UNIVERSITATEA "PETRU MAIOR" DIN TÎRGU MUREŞ
FACULTATEA DE ŞTIINŢE ŞI LITERE
DEPARTAMENTUL DE INFORMATICĂ

Tematica probei de concurs pentru ocuparea postului de Conferenţiar – Poziţia 7 din Statul de funcţiuni al Departamentului de Informatică 2014-2015

Disciplina: Securitatea informaţiei

Tematica:

1. Istoria criptografiei. Criptografia convenţională (simetrică). Moduri de cifrare (ECB, CBC, CFB, OFB, CTR). Studiu de caz: DES. Criptarea dublă. Cifruri flux. Studiu de caz: RC4.
2. Funcţii Hash. Paradoxul zilei de naştere. Proiectarea funcţiilor hash. Studiu de caz: MD5. Coduri de autentificare a mesajelor (MAC). Proiectarea MAC. Standardul HMAC.
3. Criptografia neconvenţională (asimetrică). Calcul modular. Studiu de caz: RSA. Semnături digitale. Infrastructuri de chei publice (PKI).
4. Descrierea protocoalelor de securitate. Atacuri. Protocolul SSH. Protocolul SSL/TLS.

Bibliografie:

1. Patriciu, V.V., Ene Pietroseanu, M., Bica, I., Cristea, C.: Securitatea informaţiei în UNIX şi Internet. Editura Tehnică Bucureşti, 1998.
2. Stallings, W.: Cryptography and network security: Principles and practice. Editura Prentice Hall, 2003.
3. Stallings, W., Brown, L.: Computer security: principles and practice. Editura Pearson Prentice Hall, 2008.
4. Forouzan, B.A.: Introduction to cryptography and network security. Editura McGraw-Hill, 2008.
5. Genge, B.: Introducere în implementarea aplicaţiilor criptografice. Editura Univ. Petru Maior, Tg. Mureş, 2013.

Disciplina: Programarea Sistemelor Distribuite

Tematica:

1. Arhitecturi de sisteme distribuite. Arhitecturi client-server şi peer to peer. Comunicarea în sisteme distribuite. Remote Procedure Call. Cozi de mesaje. Studii de caz: Skype şi BitTorrent.
2. Elemente specifice pentru sisteme de operare distribuite. Sincronizare. Tranzacţii. Mecanisme de detectare şi prevenire a interblocajului. Servicii de nume.
3. Servicii Web. Standarde specifice serviciilor Web. Securitatea în servicii Web. Securitatea protocolului TLS.

Bibliografie

1. Tanenbaum, A., Steen, M.: Distributed systems: Principles and Paradigms. Editura Prentice Hall, 2009.
2. Tanenbaum, A.: Sisteme de operare moderne. Editura Byblos, Bucureşti, 2004.
3. Boian, F.M., Ferdean, C., Boian, R., Dragoş, R.: Programare concurentă pe platforme Unix, Windows, Java. Editura Albastră, Cluj-Napoca, 2002.

4. Haller, P.: Proiectarea şi verificarea aplicaţiilor distribuite. Editura MatrixROM, Bucureşti, 2008.

Disciplina: <u>Protocoale de securitate în comunicaţii</u>

Tematica:

1. Rolul protocoalelor de securitate. Modelarea protocoalelor de securitate. Tehnici din teoria limbajelor formale. Modelarea atacurilor. Studii de caz: Wide-Mouthed-Frog, BAN, Lowe-BAN.
2. Atacuri cibernetice. Analiza securităţii sistemelor prin experimente de laborator şi "pen-testing". Studiu de caz: Stuxnet.
3. Proiectarea protocoalelor de securitate. Principii de proiectare. Teste de intrare-ieşire. Studii de caz: SSH, SSL/TLS şi PlanetLab.

Bibliografie

1. Patriciu, V.V., Ene Pietroseanu, M., Bica, I., Cristea, C.: Securitatea informaţiei în UNIX şi Internet. Editura Tehnică Bucureşti, 1998.
2. Doghmi, S.F., Guttman, J.D., Javier Thayer, F.: Completeness of the Authentication Tests. ESORICS 2007, LNCS 4734, pp. 106-121, 2007.
3. Stallings, W., Brown, L.: Computer security: principles and practice. Editura Pearson Prentice Hall, 2008.
4. Forouzan, B.A.: Introduction to cryptography and network security. Editura McGraw-Hill, 2008.
5. Hagerott, M.: Stuxnet and the vital role of critical infrastructure operators and engineers. International Journal of Critical Infrastructure Protection, Volume 7, Issue 4, pp. 244-246, 2014.
6. Genge, B., Siaterlis, C.: Analysis of the Effects of Distributed Denial-of-Service Attacks on MPLS Networks. International Journal of Critical Infrastructure Protection, Elsevier, Volume 6, Issue 2, pp. 87-95, 2013.

8.05.2015

DIRECTOR DEPARTAMENT,

Conf. dr. FINTA Béla