Computer Engineering – Course Presentation: Systems Security

Miguel Frade

Polytechnic Institute of Leiria

School year 2019–2020

1. Context
2. Objectives
3. Syllabus
   - Contents
4. Evaluation
   - Final grade
   - Team Evaluation
5. Bibliography

Course Context

Systems Security:

- part of the undergraduate in Computer Engineering (CE) in Information Technologies
- 3rd year, 1st semester
- 6 ECTS – 75 contact hours

Lecturers:

- **Miguel Frade** T(d) + T(pl) + PL1 + PL2 (`miguel.frade@ipleiria.pt`)
  - Office hours:
  - Thursdays 14:00 – 15:00 at office G1.5-14
    or send an email to schedule a meeting
- **Nuno Rasteiro** PL (`leonel.santos@ipleiria.pt`)
  - Office hours: send an email to schedule a meeting

Course Description

This course provides the student skills to:

- solve security problems in Computing Systems;
- define and implement security policies in organizations;
- performing tasks of monitoring and security auditing;
- design and install security solutions in information systems;

Learning objectives

Upon completion of this course, students should be able to:

1. understand the basic security services such as confidentiality, integrity, availability, authentication, authorization and non-repudiation;

Learning objectives

Upon completion of this course, students should be able to:

1. understand the basic security services such as confidentiality, integrity, availability, authentication, authorization and non-repudiation;
2. understand the functioning and application of several symmetric and asymmetric encryption algorithms;

Learning objectives

Upon completion of this course, students should be able to:

1. understand the basic security services such as confidentiality, integrity, availability, authentication, authorization and non-repudiation;
2. understand the functioning and application of several symmetric and asymmetric encryption algorithms;
3. apply the acquired knowledge in configuration of network services and automate administration tasks;

Learning objectives

Upon completion of this course, students should be able to:

1. understand the basic security services such as confidentiality, integrity, availability, authentication, authorization and non-repudiation;
2. understand the functioning and application of several symmetric and asymmetric encryption algorithms;
3. apply the acquired knowledge in configuration of network services and automate administration tasks;
4. understand and apply security policies;

Learning objectives

Upon completion of this course, students should be able to:

1. understand the basic security services such as confidentiality, integrity, availability, authentication, authorization and non-repudiation;
2. understand the functioning and application of several symmetric and asymmetric encryption algorithms;
3. apply the acquired knowledge in configuration of network services and automate administration tasks;
4. understand and apply security policies;
5. be able to select tools and / or adequate security mechanisms;

Learning objectives

Upon completion of this course, students should be able to:

1. understand the basic security services such as confidentiality, integrity, availability, authentication, authorization and non-repudiation;
2. understand the functioning and application of several symmetric and asymmetric encryption algorithms;
3. apply the acquired knowledge in configuration of network services and automate administration tasks;
4. understand and apply security policies;
5. be able to select tools and / or adequate security mechanisms;
6. configuring authentication services;

Learning objectives

Upon completion of this course, students should be able to:

1. understand the basic security services such as confidentiality, integrity, availability, authentication, authorization and non-repudiation;
2. understand the functioning and application of several symmetric and asymmetric encryption algorithms;
3. apply the acquired knowledge in configuration of network services and automate administration tasks;
4. understand and apply security policies;
5. be able to select tools and / or adequate security mechanisms;
6. configuring authentication services;
7. take decisions on the solutions and configurations and policies established in a given scenario;

Learning objectives

Upon completion of this course, students should be able to:

1. understand the basic security services such as confidentiality, integrity, availability, authentication, authorization and non-repudiation;
2. understand the functioning and application of several symmetric and asymmetric encryption algorithms;
3. apply the acquired knowledge in configuration of network services and automate administration tasks;
4. understand and apply security policies;
5. be able to select tools and / or adequate security mechanisms;
6. configuring authentication services;
7. take decisions on the solutions and configurations and policies established in a given scenario;
8. be able to clearly explain the various security protocols;

Syllabus

1. Principles and practices of network security and systems
   - Security vulnerabilities;
   - Computer crimes
2. Introduction to cryptography
   - Classical Encryption Techniques;
   - Modern encryption techniques;
3. Symmetric cryptography
   - Symmetric algorithms
   - Confidentiality with symmetric algorithms
   - Key distribution
4. Asymmetric cryptography
   - Asymmetric algorithms
   - Key distribution

