



## Segurança Informática

### Aula 1

1º Ciclo em Engenharia Informática  
1º Ciclo em Informática Web  
1º Ciclo em Matemática e Aplicações

#### Sumário

Apresentação do docente e discussão do funcionamento geral da unidade curricular: horário das aulas, critérios de avaliação, material de apoio e programa. Discussão do âmbito e da motivação para estudo dos temas que a unidade curricular aborda, bem como de alguns conceitos básicos e terminologia.

## Computer Security

### Lecture 1

B.Sc. in Computer Science and Engineering  
B.Sc. in Web Informatics  
B.Sc. in Mathematics and Applications

#### Summary

*Presentation of the lecturer and discussion of the general functioning of this course: classes schedule, evaluation criteria, support material and program. Discussion concerning the scope and motivation for studying the subjects of this course, as well as of some basic concepts and terminology. Basic concepts and terminology.*

## 1 Apresentação do Docente, Recursos e Plataforma de Apoio às Aulas e Horário de Atendimento

### *Presentation of the Lecturer and Discussion of the General Functioning of this Subject*

#### 1.1 O Docente

##### *The Lecturer*

**Pedro Ricardo Morais Inácio** é professor associado do Departamento de Informática da Universidade da Beira Interior (UBI), instituição que integra **desde 2010**. Leciona unidades curriculares relacionadas com **segurança e garantia da informação, programação e simulação assistida por computador**, a cursos de licenciatura, mestrado e doutoramento, nomeadamente aos de Engenharia Informática. É atualmente Pró-Reitor para a Universidade Digital e o *Data Protection Officer* da UBI.

*Pedro Ricardo Morais Inácio is an associate professor of the Department of Computer Science at the University of Beira Interior (UBI), which he joined in 2010. Lectures subjects related with information assurance and security, programming of mobile devices and computer based simulation, to graduate and undergraduate courses, namely to the B.Sc., M.Sc. and Ph.D. programmes in Computer Science and Engineering. He is currently the Pro-Rector for the Digital University and the Data Protection Officer of UBI.*

**Nasceu na Covilhã** e tem uma **licenciatura pré-Bolonha em Matemática Informática e um Doutoramento em Engenharia Informática**, obtidos na UBI em 2005 e 2009, respetivamente. Os trabalhos de Doutoramento foram desenvolvidos no ambiente empresarial da **Nokia Siemens Networks Portugal S.A.**, ao abrigo de

uma bolsa de investigação da Fundação para a Ciência e a Tecnologia.

*He was born in Covilhã and holds a 5-year B.Sc. degree in Mathematics/Computer Science and a Ph.D. degree in Computer Science and Engineering, obtained from UBI, Portugal, in 2005 and 2009 respectively. The Ph.D. work was performed in the enterprise environment of Nokia Siemens Networks Portugal S.A., through a Ph.D. grant from the Portuguese Foundation for Science and Technology.*

É **membro sénior IEEE**, associado ACM e **investigador do Instituto de Telecomunicações (IT)**. Os seus interesses de investigação incluem **segurança e garantia da informação, simulação assistida por computador**, e monitorização, análise e classificação de tráfego de rede. Tem cerca de 70 publicações em livros, revistas e conferências científicas internacionais com revisão por pares. Revê com frequência artigos para revistas IEEE, Springer, Wiley e Elsevier. É membro regular do Comité Técnico de diversas conferências e seminários de referência nacionais e internacionais, como a ACM SAC, a IEEE NCA, a IFIPSEC ou a ARES. É atualmente Editor Associado da revista IEEE Access.

*He is an IEEE senior member, an ACM professional member and a researcher of the Instituto de Telecomunicações (IT). His main research topics are information assurance and security, computer based simulation, and network traffic monitoring, analysis and classification. He has about 70 publications in the form of book chapters and papers in international peer-reviewed books, conferences and journals. He frequently reviews papers for IEEE, Springer, Wiley and Elsevier journals. He is a member of the Technical Program Committees of flagship national and international workshops and conferences, such as ACM SAC, IEEE NCA, IFIPSEC or ARES. Currently serves as an Associate Editor for IEEE Access.*

Mais em <https://www.di.ubi.pt/~inacio>.

## 1.2 Plataforma e Material de Apoio às Aulas

### E-Learning Platform and Classes Resources

Nas aulas teóricas recorre-se ao método expositivo e ao diálogo para apresentação dos conteúdos, acompanhados pela projeção ou elaboração de apontamentos teóricos e de exemplos.

A maior parte das aulas práticas terão um guia laboratorial com tarefas e perguntas. As aulas práticas consistem no desenvolvimento de tarefas em computadores com sistema operativo Linux (ou com o subsistema equivalente) e recorrendo a diversas ferramentas, tecnologias ou linguagens de programação, nomeadamente OpenSSL, hping3, tcpdump, openvas, iptables, GPG, Linguagem de programação C, Python ou Java.

Todos os conteúdos desta unidade curricular serão disponibilizados no sistema de gestão de aprendizagem **Moodle** (<https://moodle.ubi.pt/>), bem como todos os elementos que a acompanham (notas, propostas de trabalho de grupo, etc.). Tanto os apontamentos teóricos como os guias laboratoriais serão disponibilizados aos estudantes no formato *Portable Document Format* (PDF), no máximo, no dia anterior à realização da aula. Em princípio, os trabalhos serão também submetidos na plataforma e é possível que se venham a tentar funcionalidades mais rebuscadas (e.g., testes), no decorrer do semestre, usando outras tecnologias ou plataformas. Por exemplo, para os testes práticos desta unidade curricular será usada uma plataforma especificamente desenvolvida para avaliar o desenvolvimento de tarefas em ambiente de linhas de comandos. Para **antecipar eventuais problemas**, sugere-se a quem ainda não tenha tentado o acesso ao Moodle, que o faça logo que possível, e avise (por e-mail) caso tenha dificuldade no acesso.

