به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

Intel Software Guard Extensions(Intel SGX)

سید محمد آقامیر محمد علی

زمان: شنبه ۱ خرداد ماه ۱۳۹۵ ساعت ۹:۱۵

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهار، سالن خوارزمی

افزونه محافظ نرم‌افزار(امن)، یک تکنولوژی معرفی شده از طرف شرکت اینتل است برای استفاده‌ی برنامه‌نویسانی که به‌دنبال محافظت از بخشی از کد و یا داده‌ی خود در مقابل افشا و یا دستکاری هستند. امن این محافظت را با فراهم‌سازی و استفاده از حافظه‌های محافظت‌شده (enclaves) قادر می‌سازد که از محیط اجرا محافظت کند. برنامه‌های کاربردی می‌توانند توسط پردازنده‌ی اینتل دارای افزونه‌ی محافظ نرم‌افزار در داخل حافظه‌های محافظت‌شده قرار گیرند و اجرا شوند به‌گونه‌ای که با اطمینان به سخت‌افزار، امنیت در مقابل افشا و دستکاری توسط پردازنده تامین شود. در این سخنرانی ما قصد داریم نحوه‌ی کارکرد این افزونه را شرح دهیم.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.