الجامعة الافتراضية السورية

أمن الشبكات
Network and Infrastructure Security

د. محمد العصورة

Dr. Mohammed Assora

دكتوراه في امن شبكات الحواسب

PhD. In Computer Network Security

Objectives of Lecture

- Recognizing the various methods that can be used for user authentication.
- Present an overview of techniques for remote user authentication using symmetric encryption and asymmetric encryption.
- Present an overview of social engineering.

Contents

Entity Authentication

- Allows the *verifier* to gain assurances that the identity of the *claimant* is as declared
- Prevents impersonation
- Referred to as
  - ***user authentication***
  - ***identity verification***

  Entity authentication is one of the most vital services that can be provided by cryptography

Entity Authentication Functions

- Something that you have
- Something that you are
- Something that you know

Something you have

1. Dumb tokens

- A physical device used as an electronic key.
- Operate with a reader to authenticate the entity holding the key
- e.g., a plastic card with a magnetic stripe
- Often used in combination with another authentication techniques

Something you have

2. Smart cards

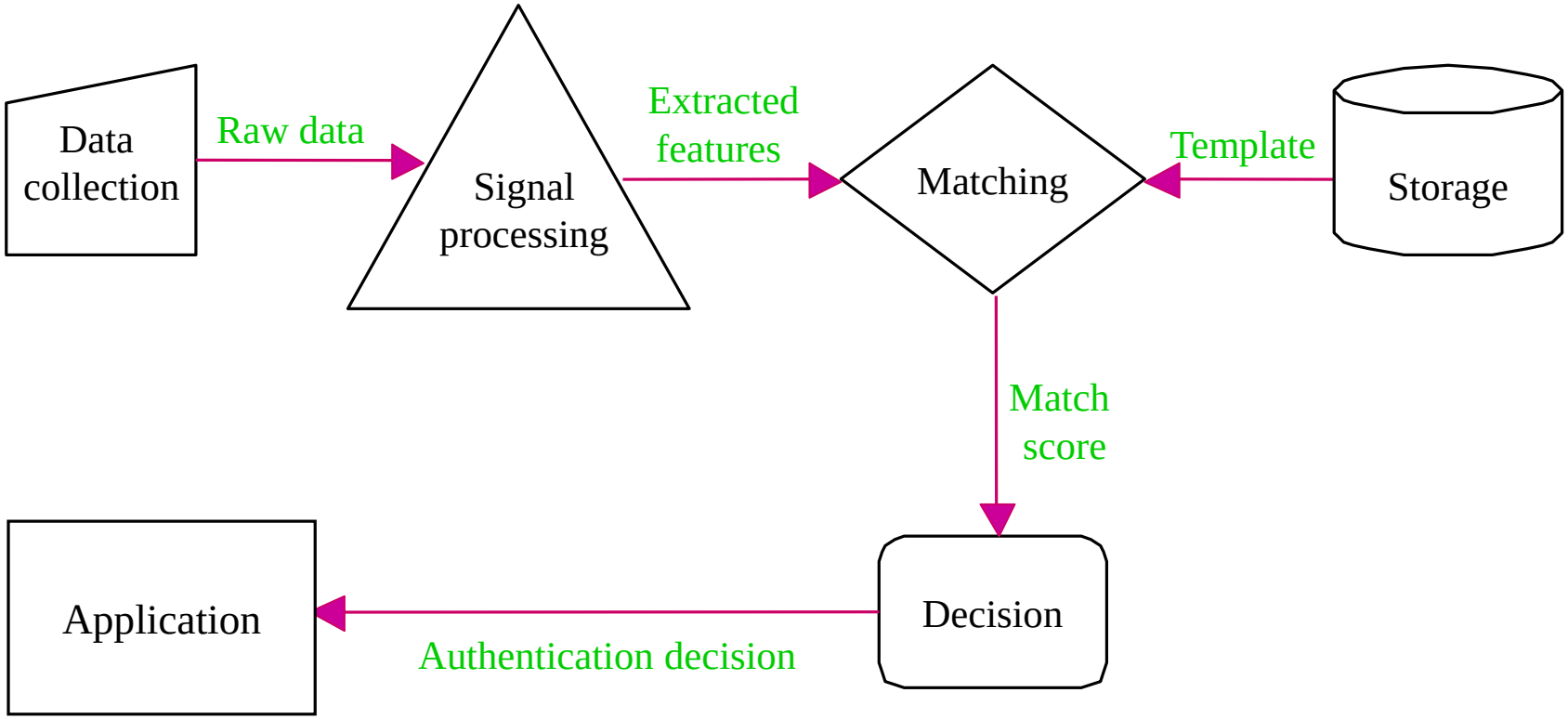
- plastic cards containing a **chip** with limited memory and processing power.
- **store** secret data securely
- engage in cryptographic processes that require computations
- e.g., smart cards used in banking operations, SIM cards, etc.