## 1.3 Horário das Aulas e do Atendimento

### Class and Office Times

#### Teoria | Lecture - TE1

Segundas-feiras, das 09h00 às 11h00, na sala 6.01.

*Mondays, from 09h00 to 11h00, in room 6.01.*

**Professor:** Doutor Pedro Inácio (inacio@di.ubi.pt)

#### Prática Laboratorial | Practice in Lab Env. - PL1

Sextas-feiras, das 09h00 às 11h00, na sala 6.27.

*Fridays, from 09h00 to 11h00, in room 6.27.*

**Professor:** Doutor João Neves (jneves@di.ubi.pt)

#### Prática Laboratorial | Practice in Lab Env. - PL2

Sextas-feiras, das 11h00 às 13h00, na sala 6.27.

*Fridays, from 11h00 to 13h00, in room 6.27.*

**Professor:** Doutor João Neves (jneves@di.ubi.pt)

#### Prática Laboratorial | Practice in Lab Env. - PL3

Quintas-feiras, das 14h00 às 16h00, na sala 6.27.

*Thursdays, from 14h00 to 16h00, in room 6.27.*

**Professor:** Doutor João Neves (jneves@di.ubi.pt)

#### Atendimento | Office Times

Segundas-feiras, das 14h00 às 15h00, no laboratório

6.10 ou no gabinete do docente.

*Mondays, from 14h00 to 15h00, in lab 6.10 or at the office.*

Note que pode recorrer a qualquer dos docentes envolvidos na unidade curricular para tirar dúvidas. Por favor, considere contactar antecipadamente os docentes para marcar o atendimento (e.g., via *Teams* ou e-mail para [prmi@ubi.pt](mailto:prmi@ubi.pt)), preparando previamente a dúvidas.

*Note that you can approach any of the professors involved in the course unit for questions. Please consider contacting the lecturers in advance (e.g. via Teams or e-mail to [prmi@ubi.pt](mailto:prmi@ubi.pt)), carefully structuring your questions.*

## 2 Avaliação

### Evaluation

### 2.1 Elementos de Avaliação

#### Evaluation Elements

Durante o **período ensino-aprendizagem**, a avaliação qualitativa a esta unidade curricular é feita recorrendo a **três elementos** principais: **um teste de aferição de conhecimentos escrito (T)**, **um teste prático (TP)** e **um trabalho prático de grupo (TG)**. T vale 50% da classificação para o período ensino-aprendizagem (o equivalente a 10 valores), enquanto que TP vale 25% (o equivalente a cinco valores) e TG vale 25% (o equivalente a cinco valores).

*During the normal classes period, the qualitative evaluation is performed resorting to three main elements: a written test for knowledge evaluation (T), a practical test (TP) and a practical team work (TG). T is worth 50% of the classification for the normal classes period (equivalent to 10 points in the final score), while TP is worth 25% (equivalent to five points) and TG is worth 25% (equivalent to five points).*

A **assiduidade** (Ass) para esta unidade curricular é de **76%** (o equivalente a **uma tolerância de seis faltas** no total das aulas teóricas e práticas). As faltas serão marcadas e a assiduidade pode ser consultada via projeção de uma folha de cálculo durante a chamada em todas as aulas.

*Attendance (Ass) for this course is 76% (equivalent to a tolerance of a total of six misses). Absences will be registered at each class. Attendance can be consulted during this process, since a spreadsheet with that information will be displayed.*

As notas do **teste prático e do trabalho de grupo continuam a contar para exame**. Após o período ensino-aprendizagem, e para aqueles(as) que forem admitidos(as) a exame, os testes de aferição de conhecimentos escritos serão substituídos pelo **exame (E)**, **que versa sobre toda a matéria lecionada e praticada** durante o período ensino-aprendizagem, valendo portanto 50% da classificação final em período de exame.

*The scores of the practical test and of the team work also count for the grade on the exam. After the normal classes period, and for those admitted to the exam, the written tests for knowledge evaluation are replaced by the exam (E), which covers all the*

material taught or practiced during classes, and is thus worth 50% of the final score.

## 2.2 Classificação Ensino–Aprendizagem

### Teaching–Learning Period Classification

A **classificação** para o **período ensino-aprendizagem** (C) é obtida da **média ponderada das classificações** obtidas nos elementos antes referidos, conforme se formaliza na equação (1):

*The score for the teaching-learning period (C) is the weighted average of the classifications obtained in the aforementioned elements, as formalized by (1):*

$$C = 0.5T + 0.25TP + 0.25TG. \quad (1)$$

A **aprovação** à unidade curricular e a **concessão de frequência depende da assiduidade e da classificação** para o período ensino-aprendizagem. O(a) estudante é aprovado(a) caso obtenha uma **classificação superior ou igual a 9.5 e assiduidade superior ou igual a 76%** durante o período ensino-aprendizagem. Em caso de aprovação, a classificação final (CF) é o número inteiro mais próximo de C, i.e.,

Se  $C \geq 9.5$  e  $Ass \geq 76\%$ ,

Então Aprovado com  $CF = \text{arredondar}(C)$ .

Em caso de aprovação no período ensino-aprendizagem, o(a) estudante é dispensado(a) de exame, embora possa ir melhorar a sua classificação em exame.

*The approval at this subject and admission to exam depends of C and of the attendance. The student is considered to be approved at the subject if he or she obtains a score higher than or equal to 9.5 and an attendance higher than or equal to 76%. In such case, the final score (CF) is the integer number closer to C, i.e.,*

*If  $C \geq 9.5$  and  $Ass \geq 76\%$ ,*

*Then Approved with  $CF = \text{round}(C)$ .*

*In case of being approved, the student is waived from the exam, though he or she may try to improve the score in the exam.*

## 2.3 Admissão a Exame

### Admission to Exam

A admissão a exame depende da obtenção de uma **classificação superior ou igual a 6 e assiduidade superior ou igual a 76%** no período ensino-aprendizagem, i.e.,

Se  $C \geq 6$  e  $Ass \geq 76\%$ , Então Admitido a Exame;

Caso contrário, Reprovado.

