به نام خدا

جلسه‌ی سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

پین: تحلیل پویای نرم‌افزار با ابزارکشی دودویی

PIN: Dynamic Software Analysis using Binary Instrumentation

بهنام مومنی

زمان: یکشنبه ۱۳۹۳/۱۰/۱۴ ساعت ۴:۱۵ عصر

مکان: دانشکده مهندسی کامپیوتر، طبقه چهارم، سالن خوارزمی (۴۰۴)

در زمینه‌های گوناگونی نیاز به تحلیل نرم‌افزار بدون دراختیار داشتن کد منبع آن به عنوان عنصر اصلی دیده می‌شود. برای نمونه تحلیل بدافزارها، خطایابی نرم‌افزار در زمان اجرا یا نمایه‌سازی نرم‌افزار (profiling) با هدف یافتن گلوگاه‌ها و بهبود کارایی آن در عمل، همگی نیازمند تحلیل نرم‌افزار به صورت دودیی و در زمان اجرا هستند. این نوع از تحلیل از جهت تعامل با نرم‌افزار در زمان اجرای آن، پویا نامیده شده و با شگردهای گوناگونی همچون اتصال به پردازه‌ی اجرایی با یاری سخت‌افزار، پایش حافظه‌ی موقت یا دایمی و قلاب‌اندازی (hooking) فراخوانی‌های سامانه‌ای انجام می‌شود. در این ارایه، پس از مروری کوتاه بر روی این روش‌ها، شیوه‌ی تحلیل پویا با بهره‌گیری از ابزارکشی دودویی (binary instrumentation) و به طور خاص بستر پین (PIN) به عنوان یک راه‌کار برای محقق ساختن آن معرفی می‌شود. پین یک بستر نرم‌افزاری است که توسط اینتل ارایه شده و برنامه‌های دودویی آماده‌شده برای سامانه‌های عامل گوناگون (از جمله لینوکس، ویندوز و اندروید) را ابزارکشی می‌کند. بدین صورت می‌توان دستورهای دلخواهی را برای پایش و کنترل رفتار نرم‌افزار در حین اجرا در میان دستورهای هم‌گذاری (assembly) نرم‌افزار درج کرد. همچنین می‌توان با رعایت محدودیت‌هایی، از شاخته‌شدن توسط نرم‌افزار در حال تحلیل و در نتیجه تاثیر بر روی رفتار آن جلوگیری کرد.

- شرکت در این جلسه برای همه‌ی دانشجوهای علاقه‌مند آزاد است -