ECP 611   Network Security

Fundamentals of security and information assurance. Overview of the main concepts and technologies used in the area of cryptography and network security. Concepts, standards and protocols for mobile and wireless networks security. Intrusion detection systems, intrusion prevention systems, anomaly detection, network forensics, ethical and legal issues in information security. Overview of business issues of risk analysis and management of resources.

This course addresses relevant issue and case studies in modern information security in the distributed world. The objective is to provide student with solid understanding and working knowledge of modern information and network security challenges. The course also emphasis case studies.

Prerequisites:
ECP 601
ECP 602
or
ECP 625

Text books for basic material

- Ross J. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems," 2nd Edition, April 2008, John Wiley & Sons, ISBN: 978-0-470-06852-6. Also Available on line at: http://www.cl.cam.ac.uk/~rja14/book.html
  - main chapters used: 1, 3, 4, 5, 6, 7, 8, 9, 17, 18, 20, 21, and 26.

- Adam Shostack, "Threat Modeling: Designing for Security," Wiley; 1 edition (February 17, 2014), ISBN-13: 978-1118809990.
  - main chapters used: 2, 3, 4, 11, 13, Appendix E: "case studies"

Additional Reading

- Sumeet Dua, Xian Du, "Data Mining and Machine Learning in Cybersecurity," Auerbach Publications; 1 edition (April 25, 2011), ISBN-13: 978-1439839423.
- John Clark and Jeremy Jacob, "A Survey of Authentication Protocol Literature: Version 1.0," 1997, http://www-users.cs.york.ac.uk/~jac/PublishedPapers/reviewV1_1997.pdf.
- Matteo Avalle, Alfredo Pironti and Riccardo Sisto, "Formal verification of security protocol implementations: a survey ," Formal Aspects of Computing (2014) 26: 99–123 , DOI 10.1007/s00165-012-0269-9 (published online 4 December 2012).

- More to be added at course delivery time.

Outline

1. Introduction and overview: threats and challenges
2. Cryptography and cryptographic protocols
3. Secure design principles
4. Threat modeling and it's applications in secure system design
5. Network and Telecom Security
6. Security economics and game theory
7. Trust and trust management
8. Assessment and assurance
9. Case studies:
    - Secure cloud systems and storage
    - Network security, massive attacks, and epidemics
    - Mobile and IoT security
    - Industrial systems security
    - Privacy and social networks

Assessment

- Final exam: 20%
- Research paper: 40%
- Project: 40%