*The admission to exam depends of getting a score higher or equal to 6 and an attendance higher or equal to 76% during classes, i.e.,*

*If  $C \geq 6$  and  $Ass \geq 76\%$ , Then Admitted to Exam;*

*Else, Fail.*

A classificação após exame (CE) é calculada usando uma fórmula semelhante à anterior (ver (2)):

*The score for the exam (CE) is obtained using a formula similar to the previous one (see (2)):*

$$CE = 0.50E + 0.25TP + 0.25TG. \quad (2)$$

## 2.4 Classificação Final

### Final Score

A **classificação final** à unidade curricular no final das atividades letivas depende da **assiduidade e da maior das duas classificações C e CE**. O(a) estudante é aprovado(a) à unidade curricular **se uma das classificações C ou CE for superior ou igual a 9.5 e a assiduidade seja superior a 76%** (faz-se notar que a assiduidade conta também para admissão a exame). A classificação final (CF) é o número inteiro mais próximo da maior das duas classificações. A classificação final será **Reprovado caso ambas as notas sejam inferiores a 9.5 ou a assiduidade inferior a 76%**:

Se  $\text{MAX}(C, CE) \geq 9.5$  e  $Ass \geq 76\%$ ,

Então Aprovado com  $CF = \text{arredondar}(\text{MAX}(C, CE))$ ;

Caso contrário, Reprovado.

*The final score of this curricular unit at the end of the exams depends of the attendance and of the biggest score between C and CE. The student is approved if one of the classifications C or CE is larger or equal to 9.5 and the attendance is larger or equal to 76% (notice that attendance counts also for the admission to exam). The final score (CF) is the integer number closer to the largest of the two scores. The student will Fail if both scores are smaller than 9.5 or the attendance is smaller than 76%:*

*If  $\text{MAX}(C, CE) \geq 9.5$  and  $Ass \geq 76\%$ ,*

*Then Approved with  $CF = \text{round}(\text{MAX}(C, CE))$ ,*

*Else Fail.*

Estes critérios aplicam-se a alunos de erasmus e trabalhadores estudantes, à exceção da eventual assiduidade às aulas e salvo situações pontuais devidamente discutidas e acordadas com o regente da unidade curricular.

*The aforementioned criteria applies to erasmus and to working students, except for maybe the attendance and for punctual situations, duly discussed and agreed with the responsible for the curricular unit.*

## 2.5 Teste Escrito e Exames

### Written Test and Exams

A avaliação do conhecimento nesta unidade curricular é sobretudo feita através de uma prova escrita. Em princípio, todas as provas escritas são **constituídas**, na íntegra, **por perguntas de escolha múltipla ou de resposta direta**. Estas provas versam sobre toda a matéria lecionada e praticada durante o período ensino-aprendizagem. O teste será agendado para o final do semestre. Os exames são ajustados pelos diretores de curso.

*Knowledge evaluation is mostly performed resorting to written tests. The written test and the exams will be constituted by multiple choice or direct answer questions. They will cover all the materials taught or practiced during classes. The written test will be scheduled for the end of the semester. The dates for exams will be adjusted by the course directors.*

## 2.6 Teste Prático

### Practical Test

A nota da componente prática desta unidade curricular resulta da soma das notas do teste prático e do trabalho de grupo. O teste prático **vale até cinco valores**, e consiste na **execução de várias tarefas em ambiente de linha de comandos**, ao estilo das aulas práticas com guias laboratoriais habituais. Incidirá sobre a matéria praticada nas aulas práticas e lecionada nas aulas teóricas até à altura do teste, focando-se no tema da **criptografia**. Cada estudante terá de executar uma série de comandos sobre ficheiros pré-estabelecidos, de forma a chegar ao resultado certo. Será avaliada a capacidade de chegarem às respostas certas, e os comandos propriamente ditos. Uma ou duas tarefas poderão incluir a implementação de pequenos programas em ANSI C, Java ou Python.

*The score of the practical component is the result of the sum of the grades on the practical test and on the team work. The practical test is worth five points, and consists on the execution of several tasks in a client line environment, in a similar format to the typical practical classes with laboratory guides. It will be mostly focused on the subjects practiced during the practical classes and lectured in the theoretical classes up to the date of the test, namely on the information security subject. Each student will have to execute a series of instructions on pre-established files, so as to get to the correct result. This activity will evaluate both the ability to get to the right answers and to devise the correct commands. One or two tasks may include the implementation of small programs in ANSI C, Java or Python.*

## 2.7 Trabalhos Práticos de Grupo

### Team Works

O trabalho de grupo **vale até cinco valores** (em 20) e deve ser **executado por grupos de cinco ou seis pessoas** (o trabalho é de grupo, e não deve ser feito individualmente). Consiste no **desenvolvimento de um tema** seguindo as melhores práticas de engenharia (nomeadamente de segurança), implementação e gestão de software e ~~na elaboração de um relatório~~. O tema é proposto e atribuído pelo docente durante as primeiras três semanas do semestre. Eventualmente, também se podem discutir propostas feitas pelos estudantes.

*The team work is worth five points (in 20), and it should be performed by groups of five or six persons (this is a team work, and should not be done individually). It consists on the development of a proposal following the best practices in terms of software (security) engineering, implementation and management ~~and in the elaboration of a report~~. Proposals are provided and assigned by the lecturer during the three first weeks of the semester. Works proposed by the students may also be discussed.*

Os **elementos** a serem **entregues** no âmbito do trabalho são o código da aplicação (devidamente documentado) e os executáveis derivados da compilação do código, bem como outros artefactos que provem a autoria do trabalho. **Por cada dia de atraso** na entrega de qualquer elemento relativo ao trabalho **descontam-se 0.5 valores à nota do mesmo**.

