Sicurezza dei sistemi informatici 1
Introduzione al corso

rif.: C.P. Pfleeger & S.L. Pfleeger, Sicurezza in informatica
Pearson Education Italia, 2004

Giuseppe Scollo

Corso di Laurea in Informatica applicata
Università di Catania, sede di Comiso (RG)

11 febbraio 2006

Sommario

Obiettivi formativi

- acquisizione della capacità di comprendere i problemi fondamentali della sicurezza per una vasta gamma di sistemi informatici, da semplici programmi a complessi sistemi operativi, sistemi di gestione di basi di dati e sistemi di rete
- sviluppo delle capacità di analizzare le vulnerabilità e le loro fonti nei sistemi informatici, di valutare i rischi a cui esse danno luogo, e di fronteggiarli adottando le tecniche di controllo delle vulnerabilità che risultino più appropriate al contesto operativo e sociale in cui si applicano
- valorizzazione degli aspetti sociali, normativi ed etici delle problematiche di sicurezza nel progetto e nella gestione dei sistemi informatici

Attività formative

- frequenza delle lezioni ed esercitazioni
- studio degli argomenti sui testi consigliati
- 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 per la collaborazione in rete: **Wiki**

Contenuti dello studio
Programma degli argomenti

- **Introduzione**
  - problemi di sicurezza nei sistemi informatici
- **Elementi di crittografia per la sicurezza informatica**
  - cenni storici, terminologia, bagaglio matematico essenziale
  - crittografia a chiave privata, standard DES, AES
  - crittografia a chiave pubblica, usi della crittografia
- **Sicurezza informatica**
  - sicurezza dei programmi
  - meccanismi di protezione nei sistemi operativi
  - progetto di sistemi operativi sicuri
  - sicurezza e protezione di basi di dati
  - problemi di sicurezza nelle reti
- **Risvolti sociali della sicurezza informatica**
  - pianificazione e gestione della sicurezza
  - aspetti legali ed etici della sicurezza informatica

Organizzazione del corso
Programma delle lezioni

- **Introduzione**
  - L01: problemi di sicurezza nei sistemi informatici
- **Elementi di crittografia per la sicurezza informatica**
  - L02: cenni storici, terminologia, bagaglio matematico essenziale
  - L03, L04: crittografia a chiave privata, standard DES, AES
  - L05, L06: crittografia a chiave pubblica, usi della crittografia
- **Sicurezza informatica**
  - L07–L09: sicurezza dei programmi
  - L10, L11: meccanismi di protezione nei sistemi operativi
  - L12–L14: progetto di sistemi operativi sicuri
  - L15, L16: sicurezza e protezione di basi di dati
  - L17: problemi di sicurezza nelle reti
- **Risvolti sociali della sicurezza informatica**
  - L18: pianificazione e gestione della sicurezza
  - L19: aspetti legali ed etici della sicurezza informatica

Modalità di valutazione dell'apprendimento

valutazione *in itinere* e finale

- valutazione *in itinere*:

  di elaborati su **problemi ed esercizi** proposti:

  bonus!
  =
  incremento del voto finale

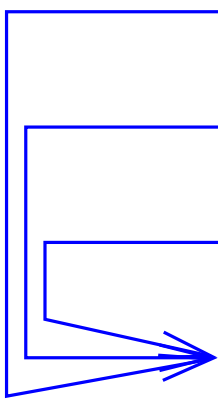
- valutazione finale:

  colloquio orale sugli argomenti trattati nel corso

Relazione con altri insegnamenti del Corso di Studio

propedeuticità. . .

un poset di 5 insegnamenti (6 + (6+6) + (3+3) = 24 CFU):



- Sicurezza dei sistemi informatici 1
  (II a., IIs., 6 CFU)
- Crittografia
  (III a., Is., 6 CFU)
- Reti di calcolatori
  (III a., Is., 6 CFU)
- Sicurezza dei sistemi informatici 2
  (III a., IIs., 3 CFU)
  Laboratorio di amministrazione di sistema
  (III a., IIs., 3 CFU)

Riferimenti bibliografici
Sicurezza dei sistemi informatici

C.P. Pfleeger & S.L. Pfleeger
Security in Computing, 3/e ; Sicurezza in informatica, 1/e
Prentice Hall PTR (2003) ; Pearson Education Italia (2004).
http://authors.phptr.com/pfleeger

J. Pieprzyk, T. Hardjono, J. Seberry
Fundamentals of Computer Security
Springer (2003).
http://www.springer.com/sgw/cda/frontpage/0,11855,5-40160-22-2227123-0,00.html

W. Stallings
Cryptography and Network Security, 4/E
Prentice Hall (2005).
http://williamstallings.com/Crypto/Crypto4e.html

Inquadramento storico, bagaglio matematico
Altri testi per consultazione

S. Singh
The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography
Anchor Books (1999).
http://www.simonsingh.net/The_Code_Book.html

V. Shoup
A Computational Introduction to Number Theory and Algebra
Cambridge University Press (2005).
http://shoup.net/ntb