Syllabus

1. Principles and practices of network security and systems
   - Security vulnerabilities;
   - Computer crimes
2. Introduction to cryptography
   - Classical Encryption Techniques;
   - Modern encryption techniques;
3. Symmetric cryptography
   - Symmetric algorithms
   - Confidentiality with symmetric algorithms
   - Key distribution
4. Asymmetric cryptography
   - Asymmetric algorithms
   - Key distribution
5. Authentication
   - Authentication functions
   - Authentication algorithms
6. Digital Signatures
   - Distribution of keys for digital signatures
7. VPNs
   - Implementation of IPSec
   - Implementation of OpenVPN
8. Intrusion detection systems
9. Security policies and risk analysis
10. Maintaining security

Course Evaluation

First assessment period (frequência)

$$\text{Final score} = \begin{cases} 40\% \text{ individual written assessment } + \\ 25\% \text{ individual practical test } + \\ 35\% \text{ team project} \end{cases}$$

There are no minimum scores in the partial evaluations.

Course Evaluation

First assessment period (frequência)

$$\text{Final score} = \begin{cases} 40\% \text{ individual written assessment } + \\ 25\% \text{ individual practical test } + \\ 35\% \text{ team project} \end{cases}$$

There are no minimum scores in the partial evaluations.

Provisional dates:

- 2019-11-07 and 2019-11-08 – individual practical assessment
- 2020-01-11 – Deadline for project submission
- 2020-01-20 – Project presentation
- 2020-01-27 – individual written assessment

Course Evaluation

Evaluation by Exam

$$\text{Final score} = \begin{cases} 40\% \text{ individual written assessment } + \\ 60\% \text{ individual practical test} \end{cases}$$

There are no minimum scores

- grades from the $1^s t$ assessment period are saved (T or P)
- to calculate the exam final grade it will be used the component's grade from the last time the student was evaluated (in the same school year);
- students who have already obtained a passing score, but still wish to improve their grades by exam, it is **mandatory** to be evaluated in **both T and P** components;

Individual evaluation of the team project (phase 1 and phase 2)

Goals

Evaluate students in a fairer way and promote the development of team work skills

Individual evaluation of the team project (phase 1 and phase 2)

Goals

Evaluate students in a fairer way and promote the development of team work skills

Individual mark $\mathrm{IM} = \mathrm{TM} \times \mathrm{ICF}$

Individual evaluation of the team project (phase 1 and phase 2)

Goals

Evaluate students in a fairer way and promote the development of team work skills

Individual mark IM $=$ TM $\times$ ICF

- Team Mark (TM)
  - score given by the teacher based on the delivered report and presentation
  - equal to all team members

Individual evaluation of the team project (phase 1 and phase 2)

Goals

Evaluate students in a fairer way and promote the development of team work skills

Individual mark IM = TM × ICF

- Team Mark (TM)
  - score given by the teacher based on the delivered report and presentation
  - equal to all team members
- Individual Contribution Factor (ICF)
  - Based on self and peer evaluation quizzes
  - Punishes free-riders → **you know them better than me!**
  - Promotes above-average contributions → motivate students to contribute more
  - But prevents individualism → maintains teamwork spirit
  - Development of team work skills becomes part of the learning process

Individual evaluation of the team project (phase 1 and phase 2)

Self and peer evaluation quiz topics:

1. **Group Participation** – Attends meetings regularly and on time.

Individual evaluation of the team project (phase 1 and phase 2)

Self and peer evaluation quiz topics:

1. **Group Participation** – Attends meetings regularly and on time.
2. **Time Management & Responsibility** – Accepts fair share of work and reliably completes it by the required time.

Individual evaluation of the team project (phase 1 and phase 2)

Self and peer evaluation quiz topics:

1. **Group Participation** – Attends meetings regularly and on time.
2. **Time Management & Responsibility** – Accepts fair share of work and reliably completes it by the required time.
3. **Adaptability** – Displays or tries to develop a wide range of skills in service of the project, readily accepts changed approach or constructive criticism.

Individual evaluation of the team project (phase 1 and phase 2)

Self and peer evaluation quiz topics:

1. **Group Participation** – Attends meetings regularly and on time.
2. **Time Management & Responsibility** – Accepts fair share of work and reliably completes it by the required time.
3. **Adaptability** – Displays or tries to develop a wide range of skills in service of the project, readily accepts changed approach or constructive criticism.
4. **Creativity/Originality** – Problem-solves when faced with impasses or challenges, originates new ideas, initiates team decisions.

