نام درس (فارسی)	**روش‌های صوری در امنیت اطلاعات**
نام درس (انگلیسی)	**Formal Methods for Information Security**

شماره درس: ۴۰-؟؟؟	**تعداد واحد:** ۳	**مقطع:** تحصیلات تکمیلی
پیش‌نیازها: امنیت داده و شبکه (۴۰-۴۴۲)		**هم‌نیازها:**
تهیه‌کننده: مرتضی امینی		

هدف

با توجه به تنوع نیازمندی‌های امنیتی، مدل‌های امنیتی مختلفی وجود دارد که در واقع هر یک از این مدل‌ها انتزاعی از یک نوع خط‌مشی امنیتی محسوب می‌گردند. با توجه به اهمیت مقوله امنیت کامپیوتری، توصیف دقیق هر یک از این مدل‌ها با استفاده از روش‌های صوری (مانند استفاده از نظریه مجموعه‌ها و انواع منطق) و سپس وارسی سازگاری توصیف از اهمیت بسزایی برخوردار است. در این درس نحوه مدل‌سازی صوری انواع مدل‌های امنیتی و مدل‌های کنترل دسترسی (مجازشماری) با استفاده از روش‌های صوری مورد مرور و بررسی قرار می‌گیرد. علاوه بر مدل‌های امنیتی، استفاده از روش‌های صوری (و به خصوص انواع منطق‌های وجهی) می‌تواند در توصیف و وارسی پروتکل‌های امنیتی نیز مورد استفاده قرار گیرد. در بخش دوم این درس به بررسی چند روش توصیف و درستی‌یابی پروتکل‌های امنیتی و بررسی چند پروتکل معروف با استفاده از این روش‌ها پرداخته می‌شود.

در طی این درس دانشجویان که چگونه از روش‌های صوری برای توصیف دقیق و صوری مدل امنیتی موردنیاز خود و یا یک پروتکل امنیتی استفاده کنند و چگونه با استفاده از روش‌های صوری و ابزار موجود برای وارسی و درستی‌یابی آنها استفاده نمایند.

سرفصل مطالب

- مقدمه
  - مفاهیم و اصطلاحات مرتبط با صوری‌سازی در امنیت اطلاعات
  - ابزارهای مدل‌سازی: نظریه مجموعه‌ها و منطق
- **روش‌های صوری در مدل‌سازی امنیت**
  - مدل‌های اختیاری (DAC)
    - مدل ماتریس دسترسی لمپسون و توصیف قواعد دسترسی اختیاری
    - مدل سیستم حفاظتی HRU
    - مساله ایمنی (Safety) در مدل‌های ماتریس-مبنا
  - مدل‌های کنترل جریان اطلاعات (Information Flow Control)
    - مدل صوری BellLapadula
    - مدل مبتنی بر مشبکه Denning
    - مدل کنترل صحت Biba
  - عدم تداخل و عدم استنتاج (Non-interference, Non-Deducibility)

- مدل‌های نقش-مبنا (RBAC)
- مدل‌های مبتنی بر جبر و منطق
  - منطق کنترل دسترسی Abadi
  - جبر ترکیب خط‌مشی دسترسی Jajodia

- **روش‌های صوری در توصیف و تحلیل پروتکل‌های امنیتی**
  - مقدمه‌ای بر منطق وجهی و مدل کریپکی
  - توصیف و درستی‌یابی با منطق احراز اصالت BAN
    - وارسی پروتکل Needham-Schroeder با منطق BAN
  - توصیف و درستی‌یابی با منطق باور (Belief) و دانایی (Epistemic)
    - وارسی یک پروتکل نمونه با منطق باور و دانایی

منابع

- 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.

نحوه ارزیابی

- امتحان پایان‌ترم (۳۵٪)
- امتحان میان‌ترم (۲۵٪)
- تمرین‌های نظری و عملی (۱۵٪)
- پروژه تحقیقاتی (۲۰٪)
- فعالیت و مشارکت در کلاس (۵٪)