# Identification and Authentication

Matus Kysel - 156605IV

Tallinn University of Technology
matus@kysel.org

## I. Introduction

The concepts of identification and authentication are intertwined, so it is important to understand the difference between them.
**Identification** - The act of a user professing an identity to a system usually in the form of a log on.
**Authentication** - The verification that the user's claimed-identity is valid. The authentication is usually implemented through a password at log on time.
There are three factor types of the authentication witch are based on:

- **Something you know** - Password, PIN, mother's maiden name, passcode, etc.
- **Something you have** - ATM card, smart card, token, key, ID Badge, driver license, or passport.
- **Something you are** - Also known as biometrics: Fingerprint, voice scan, iris scan, retina scan, body odor, DNA.

A multi-factor authentication requires from users to provide at least two authentication types to increase security of system. For example these are two-factor authentication system:

- ATM card + PIN
- Credit card + signature
- PIN + fingerprint
- Username + Password

Three-factor authentication offers the highest security, by requiring all three types of authentication, e.g.:

- password + token + Fingerprint
- PIN + driver license + voice scan

## II. Passwords

A password is series of characters used to authenticate a specific person. The most important task for system administrators is to set a limit number of failed login attempts, which when reached, locks the account. The password system for authentication is used for the following security-based reasons:

- Password checkers
- Password Generators
- Password Aging
- Limit Login Attempts

There is also password, that is based on a fact or an opinion, that is called a cognitive password. For example many systems ask for your mother's maiden name or city you were born.

A pass phrases is a different form of password, where instead of single word multiple words are used. This difference means a pass phrase will contain spaces, so it will be significantly longer than a password. That is why they may form a sentence, that is more easier for user to remember than complex single word passwords.

A one-time password (OTP) also called a dynamic password is a password, that can be used only once. Because of that OTPs do not have to be secured as they cross the network as conventional passwords. Also sniffing attack are useless for this kind of passwords. Usually OTP are generated by token devices.

Personal Identification Numbers (PINs) are nothing more than a secret numeric password. They are usually used for multi-factor authentication, when users use their PIN into the token device in order generate a one-time password to successfully login.

## III. Token-based access

Token devices are hardware or software devices used to identify an identity or generate a password. They are using a challenge/response scheme in which the user enters the challenge key in the token, that generates a password valid only once or for a certain amount of time.

There are two types of synchronous token devices:

- **Clock-based tokens** - these tokens rely on an internal clock. Combination of clock and a secret key is used to generate a time-based password. The server performs validation with the same function and if they match, the user is authenticated. A window of time is provided for user in which he can use the password.
- **Counter-based tokens** - In this method, the administrator needs to insert a specific secret into the user's token device and also to the server. For password generation user simply pushes a button on the token. Each time the user pushes the button, the token increments the internal counter combine with the owner's unique base secret.

Asynchronous tokens are based on communication between server and token device. The token receives a challenge or nonce from server and generates a password based on it. The password is then combined with a secret key inside the token. The respond is sent to the server, server performs same calculation and if the results match, user is authenticated.

Smart cards are used to provide higher level of security, where instead of usage of a simple password user could use a very secure one-time password. They are usually credit card-sized plastic cards that have an integrated microprocessor to perform calculations on data stored in them (e.g. encrypting or decrypting passwords). In general are two categories of smart cards:

- contact
- contactless

Key cards are very inexpensive plastic cards that have a magnetic strip with encrypted data as a security precaution against the card being lost or stolen. This kind of cards are wildly used for opening doors in hotels.

## IV. Characteristics-Based Access Control

Most commonly used type of authentication today is authentication performed with a password that can be easily forgotten. Completely different approach to authentication is characteristics-based access control, that means identifying or authenticating the identity of a living person is based on their physical, physiological, or behavioural characteristics.

Biometrics is another term that is connected with characteristics-based access control. These are types of biometric measurements ordered by effectiveness from most to least secure:

- Iris Scanning
- Retinal Scanning
- Hand Geometry
- Fingerprint Verification
- Voice Recognition
- Facial Recognition
- Signature Verification
- Keystroke Recognition

Currently we recognize two types of biometrics:

- **Behaviour based** - Keystroke Recognition, Signature Verification, Voice Recognition
- **Physiological based** - Iris Scanning, Retinal Scanning, Hand Geometry, Facial Recognition

Although behaviour based biometrics are less expensive, they can change over the lifetime of user, so they are less accurate as well. On the other both techniques provide a significantly higher level of identification than passwords or smart cards alone.

## V. Single Sign-On

In the single sign-on scheme a users identify only once to a central system, then all future accesses to other systems is forwarded by the central system.

Tickets are the basis of the single sign-on system. Tickets are, in essence, passwords used to authenticate to a system or service. Tickets can be described as:

- Service ticket
- Renewable tickets
- Ticket granting tickets (TGT)
- Forwardable tickets

Kerberos is a single sign-on authentication protocol, named after Cerberus the mythological three-headed dog. Kerberos provides end-to-end security by using symmetric key cryptography. Key Distribution Center (KDC) is the main component, that holds all cryptographic keys. This center provides authentication services and key distribution functionality. Components of KDC are:

- Authentication Server (AS)
- Ticket Granting Server (TGS)

SESAME is another single sign-on service, that is used mainly in EU. It was found by the European Commission under name The Secure European System for Applications in a Multi-vendor Environment (SESAME). It also uses public key cryptography for the distribution of secret keys and ticket for authorization, but it is called a Privilege Attribute Certificate.

Scripts can be also used for single sign-on, but this solution stores encrypted a user profile and automation scripts in a central location. On user log in these files are downloaded to the client. Almost all client script packages work on all versions of Windows and support sign-on automation for any application. The client software usually does not require administrator rights or rebooting.

## VI. Thin Clients

Thin clients are simple inexpensive client devices, that are used especially in a distributed networking environment, where every additional costs are big concern. This device usually takes place of desktop PC and connects to server to to process applications, access files, print, and perform other network services. The basic concept is that all of processing work is completed on the centralized system instead local client's computer.

## References

[CISSP, 2006] Certified Information Systems Security Professionals CISSP Student Guide v1.0. (2009). *Identification and Authentication*