Course Title: CMSE512 Database and File Security (3 credits)

**Spring 2024**

**AIMS & OBJECTIVES**

**The main aim** of this course is to provide students with an introductory yet comprehensive overview of database and file security issues. It also provides an opportunity to feel practically flavour of database security questions in the frame of term project

**Catalog description:** Security requirements. Confidentiality, integrity, availability, assurance, authenticity, anonymity. Security threats and attacks on security, Protection, Intruders, Access control models. Discretionary and mandatory access control, Authorization. Multilevel security. Malicious software, Trojan horses. Password protection. Symmetric and public key encryption. DES. RSA. Digital signature. Key distribution and authentication. Secure Sockets Layer protocol. Passport: Single Sign-On. Electronic commerce. Secure Electronic Transaction protocol, Goods atomicity, Certified delivery and escrow. Electronic cash. Blind signature, Security in XML-based Web-services. Kerberos. X.509 authentication service. Authentication, procedures. One-time password. Hash functions. Statistical database security, Functional dependency attack on databases with multilevel security. Flow control, Covert channel, Auditing. Auditing process, Auditing classifications and types.

**Textbooks:**

1. *A) William Stallings, Operating Systems, Prentice Hall, 4th Ed., 2001, ISBN 0-13-031999-6; B)* William Stallings, Operating Systems: Internals and Design Principles, Pearson Education, Prentice Hall, 9th Ed., Global Edition, 2018, ISBN 10: 1-292-21429-5
2. Hassan A. Afyouni, Database Security and Auditing, Thomson, 2006, ISBN 0-619
3. Michael Kifer, Arthur Bernstein, Philip W. Lewis, Database Systems, Addison Wesley, 2nd Ed., 2006, ISBN 0-321-31256-2
4. *A) William Stallings, Cryptography and Network Security, Pearson, 4th Ed., 2006, ISBN 0-13-187316-4; B)* William Stallings, Cryptography and Network Security. Principles and Practices, 5th Edition, Pearson, 2011, 721 p., ISBN 10: 0-13-609704-9, ISBN 13: 978-0-13-609704-4
5. Ramez Elmasri, Shamkant B. Navathe, Fundamentals of Database Systems, Addison Wesley, 5th Ed., 2007, ISBN 0-321-41506-X
6. Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies Security in computing, Fifth edition, Pearson Education, Inc, 2015, ISBN 978-0-13-408504-3
7. Alfred Basta, Melissa Zgola, Database Security, Course Technology, CENGAGE Learning, 2012, ISBN-13: 978-1-4354-5390-6

**CONTENT & SCHEDULE (Tentative)**

Lectures will be held on *Wednesday,8.30 - 10.20, CMPE-034, and Friday, 8.30-9.20, CMPE-034*

The lecture topics within the semester are as in the following tentative schedule:

|  |  |
| --- | --- |
| **No** | **TOPICS** |
| 1 | Introduction (2 hours) |
| 2 | Security threats, Protection, Intruders, Malicious Software, Trojan Horses (3 hours, [1A], pp. 647-691; [1B], p. 657-692; [6], Ch. 1) |
| 3 | Trusted Systems, Windows Security, Security Architecture, Database Security Levels, Confidentiality, Integrity, Availability, Types of Vulnerabilities, Threats and Risks (3 hours, [1A], pp. 647-691; [1B], p. 657-692; [2], pp. 1-32) |
| 4 | Authentication, Authorization, Encryption. Digital Signature. Key Distribution and Authentication. Authorization. Authenticated Remote Procedure Call. Electronic Commerce. Secure Sockets Layer Protocol (3 hours, [3], pp. 1136-1185) |
| 5 | Passport: Single Sign-On. Keeping Credit Cards Numbers Private, Secure Electronic Transaction Protocol, Goods Atomicity, Certified Delivery and Escrow (3 hours, [3], pp. 1136-1185) |
| 6 | Electronic Cash: Blind Signatures, Security in XML-based Web-services (2 hours, [3], pp. 1136-1185) |
| 7 | Security in XML-based Web-services. Authenticated Applications. Kerberos (3 hours, [3], pp. 1136-1185, [4A], pp. 401-428; [4B], p. 410-484) |
| 8 | Kerberos, X.509 Authentication Service (3 hours, [4A], pp. 401-428; [4B], p. 410-484) |
| 9 | Control measure, Database Security and DBA, Discretionary Access Control, Mandatory Access Control (3 hours, [5], pp. 779-798; [7], Ch. 7, 8) |
| 10 | Statistical Database Security, Flow Control, Covert Channels, Auditing (3 hours, [5], pp. 779-798, [2], pp. 258-280) |
| 11 | Auditing Process, Auditing Classifications and Types (3 hours, [2], pp. 258-280) |

**ASSIGNMENTS**

Term project assumes development of secured database using studied methods.

**METHOD OF ASSESSMENT**

Written exams: midterm (30%) and final (45%);

Two quizzes - 5%

Term project – 20%

Attendance - 0%

**ATTENDANCE Policy**

Attendance is compulsory. Attendance is taken every lecture and entered to EMU portal. Those missing more than 80% of classes without valid excuse may get NG grade.

**If students miss the midterm or final exam, they MUST submit a written report, stating their excuse, to the course coordinator within 3 days after completion of the examination. Otherwise, they will not be allowed to take the make-up examination.**

**SOURCES**

All necessary for study sources will be posted on web

**Lecturer**: Prof. Alexander Chefranov

15.02.2024