Prof.Dr. Ferucio Laurenţiu Ţiplea
Facultatea de Informatică
Univ. "Al.I.Cuza", Iaşi

Câteva subiecte orientative la "Securitatea Informaţiei"

Subiectele de mai jos vizează principii generale ce trebuiesc cunoscute, necerându-se reproducerea exactă a structurii mesajelor sau regulile protocoalelor implicate în cadrul acestora.

Dacă un subiect de examen, diferit de cele de mai jos, va viza anumite aspecte strâns legate de structura unui protocol din curs, atunci acest protocol va fi prezentat explicit ca ipoteză de lucru în enunţul subiectului. De exemplu, dacă se cere o analiză de securitate asupra protocolului Kerberos, atunci acest protocol va fi prezentat ca ipoteza de lucru în enunţul subiectului.

Sisteme de protecţie

1. Ce este un sistem de protecţie peste o mulţime de drepturi? (definiţi toate conceptele ce intervin în explicarea conceptului de sistem de protecţie)
2. In ce constă problema siguranţei sistemelor de protecţie?
3. Ce cunoşteţi despre dificultatea rezolvării algoritmice a problemei siguranţei sistemelor de protecţie?
4. Ce este o listă de control al accesului? Discutaţi cazul Unix şi Windows NT.
5. Ce este o listă de capacităţi?
6. Ce înţelegeţi prin acces discreţionar şi acces mandatar?

IPsec

1. Ce este o asociere de securitate în IPsec şi care sunt mecanismele de securitate fundamentale din IPsec?
2. Descrieţi, succint dar clar, protocolul AH în cele două moduri de utilizare pentru datagrame IPv4.
3. Descrieţi, succint dar clar, protocolul ESP în cele două moduri de utilizare pentru datagrame IPv4.
4. Descrieţi câteva combinaţii de asocieri de securitate in IPsec (end-to-end, VPN, end-to-end cu VPN).

SSL/TLS

1. Care este scopul de bază a protocolului SSL/TLS?
2. Descrieţi, succint dar clar, metodele de schimb de cheie RSA şi DH în SSL.
3. Care sunt paşii de bază ai protocolului "SSL record"?

DNS şi DNSsec

1. Descrieţi, succint dar clar, modul de funcţionare a protocolului DNS.
2. Descrieţi, succint dar clar, modul de funcţionare a protocolului $DNSsec$.
3. Prezentaţi şi discutaţi 2 argumente pentru care credeţi că $DNSsec$ asigură securitate.

RFC 822 şi MIME

1. Care sunt principalele dezavantaje ale formatului de e-mail RFC 822?
2. Care este structura de bază a unui format MIME?
3. Care sunt cele 4 metode de codificare a informaţiei în MIME?
4. In ce constă metoda de codificare "quoted-printable"?
5. In ce constă metoda de codificare Radix64?

Pretty Good Privacy (PGP)

1. Ce servicii oferă PGP?
2. Cum se realizează autentificarea în PGP?
3. Cum se asigură confidenţialitatea în PGP?
4. Cum se realizează autentificarea şi confidenţialitatea, împreună, în PGP?
5. Cum se realizează compresia informaţiei in PGP?
6. Explicaţi modul de formare şi utilizare a inelelor de chei in PGP.

S/MIME

1. Cum se realizează autentificarea în S/MIME? (atenţie: există două tipuri de autentificare în S/MIME).
2. Cum se asigură confidenţialitatea în S/MIME?
3. Cum se realizează autentificarea şi confidenţialitatea, împreună, în S/MIME?
4. Explicaţi modul de formare şi utilizare a inelelor de chei in PGP.

Elemente de criptografie

1. Ce este un criptosistem simetric?
2. Ce este un criptosistem asimetric (cu chei publice)?
3. Care este diferenţa majoră între un criptosistem simetric şi unul cu chei publice?
4. Ce este o funcţie hash?
5. Ce este o semnătură digitală? Cum se construieşte semnătura digitală RSA?
6. In ce constă metoda de demonstraţie challenge-and-response?
7. Ce se înţelege prin zero-knowledge-proof?