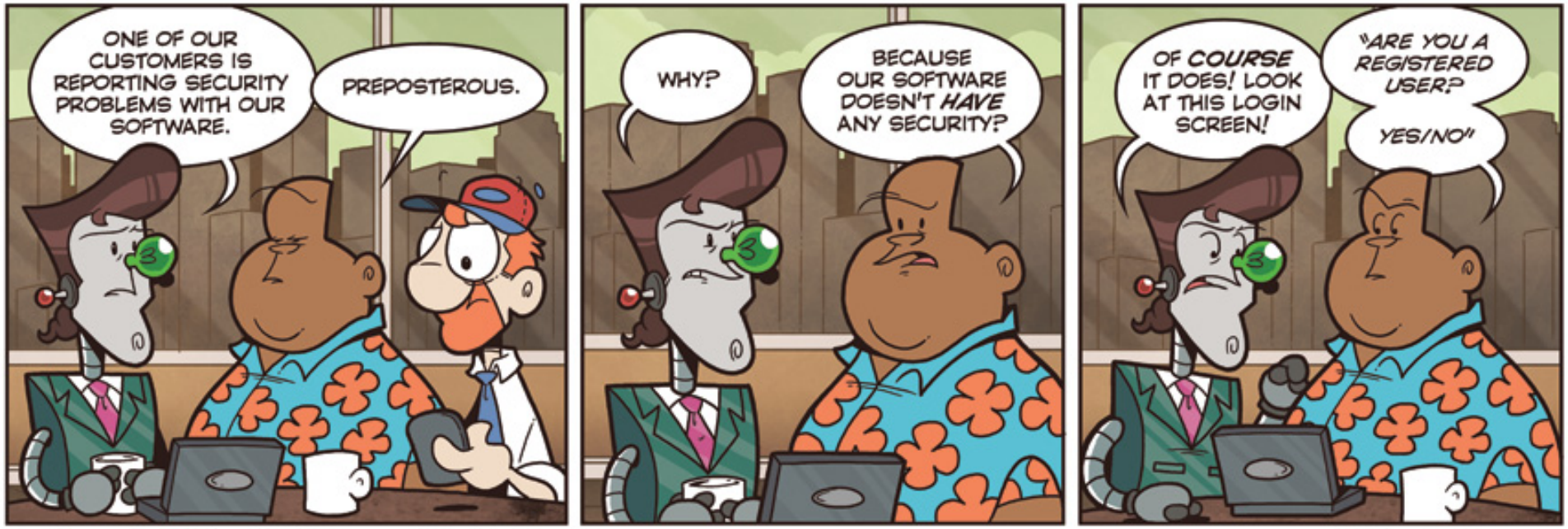
# INTRODUCTION TO THE SOFTWARE SECURITY COURSE

Software Security

Pedro Adão 2022/23

(with Ana Matos & Miguel Pupo Correia)

TÉCNICO LISBOA






NotInventedHere.com

# Teaching staff

- Pedro Adão - *coordinator + VSSD lectures + labs*
  - Office at Alameda – Office 3, Informática 3
  - Office at IST TagusPark – 2N3.3

- Ana Matos - *coordinator + LBS lectures + labs*
  - Office at Alameda – TBD
  - Office at IST TagusPark – 2N3.11

- Afonso Ribeiro - *labs*
  - Office at Alameda – TBD

# Objectives

- to give the students the mental tools necessary to understand the problem of the security of the computer and its software, vis-à-vis the security of the communication or distributed system

- to give a deep insight into the security problems in modern software systems, and present paradigms, models and tools to tackle these problems

# Program overview

- Principles of Computer Security
- Software Vulnerabilities
- Development of Secure Software
- Language-Based Security

# Program in detail

- Principles of Computer Security
  - Basic properties and concepts; Software security design principles.
- Software Vulnerabilities
  - Conventional applications (buffer overflows, race conditions); Web applications and databases; Mobile applications.
- Development of Secure Software
  - Software auditing; Validation and encoding.
- Language-Based Security
  - Information flow security; Security policies and properties; Program analysis and verification for security (taint checking, type checking, monitoring, symbolic execution).

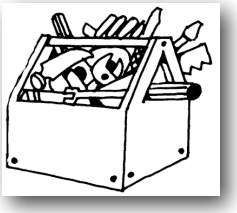
# Language-Based Security

*techniques based on programming language theory and implementation, including semantics, types, optimisation and verification, brought to bear on the security question*

Schneider et. al, 2000

Attacks: Software (program) level

Tools: Programming Languages techniques



Goal: Security by design, built into software

# Security by design

- Software applications are implemented in programming languages
- systems are modelled at different levels of abstraction (using different languages)
- security policies can be expressed and analysed at each of these levels
- security-by-design: using language-based analysis techniques to enforce specified security properties with strong guarantees

