IT322 - Security Protocols (3-0-0-3)
[3rd year B.Tech, 2nd year MTech]

Instructor: Dr. Manik Lal Das
Office: 2103, Faculty Block 2 , Extn. 617 Email: maniklal_das@daiict.ac.in

Objective
Protocols describe how communication between entities takes place. It has been observed that a protocol may fail in three ways: the protocol design may be flawed, the cryptographic primitives used in the protocol may be weak, or the implementation may contain bugs.
This course primarily covers:
- Security properties, threats, and attacks.
- Some fundamental protocols including Kerberos, SSL, SSH, IPsec, WPA.
- Design and analysis aspects of security protocols.
The course will also discuss approaches for security protocols analysis wherever necessary.

Prerequisites: IT325 – Introduction to Cryptography

Contents (Tentative)
Brief review of security properties - authentication, privacy, integrity, non-repudiation, anonymity
Fundamental Security Protocols - Needham-Schroeder, Diffie-Hellman, Kerberos, SSL/TLS, SSH, IPSec, IKE, WPA.
Threats, Attacks, and Defenses - replay, man-in-the-middle, session freshness, forward secrecy, denial-of-service
Key agreement protocols - secret key based, public key based
Payment protocols – e-cash, SET, micro-payment
Multiparty computation - Oblivious transfer, bit commitment, coin flipping
Protocol analysis - Logic based approach

Outcomes
At the end of this course, students will be able to understand:
- Assumptions and goals of security protocols;
- Some real-world security protocols including payment protocols;
- Design principles and how intended security goals of protocols are being achieved;
- Attacks and mitigation strategies of security protocols;
- Logic based formal analysis of security protocols.

Recommended Books, literature
A few classic research papers on security protocols design and analysis.