

جزئیات برگزاری کارگاه‌های آموزشی هشتمین کنفرانس بین‌المللی انجمن رمز ایران
<http://iscisc2011.um.ac.ir>

۱. کد کارگاه : W07

۲. عنوان: تروجان‌های سخت‌افزاری

۳. چکیده: امروزه مدارات مجتمع در معرض آسیب تروجان‌های سخت‌افزاری قرار دارند که تغییرات مخربی را در هنگام طراحی و یا در هنگام ساخت در مدار ایجاد می‌کنند. به دلیل عمومیت یافتن پروسه طراحی و ساخت نیمه‌هادی‌ها، IC ها بیشتر در معرض آسیب‌های ناشی از عملیات و تغییرات مخرب قرار دارند. هنگامی این تغییرات مخرب بصورت تهدیدی برای سیستم‌های نظامی، سیستم‌های مالی، امنیت حمل و نقل و تجهیزات خانگی مطرح می‌شوند، از اهمیت بیشتری برخوردار می‌شوند. دشمن می‌تواند با وارد کردن یک تروجان سبب از کار افتادن یا تخریب یک دستگاه در آینده شود و یا می‌تواند با حفره ایجاد شده بوسیله تروجان اطلاعات محرمانه و کلیدهای پنهان امنیتی را در اختیار دشمن قرار دهد. تروجان‌ها می‌توانند بصورت‌های مختلف از قبیل سخت‌افزارهای بهینه‌سازی شده در ASIC ها، قطعات تجاری‌سازی شده بوسیله تولید انبوه (COTS)، میکروپروسورها، میکروکنترلرها، پردازشگرهای شبکه و یا پردازشگرهای سیگنال‌های دیجیتال (DSP) اجرا شوند. همچنین تروجان‌ها می‌توانند بصورت برنامه‌های دائمی مانند رشته‌ای از بیت‌ها در FPGA اجرا شوند. در این کارگاه یک طبقه‌بندی از تروجان‌های سخت‌افزاری و خلاصه‌ای از شیوه‌های آشکارسازی آن‌ها ارائه خواهد شد.

۴. ارائه‌دهنده:

نام و نام خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	عنوان شغلی	وابستگی	رایانامه
رضا ابراهیمی آتانی	دکتری	مهندسی برق گرایش الکترونیک	عضو هیات علمی	دانشگاه گیلان	rebrahimi@guilan.ac.ir

۵. زندگی‌نامه ارائه‌دهنده: آقای ابراهیمی آتانی دانش‌آموخته دکتری مهندسی برق گرایش الکترونیک از دانشگاه علم و صنعت ایران می‌باشند و هم‌اکنون نیز استادیار گروه مهندسی کامپیوتر دانشگاه گیلان هستند. عنوان پایان‌نامه دوره دکتری ایشان، طراحی و پیاده‌سازی یک الگوریتم رمز دنباله‌ای جهت کاربرد در مخابرات سیار بوده است. زمینه‌های تخصصی دکتر ابراهیمی شامل طراحی، تحلیل و پیاده‌سازی الگوریتم‌های رمزنگاری، امنیت شبکه‌های بی‌سیم، طراحی سخت‌افزارهای رمزنگار و توابع جاسازی‌شده، پنهان‌گاری اطلاعات و زمینه‌های مرتبط است و تاکنون کارگاه‌های آموزشی مختلفی را از جمله در هفتمین کنفرانس بین‌المللی انجمن رمز ایران برگزار کرده‌اند.

۶. مخاطبان کارگاه:

○ دانشجویان و محققین علاقه‌مند به پیاده‌سازی سخت‌افزارهای رمزنگاری و سیستم‌های تعبیه شده

۷. سرفصل:

- مروری بر روش‌های متداول طراحی و ساخت و تست مدارات مجتمع
- معرفی جامع و مفهومی تروجان‌های سخت‌افزاری و طبقه‌بندی کلی آن‌ها
- طبقه‌بندی تروجان‌های سخت‌افزاری بر اساس مشخصات فیزیکی، حوزه عملیاتی و اساس مشخصات فعال سازی آن‌ها
- معرفی کامل روش‌های ارایه شده آشکارسازی تروجان‌های سخت‌افزاری و طبقه‌بندی جامع همگی الگوریتم‌ها و بررسی میزان موفقیت آن‌ها روی تروجان‌های سخت‌افزاری
- بررسی تهدیدات صنعتی و نظامی تروجان‌های سخت‌افزاری در کشور و ارایه راه‌کارهای کلی برای مقابله و شناسایی آن‌ها.

۸. زمان برگزاری: نیم‌روز - سه‌شنبه ۲۲ شهریور ۱۳۹۰ - ساعت ۱۴ الی ۱۸

۹. پیش‌نیاز:

- دانشجویان کارشناسی ارشد و دکتری مهندسی الکترونیک و مهندسی کامپیوتر گرایش سخت‌افزار
- مهندسين و متخصصين طراحی مدار و سخت‌افزار شرکت‌های صنعتی
- کارشناسان و کارشناسان ارشد صنایع دفاعی
- مدیران و کارشناسان شبکه

برای اطلاع از نحوه ثبت‌نام در این کارگاه به وب‌گاه <http://iscisc2011.um.ac.ir> مراجعه نمایید.