| | | | |
|---|---|---|---|
| **Subject code:**<br>M.4(2) | **Subject name:** Mobile application security | | |
| **Study load:**<br>5 ECTS | **Load of contact hours:** 50 | **Study semester:**<br>Spring | **Assessment:**<br>5-points grade credit |
| **Objectives:** | Goals of this course:<br>- obtaining basic knowledge of information security, cryptography and steganography in order to protect data against unauthorized access and provide confidentiality of information exchange in mobile systems;<br>- obtaining professional competencies in the field of modern information security technologies in mobile application development. | | |
| **Course outline:** | Topics covered:<br>1. Introduction to mobile application security<br>2. Key areas of mobile application security<br>3. Securing in the iOS<br>4. Root certificate<br>5. Secure boot<br>6. Encryption and data protection<br>7. Securing in the Android OS<br>8. Cryptography libraries<br>9. Biometry<br>10. Encryption and data protection<br>11. Password protection<br>12. Mobile application security testing<br>13. Common types of cybersecurity attacks<br>14. Static and dynamic code analysis<br>15. Authorization and authentication<br>16. HTTP, HTTPS, SSL, TLS, VPN protocols<br>17. Common methods of authorization and authentication<br>18. Interaction with the operating system<br>19. Peer to peer connection<br>20. Local data storage<br>21. Embedded tools for user authentication and authorization<br><br>Contact lessons will be divided into two parts: lectures and practical tasks. | | |
| **Learning Outcomes:** | By the end of the course students (in the terms of knowledge, skills, and attitudes) should be able to:<br>1 – critically analyse and evaluate basic theories and practical aspects of ensuring information security of mobile applications;<br>2 – critically analyse and evaluate basic principles of protecting confidential information, mobile system user identification and authentication methods, principles of organizing covert channels;<br>3 – encrypt confidential information, use steganography, information integrity control, solution of identification and authentication tasks. | | |

| | |
|---|---|
| **Assessment Methods:** | Assessment splits into three parts: tests, practical tasks and 3 mandatory presentations. |
| **Teacher(s):** | Alexander Ivankov |
| **Prerequisite subject(s):** | None |
| **Compulsory Literature:** | Rohit Tamma, Practical Mobile Forensics - Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms |
| **Replacement Literature:** | Official security iOS documentation<br>https://www.apple.com/chde/business/docs/site/iOS_Security_Guide.pdf<br>Official security Android documentation<br>https://static.googleusercontent.com/media/www.android.com/ru//static/2016/pdfs/enterprise/Android_Enterprise_Security_White_Paper_2019.pdf |
| **Participation requirements:** | Lower limit of lectures attendance is 80%, each test and practical task must be presented by the end of the course. |
| **Independent work:** | 1. Data storage<br>2. Communication with the server<br>3. Application sandbox and user partition in the iOS<br>4. Protection classes and keychain in the iOS<br>5. Root certificate and device certification in the Android OS<br>6. Root access and launchers<br>7. Access to encrypted data on the drive<br>8. Vulnerabilities<br>9. Key storage and session storage<br>10. Random sequence generation<br>11. Interaction with the hardware |
| **Grading criteria scale or the minimal level necessary for passing the subject:** | **Points distribution:**<br>Failed: < 49 points<br>Passed, grade 3: 50-69 points<br>Passed, grade 4: 70-89 points<br>Passed, grade 5: >=90 points<br>**Ongoing assessment:**<br>Tests: 30 points<br>Practical tasks: 40 points<br>Presentations (3 per student): 30 points |

Points distribution (nested table):

| | |
|---|---|
| Failed | < 49 points |
| Passed, grade 3 | 50-69 points |
| Passed, grade 4 | 70-89 points |
| Passed, grade 5 | >=90 points |

