"PETRU MAIOR" UNIVERSITY OF TÎRGU MUREŞ
FACULTY OF SCIENCES AND LETTERS
DEPARTAMENTUL OF INFORMATICS

Topics for contest for the position 7 – Associate Professor
Department of Informatics
2014-2015

Discipline: Information Security

Topics:

1. *Brief history of cryptography. Conventional cryptography (symmetric). Cipher modes (ECB, CBC, CFB, OFB, CTR). Case study: DES. Double encryption. Stream ciphers. Case study: RC4.*
2. *Hash functions. Birthday paradigm. Designing hash functions. Case study: MD5. Message Authentication Codes (MAC). Designing MAC. HMAC standard.*
3. *Unconventional cryptography (asymmetric). Modular calculus. Case study: RSA. Digital signatures. Public key infrastructures (PKI).*
4. *Security protocol specifications. Attacks. SSH protocol. SSL/TLS protocol.*

References:

1. *Patriciu, V.V., Ene Pietroseanu, M., Bica, I., Cristea, C.: Securitatea informației în UNIX și Internet. Editura Tehnică București, 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 aplicațiilor criptografice. Editura Univ. Petru Maior, Tg. Mureș, 2013.*

Discipline: Distributed Systems Programming

Topics:

1. *Architectures of distributed systems. Client-server and peer to peer architecture. Communication in distributed systems. Remote Procedure Call. Message Queues. Case studies: Skype and BitTorrent.*
2. *Aspects specific to distributed operating systems. Synchronization. Transactions. Detecting and preventing interblocking. Name services.*
3. *Web services. Standards specific to Web services. Security of Web services. Security of TLS.*

References:

1. *Tanenbaum, A., Steen, M.: Distributed systems: Principles and Paradigms. Editura Prentice Hall, 2009.*
2. *Tanenbaum, A.: Sisteme de operare moderne. Editura Byblos, București, 2004.*
3. *Boian, F.M., Ferdean, C., Boian, R., Dragoș, R.: Programare concurentă pe platforme Unix, Windows, Java. Editura Albastră, Cluj-Napoca, 2002.*
4. *Haller, P.: Proiectarea și verificarea aplicațiilor distribuite. Editura MatrixROM, București, 2008.*

Discipline: ***<u>Security protocols in communications</u>***

Topics:

1. *The role of security protocols. Modeling of security protocols. Techniques from formal languages. Modeling attacks. Case studies: Wide-Mouthed-Frog, BAN, Lowe-BAN.*
2. *Cyber attacks. Analyzing systems by means of laboratory experiments and „pen-testing". Case study: Stuxnet.*
3. *Designing security protocols. Design principles. Input-output tests. Case studies: SSH, SSL/TLS and PlanetLab.*

References

1. *Patriciu, V.V., Ene Pietroseanu, M., Bica, I., Cristea, C.: Securitatea informației în UNIX și Internet. Editura Tehnică București, 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

HEAD OF DEPARTMENT,

Assoc.Prof.Dr. FINTA Béla