به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

تحلیل پروتکل های رأی گیری الکترونیکی با رویکرد امنیت اثبات‌پذیر

علیرضا طرقی حقیقت

زمان: شنبه ۱۶ شهریور، ساعت ۹:۰۰

مکان: دانشکده کامپیوتر، آزمایشگاه امنیت داده و شبکه

تاکنون تلاش‌های زیادی به منظور ارائه پروتکل‌های رأی‌گیری الکترونیکی امن انجام گرفته است. این پروتکل‌ها دارای ویژگی‌های امنیتی متعددی مانند صحت، وارسی‌پذیری، مجازبودن، مقاومت در برابر اجبار، بی‌رسیدی، و حفظ حریم خصوصی هستند. هریک از پروتکل‌های رای‌گیری الکترونیکی موجود تلاش کرده‌اند تا برخی از این ویژگی‌ها را فراهم کنند. با این حال در اغلب موارد، برای اثبات ویژگی‌های امنیتی از اثبات‌های دقیق استفاده نشده، و صرفاً به تحلیل‌های شهودی بسنده شده است. در نتیجه بسیاری از ویژگی‌های امنیتی مورد ادعای این پروتکل‌ها نقض شده است. امنیت اثبات‌پذیر یکی از روش‌های قاعده‌مند و مبتنی بر ریاضیات در تحلیل پروتکل‌های امنیتی است که مزیت اصلی آن، گره زدن امنیت یک پروتکل به یک مسئله سخت در نظریه محاسبات است. در این ارائه ضمن مروری بر مفاهیم رای‌گیری الکترونیکی و امنیت اثبات‌پذیر، به تشریح کارهای انجام شده در طول این پژوهش می‌پردازیم.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.