

**BEM VINDOS!**

## Introdução & Conceitos de Segurança de Software

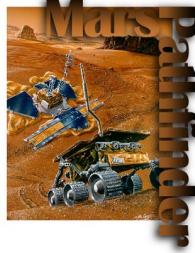
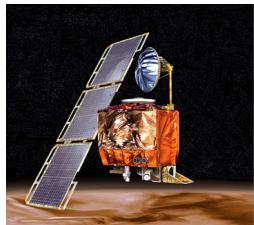
**Parte I: Enquadramento e Protecção**

Segurança de Software  
2019  
Nuno Santos

**TÉCNICO LISBOA**

### O software actual tem deficiências

- ▶ NASA Mars Climate Orbiter
  - ▶ Falhou devido a um bug de conversão de unidades (\$165 million)
- ▶ NASA Mars Pathfinder
  - ▶ Parou por várias horas por causa de um bug de inversão de prioridades (\$265 million)



▶ 2 SS - Nuno Santos 2019

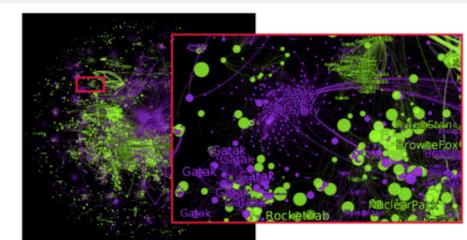


## Quando se tornam vulnerabilidades?

- ▶ Quando um **atacante** tira partido dessas deficiências para atingir um fim malicioso

### Study: Financial Firms Hit Hard By Targeted Attacks

POSTED BY: PAUL JUNE 25, 2018 12:16 · 0 COMMENTS



A graphic shows threats targeting financial industry organizations vs. non financial services focused attacks in purple. (Image courtesy of Websense/Raytheon.)

In-brief: A new report from the firm Websense finds that financial services firms are being hit hard by cyber attacks, including targeted attacks aimed at luring employees into installing malicious software on corporate networks.

▶ 3

SS - Nuno Santos

2019



## Mais notícias do mundo real

**COMPUTERWORLD**

Home > Vertical IT > Healthcare IT

NEWS

**More than 80% of healthcare IT leaders say their systems have been compromised**

Credit: Thinkstock

Only half of IT managers feel they are adequately prepared to prevent future attacks

Infidelity site Ashley Madison hacked as attackers demand total shutdown

Site's hackers claim 37m personal records have been stolen from notorious dating site, with Cougar Life and Established Men also compromised



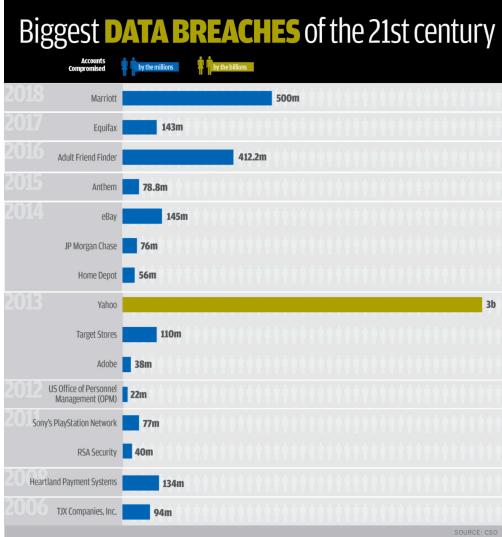
▶ 4

SS - Nuno Santos

2019



## Casos de roubo de dados



▶ 5

SS - Nuno Santos

2019



## Porquê? Qual a motivação dos atacantes?

- ▶ **Roubo** – homebanking, cartões de crédito, extorsão...
  - ▶ <http://www.seguranca-informatica.net/2013/07/kins-novo-cavalo-de-troia-ameaca-bancos.html>
- ▶ **Espionagem** – entre as nações, espionage industrial
  - ▶ <http://www.seguranca-informatica.net/2013/08/xkeyscore-um-motor-de-busca-para.html>
- ▶ **Guerra** – Estonia, Georgia,...
  - ▶ <http://www.seguranca-informatica.net/search/label/ciber-guerra>
- ▶ **Terrorismo**
  - ▶ <http://www.seguranca-informatica.net/2013/03/ataques-instituicoes-financeiras.html>

