User authentication

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres

José María de Fuentes García-Romero de Tejada

Lorena González Manzano

Sergio Pastrana Portillo

uc3m | Universidad Carlos III de Madrid

COSEC

OUTLINE

- 13. User authentication
  - Introduction
  - Authentication based on something you know
  - Authentication based on something you have
  - Authentication based on something you are

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 13. User authentication
  - Introduction
  - Authentication based on something you know
  - Authentication based on something you have
  - Authentication based on something you are

INTRODUCTION

- Authentication
  - Process to verify the identity of a user
    - Identification step
    - Verification step

- Authentication factors
  - Something the user knows (secrets)
  - Something the user has (tokens)
  - Something the user is/does (biometrics)
  - Combinations of the previous three (various factors)

OUTLINE

- 13. User authentication
  - Introduction
  - Authentication based on something you know
  - Authentication based on something you have
  - Authentication based on something you are

AUTHENTICATION BASED ON SOMETHING YOU KNOW

- User knows certain information that only he and the system know
- Includes methods based on passwords, PIN, challenge-response, etc.
- Simple and extended method
- Password management needed

AUTHENTICATION BASED ON SOMETHING YOU KNOW – PASSWORDS MANAGEMENT

- Quality criteria
  - Easy to remember (weak) versus random (less weak)
  - Length, complexity
- Storage of the password by the user
  - Must not be disclosed (social engineering, phishing, etc.)
- Storage of passwords in systems
  - Storage of a password hash value
  - Password encryption
- Password expiration
  - The more critical a system is, the shorter the period of validity of their passwords should be.

AUTHENTICATION BASED ON SOMETHING YOU KNOW – PASSWORDS MANAGEMENT

- Remembering passwords
  - A minimum number of different consecutive passwords must be established.
- Password blocking / cancellation of user accounts
  - If a fraudulent use is suspected
- Problems when reusing passwords to access into different systems
- Threats
  - Brute force and dictionary attacks
  - Password interception
  - Attack to the system database (Achilles' heel)
  - Social engineering

AUTHENTICATION BASED ON SOMETHING YOU KNOW – PASSWORDS MANAGEMENT

- **Programs to break passwords**
  - L0phtcrack , John the Ripper, Pwdump
  - Dictionaries and lists (phone numbers, plates…)

- **Programs for password management**
  - Password Safe (http://www.schneier.com/passsafe.html)
  - SplashID (http://splashdata.com/splashid/)

OUTLINE

- 13. User authentication
  - Introduction
  - Authentication based on something you know
  - Authentication based on something you have
  - Authentication based on something you are

AUTHENTICATION BASED ON SOMETHING YOU HAVE

- Cryptographic devices
  - Smart cards, USB tokens
  - Authentication with digital signature
- One Time Pass (OTP) Tokens

AUTHENTICATION BASED ON SOMETHING YOU HAVE - OTP

- OTP (*One-Time Password*)

- Single use passwords (session, transaction)

