

COMPSCI4062/COMPSCI5063 Cyber Security Fundamentals (CSF)

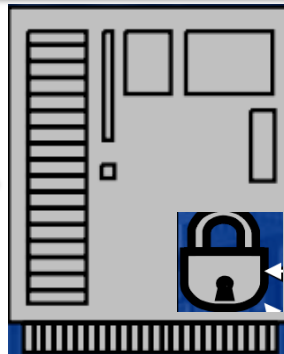
Identification and Authentication

**Identification &
Authentication**



**Identity (a user, an
application)**

**Access
Control**



**System/
network
resources**

Identity, Identification and Authentication

- **Definitions**

- Identity

- Representation of an entity inside a computer system
 - It often implies the use of a unique name for an entity
 - ❖ A person's identity can change or be falsified, e.g., last name

- Identification

- is the claim of a user or an application that is using/running in the system
 - This could be achieved by a user ID, process ID, a smart card or anything else that may uniquely identify a subject or a person.
 - ❖ The ID, smart card could be stolen

- Authentication

- Verification/prove process of the identity of an entity

Identity

- Purposes
 - For access control
 - For accountability
 - Logging & Auditing
- Identities in a security system
 - A data file (an object in general)
 - File name: for the human being
 - File descriptor: for a process
 - File allocation table entry: for the kernel (MS-DOS and Windows 9x OS)
- A user
 - Any name comprised of an arbitrary number of alphanumeric characters
 - May be constrained in some ways, e.g., name + organization

Groups and Roles

- An identity may refer to an entity that is comprised of **a group of entities**
 - A convenient way of performing access control and other security functions to a set of entities at the same time
 - Models of groups
 - Static: alias to a set of entities
 - Dynamic: construct for grouping a set of entities
- An identity may refer to **a role**
 - To tie entities together
 - To represent rights or security functions to which entities are assigned or entitled

Identity and Certificate

- Certificate issued by a certificate authority (CA)
- CA acts as a trusted 3rd party
 - Class 1
 - Authentication of an e-mail address, web application,
 - Class 2
 - Verification of real name and address through an online database - online purchasing
 - Class 3
 - Background check by an investigative service- a higher level of assurance
 - Example: Certificate Authority Security Council (CASC) funded in 2013- dedicated to addressing industry issues and educating the public on internet security.

Trust of Identity

- Trust of a certificate
 - Depending on the trustworthiness of the certificate authority (CA)
 - Depending on the level of trust indicated by the CA
 - High: a passport
 - Low: an unsworn statement
 - It's all relative
- The point
 - Identity has the trust issue
 - Certificate also has the trust issue

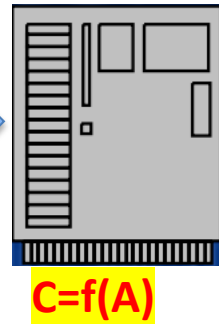
Authentication

- Purpose
 - To verify that a stated identity really belongs to the right entity
- Methods
 - What the entity knows – knowledge-based authentication
 - Password, PIN, DoB, mother's maiden name, etc
 - What the entity has – token-based authentication
 - Badge, ID card, key, etc.
 - What the entity is – Biometric authentication
 - Fingerprints, personal characteristics, gait and motion biometrics, etc.
 - Where the entity is
 - Specific terminal, special access device, etc

Authentication Components

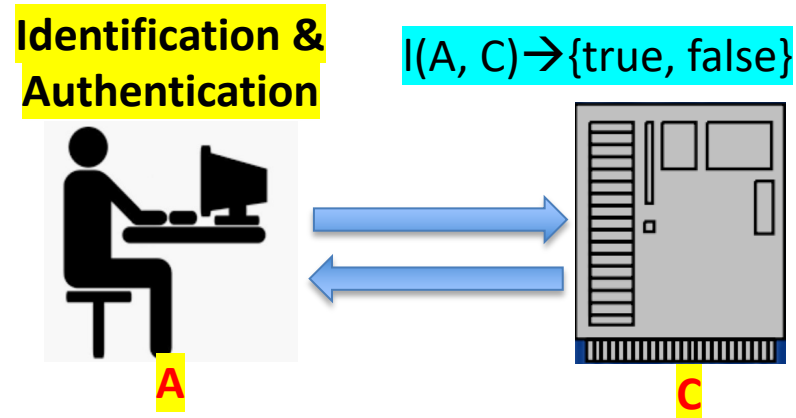
- For creating and storing authentication information
 - Authentication information: A
 - For an entity to prove its identity
 - Complementary information: C
 - For a system to store authentication information along with the corresponding identity
 - For a system to verify authentication information
 - Complementary functions: F
 - For a system to generate the complementary information from the authentication information
 - For f belongs to F, $f: A \rightarrow C$

