



UNIVERSITÀ  
DEGLI STUDI DI MILANO-BICOCCA

## COURSE SYLLABUS

### Computer Security

2425-2-F1801Q123

---

#### Obiettivi

Capacità di leggere correttamente le tendenze nel settore sicurezza informatica

Uso corretto dei sistemi crittografici

Uso di strumenti di analisi statica del software

Uso di strumenti di "model checking" per la sicurezza

#### Contenuti sintetici

presentazione di tecniche e strumenti avanzati per attacco e difesa dei sistemi informatici

#### Programma esteso

1 "Richiamo dei principi alla base della disciplina Sicurezza Informatica

Tendenze nel settore della sicurezza informatica

Analisi di alcuni episodi di attacco informatico recenti e di grande impatto"

2 "Uso dei sistemi crittografici: approccio simmetrico e asimmetrico

implementazioni degli algoritmi crittografici

la scelta degli algoritmi crittografici, il contesto in cui inserirli"

3 la crittografia nelle reti senza fili e cellulari

4 "L'analisi statica della sicurezza del software: motivazioni, limiti

rappresentazioni astratte di alcuni aspetti dell'esecuzione

caso d'suo: analisi statica di vulnerabilità "buffer overflow"

5 "Analisi tramite "model checking" per la sicurezza: motivazioni, altri usi

formalismi di rappresentazione degli stati logiche per la descrizione di proprietà, esempi di proprietà da modellare per controlli di sicurezza"

6 "strumenti per il "model checking"

esempi di uso del model checking per i protocolli su rete, tecnologie di

implementazione"

7 Esercitazione competitiva di attacco a software vulnerabile appositamente predisposto ("Capture the Flag")

## **Prerequisiti**

Si richiamano nozioni relative a Sistemi Operativi, Reti, Programmazione

## **Modalità didattica**

- 18 lezioni da 2 ore svolte in modalità erogativa in presenza;
- 2 lezioni da 2 ore svolte in modalità erogativa in remoto asincrono;
- 10 ore totali su 4 esercitazioni svolte in presenza in modalità 50% erogativa 50% interattiva;

## **Materiale didattico**

articoli scientifici e divulgativi disponibili in Internet

consultazione: Pfleeger, Pfleeger - "Sicurezza in Informatica", Pearson

## **Periodo di erogazione dell'insegnamento**

secondo Semestre

## **Modalità di verifica del profitto e valutazione**

La verifica dell'apprendimento comprende una prova scritta (50% del voto finale) e una breve relazione presentata a colloquio orale (50% del voto finale):

lo scritto consiste in alcune domande discorsive su una selezione di argomenti presentati a lezione (indicata all'inizio delle lezioni),

la relazione deve riguardare attività sperimentali su uno degli argomenti presentati a lezione, scelto dallo studente.

## **Orario di ricevimento**

Su appuntamento concordato via email, usualmente i martedì mattina.

## **Sustainable Development Goals**

---