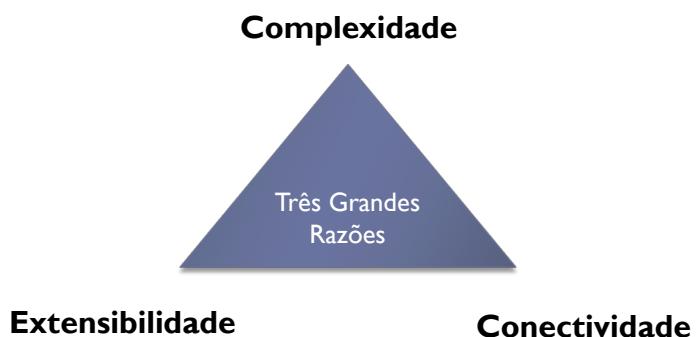
▶ 6

SS - Nuno Santos

2019



## Porque existem vulnerabilidades no software?



▶ 7

SS - Nuno Santos

2019



## Complexidade do software

- ▶ Ataques exploram erros no código chamados **bugs**
  - ▶ Estimativas de 5-50 bugs por 1000 linhas de código
- ▶ O software actual é **muito complexo!**
  - ▶ Exemplos:
    - ▶ Windows 10: > 50 Mloc
    - ▶ Linux Kernel 3.6: ~16 Mloc
- ▶ Complexidade do software tende a aumentar

▶ 8

SS - Nuno Santos

2019



## Extensibilidade do software

- ▶ O software actual é por natureza **extensível**
  - ▶ Device drivers, plug-ins, módulos, apps, etc...
  - ▶ Máquinas virtuais e código móvel (JavaScript, Java, etc.)
  - ▶ Combinação de componentes e formas de execução (web apps)
- ▶ Difícil garantir **segurança global** de todos os componentes
- ▶ Mais susceptível a incorporar **software malicioso**
  - ▶ Vírus, cavalos de tróia, vermes, etc.

▶ 9

SS - Nuno Santos

2019



## Conectividade dos sistemas

- ▶ **Internet** (PCs, smartphones, tablets, etc.)
  - ▶ Pequenas falhas podem propagar-se em grande escala
    - ▶ Difusão de malware, como Melissa, ILOVEYOU, etc.
    - ▶ Ataques de DDoS
  - ▶ Vulnerabilidades expostas remotamente
  - ▶ Ataques podem ser lançados remotamente
- ▶ **Internet das coisas** (Internet of Things)



▶ 10

SS - Nuno Santos

2019



## Futuro (próximo) do software

- ▶ Mais componentes
- ▶ Mais frameworks, mais combinação de código
- ▶ Mais wireless
- ▶ Mais dispositivos móveis e “coisas” embebidas
- ▶ Mais distribuição
- ▶ Mais código móvel

**Mais complexidade, extensibilidade e connectividade**

► 11

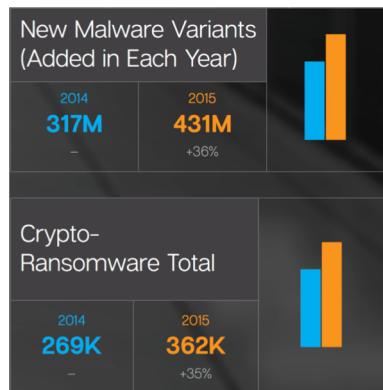
SS - Nuno Santos

2019

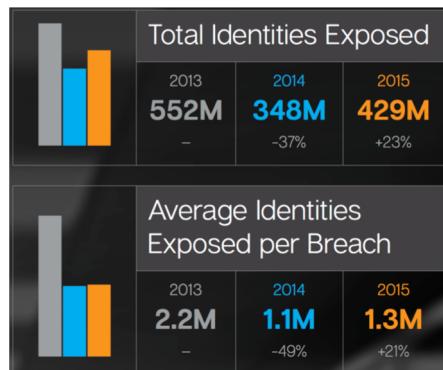


## Alguns números de 2015

### ▶ Malware



### ▶ Roubo de identidade



Source: Symantec Internet Security Threat Report 2016, Vol. 21, Apr. 2016

► 12

SS - Nuno Santos

2019



## Alguns números de 2015

### ▶ Web

Scanned Websites with Vulnerabilities ...