Something you are

- **Biometrics**
  - Authentication techniques based on physical characteristics of the human body.
  - A physical characteristic is stored in a database as a digital template
  - At authentication, the physical characteristic is measured by a reader, digitally encoded, and then compared with the template

Something you are

- Biometric system model



- *e.g.,* video camera, fingerprint scanner, digital tablet (signatures), microphone, accelerometer (gait recognition)

Something you are

- Biometrics
  - **Static** (unchanging) measurements include fingerprints, hand geometry, face recognition, retina scan.
  - **Dynamic** (changing) measurements include handwriting measurements and voice recognition.
  - There are many implementation issues

Something you are

Something you know

1. **Passwords**
   - Most popular authentication techniques
   - A password may be a sequence of characters
     - e.g., 15 digits, a string of letters, *etc*.
   - A password may be a sequence of words
     - e.g., pass-phrases

2. **Algorithms**
   - e.g., one-time passwords, challenge-response.

Passwords

- Passwords stored in plaintext files
  - If password file compromised, all passwords are revealed
  - Usually password files are read- and write-protected
- Passwords stored in encrypted file
  - Encrypted/hashed versions of passwords are stored in a password file

- e.g., Unix password.

Password Authentication Vulnerabilities

- A key problem with user name and password (ID/Password), the human factor:
  - Most users select passwords from a small subset of the password space (e.g., short passwords, dictionary words, proper names)
  - Passwords are easy to guess or search if easy to remember
  - Passwords are easily stolen if written down
  - Users may share passwords
  - Passwords can be forgotten if difficult to remember

Attack on passwords

- There are various forms of password attacks, the most important ones are:
  - Brute force attack
  - Dictionary attack
  - Phishing
  - Rainbow table attack
  - Credential stuffing
  - Password spraying
  - Key logger Attack
  - Traffic interception
  - Man-in-the-middle

Selecting a good password

Good passwords can be constructed in several ways:

- Contain both upper and lower case characters
- Have digits and punctuation characters as well as letters e.g., 0-9, @#$%^&*()_+|~- =\`{}[]:";'<>?,./)
- Are at least 12 alphanumeric characters long and is a passphrase.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, ..
- Passwords should never be written down or stored on-line
- Try to create passwords that can be easily remembered

One-Time Passwords

- Problem with fixed passwords:
  - If an attacker sees a password, he/she can later *replay* the password
- A partial solution: one-time passwords
  - Password that can be used exactly *once*
  - After use, it is immediately invalidated

✘ Problems

  - Synchronization of user and system
  - Generation of good random passwords
  - Password distribution problem