*The elements that need to be delivered in the scope of this work are the code of the developed application (duly documented) and the executable files resulting from the compilation of the code, along with other artifacts that prove the authorship of the work. For each day behind schedule, a penalty of 0.5 points is applied to the score for this work.*

**Nota:** para além dos elementos a entregar no âmbito do trabalho de grupo, é ainda assumido que todos os trabalhos serão **defendidos oralmente** no final do semestre, numa **apresentação** que não deve demorar mais do que **10 minutos, acompanhada por um breve conjunto de diapositivos**.

*Note: besides the elements to be delivered in the scope of the team work, it is also assumed that all works are to subject to an oral discussion in a 10 minutes presentation, dully backed up with a small slide set.*

## 2.8 Momentos de Avaliação

### Important Dates

O **teste prático** será numa das aulas práticas da semana que começa a 01/05/2023 (segunda-feira), na sala 6.27.

*The practical test will be on one of the practical classes of the week starting in 01/05/2023 (Monday), in room 6.27.*

A **constituição do grupo de trabalho e o tema escolhido** devem ser comunicados por e-mail até dia 10/03/2023 (sexta-feira). As propostas serão colocadas no moodle oportunamente. A atribuição de temas (aleatória) é feita na mesma semana.

*The constitution of the work team and the selected proposal should be reported by e-mail until 10/03/2023 (Friday). The proposals will be opportunely published on moodle. The (random) assignment of proposals is performed in the same week.*

O **trabalho de grupo** (código + scripts + executáveis + outros artefactos) pode ser entregue até dia 26/05/2023 (sexta-feira) às 23h55. A submissão é feita exclusivamente via Moodle.

*The team work (code + scripts + executable files + other artifacts) should be delivered before the 23h55 of the 26/05/2023 (Friday). Submission of works is performed exclusively via Moodle.*

O **teste escrito** é no dia 05/06/2023 (segunda-feira), das 09h00 às 11h00, na sala 6.01.

*The date for the second written test is 05/06/2023 (Monday), from 09h00 to 11h00, on room 6.01.*

As **defesas dos trabalhos** de grupo serão agendadas para uma das aulas das últimas semanas de aulas, ou em horário a combinar (a agendar oportunamente com cada um dos grupos);

*The presentations of the team works are to be scheduled with the students for one of the classes in the last two weeks of the Teaching-Learning period.*

## 2.9 Bibliografia

### Bibliography

## Bibliografia Principal *Main References*

1. Pedro R. M. Inácio, *Apontamentos teóricos e guias práticos laboratoriais de Segurança Informática*, 2021.
2. André Zúquete, *Segurança em Redes Informáticas*, 4ª Ed. (actualizada e aumentada): FCA – Editora de Informática, Abril 2013, pp. 432.
3. William Stallings e Lawrie Brown, *Computer Security: Principles and Practice*, 3ª edição: Pearson, 2014, pp. 848.
4. Alfred J. Menezes, Paul C. van Oorschot e Scott A. Vanstone, *Handbook of Applied Cryptography*, 5ª impressão: CRC Press, Agosto 2001, pp. 816 (disponível online em <http://www.cacr.math.uwaterloo.ca/hac/>).

## Bibliografia Complementar

1. Margaret Cozzens e Steven J. Miller, *The Mathematics of Encryption: An Elementary Introduction*: American Mathematical Society (AMS), 2013, pp. 332.
2. William Stallings, *Cryptography and Network Security*, 7ª edição: Pearson India, 2017, pp. 768.
3. Henrique São Mamede, *Segurança Informática nas Organizações*: FCA - Editora de Informática, 2006, pp. 512.

## 2.10 Objetivos da Unidade Curricular

### *Objectives of this Course*

Introduzir e **praticar a correta utilização de conceitos e mecanismos da segurança da informação**, assim como estudar vulnerabilidades de segurança em sistemas ligados por redes de computadores, e ferramentas de auditoria e mitigação dessas vulnerabilidades.

*Introduce and practice the correct use of information security related concepts and mechanisms, as well as to study security vulnerabilities in systems interconnected via computer networks, and audit tools and mitigation techniques for these vulnerabilities.*

No final da Unidade Curricular o estudante deve ser capaz de:

- **Estudar problemas de segurança informática do ponto de vista prático** e contemporâneo, bem como **descrever e implementar boas práticas** e soluções que minimizam o impacto de potenciais ameaças, ou procurar essas soluções de modo autónomo;
- **Configurar ferramentas de segurança**, nomeadamente *firewalls* e sistemas de deteção de intrusões (robustecer um sistema exposto à Internet ou a uma rede de computadores com configurações de *firewall* adequadas);

- **Integrar mecanismos da criptografia moderna em aplicações de *software*** que esteja a desenvolver;
- **Utilizar corretamente algoritmos de cifra, mecanismos de autenticação, de assinatura digital, de proteção de sistemas** e domínios administrativos e implementação de redes privadas virtuais seguras;
- Compreender e saber implementar formas de transmitir e armazenar dados de uma forma segura;
- Fazer a engenharia de aplicações web seguras;
- **Saber instalar, configurar e ativar protocolos de comunicação seguros em aplicações Web.**

*At the end of this course unit the student should be able to:*

- *Study computer security problems from a practical and contemporary perspective, as well as describing and implementing best practices and solutions that minimize the impact of potential threats, or search for these solutions independently;*
- *Configure security tools, including firewalls and intrusion detection systems (harden systems exposed to the Internet or a computer network with proper firewall settings);*
- *Integrating mechanisms of information security in software applications he/she is developing;*
- *Properly utilize encryption algorithms, authentication mechanisms, digital signatures, protection systems and administrative domains and implementation of secure virtual private networks;*
- *Understand and know to implement secure means to store and transmit data;*
- *Engineer secure web applications;*
- *Know how to install, configure and activate secure communication protocols for web applications.*

