Course name	Formal Methods for Information Security

Course ID: 40-???	**Credits:** 3	**Program:** Graduate
Prerequisites: Data & Network Security (40442)		**Co-requisites:**
Prepared by: Morteza Amini		

1. Aim

Diversity of computer security requirements results in introducing of different kinds of security models. In fact, each security model is an abstraction of a security policy. Importance of computer security motivates us to precisely specify and verify such security models using formal methods (such as set theory and different types of logics). In the first part of this course, different approaches for formal modeling and specification of security and access control (authorization) models are introduced and surveyed. In the second part of the course, formal specification and verification of security properties in security protocols using formal methods (especially different types of modal logics) are introduced. Introduction of BAN logic as well as Epistemic and Belief logic and using them for verification of some famous security protocols are the main topics of this part.

During this course, students learn how to use formal methods to formally and precisely specify their required security model or security protocol and how to verify them using existing formal approaches and tools.

2. Outline

- Introduction
  - Preliminaries on Formalization for Information Security
  - Modeling Methods: Set Theory and Logics
- **Formal Methods for Security Modeling**
  - Discretionary Security Models
    - Lampson Access Matrix Model and Discretionary Access Rule Definition
    - HRU Protection System
    - Safety Problem in Access Matrix Models
  - Information Flow Control Models
    - BellLapadula Formal Model
    - Denning's Lattice-based Model
    - Biba Integrity Model
  - Non-Interference and Non-Deducibility
  - Role-based Access Control Models
  - Security Models based on Algebra and Logics
    - Abadi's Access Control Calculus
    - Jajodia's Policy Composition Algebra
- **Formal Methods for Formal Specification and Verification of Security Protocols**

- Introduction to Modal Logics and Kripke Model
- Specification and Verification of Authentication Protocols using BAN Logic
  - Verification of Needham-Schroeder Protocol using BAN Logic
- Specification and Verification of Protocols using Epistemic and Belief Logics
  - Verification of Sample Protocols using Epistemic and Belief Logics

3. Evaluation Criteria

1. Mid-term Exam (35%)
2. Final Exam (25%)
3. Theoretical & Practical Assignments (15%)
4. Research Project (20%)
5. Class Activities (5%)

4. References

- G. Bella, "Formal Correctness of Security Protocols", Springer, 2007.
- P. Ryan, S. Schneider, and M.H. Goldsmith, "Modeling and Analysis of Security Protocols", Addison-Wesley, 2000.
- M. Bishop, "Computer Security", Addison-Wesley, 2003.
- Related papers and technical reports such as
  - D. E. Bell and L. J. La Padula, "Secure Computer System: Unified exposition and Multics interpretation", *Technical Report ESD-TR-75-306*, Mitre Corporation, Bedford, MA, March 1976.
  - M. Abadi, M. Burrows, B. Lampson, and G. Plotkin, "A Calculus for Access Control in Distributed Systems", *ACM Transactions on Programming Languages and Systems*, Vol. 15, No. 4, pp. 706-734, 1993.
  - D.F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn, R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control", *ACM Transactions on Information and System Security (TISSEC)*, Vol. 4, No. 3, pp. 224-274, ACM Press, 2001.
  - D. Wijesekera and S. Jajodia, "A Propositional Policy Algebra for Access Control", *ACM Transactions on Information and System Security*, Vol. 6, No. 2, pp. 286-325, ACM Press, 2003.
  - J.M. Rushby, "Noninterference, Transitivity, and Channel Control Security Policies", *Technical Report CSL-92-02*, SRI International, 1992.
  - K.J. Biba, "Integrity Considerations for Secure Computing Systems", *Technical Report TR-3153*, Mitre Corporation, Bedford, MA, April 1977.
  - D. E. Denning, "A Lattice Model of Secure Information Flow", *Communication of the ACM*, Vol. 19, No. 5, pp. 236-243, 1976.
  - M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication", ACM Transactions on Computer *Systems*, Vol. 8, pp. 18-36, 1990.