به نام خدا

جلسه‌ی ارایه‌ی هفتگی آزمایشگاه امنیت داده و شبکه


# ابهام زدایی نرم‌افزار و کاربردهای آن در تحلیل بدافزار

# *Software De-Obfuscation and its Applications to Malware Analysis*

بهنام مومنی

## زمان: شنبه ۱۳۹۳/۰۶/۰۸ ساعت ۳ عصر

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

مبهم‌سازی نرم‌افزار با ایجاد تغییرهای ظاهری و پیچیده‌ساختن آن، فهم کارکرد نرم‌افزار را دشوار می‌سازد. امروزه مبهم‌سازی به عنوان ابزاری در دست توسعه‌دهندگان بدافزارها شناخته شده تا آنجا که کمتر بدافزاری وجود دارد که دست کم از یک لایه‌ی مبهم‌سازی بهره نگیرد. رویکرد متداول برای ابهام‌زدایی از برنامه‌های رایانه‌ای فرآیندی تدافعی است که طی آن محقق‌ها پس از شناخت هر روش مبهم‌سازی، برای معکوس نمودن آن اقدام می‌کنند. این رویکرد با پیچیده‌تر شدن روش‌های مبهم‌سازی و پایین آمدن هزینه‌ی کاربرد چندین لایه‌ی مبهم‌سازی در کنار هم در بدافزارها نیاز به ابهام‌زدایی خودکار را تقویت کرده است.

در این ارایه شیوه‌های مبهم‌سازی که می‌توانند مورد بهره‌گیری بدافزارها قرار گیرند و روش‌های دفاعی موجود در برابر آن‌ها مرور گشته و چارچوبی برای ابهام‌زدایی از آن‌ها معرفی می‌شود. چارچوب پیشنهادی با کاهش کوک از الگوریتم ابهام‌زدایی به سه الگوریتم دیگر برای اجرای عینی-نمادین برنامه‌ها، تحلیل مسیرهای اجرایی برنامه‌ها و حل معادله‌های نمادین اجازه‌ی ابهام‌زدایی از روش‌های مبهم‌سازی شناخته‌شده را فراهم می‌کند. این چارچوب از شگردهای خاص مبهم‌سازها نابسته بوده و در نتیجه می‌تواند در برابر روش‌های ناشناخته‌ی آتی نیز سودمند باشد. حاصل ابهام‌زدایی در قالب کد همزاد نوشته شده و همچنین یک معماری برای تولید کد همزاد برنامه‌ی مبهم‌شده‌ی دلخواه با نمونه‌سازی از روی چارچوب پیشنهادی معرفی می‌شود.

شرکت در این جلسه برای همه‌ی دانشجوهای علاقه‌مند آزاد است