# Secure? (w.r.t. ...)

$y_H := x_L$ ✓

$x_L := y_H$ ✗

Explicit leak

if $y_H$ then $x_L := 0$ else $x_L := 1$ ✗

while $y_H$ do skip ; $x_L := 0$ ✓

Implicit leak

# Secure? (w.r.t. ...)

$y_H := x_L$ ✓

$x_L := y_H$ ✗

if $y_H$ then $x_L := 0$ else $x_L := 1$ ✗

while $y_H$ do skip ; $x_L := 0$ ✗

Termination leak

# Ethics and law

- The purpose of the course is to learn how to protect computer systems from cyber-attacks
  - but some of the things you learn may also be used to attack them
- Notice that
  - **Attacking systems is unethical and punished by law**
  - Even just "testing" systems without written permission may be punished by law
- *Don't try this at home* → *Try this just at home*

# ORGANIZATION OF THE COURSE

# Communication

- Primarily via mattermost, for a quicker response, and so that all students can benefit from the information

- Official announcements and resources via:
  - the course's website (Fenix),
  - email, using your official email address

- Course's website @ Fenix: https://fenix.tecnico.ulisboa.pt/disciplinas/SSof/2022-2023/1-semestre

# Classes

- 1 Lecture and 1 Lab on VSSD per week
  - Alameda: Lecture Mo + Labs Tu and We (8am)
  - Tagus: Lecture Thu + Labs Thu

VSSD T01

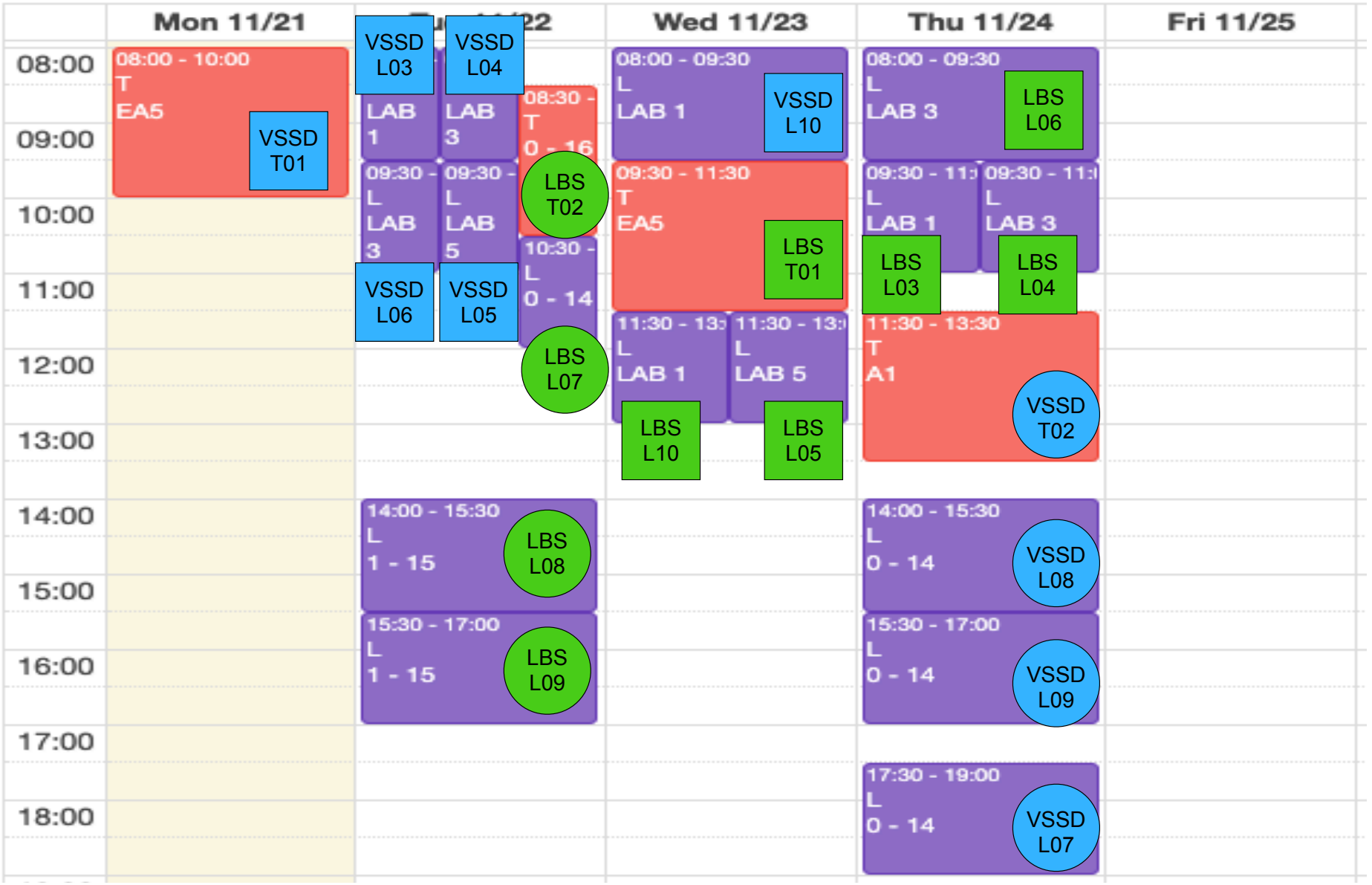
VSSD T02

- 1 Lecture and 1 Lab on LBS per week
  - Alameda: Lecture We + Labs We (11.30am) + Th
  - Tagus: Lecture Tu + Labs Tu