2013	2014	2015	
<b>77%</b>	<b>76%</b>	<b>78%</b>	-1% pts
-	-	+2% pts	
... Percentage of Which Were Critical			
<b>16%</b>	<b>20%</b>	<b>15%</b>	+4% pts
-	-	-5% pts	

### ▶ Mobile

New Android Mobile Malware Families

2013	2014	2015
<b>57</b>	<b>46</b>	<b>18</b>
-	-19%	-61%

New Android Mobile Malware Variants

2013	2014	2015
<b>3,262</b>	<b>2,227</b>	<b>3,944</b>
-	-32%	+77%

Source: Symantec Internet Security Threat Report 2016, Vol. 21, Apr. 2016

▶ 13

SS - Nuno Santos

2019



## Principais objectivos desta cadeira

- ▶ Abordar os problemas mais comuns de segurança em software, bem como a sua origem, analizando criticamente conceitos e técnicas de codificação segura, de gestão de riscos em segurança, validação e verificação
- ▶ Proporcionar conhecimentos sobre as formas mais adequadas de tornar o software seguro e resiliente ao longo de todo o seu processo de desenvolvimento

▶ 14

SS - Nuno Santos

2019



## Organização

► Professor e contacto:

- Nuno Santos  
[nuno.m.santos@tecnico.ulisboa.pt](mailto:nuno.m.santos@tecnico.ulisboa.pt)

► Site da disciplina:

- <https://nuno-santos.github.io/acite2019>

► Duas componentes teórica e laboratorial (3h/dia)

- Aulas teóricas de 1h
- Aulas laboratoriais de 2h

► 15

SS - Nuno Santos

2019



## Programa da cadeira

► **Parte I: Enquadramento e protecção (2 aulas)**

- Conceitos de segurança de software, mecanismos básicos de segurança

► **Parte II: Vulnerabilidades (3 aulas)**

- Buffer overflows, corridas e validação de entradas, vulnerabilidades na web e em bases de dados

► **Parte III: Técnicas de protecção (4 aulas)**

- Auditoria e teste de software, análise estática de código, protecção dinâmica, validação e codificação

► **Parte IV: Tópicos avançados (1 aula)**

- Trusted computing

► 16

SS - Nuno Santos

2019



## Componente laboratorial

- ▶ **Preparação do laboratório (1 aula)**
- ▶ **Guia Lab I: Vulnerabilidades buffer overflow (4 aulas)**
  - ▶ Tarefa 1: Programação em ambiente Linux
  - ▶ Tarefa 2: Organização de memória
  - ▶ Tarefa 3: Vulnerabilidades buffer overflow
  - ▶ Tarefa 4: Exploração de buffer overflow
- ▶ **Guia Lab II: Ataques cross-site scripting (2 aulas)**
  - ▶ Tarefa 1: Introdução a aplicações Web
  - ▶ Tarefa 2: Ataques XSS
- ▶ **Guia Lab III: Ataques SQL injection (2 aulas)**
  - ▶ Tarefa 1: Introdução a bases de dados SQL
  - ▶ Tarefa 2: Ataques SQL injection

▶ 17

SS - Nuno Santos

2019



## Avaliação da cadeira

**Nota final = exercícios laboratório + exame**

- ▶ **Exercícios laboratório (50%)**
  - ▶ Realizado em grupos
  - ▶ Exercícios feitos na aula e avaliados pelo professor na aula
  - ▶ Nota laboratórios = 50% Guia Lab 1 + 25% Guia Lab2 + 25% Guia Lab3
- ▶ **Exame (50%)**
  - ▶ Sobre os conteúdos apresentados nas aulas teóricas
  - ▶ 19 de Julho

