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 2008-9

Indice

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 di uno o più testi di riferimento

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**

Programma delle lezioni (1)

1. Problemi di sicurezza nei sistemi informatici
2. Elementi di crittografia
3. Tecniche tradizionali di cifratura
4. Sistemi di crittografia, crittografia asimmetrica: RSA
5. Standard di crittografia simmetrica: DES, AES
6. Usi della crittografia: controllo d'integrità
7. Usi della crittografia: scambio di chiavi, firme digitali, certificati
8. Qualità di sicurezza dei programmi
9. Minacce alla sicurezza dei programmi
10. Codice maligno generico e finalizzato
11. Controlli contro le minacce dei programmi
12. Risvolti sociali della sicurezza informatica

Programma delle lezioni (2)

13. Protezione nei sistemi operativi
14. Controllo di accesso a risorse condivise
15. Protezione dei file, autenticazione di utente
16. Autenticazione nei sistemi distribuiti
17. Requisiti di sistemi operativi sicuri
18. Modelli di sicurezza
19. Sviluppo di sistemi operativi sicuri
20. Trusted Computing Base
21. Valutazione di sistemi operativi sicuri
22. Certificazione di sistemi operativi sicuri
23. Requisiti di protezione delle basi di dati
24. Tecniche di protezione delle basi di dati

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.

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

Testi consigliati

Testi di riferimento

D. Gollmann, *Computer Security , 2/e*
John Wiley & Sons (2006)

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)

Siti utili

Un testo liberamente disponibile (fuori commercio):

Morrie Gasser, *Building a Secure Computer System*
Van Nostrand Reinhold (1988) [PDF]

Un testo di Crittografia liberamente disponibile:

A. Menezes, P. Van Oorschot, S. Vanstone,
Handbook of Applied Cryptography
CRC Press, 5th Printing (2001)

Stanford Security Laboratory : http://crypto.stanford.edu/seclab

Un sito poco accademico, ma molto interessante: http://www.phrack.org