Identification &
Authentication



Authentication Components

- For performing authentication
 - Authentication functions: L
 - For the system to verify an identity
 - For $l \in L$, $l: A \times C \rightarrow \{\text{true}, \text{false}\}$
- For managing authentication information
 - For an entity to create or to alter the authentication and the corresponding complementary information



Passwords

- Purpose
 - To use information that an entity knows to verify that a stated identity really belongs to the entity
- Authentication method
 - What an entity knows
- Password protection
 - Passwords are **not allowed** to be transmitted without proper protection
 - For $f \in F$, $f: A \rightarrow C$ uses a one-way hash function

Password Attacks-Dictionary Attack

- Dictionary attack
 - Most passwords are not random sequences of characters and numbers, but instead are combinations of “normal” words, proper names, acronyms, etc.
 - E.g., “Betty23” or “ChocolateFrog”
 - In a dictionary attack a list of possible passwords is used in order to break into an account
 - The list might contain common words, names, acronyms, common passwords, etc.
 - This vastly reduces the search space

Password Attacks- Brute-Force Attacks

- Brute-Force Attacks (exhaustive attack) involves trying every possible combination of characters until the correct password is found
- The time required to crack a password depends upon the length of the password
 - e.g., if a password is between 1 and 8 characters long, and is comprised of upper or lower case letter (52), numbers (10), or special characters (32 in an English keyboard). Then there are $\sum_{i=1}^8 94^i = 6.1 \times 10^{15}$ possible passwords
 - If the password is exactly 8 characters long, then there are 94^8 possible passwords. ($\sum_{i=1}^7 94^i$ less possible passwords)
 - Making a password standards public can be a security risk

Counter-Measures to Password Guessing

- Goal
 - To maximize the amount of time consumed before the password is correctly guessed
- Calculation
 - P: probability of correctly guessing a password in a specified period of time, e.g., 0.5
 - In number of time units
 - G: number of password guesses that can be carried out in one time unit
 - T: number of time units for the calculation
 - N: total number of possible passwords
 - **Anderson's Formula:** $P \geq TG/N$ or $N \geq TG/P$

An Example of Password Guessing

- The objective
 - To determine the minimum length of password in a system
- Parameters
 - $A=96$ characters
 - $G=10^4$ per second
 - $P=0.5$
 - $T=365$ days $=365 \times 24 \times 60 \times 60$ seconds $=31.536 \times 10^6$
- Assumptions
 - The length of time required to try out each password is constant
 - All passwords are equally like to be selected
- The result
 - $N \geq TG/P = 6.31 \times 10^{11}$
 - $N = \sum_{i=1}^S 96^i \geq 6.31 \times 10^{11} \longrightarrow S \geq 6$

Password Selection

- Theorem
 - When the selection of a password from a set of possible passwords is equally probable, the expected time that is needed for guessing a password is the longest
- Strong passwords
 - At least one digit
 - At least one letter (upper and lower)
 - At least one special character, e.g., punctuation, control character

Methods against Password Guessing

- Exponential back-off
 - Wait for t^{n-1} seconds before the next log-in when the n^{th} authentication attempt fails
 - t is a system parameter
- Disconnection
 - Disconnect after a specified number of failed attempts
- Disabling
 - Disable after a specified number of failed attempts
- Jailing (Honey pot)
 - Fool the attacker, then record all the activities that the attacker conducts