## 2.11 Programa

### *Syllabus*

#### 1. Criptografia Simétrica e de Chave Pública

*Symmetric and Public-Key Encryption*

(a) Da Criptografia Clássica à Moderna  
*From Classical to Modern Cryptography*

(b) Cifras Simétricas Contínuas  
*Stream Ciphers*

(c) Cifras por Blocos  
*Block Ciphers*

(d) Funções de Hash e Cifra Autenticada  
*Hash Functions and Authenticated Encryption*

(e) Problemática de Distribuição e Acordo de Chaves: o Protocolo de Acordo de Chaves Diffie-Hellman  
*Problems Associated with the Distribution and Agreement of Encryption Keys: the Diffie-Hellman Key Agreement Protocol*

- (f) Cifras de Chave Pública e Assinaturas Digitais  
*Public Key Encryption and Digital Signatures*

2. Gestão e Utilização de Chaves Públicas  
*Usage and Management of Public Keys*

- (a) Infraestrutura de Chave Pública; Rede de Confiança  
*Public Key Infrastructure; Web of Trust*
- (b) Caso de Estudo: PGP (Pretty Good Privacy)  
*Case Study: PGP (Pretty Good Privacy)*
- (c) Caso de Estudo: Cartão do Cidadão Português  
*Case Study: Portuguese Citizen Card*

3. Vulnerabilidades e Proteção de Sistemas Distribuídos  
*Vulnerabilities and Protection in Distributed Systems*

- (a) Vulnerabilidades em Sistemas Distribuídos  
*Vulnerabilities on Distributed Systems*
- (b) Vulnerabilidades e Ataques em Redes Locais e de Larga Escala  
*Vulnerabilities and Attacks on Local Area Networks and Large Scale*
- (c) Arquitetura e Modo de Operação de Firewalls  
*Architecture and Functioning of Firewalls*
- (d) Sistemas de Detecção e Prevenção de Intrusões  
*Intrusion Detection and Prevention Systems*

4. Protocolos e Comunicações Seguras

- (a) Protocolos de Segurança e Redes Privadas Virtuais - SSL/TLS e IPSec  
*Security Protocols and Virtual Private Networks - SSL/TLS and IPSec*
- (b) Segurança em Redes sem Fios 802.11 (o exemplo WEP)  
*Wireless Network Security 802.11 (the WEP example)*

5. Lei Portuguesa sobre o Cibercrime e Centro Nacional de Cibersegurança  
*Portuguese Cybercrime Law and National Center for Cybersecurity*

### 3 Âmbito e Motivação

#### *Scope and Motivation*

#### 3.1 Âmbito

##### *Scope*

Quando se interligam os termos *segurança* e *sistemas de computadores*, podem-se considerar, de um modo geral, três áreas adequadas ao resultado da interligação:

1. Esta **unidade curricular não trata o tema da segurança contra catástrofes físicas, nomeadamente**

**ambientais** (Tremores de terra, incêndios, inundações, tempestades, queda de raios, tempestades magnéticas, etc.), **políticas** (Terrorismo, motis, etc.), ou **materiais** (e.g., degradação ou roubo de equipamento). Estas catástrofes resolvem-se sobretudo com mecanismos de sobrevivência e redundância, nomeadamente usando cópias de segurança. A garantia da sobrevivência dos dados, serviços ou sistemas requer algum planeamento e análise, principalmente no que diz respeito à colocação dos sistemas redundantes e à forma como as cópias são feitas ou repostas, e onde é que os sistemas redundantes são colocados (e.g., *datacenters* são colocados em locais de pouca atividade sísmica). Como exemplo histórico deste tipo de catástrofe, pode mencionar-se a destruição do *World Trade Center* e de todos os dados que isso implicou.

2. Também **não trata o tema relativo a faltas ou falhas previsíveis num sistema**, como a quebra no fornecimento de energia elétrica; bloqueio na execução de aplicações ou sistemas operativos (e.g., *kernel panic*); ou falhas temporárias de conectividade em troços de rede. Estes problemas resolvem-se com mecanismos de redundância de sistemas, mecanismos de recuperação de falhas baseados em *logs* (e.g., usados em sistemas transacionais como Sistemas de Gestão de Bases de Dados), ou redundância de canais de comunicação ou mecanismos de retransmissão, que encontram implementações na Internet.

3. Esta unidade curricular **trata o tema da segurança contra ataques ilícitos e propositados**. Sem retirar importância às outras áreas, este **tema é mais complexo e exigente**, porque trata a **malícia e a imprevisibilidade humana** e não ocorrências que podem ser associadas a uma determinada probabilidade. Por exemplo, um humano preocupa-se em apagar as pistas de determinada atividade ilícita, enquanto que as catástrofes ou erros não.

Há cinco tipos base para atividades ilícitas:

1. **Acesso a Informação**  
Acesso a dados confidenciais ou que não deveriam ser públicos.
2. **Alteração da Informação**  
Alteração de dados em prol do utilizador que o faz.
3. **Utilização Exagerada ou Abusiva de Recursos Computacionais**
- Exagerada – Utilização de recursos a que tem direito acima do máximo;
  - Abusiva – Utilização abusiva de recursos a que não tem direito.
4. **Impedimento de prestação de serviço**, da designação inglesa *Denial of Service* (DoS)  
Um DoS é um caso extremo do anterior, na medida

em que o atacante opera apenas com a intenção de impedir a utilização dos recursos a quem estes pertencem ou estão afetos.

### 5. Vandalismo

Um caso extremo de DoS, já que para além do atacante não tentar tirar qualquer partido, também só incorre nesta prática pela destruição causada, mas sem motivação dirigida.

Há duas origens possíveis para atividades ilícitas:

1. Sujeitos que pertencem à organização proprietária do sistema computacional atacado;
2. Sujeitos exteriores a essa organização.

Apesar do risco associado aos primeiros ser maior que o risco associado aos segundos, o peso estatístico esmagador do número de utilizadores da Internet tende a colocá-los quase em pé de igualdade. O segundo tipo de sujeitos advém de um universo mais heterogéneo: uma fonte maior de imaginação e engenho humano.