- Generated with some token that the user has or wi specific software

- Avoid problems derived from password management

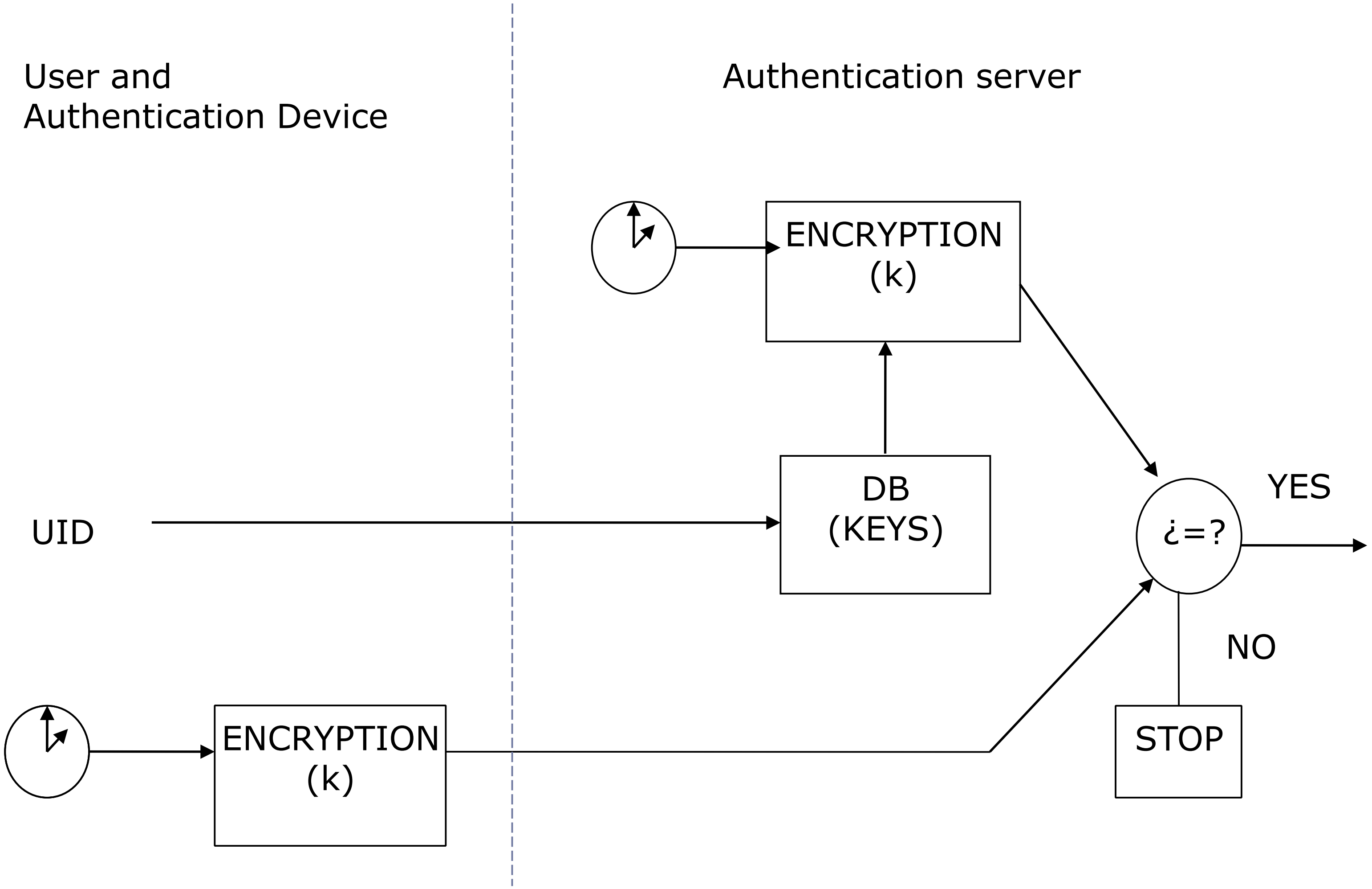
- Secure storage of the token

AUTHENTICATION BASED ON SOMETHING YOU HAVE - OTP

- Based on randomness, thus avoiding prediction attacks

- Types
  - **Synchronous**: there’s a synchronization between token clocks and the authentication server
  - **Chained**: the generation of an OTP depends on previous OTP
  - Based on a **challenge**: the generation of an OTP depends on a challenge issued by the authentication server and an internal counter

AUTHENTICATION BASED ON SOMETHING YOU HAVE – SYNCHRONOUS OTP



AUTHENTICATION BASED ON SOMETHING YOU HAVE – CHAINED OTP

- A one way function f is applied sequentially

- A series of OTPs is generated based on the previous

  f(s), f(f(s)), f(f(f(s))) … f(…(f(f(f(s)))…)

- OTPs are used in reverse order

  f(…(f(f(f(s)))…)… f(f(f(s))) , f(f(s)), f(s)