▶ 18

SS - Nuno Santos

2019

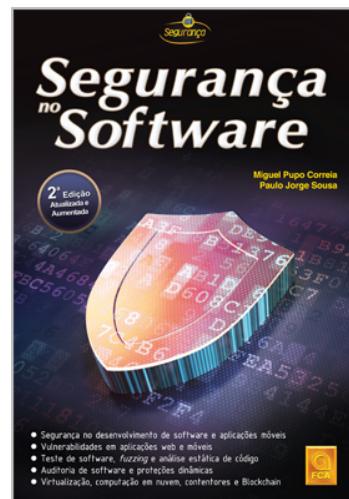


## Bibliografia

- ▶ Principal: Slides das teóricas

- ▶ Livro: [Correia17]

▶ Miguel Pupo Correia e Paulo Jorge Sousa, Segurança no Software, 2ª edição, FCA, 2017



▶ 19

SS - Nuno Santos

2019



## Programa

semana		aulas teóricas (1 hora)				aulas lab (2 horas)	
#	datas	dia	aula #	tópico	aula #	tópico	
I	8-12 Julho	8 Julho	1	Parte I: Introdução e Conceitos de Segurança de Software	1	Preparação dos Laboratórios	
		9 Julho	2	Parte I: Mecanismos Básicos de Segurança: Sistemas Operativos e Linguagens de Programação	2	Guia Lab I: Vulnerabilidades Buffer Overflows - Tarefa 1: Programação em Ambiente Linux	
		10 Julho	3	Parte II: Vulnerabilidades em Software: Buffer Overflows	3	Guia Lab I: Vulnerabilidades Buffer Overflows - Tarefa 2: Organização de Memória	
		11 Julho	4	Parte II: Vulnerabilidades em Software: Corridas e Validação de Entradas	4	Guia Lab I: Vulnerabilidades Buffer Overflows - Tarefa 3: Vulnerabilidades Buffer Overflow	
		12 Julho	5	Parte II: Vulnerabilidades na Web e em Bases de Dados	5	Guia Lab I: Vulnerabilidades Buffer Overflows - Tarefa 4: Exploração de Buffer Overflows	
2	15-19 Julho	15 Julho	6	Parte III: Auditoria e Teste de Software	6	Guia Lab II: Ataques Cross-Site Scripting - Tarefa 1: Introdução a Aplicações Web	
		16 Julho	7	Parte III: Análise Estática de Código	7	Guia Lab II: Ataques Cross-Site Scripting - Tarefa 2: Ataques XSS	
		17 Julho	8	Parte III: Proteção Dinâmica	8	Guia Lab III: Ataques Cross-Site Scripting - Tarefa 1: Introdução a Bases de Dados SQL	
		18 Julho	9	Parte III: Validação e Codificação	9	Guia Lab III: Ataques Cross-Site Scripting - Tarefa 2: Ataque SQL Injection	
		19 Julho	10	Parte IV: Tópico Avançado e Conclusões		Exame	

▶ 20

SS - Nuno Santos

2019

## Conceitos de segurança de software

21

SS - Nuno Santos

2019



## Três atributos de segurança

### ▶ Confidencialidade

- ▶ Dados não podem ser revelados a entes não autorizados

### ▶ Integridade

- ▶ Dados não podem ser modificados por entes não autorizados

### ▶ Disponibilidade

- ▶ O sistema deve estar sempre pronto a oferecer o serviço

▶ 22

SS - Nuno Santos

2019



## Vulnerabilidade + Ataque => Intrusão

### ► Vulnerabilidade

- ▶ Deficiência num sistema (sw/hw) que possa ser alavancado para comprometer uma política de segurança
- ▶ Existem vários tipos de vulnerabilidades num sistema

### ► Ataque

- ▶ Acções por agente malicioso que tiram partido de vulnerabilidades
- ▶ Tipicamente activados por código malicioso chamado exploit



### ► Intrusão

- ▶ Permite o agente malicioso violar a política de segurança e ganhar acesso ao sistema

► 23

SS - Nuno Santos

2019



## Vulnerabilidades Zero-Day

### ► Vulnerabilidades que não são conhecidas publicamente

At least three zero-day exploits have been uncovered so far among the trove of data leaked by the attacker who breached Hacking Team. Hacking Team buys zero-day exploits in order to install its spyware, known as RCS, on