### Como se resolve?

Nunca totalmente e, na maior parte das vezes, com alguma dificuldade. É precisamente neste aspeto que esta cadeira se centra.

## 3.2 Motivação para Estudar Criptografia

### *Motivation for Studying Cryptography*

A maior motivação para estudar Criptografia, que compreende a primeira parte do curso, é que esta **está presente** inerentemente **em muitas atividades da era moderna**:

- A **Internet** é um dos ambientes onde a Criptografia mais encontra aplicação nos dias de hoje, estando em clara expansão, e instigando naturalmente o desenvolvimento das técnicas desta ciência. Todos os utilizadores da Internet já usaram, invariavelmente, diversos mecanismos criptográficos:
  - O tráfego web pode ser protegido contra escutas e alterações maliciosas usando o **Hyper-Text Transfer Protocol Secure (HTTPS)**, que cifra e autentica os dados;
  - O tráfego da rede **wireless local é cifrado e autenticado** entre cada utilizador da rede e o ponto de acesso, para que uns utilizadores não possam ver o tráfego dos outros.
- As organizações e empresas internacionais, bem como os utilizadores mais precavidos, necessitam que alguns dos **dados que manuseiam em sistemas computacionais sejam protegidos contra roubo, investigação, roubo ou alteração**, pelo que recorrem à cifra e cifra autenticada dos ficheiros em

discos (e.g., usando *Encrypting File System (EFS)* ou *TrueCrypt*<sup>1</sup>).

- A **distribuição, controlo e proteção de conteúdos multimédia** (e.g., via *Digital Versatile Disc* ou *Digital Video Disk (DVD)*, Blu-ray, Jogos de Video) só é possível através de mecanismos da criptografia moderna, sobretudo para dificultar a sua cópia e distribuição não autorizada (pirataria).
- A distribuição de conteúdos em redes *Peer-to-Peer (P2P)* (e por vezes a própria pirataria) recorre à criptografia como forma de proteção de quem a utiliza e em mecanismos de controlo da integridade dos dados.
- A **identificação de utilizadores e a assinatura digital** com cartões de identificação pessoais só é possível graças à Criptografia moderna. A própria assinatura digital é considerada mais forte do que a assinatura manual.

O estudo da Criptografia apresenta-se como uma **tarefa difícil**, mas muito **aliciante**. Enquanto que todos os especialistas na área defendem que **o desenvolvimento de novos algoritmos ou sistemas criptográficos não é para todos**, também é certo dizerem que é necessário compreender bem a maior parte dos sistemas criptográficos para produzirem aplicações, sistemas e protocolos seguros e robustos. Por outras palavras, não se deve tentar desenvolver o próprio sistema ou algoritmo, **mas deve saber-se implementar corretamente os já existentes**. Esta área é, portanto, fulcral para engenheiros informáticos e para técnicos de sistemas.

## 3.3 Motivação para Estudar Vulnerabilidades e Segurança em Sistemas Distribuídos

### *Motivation for Studying Vulnerabilities and Security in Distributed Systems*

Para tentar dar uma ideia do quão necessário é estudar e formar profissionais na área da segurança informática, e na área específica das vulnerabilidades e segurança em sistemas distribuídos, foram copiados para aqui alguns recortes da imprensa nacional e internacional dos dias 16 de fevereiro de 2022, 28 de Agosto de 2018, 31 de Julho e de Agosto, e 19 de Agosto de 2014.

**Site do Parlamento. Passes de acesso circulavam na dark web e internet foi bloqueada para evitar ataque de larga escala** – “Alerta partiu de fora: PJ ou Secretas, as entidades que vigiam hackers, detetaram partilha de “credenciais administrativas” na internet. Parlamento fechou site para evitar ataque de larga escala.”

Fonte: <https://observador.pt/especiais/site-do-parlamento-passes-de-acesso-circulavam-na-dark-web-e-internet-foi-bloqueada-para-evitar-ataque-de-larga-escala/>

<sup>1</sup> Software para cifragem de ficheiros gratuito e de código aberto, para Windows 7/Vista/XP, Mac OS X, e Linux, cuja idoneidade foi posta em causa por notícias acerca da existência de *backdoors* em 2014.



### Hackers russos atacam segredos do Estado português – “(...)

*Ciberespões de várias nacionalidades suspeitos de entrarem na rede do ministério dos negócios estrangeiros. Sistemas informáticos vulneráveis a novas ameaças.”*

Fonte: <http://visao.sapo.pt/revistas/2018-08-29-Edicao-1330>

### AntiVirus Firm BitDefender Hacked; Turns Out Stored Passwords Are UnEncrypted – “(...)

*One of the most popular and much-respected Antivirus and computer security firms 'BitDefender' has recently been hacked and has had a portion of its customer data leaked. The Data Breach in BitDefender is incredibly embarrassing for the security firm, not because the company failed to prevent its customers data from hackers, but because the Security company failed to encrypt its customers most sensitive data.”*

Fonte: <http://thehackernews.com/2015/07/bitdefender-hacked.html>

### Using Samsung's Internet-Enabled Refrigerator for Man-in-the-Middle Attacks – “(...)

*Whilst the fridge implements SSL, it FAILS to validate SSL certificates, thereby enabling man-in-the-middle attacks against most connections. This includes those made to Google's servers to download Gmail calendar information for the on-screen display. So, MITM the victim's fridge from next door, or on the road outside and you can potentially steal their Google credentials.”*

Fonte: [https://www.schneier.com/blog/archives/2015/08/using\\_samsungs\\_.html](https://www.schneier.com/blog/archives/2015/08/using_samsungs_.html)

### Hackers hit 200 hospitals in US, steal data on 4.5 million patients – 4 hospitals hit in Washington –

*“Community Health Systems, which operates 206 hospitals across the United States, announced on Monday that hackers recently broke into its computers and stole data on 4.5 million patients.*

*Hackers have gained access to their names, Social Security numbers, physical addresses, birthdays and telephone numbers.”*

Fonte: <http://q13fox.com/2014/08/18/hackers-hit-200-hospitals-in-us-steal-data-on-4-5-million-patients-4-hospitals-in-washington/>

### ZeroLocker Ransomware Poses as Crypto-Malware Decryption Tool – “Unlike most crypto-malware ransomware announcing the encryption of the files on the computer and asking for a fee to unlock them, the new ZeroLocker claims to be a decryption tool that can rescue the data locked by a different threat, if a license of the program is purchased.”

