IN5 Tecniche di Sicurezza dei Dati e delle Reti

A.A. 2006/2007

Roberto Di Pietro, PhD

1. Introduzione Il corso ha l'obbiettivo di introdurre lo studente ai concetti della sicurezza informatica, dei fondamenti ad essa associati ed alle tecniche per poter progettare, implementare e valutare soluzioni di sicurezza.

2. Fondamenti di Networking Si introdurra' il modello ISO/OSI, la terminologia di riferimento nel contesto di reti e le principali tipologia di rete.

3. Fondamenti di TCP/IP Si introdurranno i concetti di base del TCP/IP, quali: Indirizzi IP; Subnet Mask; Frame IP; Meccanismi di comunicazione tra reti diverse; Classi di indirizzi IP; Indirizzi IP privati e pubblici.

4. Crittografia classica Si vedranno i seguenti argomenti: Cifrari di Cesare, Cifrari Vignere, esempi di crittoanalisi, Il cifrario perfetto (one time pad).

5. Funzioni hash Si caratterizzeranno le funzioni hash e si forniranno i principali protocolli crittografici che ne prevedono l'uso (uso come MAC/HMAC e come MDC o MIC).

6. Crittografia simmetrica Si tratteranno i seguenti argomenti: cifrari a blocchi, cifrari a flusso, Feistel, DES, 3-DES ed AES.

7. Modalita' operazionali dei cifrari Si studieranno le seguenti modalita' operazionali dei cifrari: ECB (Electronic Code Book), CBC (Cipher Block Chaining Mode), OFB (Output Feedback Mode), CFB (Cipher Feedback Mode).

8. Crittografia asimmetrica Si riprenderanno i concetti elementari di teoria dei numeri per poter trattare gli algoritmi asimmetrici quali: Diffie-Hellman; RSA; ElGamal.

9. Firme camaleontiche Si introdurra' una innovativa tecnica che consente di rendere le firme digitali non trasferibili, per il tramite di hash camaleontici.

10. Principii di progettazione Si discutera' dei principi fondamentali necessari per poter progettare correttamente meccanismi per la sicurezza.

11. Un case study di crittoanalisi Si esporra' lo studio di un caso reale di crittoanalisi, applicato al protocollo WEP.

12. Tecniche di Autenticazione Si illustreranno i principii fondanti del concetto di autenticazione e si esporranno le tecniche piu' diffuse per garantire tale proprieta' nei sistemi di calcolo.

13. Tecniche di comunicazione sicura multicast Si trattera' la sicurezza delle comunicazioni multicast, dove i dispositivi finali sono caratterizzati da: (a) stato aggiornabile; (b) stato non aggiornabile.

14. Tecnologie per la Sicurezza In questo modulo verranno trattati le tecnologie per i Firewalls, la Sicurezza dei sistemi di e-mail, il protocollo SSL ed i sistemi per la rilevazione delle intrusioni (IDS).

Testi consigliati

[1] A.J. Menezes et al., *Handbook of Applied Cryptography*. CRC press, (2001).
[2] B. Schneier, *Schneider, Applied Cryptography. Protocols, Algorithms, and Source Code in C.*. John Wiley & Sons, (1996).

Bibliografia supplementare

[3] William Stallings, *Network Security Essentials*. Prentice Hall, (2002).

Modalità d'esame

- valutazione in itinere ("esoneri")		☐ SI	■ NO
- esame finale	scritto	■ SI	☐ NO
	orale	■ SI	☐ NO
- altre prove di valutazione del profitto (meglio descritte sotto)		☐ SI	■ NO

La modalita' di esame si compone di uno scritto e di un orale. Sono previsti progetti, su base facoltativa, che non sostituiscono le due prove citate.