Hacking Team hack (!) 2015: <http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/>

► 24

SS - Nuno Santos

2019



## Tipos de vulnerabilidades

### ► Vulnerabilidades de projeto

- ▶ Causado durante a fase de concepção do software

### ► Vulnerabilidades de implementação

- ▶ Produzido durante a fase de codificação do software (bugs)

### ► Vulnerabilidades operacionais

- ▶ Causado pelo ambiente no qual o software se executa ou relacionado com a sua configuração

► 25

SS - Nuno Santos

2019



## Fontes de informação sobre vulnerabilidades

### ► Repositório de vulnerabilidades recentes (CERTs)

- ▶ <http://www.cert.pt/>    <http://www.us-cert.gov/>

### ► Classificação de vulnerabilidades

- ▶ Common Weakness Enumeration (CWE)
- ▶ <http://cwe.mitre.org/>    <http://cwe.mitre.org/data/>

### ► Catálogo de vulnerabilidades

- ▶ Common Vulnerabilities and Exposures (CVEs)
- ▶ <http://cve.mitre.org/> - Example: [CVE-2014-0160](#) (Heartbleed)

### ► Vulnerabilidades recentes: Bugtraq

- ▶ <http://www.securityfocus.com/archive/1>

► 26

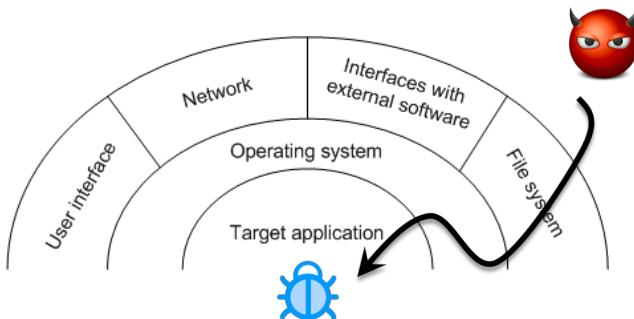
SS - Nuno Santos

2019



## Superfície de ataque

- ▶ Ataques acontecem através de uma **interface** chamada superfície de ataque



- ▶ Compreender qual é a superfície de ataque é a primeira medida para avaliar a segurança de software

▶ 27

SS - Nuno Santos

2019



## Malware

- ▶ Todo o software malicioso concebido intencionalmente para causar dano num computador, servidor, ou rede

- ▶ Causa dano depois de ter sido implantado ou introduzido de alguma forma no computador alvo
  - ▶ Pode assumir a forma de código executável, scripts, etc.

- ▶ **Como se propaga? Qual o vector de ataque?**
- ▶ **Que danos causa?**



▶ 28

SS - Nuno Santos

2019



## Vermes, virus, cavalos de troia

### ► Verme (worm)

- ▶ Programa infectado com código malicioso que se autoreplica

### ► Virus

- ▶ Programa malicioso que se propaga anexo a software legítimo ou num meio de armazenamento

### ► Cavalo de tróia (trojans)

- ▶ Programa malicioso dissimulado de programa legítimo executado pela vítima (forma de engenharia social)

► 29

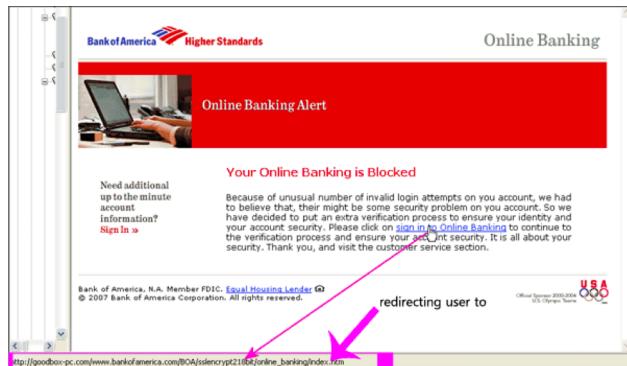
SS - Nuno Santos

2019



## Phishing

- ▶ Acto de enviar um mail não solicitado alegando falsamente ter sido enviado por entidade confiável
  - ▶ Normalmente é feito para obter acesso a informação pessoal da vítima



