CS 704: SELECTED TOPICS IN NETWORK SECURITY (3-0-0:3)

Course Description

This course focuses on selected hot research topics in network security and is intended for Master or doctoral students who are interested in network security. Through this course, students can learn the state of the art and open problems in Internet and wireless security, thus enhancing their potential to do research or pursue a career in this exciting area. This course is structured as a research seminar where research papers from leading conferences & journals will be presented by a student or the instructor. There will one selected topic in each week, on which three to four papers will be assigned and discussed in class. The list of topics will be updated throughout the semester, depending on the availability of high-quality papers published or to appear in most recent top conferences & journals. Tentative topics may include (but not limited to):

- Distributed Denial-of-Service (DDoS) attacks and defense
- Worm defense
- Botnets defense
- Security of peer-to-peer (P2P) networks
- Security of IEEE 802.11 WLANs
- Anonymous communications
- Mobile malware detection and defense
- Modern telecom network security
- Social network security and privacy
- Security of mobile ad hoc networks
- Security of wireless sensor networks
- Security of vehicular networks
- Security of RFID networks
- Security in cloud computing

References:

1. Handbook of Applied Cryptography by Menezes, van Oorschot, and Vanstone (Free online version is available)
2. Cryptography and Network Security: Principles and Practice by William Stallings
3. Network Security: Private Communication in a Public World by Charlie Kaufman, Radia Perlman, Mike Speciner
4. RSA's Crypto FAQ: Frequently Asked Questions about Today's Cryptography, Version 4.1
5. Papers published in leading conferences and journals.