باسمه تعالی

طرح درس جهت ارائه در نیمسال تحصیلی اول ۱۴۰۳-۱۴۰۲

دانشکده	**مهندسی برق و کامپیوتر**	**گروه**	**معماری سیستم‌های کامپیوتری**
گرایش	**امنیت سایبری**	**مقطع**	**کارشناسی ارشد**
نام درس	**روش‌های صوری برای امنیت اطلاعات**	**نوع درس**	**پایه** ☐ **نظری** ☑ **تخصصی** ☑ **عملی** ☐ **اختیاری** ☑ **نظری-عملی** ☐
تعداد واحد	**۳**	**نام استاد**	**حسین همائی**
دروس پیش‌نیاز	**ندارد**	**تلفن دفترکار**	**۳۹۰۵**
دروس هم‌نیاز	**ندارد**	**پست الکترونیک**	homaei@modares.ac.ir

✓ **اهداف درس:**

۱. آشنایی با انواع مدل‌های صوری
۲. آشنایی با مدل‌های صوری کنترل دسترسی
۳. آشنایی با مدل‌های صوری جریان اطلاعات
۴. آشنایی با روش‌های تحلیل صوری پروتکل‌های امنیتی

✓ **رئوس مطالب و برنامه ارائه در کلاس:**

شماره جلسه	موضوع جلسه درس	توضیحات
جلسات هفته اول	مقدمات	معرفی درس، اهمیت، تعاریف پایه، کاربردها، منطق و انواع آن، روش‌های اثبات، مجموعه‌ها
جلسات هفته دوم	مدل HRU	بیان مدل، اثبات تصمیم‌ناپذیری قضیه safety در حالت کلی، اثبات تصمیم‌پذیری قضیه safety برای سیستم‌های mono-operational
جلسات هفته سوم	مدل Take-Grant	بیان مدل، بررسی مسأله safety در گراف Take-Grant
جلسات هفته چهارم	سیستم‌های نوع	مفهوم نوع و عبارات خوش نوع، مفهوم زبان‌های safe، حساب‌های lambda و typed-lambda و بررسی safety
جلسات هفته پنجم	مدل محافظتی شماتیک	بیان مدل و نحوه تغییر حالت
جلسات هفته ششم	مدل محافظتی شماتیک	میرایی، مفهوم maximal state
جلسات هفته هفتم	مدل محافظتی شماتیک	تحلیل safety
جلسات هفته هشتم	مدل BLP	بیان مدل، خصیصه‌های امنیتی، اثبات برآورده‌سازی خصیصه‌های امنیتی
جلسات هفته نهم	عدم تداخل	کانال نهان، مبانی عدم تداخل، مدل‌سازی سیستم‌های ایستا و پویا، بیان صوری خط‌مشی‌های امنیتی
جلسات هفته دهم	ارزیابی پروتکل‌های امنیتی	مبانی و انواع روش‌های تحلیل صوری پروتکل‌های امنیتی، مدل مهاجم، تفاوت با تحلیل رمز
جلسات هفته یازدهم	منطق BAN	معرفی، صوری‌سازی پروتکل‌ها، تحلیل پروتکل‌ها
جلسات هفته دوازدهم	حساب pi	معرفی (صرف و نحو و معنا) حساب pi، مدل‌سازی پروتکل‌ها

جلسات هفته سیزدهم	حساب Spi	معرفی حساب Spi، مدل‌سازی و تحلیل پروتکل‌های امنیتی
جلسات هفته چهاردهم	Proverif	تئوری، معرفی و کاربرد ابزار
جلسات هفته پانزدهم	وارسی مدل	مقدمات وارسی مدل، منطق LTL، ابزار SPIN، کاربرد در تحلیل پروتکل‌های امنیتی
جلسات هفته شانزدهم	اثبات کننده قضیه	تئوری حل‌کننده محدودیت‌ها، SAT و SMT، ابزار Z3 Isabelle/HOL و کاربرد آن در تحلیل پروتکل‌های امنیتی

✓ **روش ارزشیابی:**

سمینار (۴ نمره)، تمرین‌ها و پروژه‌ها (۲ نمره)، امتحانات (۱۴ نمره)

✓ **منابع :**

[1] M. Huth and M. Ryan. *Logic in Computer Science: Modelling and reasoning about systems*. Cambridge University Press, 2004.
[2] M. Ben-Ari. *Mathematical logic for computer science*. Springer Science & Business Media, 2012.
[3] M. Sipser. *Introduction to the Theory of Computation*. Cengage Learning, 2012.
[4] D. W. Cunningham. *Set Theory: a first course*. Cambridge University Press, 2016.
[5] M. Bishop. *Computer Security: Art and Science*. 2nd edition, Addison-Wesley, 2019.
[6] M. Harrison, W. L. Ruzzo, and J. D. Ullman. "Protection in operating systems." *Communications of the ACM* 19.8 (1976): 461-471.
[7] 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, 1976.
[8] R. J. Lipton and L. Snyder. "A linear time algorithm for deciding subject security." *Journal of the ACM (JACM)* 24.3 (1977): 455-464.
[9] J.A. Goguen and J. Meseguer, "Security Policies and Security Models", IEEE Symposium on Security and Privacy, pp. 11-20, 1982.
[10] R. S. Sandhu. "The schematic protection model: its definition and analysis for acyclic attenuating schemes." *Journal of the ACM (JACM)* 35.2 (1988): 404-432.
[11] C. Cremers and S. Mauw. *Operational Semantics and Verification of Security Protocols*. Springer-Verlag, 2012.
[12] V. Cortier, and S. Kremer, *Formal Models and Techniques for Analyzing Security Protocols*, IOS Press, 2011.
[13] P. Ryan and S. A. Schneider. "The modelling and analysis of security protocols: the CSP approach." (2001).
[14] M. Burrows, et al. "A logic of authentication." *Digital Equipment Corporation Systems Research Center*, Report 39, Feb. 1989.
[15] M. Abadi and A. D. Gordon. "A calculus for cryptographic protocols: The spi calculus." *Information and computation* 148.1 (1999): 1-70.
[16] G. J. Holzmann, "The model checker SPIN," IEEE Transaction on Software Engineering, vol. 23, no. 5, p.279–295, May 1997.
[17] B. Blanchet, *Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif*. now Publishers, 2016.
[18] L. De Moura and N. Bjørner, "Satisfiability modulo theories: Introduction and applications," Commun. ACM, vol. 54, no. 9, p. 69–77, Sep. 2011.
[19] L. De Moura and N. Bjørner, "Z3: An efficient SMT solver," in International conference on Tools and Algorithms for the Construction and Analysis of Systems. Springer, 2008, pp. 337–340.
[20] T. Nipkow, L. C. Paulson, and M. Wenzel, Isabelle/HOL – A Proof Assistant for Higher-Order Logic, ser. Lecture Notes in Computer Science. Springer, 2002, vol. 2283.