Challenge-Response

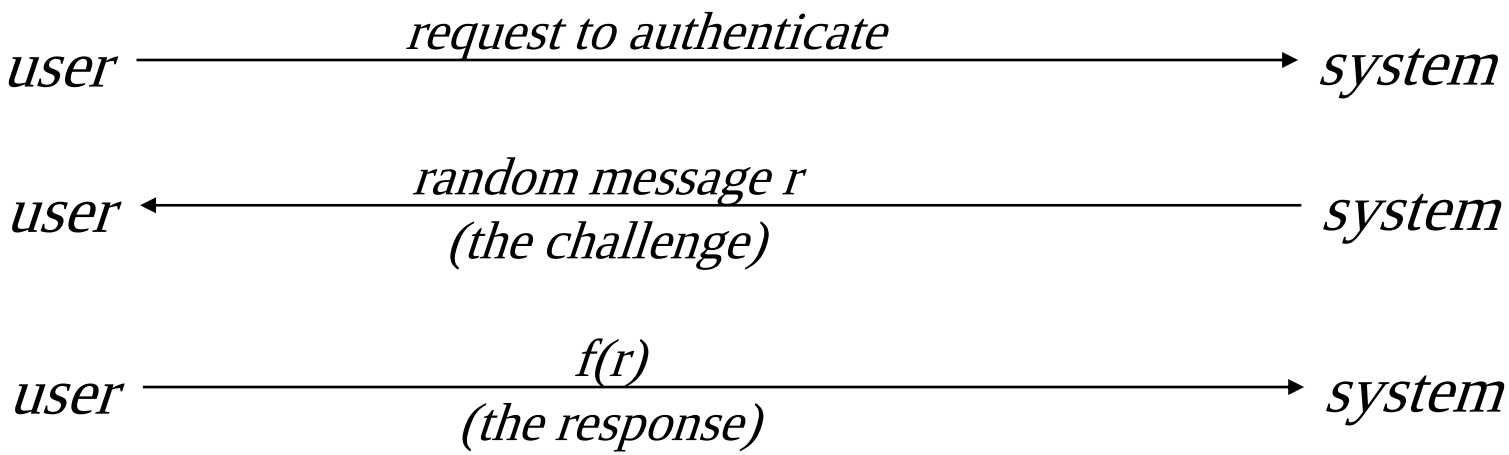
(Strong authentication)

- Let a user *u* wishing to authenticate himself to a system *S*. Let *u* and *S* have an agreed-on secret function *f*.
- A ***challenge-response*** authentication system is one in which *S* sends a random message *m* (the *challenge*) to *u*, and *u* replies with the transformation *r* = *f*(*m*) (the *response*). *S* then validates *r* by computing it separately.
- The challenge may be a ***nonce***, ***timestamp***, ***sequence number***, or any combination.

Challenge-Response

(by symmetric-key techniques)

- The user and system share a secret function *f* (in practice, *f* can be a known function with unknown parameters, such as a cryptographic key).
- This called challenge-response by symmetric-key techniques.



Challenge-Response
(by public-key techniques)

- *A* identifies *B* by checking whether *B* holds the secret (private) key KR_B that matches the public key KU_B
- *A* chooses a random challenge (nonce) r_A. *B* uses its random nonce r_B. *B* applies its public-key system for authentication
- Message sequence:

  1. $A \rightarrow B$: r_A.
  2. $B \rightarrow A$: r_B, $E_{KR_B}(r_A, r_B)$

Social Engineering

- Social engineering is the art of manipulating people so they give up confidential information.

- The criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software

Human-based Social Engineering

Common human-based social engineering attacks:

- Impersonating an Employee or Valid User
- Posing as an Important User
- Using a Third Person
- Calling Technical Support
- Dumpster Diving
- Reverse social engineering

Computer-based Social Engineering

Common Computer-based social engineering attacks:

- Phishing Attacks
- Online Scams
- Pop-up windows
- URL Obfuscation

Social-Engineering Countermeasures

Documented and enforced security policies and security awareness, security policy should address:

- How and when accounts are set up and terminated,
- How often passwords are changed,
- Who can access what information,
- How policy violations are to be handled.
- Spell out help desk procedures
- The destruction of paper documents and physical access restrictions.
- use of modems, wireless networks, Internet Access, and virus control.

The most important countermeasure for social engineering is employee education.