IN520 Tecniche di Sicurezza dei Dati e delle Reti

A.A. 2010/2011

Alessandro Colantonio

1. Introduzione Gli obiettivi formativi sono i seguenti:

- catturare il nesso tra matematica discreta ed il contributo alla sicurezza dei sistemi;
- fornire agli studenti la capacità di sviluppare in maniera autonoma approfondimenti nel settore della sicurezza informatica;
- renderli in grado di comprendere le problematiche di sicurezza di realtà medio-piccole;
- fornire soluzioni alle problematiche di sicurezza sopra identificate.

2. Introduzione alle Reti di Calcolatori Definizione di rete di calcolatori. Principali classificazioni delle reti di calcolatori. Modelli ISO/OSI e TCP/IP e principali differenze fra loro. Principali protocolli della famiglia IEEE 802. Repeater, hub, bridge, switch e router. Protocollo IP e relativo schema d'indirizzamento. Protocolli TCP e UDP. Introduzione al concetto di natting. Protocolli di livello applicazione: DNS, HTTP e SMTP.

3. Crittografia Classica Il concetto di conventional encryption e rappresentazione matematica di un cryptosystem. Cifrari a sostituzione e a trasposizione. Attacchi ai cifrari e principali strumenti di criptoanalisi. La teoria di Shannon per la comunicazione nei sistemi crittografici. Il one-time-pad e il cifrario di Vernam.

4. Crittografia Simmetrica Cifrari a blocchi, cifrari a flusso, rete di Feistel, DES, 3-DES ed AES. Modalità operazionali dei cifrari: ECB (Electronic Code Book), CBC (Cipher Block Chaining Mode), OFB (Output Feedback Mode), CFB (Cipher Feedback Mode). Generazione di un MIC attraverso l'uso di un cifrario a blocchi.

5. Teoria dei Numeri per la Crittografia Teoria dei campi finiti. Teoremi di Fermat e di Eulero.

6. Crittografia Asimmetrica Principii di crittografia asimmetrica. Diffie-Hellman, El Gamal, RSA.

7. Funzioni Hash Funzioni Hash e principali proprietà richieste. Paradosso del compleanno. Modello generale di iterazione delle funzioni hash e metodi per l'integrità dei dati.

8. Autenticazione Concetto di autenticazione e tecniche più diffuse per garantire tale proprietà nei sistemi di calcolo.

9. Test di Primalità Principio di funzionamento dei test di primalità probabilistici. Test di Fermat e di Eulero.

10. Certificati Digitali Certificati digitali, scopo delle CRL e del protocollo OCSP.

11. Firme Digitali e Firme Camaleontiche La firma digitale e le principali caratteristiche. Principali differenze fra firme camaleontiche e firme digitali classiche.

12. Gestione e Distribuzione delle Chiavi Schema di funzionamento di una public-key authority. Principali caratteristiche delle curve ellittiche.

13. Principii di Progettazione Principii fondamentali necessari per poter progettare correttamente meccanismi per la sicurezza.

14. Controllo degli Accessi Politiche, meccanismi e modelli di controllo degli accessi. Esempi di modelli di controllo degli accessi. Modello RBAC.

15. Internet Security Protocollo IPSec e principali servizi offerti. Obiettivo dei protocolli SSL/TLS e principali servizi offerti. Firewall e configurazioni tipiche di utilizzo. Email Security e principali caratteristiche del programma PGP. Attacchi. Malicious Software. Intrusion detection. Classificazione dei programmi maliziosi.

16. Analisi e Gestione del Rischio Passi principali di un processo di analisi del rischio.

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).
[3] William Stallings, *Cryptography and Network Security, 4^a ed.* Prentice Hall, (2006).

Bibliografia supplementare

Testi di sicurezza reperibili in biblioteca, segnalati a seconda dell'argomento.

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