AUTHENTICATION BASED ON SOMETHING YOU HAVE – CHAINED OTP

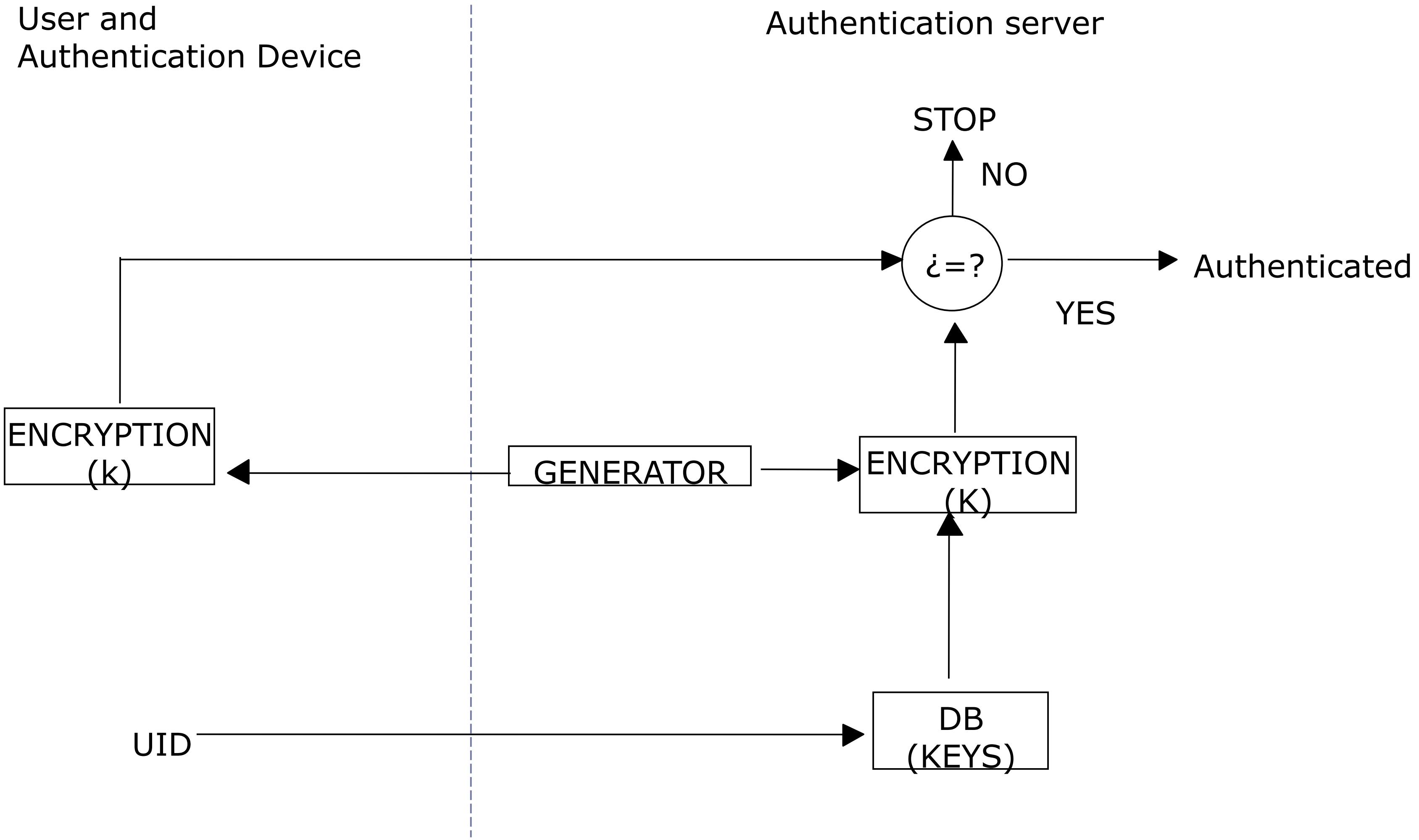
- Initialization
  1. The authentication server chooses the function *f*
  2. The user chooses the maximum number of authentications (n)
  3. The token initializes the seed s and calculates $f^n(s)$
  4. The user sends n and $f^n(s)$ to the authentication server through a secure channel
  5. The authentication server registers $f^n(s)$ with the user ID
- Use
  6. The token sends the ID and $f^{n-1}(s)$ to the authentication server
  7. The authentication server access $f^n(s)$ by means of the ID

AUTHENTICATION BASED ON SOMETHING YOU HAVE – CHAINED OTP

8. The authentication server calculates $f(f^{n-1}(s))$ and verifies if it matches with the stored $f^{n}(s)$
9. The authentication server removes $f^{n}(s)$ from the database and stores $f^{n-1}(s)$
10. The authentication server subtract 1 from n
11. The process is repeated until n=0

- An attacker who intercepts one OTP have to invert the function *f* in order to obtain the next OTP value
  - Hash functions are normally used

AUTHENTICATION BASED ON SOMETHING YOU HAVE – CHALLENGED BASED OTP



OUTLINE

- 13. User authentication
  - Introduction
  - Authentication based on something you know
  - Authentication based on something you have
  - Authentication based on something you are

AUTHENTICATION BASED ON SOMETHING YOU ARE

- Systems authenticate users by looking its biometrics characteristics (unique and unrepeatable)
- There is a previous enrollment process (extraction and storing the biometric pattern)
- The authentication process includes obtaining the biometric pattern and comparing it with stored pattern
  - Verification
  - Identification
- Several techniques (fingerprint, iris, retinal pattern, hand geometry, handwriting, voice, …)
  - With different accuracy (false negatives/ false positives)

AUTHENTICATION BASED ON SOMETHING YOU ARE

CRYPTOGRAPHY AND COMPUTER SECURITY

COSEC

uc3m | Universidad Carlos III de Madrid