LANGUAGE-BASED TECHNOLOGY FOR SECURITY

GIAN-LUIGI FERRARI

Anno accademico	2021/22
CdS	CYBERSECURITY
Codice	714AA
CFU	9

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

Obiettivi di apprendimento

Conoscenze
Tradizionalmente, la sicurezza dei sistemi informatici è stata in gran parte affrontata a livello di sistemi operativi. Tuttavia, le politiche di sicurezza del sistema operativo sono politiche di basso livello (ad esempio le politiche di controllo dell'accesso, che proteggono particolari file), mentre molti attacchi sono di alto livello, o a livello di applicazione (come i worm di posta elettronica che passano attraverso i controlli di accesso fingendo di essere eseguiti per conto di un'applicazione mailer). La chiave per difendersi dagli attacchi a livello di applicazione è la sicurezza a livello di applicazione. Con il termine Language-based security si identificano quell'insieme di tecniche e strumenti che affrontano le problematiche di sicurezza a livello del linguaggio di programmazione. Il vantaggio diretto della laguage-based security è la capacità di esprimere in modo naturale le politiche di sicurezza e i loro meccanismi di esecuzione e verifica utilizzando le tecniche sviluppate per la realizzazione linguaggi di programmazione.

Modalità di verifica delle conoscenze
La valutazione continua è lo strumento principale adottato per la verifica delle conoscenze e monitorare i progressi di apprendimento degli studenti. Per effettuare la valutazione continua saranno considerati test di programmazione, progetti e gruppi di discussione tra il docente e gli studenti.

Capacità
L'obiettivo del corso è quello portare gli studenti ad sviluppare una comprensione approfondita delle problematiche di sicurezza del software, insieme ad una familiarità più generale con le linee innovative delle ricerche nel settore. Il corso intende fornire una varietà di metodi e strumenti per affrontare i problemi di sicurezza del software. In dettaglio il socrso di propone di far

- acquisire una comprensione e una familiarità con i metodi e gli strumneti di language-based security.
- comprendere metodologie innovative per la progettazione e l'implementazione dei meccanismi di sicurezza.
- compremdere a navigare all'interno della ricerca nell'area dei linguaggi di programmazione e della sicurezza.

Dopo il corso, gli studenti saranno in grado di applicare la conoscenza pratica della sicurezza per i moderni linguaggi di programmazione. Questo include la capacità di identificare le minacce alla sicurezza a livello di applicazione e di linguaggio, progettare e argomentare politiche di sicurezza a livello di applicazione e di linguaggi. Lo studente saranno in grado di dimostrare la conoscenza critica dei principi alla base di attacchi a livello applicativo come race condition, buffer overflow, code injection (per citare alcuni esempi).

Modalità di verifica delle capacità
Sono previste attività sperimentali di laboratorio su specifiche problematiche di sicurezza. La verifica delle capacità prevede la presentazione operativa dei progetti e una relazione scritta che documenti le attività svolte.

Comportamenti
Gli studenti acquisiranno le tecniche per rilevare e prevenire le vulnerabilità dei sistemi software sfruttando una varietà di metodologie e strumenti di language-based security.

Modalità di verifica dei comportamenti
I gruppi di discussione, il lavoro di gruppo e le attività sperimentali (laboratorio) costituiranno lo strumento principale di verifica dei comportamenti. All'interno di questa verifica verranno affrontati gli aspetti di modellazione delle minacce, standard di codifica, le revisioni del codice, test di sicurezza, strumenti di analisi statica (taint analysis), l'analisi del flusso di informazioni, la verifica del programma e la compilazione sicura.

Prerequisiti (conoscenze iniziali)
Competenze di base di programmazione, inclusa la familiarità con C e Java.
Competenze di base sui principi dei linguaggi di programmazione, incluso il compilatore e la struttura di run-time
Competenze di base sull'organizzazione del sistema (sistemi operativi e networking)
Competenze di base sulla crittografia.

Indicazioni metodologiche
Le lezioni e le attività di laboratorio si concentreranno sulle cause sottostanti e sulle tecniche generali per migliorare la sicurezza del 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
- Taint analysis
- Information Flow and JS-Flow
- Control Flow Analysis for Security
- Secure Compilation
- Lab and programming assignments

Bibliografia e materiale didattico
Il materiale didattico include il materiale presentato a lezionie (vidoregistrazioni delle lezioni), i articoli scientifiici e note didattiche. Il materiale sarà reso disponibile sull'infrastruttura accademica di e-learning.

Indicazioni per non frequentanti
Il programma e il contenuto delle lezioni e delle sessioni di laboratorio saranno resi disponibili sull'infrastruttura accademica di e-learning.

Modalità d'esame
La prova di esame consiste in diverse parte:

- Partecipazione alla lezione (gruppi di discussione)
- Lavoro di progetto: progettazione e realizzazione di un prototipo di software
- Prova scritta
- Discussione orale

Ultimo aggiornamento 06/08/2021 08:19