*Unlike most crypto-malware ransomware announcing the encryption of the files on the computer and asking for a fee to unlock them, the new ZeroLocker claims to be a decryption tool that can rescue the data locked by a different threat, if a license of the program is purchased.”*

Fontes: <http://news.softpedia.com/news/ZeroLocker-Ransomware-Poses-as-Crypto-Malware-Decryption-Tool-455412.shtml>

Estes 6 recortes foram retirados de *feeds* bastante ativos de notícias da especialidade, e não correspondem a incidentes isolados no tempo, o que demonstra bem o **dinamismo e a gravidade das atividades nesta área.**<sup>2</sup>

<sup>2</sup>Para mais detalhe na situação atual da ciber-segurança a nível

Os(as) engenheiros(as) e técnicos(as) responsáveis pela segurança numa organização são normalmente **pe-soas mais especializadas** e, por isso, tipicamente **com salário acima da média**. Para além disso, esta é uma **área onde o emprego está a aumentar rapidamente** e onde há relativamente pouca concorrência. O **ciber-espaço é hoje considerado um palco de guerra**, sendo **usado** inclusive por divisões e **equipas governamentais ou empresas especializadas** para ganhar vantagem estratégica e conduzir espionagem remotamente. Dada a rapidez na evolução e imersão no mercado das novas tecnologias, nomeadamente dispositivos móveis e computação na nuvem, **esta é uma área que não conhecerá um declínio nos próximos anos**, sendo talvez uma das que conhecerá maior aumento na procura de especialistas.

## 3.4 Terminologia e Conceitos Básicos

### Terminology and Basic Concepts

Neste secção dá-se a definição de alguns conceitos e termos básicos do jargão da segurança informática, que por vezes são usados de modo errado por pessoas não especializadas na área.

### 3.4.1 Criptografia Moderna

**Texto-limpo:** no âmbito da Criptografia, texto-limpo, da designação inglesa *plaintext* ou, por vezes, *cleartext*, define a informação que determinada entidade (transmissora) quer enviar para outra ou para ela mesma no futuro (recetor). O transmissor e o recetor podem ser a mesma entidade, já que, e.g., também se cifram ficheiros agora (transmitir) para os decifrar no futuro.

**Cifra ou Esquema Criptográfico:**<sup>3</sup> uma cifra é tipicamente um conjunto de dois algoritmos eficientes, em que um é usado para transformar o **texto-limpo** numa mensagem com significado obscurecido – o **criptograma** – e outro faz a operação inversa, mediante a especificação de uma **chave de cifra**. A operação de cifragem é normalmente aleatorizada, enquanto que a de decifra é determinística.

Diz-se cifrar e decifrar, ou encriptar e desencriptar, mas não se diz criptografar ou descriptografar nem criptar ou deciptar.

**Criptograma:** o criptograma, da designação inglesa *cyphertext*, é o resultado da operação de cifra e dele pode ser recuperada a mensagem original em texto-limpo mediante decifra e apresentação da chave de cifra. O criptograma pode ser constituído pela mensagem

mundial, recomenda-se a leitura de: Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, and Pedro R. M. Inácio, "A Quick Perspective on the Current State in Cybersecurity," in *Emerging Trends in Information and Communication Technologies Security*, Babak Akhgar, Hamid R. Arabnia (Eds.) Elsevier (Morgan Kaufmann), September, 2013.

<sup>3</sup>A definição formal será dada na próxima aula.



obscurecida apenas, mas é comum que seja constituído por mais elementos, nomeadamente códigos de autenticação da origem da informação.

**Chave de cifra:** a chave de cifra, com designação inglesa *encryption key* ou apenas *key* é o parâmetro de segurança dos algoritmos de cifra e decifra. A chave de cifra é normalmente o elemento que introduz aleatorização na operação de cifra.

Chave de cifra é diferente de palavra-passe (*password*).

**Sistema criptográfico:** especificação das operações de inicialização; cifra e decifra.

**Modelo de Ataque:** na Criptanálise, os modelos de ataques compreendem uma classificação para os possíveis ataques baseada na quantidade de informação a que um criptanalista tem acesso enquanto tenta quebrar um esquema criptográfico, nomeadamente obter o texto-limpo a partir do criptograma.

**Ataque:** o ataque propriamente dito corresponde ao comprometimento dos objetivos da técnica criptográfica (e.g. obtenção do texto limpo sem conhecimento da chave; descobrir a chave utilizada; etc.), e à especificação dos passos que levaram a esse comprometimento.

**Atacante ou Adversário:** entidade que personifica quem pretende comprometer os objetivos da técnica criptográfica.

### 3.4.2 Segurança em Redes e Sistemas Distribuídos

**Firewall:** uma *firewall* é um sistema ou um conjunto de módulos de *software* relacionados, localizados num *gateway* da rede ou nos nós terminais, que protege e controla o acesso aos recursos de uma rede privada ou de uma máquina anfitriã.

**Hacker:** nome pelo qual é conhecido um indivíduo habilidoso na arte de atacar sistemas computacionais.

*A "computer hacker," then, is someone who lives and breathes computers, who knows all about computers, who can get a computer to do anything. Equally important, though, is the hacker's attitude. Computer programming must be a hobby, something done for fun, not out of a sense of duty or for the money. (It's okay to make money, but that can't be the reason for hacking.)*

Fonte: <http://www.cs.berkeley.edu/bh/hacker.html>

**White Hat:** designação normalmente atribuída aos *hackers* éticos ou a um especialista em segurança informática que é normalmente e particularmente bom em testes de penetração (*pentesting*) e em métodos de teste de segurança. A conotação dada a um *White Hat* é positiva, no que diz respeito à utilização que faz do seu conhecimento e especialidade, e contrapõe-se a *Black Hat*.