Biometrics

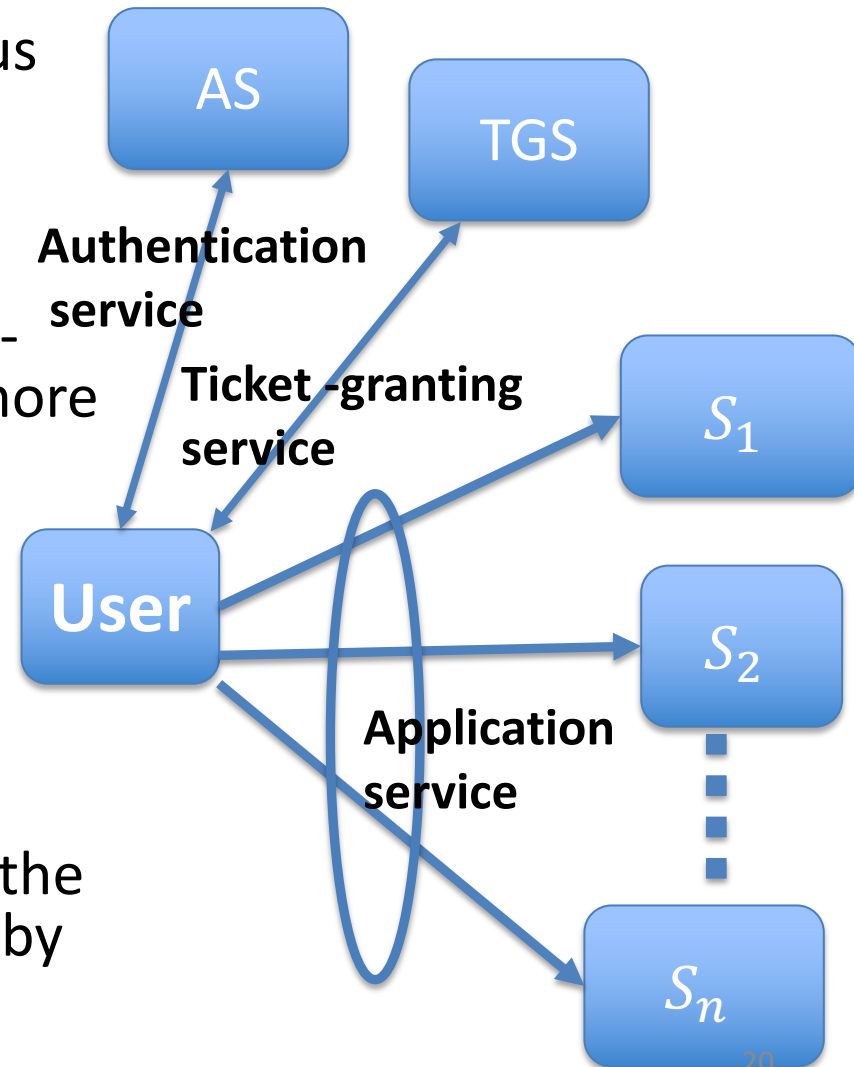
- Purpose
 - The use of automated measurement of biological or behavioural features to characterize and hence, identify an entity
- Methods (requires special sensors)
 - Fingerprints
 - Voices recognition
 - Eyes
 - Faces
 - Keystrokes (pressure, interval, duration, position, etc)
 - Gaits and motion biometrics

Strong authentication

- Authentication mechanisms utilize one or more of the following to establish a user's identity:
 - What the entity knows – knowledge-based authentication
 - Password, PIN, DoB, mother's maiden name, etc
 - What the entity has – token-based authentication
 - Badge, ID card, key, etc.
 - What the entity is – Biometric authentication
 - Fingerprints, personal characteristics, gait and motion biometrics, etc.
 - Where the entity is
 - Specific terminal, special access device, etc
- Combining two or more of these authentication mechanisms strengthens the authentication process

Kerberos Authentication

- Foundation
 - Needham-Schroeder protocol plus Denning and Sacco modification
- Kerberos application scenario
 - A system consist of a central authentication server AS, a ticket-granting server TGS and one or more application servers S_1, \dots, S_n
 - AS authenticates a user to the Kerberos system
 - TGS issues tickets to the user to authenticate to the application servers
 - S_1, S_2, \dots, S_n can be accessed by the user by presenting tickets issued by TS



Components of the Kerberos Protocol

- Secret key based cryptography
- The authentication server AS shares a secret key with each and every user and with the ticket-Granting server TGS
 - Question: how to achieve the above?
- The ticket-Granting Server TGS shares a secret key with each and every of the applications servers S_1, \dots, S_n

