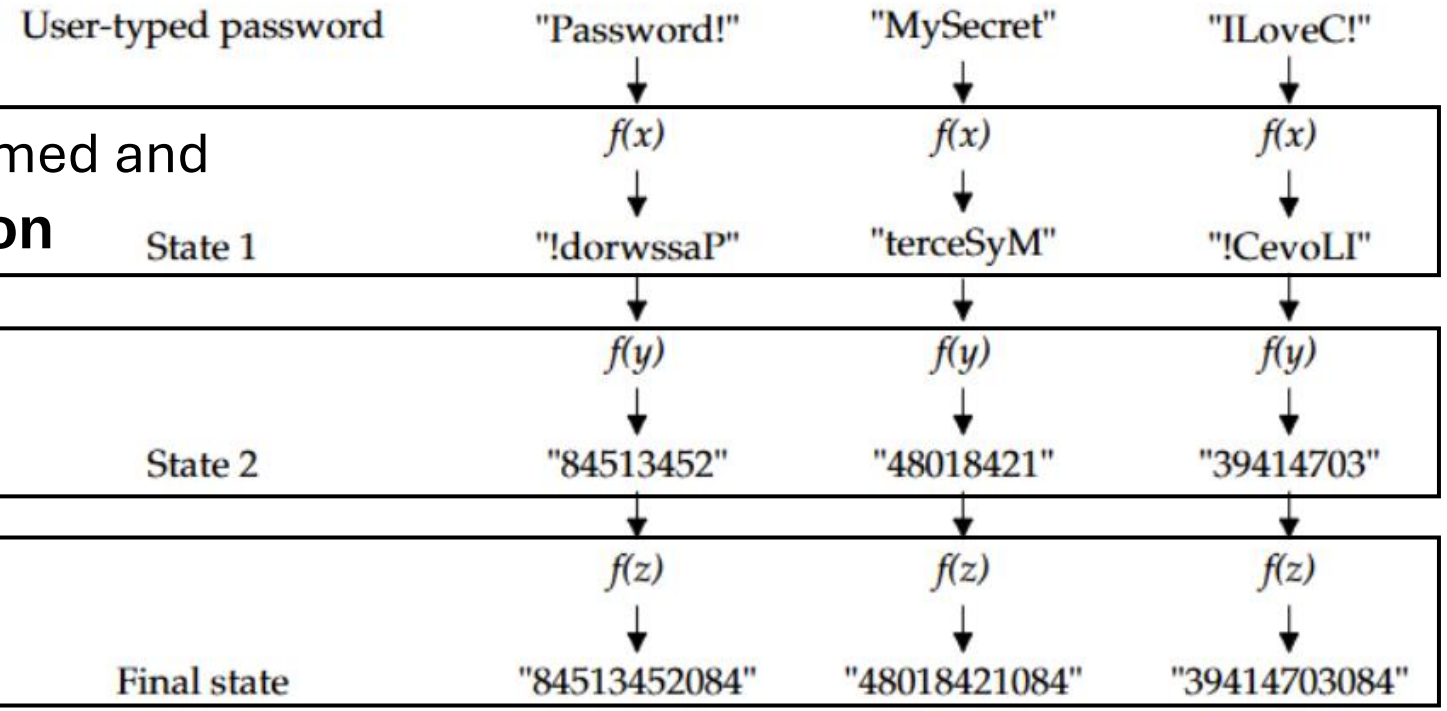
Previous states have been transformed and varies in length, so **f(y) is encryption**

All final states have a fixed length of 8, so **f(z) is hashing**

Question 3.4.1: Each of the three functions *f(x)*, *f(y)*, and *f(z)* are performing either encryption, hashing or salting. From the inputs and outputs, what do you deduce each function is doing? State your reasons for your conclusions. Note that *f(x)* is the same function in all three columns, as is *f(y)* and *f(z)*, and that encryption, hashing, and salting are all used.

Example : Rerexam 2023/2024

The following diagram shows the state of three user-typed password strings as they are transformed by three functions. So for instance the user-typed password "Password!" is transformed by the function *f(x)* into the string "!dorwssaP" as seen in State 1.



Previous states have been transformed and varies in length, so **f(x) is encryption**

All new states have a fixed length of 8, so **f(y) is hashing**

We add "084" at the end of all Previous states, so **f(z) is salting**

Question 3.4.1: Each of the three functions *f(x)*, *f(y)*, and *f(z)* are performing either encryption, hashing or salting. From the inputs and outputs, what do you deduce each function is doing? State your reasons for your conclusions. Note that *f(x)* is the same function in all three columns, as is *f(y)* and *f(z)*, and that encryption, hashing, and salting are all used.

End Note

If you have been focusing on preparing for exam, and have not attended today's lecture, or read today's chapters.

Then I would highly recommend you check out today's lecture slides and chapters, as they are very relevant for the network security part of the exam.

Thank you for listening!

:3