LBS T01

LBS T02

- in person, in your own shift


Mon 11/21
Wed 11/23
Thu 11/24
Fri 11/25
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
08:00 - 10:00
T
EA5
VSSD T01
VSSD L03
VSSD L04
LAB 1
LAB 3
08:30 -
T
0 - 16
LBS T02
09:30 -
L
LAB 3
09:30 -
L
LAB 5
10:30 -
L
0 - 14
VSSD L06
VSSD L05
LBS L07
14:00 - 15:30
L
1 - 15
LBS L08
15:30 - 17:00
L
1 - 15
LBS L09
08:00 - 09:30
L
LAB 1
VSSD L10
09:30 - 11:30
T
EA5
LBS T01
11:30 - 13:
L
LAB 1
11:30 - 13:
L
LAB 5
LBS L10
LBS L05
08:00 - 09:30
L
LAB 3
LBS L06
09:30 - 11:
L
LAB 1
09:30 - 11:
L
LAB 3
LBS L03
LBS L04
11:30 - 13:30
T
A1
VSSD T02
14:00 - 15:30
L
0 - 14
VSSD L08
15:30 - 17:00
L
0 - 14
VSSD L09
17:30 - 19:00
L
0 - 14
VSSD L07

# Labs/practical classes

- Labs (hands-on)
  - Cross site scripting
  - SQL injection
  - Buffer overflows
  - Format string vulnerabilities
  - Race conditions
- Lab (hands-on) + practical classes
  - Taint checker + information flow policies
  - Language interpreter + formal semantics
  - Language analyzer + enforcement mechanisms
  - Static analyzer + type systems
  - Dynamic analyzer + monitors
  - Symbolic analyzer + verification and bugs

# Labs

- VSSD labs will be CTF-style labs
  - BYOD
  - Login at https://gitlab.rnl.tecnico.ulisboa.pt/
  - There will be 6 Lab assignments starting week 2
    - Lab assignments are individual
    - Write-ups need to be submitted weekly
      - by Saturday 5pm

# Evaluation

- 1 Exam (50%) that can be repeated
- Practical components:
  - Lab Exercises (15%) - Individual
  - Project (35%) - Groups of 3 students (registration in Fenix)
    - All students are expected to participate, and are responsible for, all parts of the project
- Min. grade: >=9 for Project; >=8 for Exam
- Partial grades from previous years not reused

Read “Métodos de Avaliação”, Fénix

# Tests

- Important Dates
  - Exam 1 - 26 January 2023, 10:30
  - Repetition - 06 February 2023, 08:00
- Cover Theoretical and Lab classes
- Can be answered in Portuguese or English
- Tests from last years will be made available, but note:
  - Detailed content and highlights are adjusted every year.
  - Use slides and summaries as reference.

Check “Avaliação / Evaluations”, Fénix

# Project

- Assignment published on W3
- Code - due 06 January 2023
- Report - due 13 January 2023
- Project Discussions: 16-20 January 2023
  - Mandatory to all group members to participate

☞ Check “Avaliação / Evaluations”, Fénix

# Bibliography

- ***Segurança no Software***
  Miguel Correia and Paulo Sousa
  FCA, September 2010/2017


- Complementary:
  - ***The 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them***, Michael Howard, David LeBlanc and John Viega, 2009, McGraw-Hill ISBN 9780071626750
  - ***Building Secure Software: How to Avoid Security Problems the Right Way***, John Viega and Gary McGraw, 2002, Addison-Wesley ISBN 9780201721522
  - ***Introduction to Computer Security***, Matt Bishop, 2005, Addison-Wesley

- Alternative texts for non-Portuguese speaking students (email me)

# Study materials

- Book / other texts
- Papers
- Lab guides
- Slides
- Problem sets

# CYBER-SECURITY SPECIALIZATION @ TÉCNICO

# Cyber-Security Specialization @ Técnico

- New in the restructured MEIC (start: Sept. 2015)
- Implements the Information Assurance and Security Knowledge Area of the ACM/IEEE Computer Science Curricula 2013
- Aims to give students the technical skills necessary to analyse, protect and manage the security of personal, corporate and governmental computer systems from cyber threats

# Cyber-Security specialisation

- Courses:
  - Network and Computer Security (SIRS)
  - Software Security (SSof)
  - Forensics Cyber-Security (CSF)
  - Cryptography and Security Protocols (CPS)
  - Highly Dependable Systems (SEC)

# WHO WANTS TO HACK?

Creating a (ethically-responsible) hacking team@IST

# How do we want to do it?

- Invite ALL students with interest in Security to participate
- Teach Computer Security in an ethically responsible and competitive environment
- Meet regularly (every week Mo, 5.30pm) to learn new tricks
- Participate in CTF competitions

- More info at https://sectt.github.io