Components of the Kerberos Protocol

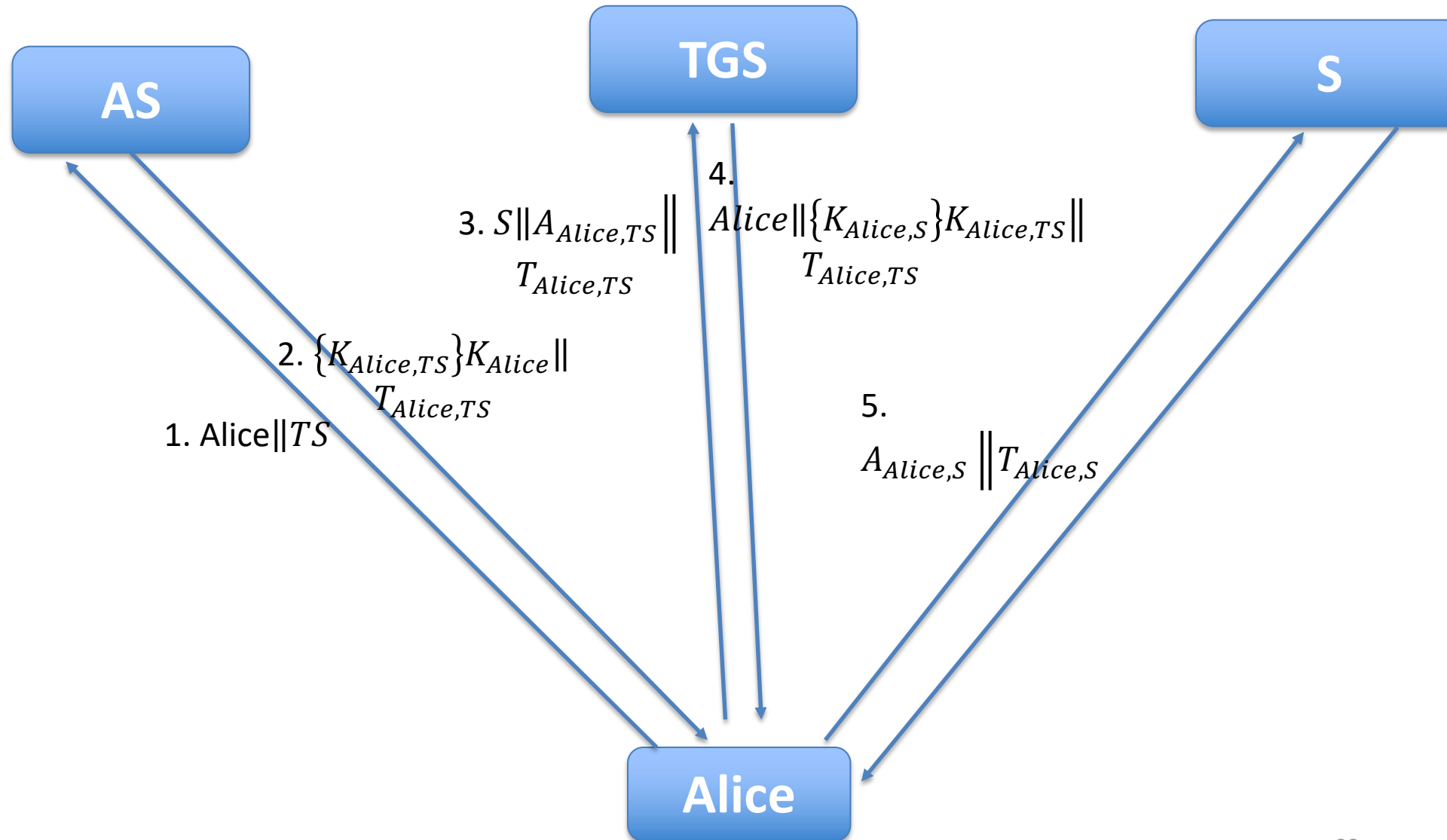
- Ticket

- $T_{Alice,Server} = \{Alice || Alice's\ address || valid\ time || K_{Alice,Server}\} K_{server}$
 - ❖ $K_{Alice,Server}$ is the session key generated by the server that created the ticket to be shared between “Alice” and “Server” so as to access “Server”
 - ❖ K_{server} is the secret key that “Server” shares with the server that created the ticket
- To be presented by Alice to Server for access

