UNIVERSITÀ DI PISA

LANGUAGE-BASED TECHNOLOGY FOR SECURITY

GIAN-LUIGI FERRARI

Anno accademico	2020/21
CdS	CYBERSECURITY
Codice	714AA
CFU	9

Moduli	Settore/i	Tipo	Ore	Docente/i
LANGUAGE-BASED TECHNOLOGY FOR SECURITY	INF/01	LEZIONI	72	GIAN-LUIGI FERRARI

Obiettivi di apprendimento

Conoscenze
Traditionally, computer security has been largely enforced at the level of operating systems. However, operating-system security policies are low-level (such as access control policies, protecting particular files), while many attacks are high-level, or application-level (such as email worms that pass by access controls pretending to be executed on behalf of a mailer application). The key to defending against application-level attacks is application-level security. Because applications are typically specified and implemented in programming languages, this area is generally known as language-based security. A direct benefit of language-based security is the ability to naturally express security policies and enforcement mechanisms using the developed techniques of programming languages.

Modalità di verifica delle conoscenze
Ongoing assessment in the form of programming tests or discussion gruops between the lecturer and students will be carried out to monitor the learning progress of students.

Capacità
The aim of the course is to allow each student to develop a solid understanding of application level security, along with a more general familiarity with the range of research in the field. In-course discussion will highlight opportunities for cutting-edge research in each area. The course intends to provide a variety of powerful tools for addressing software security issues

- To obtain a deeper understanding of programming language-based concepts for computer security.
- To understand the design and implementation of security mechanisms.
- To understand and move inside the research in the area of programming languages and security.

After the course, students should be able to apply practical knowledge of security for modern programming languages. This includes the ability to identify application- and language-level security threats, design and argue for application- and language-level security policies, and design and argue for the security, clarity, usability, and efficiency of solutions, as well as implement such solutions in expressive programming languages. Student should be able to demonstrate the critical knowledge of principles behind such application-level attacks as race conditions, buffer overruns, and code injections. You should be able to master the principles behind such language-based protection mechanisms as static security analysis, program transformation, and reference monitoring.

Modalità di verifica delle capacità
There are lab assignments. The lab assignments are experimental activities about specific problems. To pass the course, students must pass the labs by making a presentation of the assignments in class and pass the requirements on a written report that documents the activities done.

Comportamenti
Students will acquire the techniques to detect and prevent vulnerabilities of software systems by exploiting a variety of programming language-based machineries.

Modalità di verifica dei comportamenti
The discusssion groups and the expermental activities (lab) will asses the echniques to prevent or detect security vulnerabilities. This will include include threat modeling, coding standards, code reviews, "safe" programming languages, LangSec (language-theoretic security), security testing, static analysis tools and source code analyzers, information flow analysis (incl. tainting), program verification, and secure compilation.

Prerequisiti (conoscenze iniziali)

UNIVERSITÀ DI PISA

Basic programming skills, incl. familiarity with C and Java.
Basic skills on principle of programming languages inclu compiler and run-time structure
Basic slkils on system organization (operating systems and networking)
Basic skills on cryptography.

Indicazioni metodologiche

Lectures and lab activities will focus on (addressing) the underlying causes and general techniques to improve the security of software.

Programma (contenuti dell'insegnamento)

- Security in the Software Development Life Cycle
- The science of software security
- Memory-corruption flaws
- Control Flow Integry & Software Fault Isolation
- Safe Programming Languages
- Access Control, Sand-Boxing and Stack Inspection
- Inline-Reference Monitor (Theory & Sperimentation)
- Function as a Service
- Local Security Policies in Java
- Information Flow and JS-Flow
- Control Flow Analysis for Security
- Secure Compilation
- Lab and programming assignments.

Bibliografia e materiale didattico

The reading material and exam material for the course includes the slides, academic research papers and notes. The reading material will be made available on the academic e-learning infrastructure.

Indicazioni per non frequentanti

The schedule and the contents of lectures and lab sessions will be made available on the e-learning academic infrastructure.

Modalità d'esame

The exam consits of

?Class participation (discussion groups): discuss topis ?Project work: design and implementation.of asoftware prototyoe ?Written exam (40%)

Ultimo aggiornamento 16/02/2021 15:37