به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

تحلیل بمب منطقی در بدافزارهای اندرویدی با استفاده از اجرای پویا-نمادین

Analyzing Logic Bomb in Android Malware through Concolic Execution

محمود اقوامی پناه

زمان: شنبه ۳۱ فروردین ماه ۱۳۹۸ ساعت ۹:۱۵

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

بمب‌منطقی به دسته خاصی از بدافزارهای اندرویدی گفته می‌شود که تحت برآورده شدن شرایط مشخص رفتار بدخواهانه خود را به نمایش می‌گذارند. به‌عنوان نمونه‌هایی از بمب منطقی می‌توان به بدافزارهایی اشاره کرد که بر اساس یک زمان‌بندی خاص، قرار گرفتن در یک مکان خاص جغرافیایی و یا دریافت یک پیامک با محتوای مشخص، رفتار بدخواهانه خود را به اجرا می‌گذراند. تشخیص این دسته از بدافزارها مشکل است زیرا برای مشاهده رفتار بدخواهانه آن‌ها باید، شرط تلنگر بدافزار در زمان اجرا فعال گردد. ما در این ارایه اجرای پویا-نمادین در سطح کد اجرایی برنامه‌های اندرویدی را شرح می‌دهیم. این اجرا مبتنی بر فایلOAT برنامه اندرویدی صورت می‌گیرد و به ما کمک می‌کند تا با فعال‌سازی نقاط تلنگر بمب‌منطقی، پوشش کد بیش‌تری را در هنگام تحلیل فراهم آوریم.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.