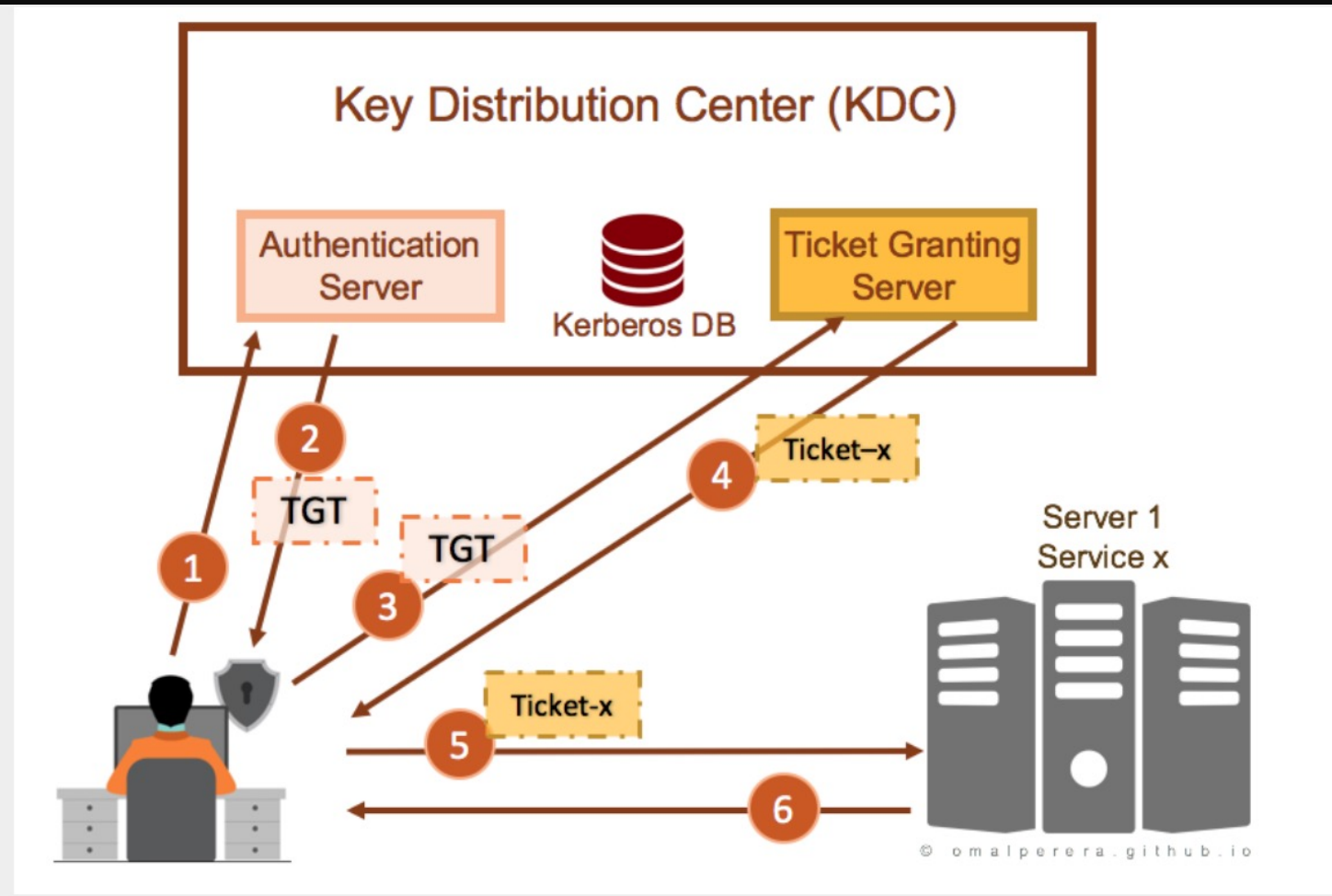
- Authenticator

- $A_{Alice,Server} = \{Alice || t || K_t\} K_{Alice,Server}$
 - ❖ $K_{Alice,Server}$ is the session key that is shared between “Alice” and “Server” so as to access “Server”
 - ❖ t is the timestamp when the authenticator is created
 - ❖ K_t is an alternative session key
- To prove to Server that Alice has the session key

The Kerberos Protocol



The Kerberos Protocol



- Kerberos protocol messages are protected against eavesdropping and replay attacks.

Significance of Kerberos

- **Single sign-on**
 - User only needs to log in once with the Authentication Server (AS)
 - ❖ Result: a ticket-issuing ticket is issued to the user to access the Ticket-Granting Server (TGS)
 - TGS issues tickets to the user to access the application servers
 - ❖ Result: logging-in to the application servers is transparent to the user
- Widely used in financial systems and large-scale e-commerce applications

Summary

- Identity
- Identification
- Authentication
- Passwords and password attacks
 - Challenge and response
 - Biometrics
 - The Kerberos protocol
- **Reference book:** Introduction to Computer Security by Matt Bishop, 2004

Lab report

- [Lab work and report instruction](#)
- [Moodle group](#) (COMPSCI5063)
- [Moodle group](#) (COMPSCI4062)
- [Lab 1 example](#)