► 30

SS - Nuno Santos

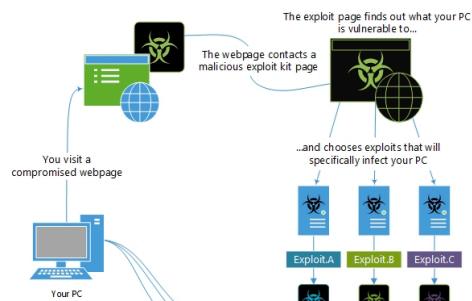
2019



## Drive-by download

- ▶ Páginas web contêm malware tal que, basta que o utilizador com browser vulnerável visite esse site para ficar infectado
- ▶ Vulnerabilidade pode estar no browser, ActiveX engine, JVM, Flash Player, PDF reader,...

- ▶ **Exploit kits** são conjuntos de ferramentas que contêm coleções de exploits



▶ 31

SS - Nuno Santos

2019



## Ransomware

- ▶ Malware que cifra discos ou bases de dados e pede por um resgate
- ▶ Muitas vezes o pagamento é feito usando bitcoin



▶ 32

SS - Nuno Santos

2019



## Backdoors, Rootkits, Bots

### ▶ Backdoor

- ▶ Permite ao atacante voltar a contactar a máquina da vítima

### ▶ Rootkit

- ▶ Conjunto de programas que tem por objectivo esconder a presença de malware na vítima

### ▶ Bot

- ▶ Malware controlado remotamente por um servidor e que permite efectuar um conjunto diversificado de ataques

▶ 33

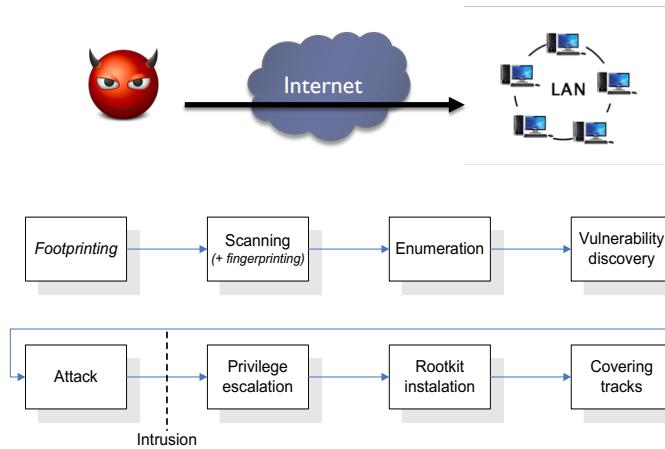
SS - Nuno Santos

2019



## Ataque manual

### ▶ Exemplo: infiltração numa rede de computadores



▶ 34

SS - Nuno Santos

2019



## Sumário de perspectivas sobre ataques

- ▶ **Vector de ataque:** vários sentidos
  - ▶ Tipo de vulnerabilidade (buffer overflow, SQL injection,...)
  - ▶ Modo de ataque (virus, worm,...)
- ▶ **Frequentemente os ataques envolvem malware**
  - ▶ Virus, worms, bots, rootkits, trojans,...
- ▶ **Pode ser técnicos vs. por engenharia social**
- ▶ **Podem ser direcionados ou não**
- ▶ **Podem ser manuais ou automatizados**
  - ▶ Separação não é muito óbvia (ataques manuais nunca são inteiramente)

▶ 35

SS - Nuno Santos

2019



## Conclusões

- ▶ Os sistemas são concebidos para oferecerem determinadas propriedades de segurança, em termos de confidencialidade, integridade, e disponibilidade
- ▶ Essas propriedades podem ser comprometidas pela existência de vulnerabilidades no software
- ▶ Essas vulnerabilidades podem ser exploradas por atacantes utilizando malware e sob formas variadas

▶ 36

SS - Nuno Santos

2019



## Referências e próxima aula

### ► Bibliografia

- ▶ [Correia17] Capítulo 1

### ► Próxima aula

- ▶ Mecanismos básicos de segurança