Contents

Security engineering: specifying, analyzing and verifying of security requirements, protection goals and protection mechanisms, risk management based on threat analyses,

security standards, formal models for computer security, cryptographic foundations and algorithms, specifying and analyzing security protocols, challenges in security engineering

Schedule & Slides

|  |  |  |
| --- | --- | --- |
| Date | Topic | Exam Preparation |
|  | **Introduction and Motivation** |  |
| **15.10.2018** | Examples of vulnerabilities in software systems, basic terms, dependability defined by Lapri | Mandatory |
| **22.10.2018** | Malware categorisation, computer virus vs. worm, adware, spyware, trojan horse | Do |
| **24.10.2018** | Buffer overflows, storage management, stack frames, code injection | Do |
| **29.10.2018** | Exercise: Buffer overflow | Do |
|  | Foundations & Motivation  1. Overview and basic terms (mandatory)  2. Malware categorisation (mandatory)  3. Examples for software vulnerabilities, e.g. buﬀer overﬂow (mandatory) |  |
|  |  |  |
|  | **Anonymity and Pseudonymity** |  |
| **05.11.2018** | Anonymity definitions, pseudonymity, remailer | probably |
| 07.11.2018 | Anonymous web browsing, JAP and Tor, Diffie-Hellman key exchange | probably |
| 12.11.2018 | Diffie-Hellman key exchange and Tor for Hidden Services | probably |
|  | **Security Analysis and Design Methods** |  |
| **14.11.2018** | Dining cryptographers, DC-Nets, Security engineering, process models, security analyses using misuse cases & attack trees, protection goals, conflicting objectives and strengthening goals  Reference : <https://www.youtube.com/watch?v=b6uBFTMeLL4>, Dining cryptographers, & DC Nets. | Mandatory |
| **19.11.2018** | Attack trees, Security design: Multilateral vs. multilevel security, Bell-LaPadula model | probably |
| **21.11.2018** | Multilevel Security and Information Flow Control using JiF | probably |
| **26.11.2018** | Exercise: Information Flow Control using JiF | probably |
|  | Security Analysis, Design & Anonymity (Part I)  4. Security process, misuse cases & attack trees (mandatory)  5. Multi-Level security, e.g. BLP & BIBA (probably)  6. Information ﬂow control, e.g. JiF (probably)  7. Anonymity & pseudonymity, e.g. TOR & DC (probably) |  |
|  |  |  |
|  | **Cryptological Encryption Techniques** |  |
| **28.11.2018** | Introduction to the history of cryptology, monoalphabetic and polyalphabetic cipher, one-time pad, Enigma | mandatory |
| **03.12.2018** | Pseudo-one-time pad, s2-mod-n generator, symmetric and asymmetric variant | probably |
| **05.12.2018** | GMR - strong cryptographic signature system |  |
| **10.12.2018** | Asymmetric encryption and digital signatures using RSA | probably |
| **12.12.2018** | Exercise: Calculations for RSA, s2-mod-n and GMR | probably |
| **17.12.2018** | Symmetric encryption using DES, Triple-DES and AES  Ref: https://www.youtube.com/watch?v=FUdEpUoA4mc | probably |
| **19.12.2018** | Cryptographic systems in operation: block cipher vs. stream cipher, ECB, CBC, CFB, OFB, CTR | probably |
| **07.01.2019** | Specific block or stream cipher for hard disk encryption, key management, attacks on hardware |  |
|  | Encryption Techniques (Part II)  8. History of cryptology, monoalphabetic and polyalphabetic cipher, one-time pad, Pﬁtzmann’s table (mandatory)  **Design and attacks for Enigma (probably not)**  9. Pseudo-one-time pad using s2-mod-n generator (probably)  **10. GMR - strong cryptographic signature system (probably not)**  11. RSA - encryption & signatures (probably)  12. DES/AES - symmetric encryption (probably)  13. Operation modes: block cipher vs. stream cipher (probably)  **Operation modes for full disc encryption (probably not)** |  |
|  |  |  |
|  | **Security Protocols and Verification Techniques** |  |
| **09.01.2019** | Needham-Schroeder protocol, typical attacks, man-in-the-middle attack and replay attack |  |
| **14.01.2019** | Kerberos protocol, differences between v4 and v5, time stamps and nonces to prevent replay attacks |  |
| **16.01.2019** | CSP and FDR, Verification of the Needham-Schroeder protocol using model checking |  |
| **21.01.2019** | Exercise: Protocol verification using FDR model checking |  |
| **23.01.2019** | Burrows-Abadi-Needham logic (BAN), analysis of the Wide Mouth Frog protocol |  |
| **28.01.2019** | Exercise: Protocol verification using ProVerif |  |
|  | Security Protocol Engineering (Part III)  14. Needham-Schroeder protocol (probably)  15. Kerberos protocol, v4 & v5 (probably)  **16. Analysis using BAN logic (probably not)**  **17. Veriﬁcation using CSP/FDR (probably not)** |  |
|  |  |  |
|  | Conclusions and Outlook |  |
| 30.01.2019 | Repetition of important content and preparation for the exam |  |

Exercise Sheets

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Exercise sheet publication | Deadline for submission | Contents | Documents |
| 1. | 28.11.18 | 07.01.19 | Security and information flow analyses |  |
| 2. | xx.xx.xx | xx.xx.xx | Protocol verification |  |

What are typical activities of a security analysis?