

Guida rapida all'insegnamento

Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)

Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Studi in Informatica applicata, AA 2006-7

Indice

1. Guida rapida all'insegnamento
2. Organizzazione dell'insegnamento
3. Obiettivi formativi
4. Attività formative
5. Relazione con altri insegnamenti
6. Modalità di valutazione
7. Programma dell'insegnamento
8. Testi consigliati
9. Strumenti per l'interazione formativa

Organizzazione dell'insegnamento

- **modalità:** blended e-learning
 - proposta: proviamo a usare il Wiki, ad es. per lo sviluppo di approfondimenti dei temi in programma, o altri rilevanti?
- sviluppo progettuale cooperativo
 - non solo di progetti di studio
 - ma anche dello stesso progetto formativo dell'insegnamento
- condivisione di obiettivi formativi
 - comprendere i **concetti** e i **problemi** di sicurezza dei sistemi informatici
 - valutare le **soluzioni** ad essi

Obiettivi formativi

Acquisizione e sviluppo della capacità di:

comprendere i problemi fondamentali della sicurezza
per una vasta gamma di sistemi informatici

da semplici programmi a complessi sistemi operativi e sistemi di gestione di basi di dati

analizzare le vulnerabilità e le loro fonti nei sistemi informatici

valutare i rischi a cui esse danno luogo

fronteggiare tali rischi adottando le tecniche di **controllo delle vulnerabilità** che risultino più appropriate al contesto operativo e sociale in cui si applicano
valorizzare gli aspetti sociali, normativi ed etici delle problematiche di sicurezza nel **progetto** e nella **gestione** dei sistemi informatici

Attività formative

L'organizzazione didattica dell'insegnamento prevede 48 ore di lezione (ed esercitazione)

L'acquisizione di metodi e competenze professionali nella disciplina è sostenuta da:

frequenza delle lezioni ed esercitazioni
studio del testo [Pfleeeger & Pfleeeger, 2004]
elaborazione di soluzioni a problemi ed esercizi proposti
consultazione di altri testi e materiali didattici
interazione con il docente: ricevimento settimanale + ...
collaborazione con i colleghi: diretta + ...
sperimentazione di un servizio di collaborazione in rete: Wiki

Relazione con altri insegnamenti

L'insegnamento non ha prerequisiti, ed è

- raccomandato
 - significa: nessun vincolo di propedeuticità sugli esami, ma seguire i due insegnamenti nella sequenza naturale è ottimale per il conseguimento degli obiettivi formativi

quale bagaglio preliminare per l'insegnamento di **Sicurezza dei sistemi informatici 2**

Modalità di valutazione

- valutazione in itinere:
 - contributi prodotti dagli studenti in risposta a problemi ed esercizi proposti
=> bonus!
- valutazione finale: colloquio individuale sugli argomenti del programma
 - a partire da un approfondimento prodotto dallo studente,
 - possibilmente in collaborazione con altri studenti.

Il superamento della prova porta all'acquisizione di 6 crediti.

Programma dell'insegnamento

Introduzione

problemi di sicurezza nei sistemi informatici: L.01.

Elementi di crittografia per la sicurezza informatica

cenni storici, terminologia, sistemi di crittografia: L.02, L.03, L.04;

standard di crittografia pubblica: RSA, DES, AES: L.05, L.06;

uso della crittografia per la sicurezza informatica: L.07.

Sicurezza informatica

sicurezza dei programmi: L.08, L.09, L.10, L.11, L.12, L.13.

meccanismi di protezione nei sistemi operativi: L.14, L.15, L.16.

progetto di sistemi operativi sicuri: L.17, L.18, L.19, L.20, L.21, L.22.

sicurezza e protezione di basi di dati: L.23, L.24.

Testi consigliati

Testo di riferimento (adottato)

C.P. Pfleeger & S.L. Pfleeger

Security in Computing, 3/e ; *Sicurezza in informatica*, 1/e

Prentice Hall PTR (2003) ; Pearson Education Italia (2004)

Altri testi consigliati (per consultazione)

J. Pieprzyk, T. Hardjono, J. Seberry, *Fundamentals of Computer Security*, Springer (2003)

S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books (1999)

V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press (2005)

Strumenti per l'interazione formativa

Forum e Wiki: cosa va dove?

- Forum: discussioni di
 - organizzazione dell'insegnamento
 - argomenti delle lezioni
- Wiki: è incoraggiata la documentazione in corso d'opera dello sviluppo di esercizi e approfondimenti, facendo pieno uso della funzionalità Wiki per il controllo di versione e per la gestione di discussioni