Individual evaluation of the team project (phase 1 and phase 2)

Self and peer evaluation quiz topics:

1. **Group Participation** – Attends meetings regularly and on time.
2. **Time Management & Responsibility** – Accepts fair share of work and reliably completes it by the required time.
3. **Adaptability** – Displays or tries to develop a wide range of skills in service of the project, readily accepts changed approach or constructive criticism.
4. **Creativity/Originality** – Problem-solves when faced with impasses or challenges, originates new ideas, initiates team decisions.
5. **Communication Skills** – Effective in discussions, good listener, capable presenter, proficient at diagramming, representing, and documenting work.

Individual evaluation of the team project (phase 1 and phase 2)

Self and peer evaluation quiz topics:

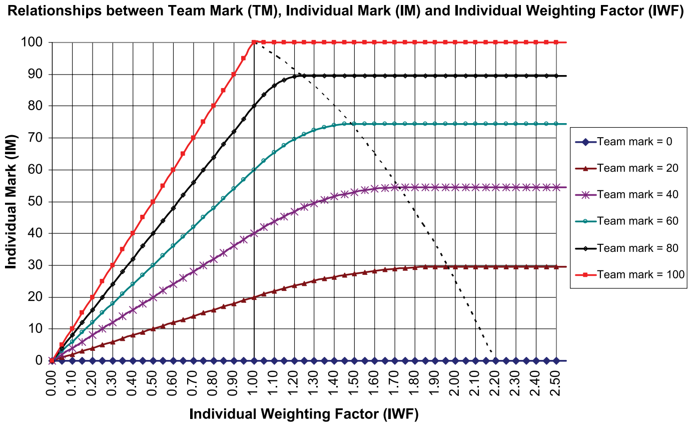
1. **Group Participation** – Attends meetings regularly and on time.
2. **Time Management & Responsibility** – Accepts fair share of work and reliably completes it by the required time.
3. **Adaptability** – Displays or tries to develop a wide range of skills in service of the project, readily accepts changed approach or constructive criticism.
4. **Creativity/Originality** – Problem-solves when faced with impasses or challenges, originates new ideas, initiates team decisions.
5. **Communication Skills** – Effective in discussions, good listener, capable presenter, proficient at diagramming, representing, and documenting work.
6. **Team Skills** – Positive attitude, encourages and motivates team, supports team decisions, helps team reach consensus, helps resolve conflicts in the group.

Individual evaluation of the team project (phase 1 and phase 2)

Self and peer evaluation quiz topics:

1. **Group Participation** – Attends meetings regularly and on time.
2. **Time Management & Responsibility** – Accepts fair share of work and reliably completes it by the required time.
3. **Adaptability** – Displays or tries to develop a wide range of skills in service of the project, readily accepts changed approach or constructive criticism.
4. **Creativity/Originality** – Problem-solves when faced with impasses or challenges, originates new ideas, initiates team decisions.
5. **Communication Skills** – Effective in discussions, good listener, capable presenter, proficient at diagramming, representing, and documenting work.
6. **Team Skills** – Positive attitude, encourages and motivates team, supports team decisions, helps team reach consensus, helps resolve conflicts in the group.
7. **Technical Skills** – Ability to create and develop materials on own initiative, provides technical solutions to problems.

Individual Contribution Factor (ICF)



Source: Kali Prasad Nepal (2012), "*An approach to assign individual marks from a team mark: the case of Australian grading system at universities*", Assessment & Evaluation in Higher Education, 37:5, 555-562 (`http://dx.doi.org/10.1080/02602938.2011.555815`)

Teams formation

Teams:

- 5 students per team
    - exceptions must be approved by the teacher
- students are allowed to choose their teams – enroll in the Moodle platform

Course bibliography

Main bibliography

- W. Stallings, Cryptography and Network Security: Principles and Practice (7th edition), Oct. 2016, ISBN-13: 978-1292158587
- Zúquete, A., Segurança em redes informáticas, (4th edition), FCA, 2013, ISBN-13: 978-9727227679

Complementary:

- RFC2504, Users' Security Handbook, IETF, Feb. 1999
- RFC 2196, The Site Security Handbook, IETF, Sep. 1997
- RFC6071 IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. S. Frankel, S. Krishnan. Feb. 2011, IETF
- RFC4302 IP Authentication Header. S. Kent. Dec. 2005, IETF
- RFC4303 IP Encapsulating Security Payload (ESP). S. Kent. Dec. 2005, IETF
- RFC2411 IP Security Document Roadmap R. Thayer, N. Doraswamy, R. Glenn, Nov. 1998
- E. Crist and J. Keijser, Mastering OpenVPN, Aug. 2015, ISBN-13: 978-178355313