به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

مروری بر روش‌های درون نگر ماشین مجازی

An Overview of Virtual Machine Introspection Techniques

مریم السادات مسعودیان

زمان: شنبه ۱۱ اسفندماه ۱۳۹۴ ساعت ۱۵: ۹

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

درحوزه امنیت و تحلیل بدافزارها، ابزارهای بازبینی متعددی از جمله ضدبدافزارها، برای تحلیل حافظه و ردیابی رخدادهای صورت گرفته برروی آن ارائه شده‌اند. یکسان بودن محیط تحلیل و اجرا در این ابزارها، امکان شناسایی و دور زدن روش‌های بازبینی را فراهم کرده و یک چالش مهم به شمار می‌رود. با پدید آمدن مفهوم مجازی‌سازی و امکان مدیریت و کنترل برنامه‌های درونی ماشین‌های مجازی از بیرون، روش‌های متعددی برای بازبینی و وارسی درستی رفتار این ماشین‌ها، بانام درون‌نگر ماشین مجازی ارائه شده‌اند. این روش‌ها، باجداسازی مکان قرارگیری ابزار بازبین و محیط اجرایی، برای رفع مشکل شناسایی و دور زدن ابزار بازبین تلاش کرده‌اند. هدف این ارایه، معرفی روش‌های درون نگری ماشین مجازی و بررسی مشکلات این روش‌ها است.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.