

Data Protection Technics and Cryptographic Protocols in Modern Computer Networks

Course Duration: 3 - 6 hours

Proposed Content:

1. Introduction
2. Information System Security – Key Questions of Security
3. Trends in Computer Network Security
4. Three lists of main security mistakes – end users
5. Three lists of main security mistakes – corporate management
6. Three lists of main security mistakes – professional informaticians
7. Potential attacks on computer networks of Intranet/Internet type
8. Possible ways of protecting from the considered attacks
9. Information eavesdropping
10. Faking identities
11. Destroying of valid messages or their replaying
12. Non-authorized modification of message contents
13. Repudiation
14. Security technologies
15. Cryptography and algorithm types
16. Types of cryptographic systems
17. Absolutely secret cryptographic system
18. Conditions of absolute secrecy – Shannon theorem
19. Symmetrical cryptographic systems
20. Stream cipher cryptographic systems
21. An example: RC4
22. Block ciphers
23. Features of block cipher algorithms
24. Working modes of the block cipher algorithms
25. Examples: DES, 3DES

26. An example: IDEA
27. An example: AES
28. Asymmetrical cryptographic systems
29. Diffie-Hellman system
30. An example: RSA algorithm
31. An example: DSA algorithm
32. An example: ECDSA algorithm
33. Hash functions
34. Examples: MD5 and SHA-1 algorithms
35. Digital signature technology
36. Digital envelope technology
37. PKCS standards
38. Multilayer architecture of the secure modern computer networks
39. Application layer security
40. S/MIME cryptographic protocol
41. Cryptographic API
42. PKCS#7 standard format of cryptographic messages
43. An example: FileSecure system
44. Transport layer security
45. SSL protocol
46. An example: SWT system
47. An example: WebWatch system
48. An example: WTLS protocol
49. Network layer security
50. IPSec cryptographic protocol
51. Firewalls
52. Cryptographic proxy security servers
53. Multilevel firewall configuration
54. Software and hardware security solutions
55. Smart cards
56. Cryptographic coprocessor modules
57. An example: NST 2000 crypto card
58. PKI systems

59. Component of PKI systems
60. Basic documents of PKI systems
61. Certification Authority (CA)
62. CA – security aspects
63. X.509 digital certificates
64. Digital certificate extensions
65. Certificate life cycle management
66. Certificate distribution systems
67. Registration Authority
68. PKI applications
69. An example: NetCert PKI system
70. E-government systems
71. Open problems in e-government systems applying
72. Digital signature law
73. European experiences in applying digital signature laws
74. Qualified electronic signatures and criteria for its creation
75. Secure Signature Creation Devices and conforming criteria
76. Criteria for certification authorities issuing qualified certificates
77. PKI systems – some experiences and open questions
78. PKI systems – some Serbian experiences
79. Conclusions

Brief biography of Milan Marković

Milan Marković received the B.S.E.E., M.S.E.E., and Ph.D. degrees in electrical engineering from Faculty of Electrical Engineering, University of Belgrade, Belgrade, Serbia, in 1989, 1992, and 2001, respectively. He is a leading researcher at the Mathematical Institute SANU, Belgrade and is currently a lecturer on Military Technical Academy for the “Secure Computer Networks” course and Faculty of Business Informatics Belgrade. His research interests are in cryptographic algorithms, public key infrastructure, combined SW/HW security solutions, smart cards, robust speech analysis, coding and recognition, statistical pattern recognition, signal processing, multimedia communication, wireless communications and wearable computing. He has been included in very sophisticated security projects, such as: PKI systems for s National Bank of Serbia, PKI systems for commercial banks, PKI systems for Ministries of Internal and Foreign Affaires, as well as PKI systems for ongoing Serbian smart card ID project. He is currently in Banca Intesa ad Beograd, as a Project Manager for security and is included in project of developing security policies, as well as in PKI consolidation project in the bank and in project of EMV DDA MasterCards with PKI applications on them.

Full contact address:

Milan Marković, Ph.D.E.E

Project Manager

IT Department

Banca Intesa ad Beograd

Vladimira Popovića 8

11070 Belgrade

Serbia and Montenegro

Tel.: +381 11 311 1106

Fax: +381 11 201 1517

Mobile: +381 64 8111 636

+381 63 7399 927

E-mail: milan.markovic@bancaintesacbeograd.com

www.bancaintesabeograd.com

Mathematical Institute SANU

Kneza Mihaila 35

P. F. 367

11001 Belgrade

Serbia and Montenegro

E-mail: mmarkov@beotel.yu