| **Information about the course:** | Room ___, on ___ at ___ |
|---|---|
| **1) Date 1** | **Lecture 1**<br>Classroom presentation: Introduction to mobile application security<br>Classroom presentation: Key areas of mobile application security<br>Homework: Data storage |
| **2) Date 2** | **Practical task 1**<br>Students presentations: Data storage (10 points)<br>Classroom test: Key areas of mobile application security (3 points) |
| **3) Date 3** | **Practical task 2**<br>Classroom task: Realization of the Advanced Encryption Standard algorithm (3 points) |
| **4) Date 4** | **Lecture 2**<br>Classroom presentation: Securing in the iOS<br>Classroom presentation: Root certificate<br>Homework: Application sandbox and user partition in the iOS |
| **5) Date 5** | **Practical task 3**<br>Students presentations: Application sandbox and user partition in the iOS (10 points)<br>Classroom test: Securing in the iOS (3 points) |
| **6) Date 6** | **Practical task 4**<br>Classroom task: Realization of the TLS connection (3 points) |
| **7) Date 7** | **Lecture 3**<br>Classroom presentation: Secure boot<br>Classroom presentation: Encryption and data protection<br>Homework: Protection classes and keychain in the iOS |
| **8) Date 8** | **Practical task 5**<br>Students presentations: Protection classes and keychain in the iOS (10 points)<br>Classroom test: Encryption and data protection (3 points)<br>Homework: Communication with the server |
| **9) Date 9** | **Practical task 6**<br>Students presentations: Communication with the server (10 points)<br>Classroom task: Development of a program providing OAUTH 2.0 server connection (3 points) |
| **10) Date 10** | **Lecture 4**<br>Classroom presentation: Securing in the Android OS<br>Classroom presentation: Cryptography libraries<br>Homework: Root certificate and device certification in the Android OS |
| **11) Date 11** | **Practical task 7**<br>Students presentations: Root certificate and device certification in the Android OS (10 points)<br>Classroom test: Securing in the Android OS (3 points)<br>Homework: Root access and launchers |
| **12) Date 12** | **Practical task 8**<br>Students presentations: Root access and launchers (10 points)<br>Classroom test: Cryptography libraries (3 points) |
| **13) Date 13** | **Lecture 5**<br>Classroom presentation: Biometry |

| | |
|---|---|
| | Classroom presentation: Encryption and data protection<br>Classroom presentation: Password protection<br>Homework: Access to encrypted data on the drive |
| **14) Date 14** | **Practical task 9**<br>Students presentations: Access to encrypted data on the drive (10 points)<br>Classroom test: Biometry (3 points) |
| **15) Date 15** | **Practical task 10**<br>Classroom task: Development of a program providing secure key storage using biometrics (5 points) |
| **16) Date 16** | **Lecture 6**<br>Classroom presentation: Mobile application security testing<br>Classroom presentation: Common types of cybersecurity attacks<br>Classroom presentation: Static and dynamic code analysis<br>Homework: Vulnerabilities |
| **17) Date 17** | **Practical task 11**<br>Students presentations: Vulnerabilities (10 points)<br>Classroom test: Common types of cybersecurity attacks (3 points) |
| **18) Date 18** | **Practical task 12**<br>Classroom task: Modelling of the man in the middle attack (4 points) |
| **19) Date 19** | **Lecture 7**<br>Classroom presentation: Authorization and authentication<br>Classroom presentation: HTTP, HTTPS, SSL, TLS, VPN protocols<br>Classroom presentation: Common methods of authorization and authentication<br>Homework: Key storage and session storage |
| **20) Date 20** | **Practical task 13**<br>Students presentations: Key storage and session storage (10 points)<br>Classroom task: User authorization program development (6 points)<br>Homework: Random sequence generation |
| **21) Date 21** | **Practical task 14**<br>Students presentations: Random sequence generation (10 points)<br>Classroom task: User authentication program development (6 points) |
| **22) Date 22** | **Lecture 8**<br>Classroom presentation: Interaction with the operating system<br>Classroom presentation: Peer to peer connection<br>Classroom presentation: Local data storage<br>Classroom presentation: Embedded tools for user authentication and authorization<br>Homework: Interaction with the hardware |
| **23) Date 23** | **Practical task 15**<br>Students presentations: Interaction with the hardware (10 points)<br>Classroom task: Development of a client-server mobile application with completely protected user data (10 points) |
| **24) Date 24** | **Practical task 16**<br>Students presentations: mobile application projects demonstration (10 points) |
| **25) Date 25** | **Practical task 17**<br>Classroom test: Final mobile application security test (9 points) |