**Black Hat:** um *hacker* que viola a segurança de sistemas computacionais sem razões que vão para além do regozijo próprio e malícia, e que tipicamente penetram

redes ou sistemas para destruir dados ou causar a negação de serviços. É este tipo de *hackers* que forma o estereótipo que é normalmente caricaturado na cultura popular, nomeadamente filmes.

**Script kiddie:** nome pelo qual é conhecido o indivíduo que efetua atos ilícitos num sistema computacional por brincadeira, benefício ou regozijo próprio, e que normalmente não partilha dos conhecimentos técnicos de um *hacker*. O termo *script* deriva do facto de estes recorrerem ao plano de ação e a ferramentas automáticas de exploração de vulnerabilidades feitas pelos verdadeiros especialistas, enquanto que o termo *kiddie* aponta diretamente para a imaturidade, falta de conhecimentos e experiência na área.

**Sistema de Detecção de Intrusões:** conhecido sobretudo pela sua designação inglesa, Intrusion Detection System (IDS), é um sistema ou software que monitoriza e tenta detetar atividades maliciosas ou violações à política de segurança em sistemas computacionais ou redes de computadores, produzindo relatórios para o administrador do sistema. Alguns IDSs deste tipo podem tentar impedir intrusões ou tomar outras medidas, embora tal não seja esperado de sistemas com esta designação.

**Sistema de Detecção e Prevenção de Intrusões:** para além das funções realizadas pelos IDSs, estes sistemas servem também para identificar problemas nas políticas de segurança, documentar ameaças atuais e desmotivar os indivíduos a violar essas políticas. Estes sistemas também podem implementar técnicas de resposta, que podem inclusive possibilitar o bloqueio dos ataques enquanto ocorrem, por exemplo através da reconfiguração da *firewall* da rede.

**Vulnerabilidade:** característica do sistema que o torna vulnerável a determinados ataques.

**Exploit:** um *exploit* é um pacote de *software* construído com o propósito de tirar vantagem de uma dada vulnerabilidade.

**Ataque:** conjunto de passos executados com o intuito de explorar uma vulnerabilidade e que permitem concretizar uma ação ilícita, nomeadamente explorar uma vulnerabilidade para obter acesso a dados que não pertencem ao atacante.

**Risco ou Ameaça:** é o dano que pode resultar da execução bem-sucedida de um ataque. É a noção de risco que permite quantificar a necessidade de aplicar mecanismos de segurança informática antes da ocorrência de incidentes de segurança.

**Defesa:** conjunto de políticas e mecanismos desenhados, concretizados e implantados para (i) diminuir o número e severidade das vulnerabilidades; (ii) detetar e contrariar / anular ataques futuros ou atuais; e (iii) minimizar os riscos decorrentes de ataques bem-sucedidos.

**Políticas de Segurança:** definem o foco da segurança e o que precisa ser garantido nesse aspeto num sis-

tema, organização ou entidade. Em termos de sistemas, esta política contempla limitações na utilização ou instalação de aplicações, acesso ou distribuição de ficheiros, e acesso a sistemas, serviços ou programas externos. A política de segurança é implementada através de **mecanismos de segurança** (e.g., mecanismos de controlo de acesso numa *firewall*) e vigora no universo de recursos (máquinas, redes, impressoras, etc.) e pessoas que é chamado de **domínio de segurança**.

**Vírus de Computador:** é um programa que se pode replicar e espalhar de computador para computador, mas com intervenção humana (e.g., o utilizador aceita abrir um ficheiro executável que vem anexo a um *e-mail*). O termo *vírus* é usado erradamente para referir outros tipos de *malware*, nomeadamente *adware* e *spyware* que não apresentam a funcionalidade da reprodutibilidade.

**Worm:** é um programa que é capaz de se replicar e disseminar sozinho (i.e., potencialmente sem intervenção humana), através da exploração de vulnerabilidades em sistemas interligados em rede ou de gravação e leitura de meios amovíveis (e.g., Universal Serial Bus (USB) PEN). Contrariamente aos vírus de computador, não precisa acoplar-se a outros programas para se disseminar.

**Cavalo de tróia:** os *trojan horses*, designação inglesa pela qual são mais conhecidos, são um tipo de *malware* que se apresenta como um ficheiro ou programa legítimo com o propósito de fornecer acesso não autorizado, e tipicamente remoto, ao sistema computacional infetado. Os cavalos de tróia não tentam normalmente injetar-se automaticamente noutros ficheiros para se espalhar. Os atacantes preferem introduzi-los em ficheiros que são descarregados da Internet, como por exemplo instaladores de jogos online ou aplicações orientadas para a Internet. As redes P2P são também bastante utilizadas para este fim.

### **Offtopic**

**Q1.: Quem já pensou em como se guardam os dados na Dropbox? I.e., os empregados da Dropbox têm acesso aos vossos dados?**

**Q2.: Quando usam o gmail ou o outlook para enviar um mail, a mensagem passa exatamente por onde?**

**Q3.: Será que o(a) colega do lado consegue ver os dados que o seu computador transmite pelo ar?**

**Q4.: E se alguém retirar o cabo do ponto de acesso mais próximo, e aí colocar uma escuta que comprou por 50 euros na Internet?**

**Q5.: Será que uma equipa de hackers podia mudar o aspeto da página da UBI (<http://www.ubi.pt>) apenas pelo campo de pesquisa que a primeira página disponibiliza?**

**Nota:** o conteúdo exposto na aula e aqui contido não é (nem deve ser considerado) suficiente para total entendimento do conteúdo programático desta unidade curricular e deve ser complementado com algum empenho e investigação pessoal.