به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

به‌کارگیری مکانیزم بدافزارها در قالب روش‌های دفاعی در مقابل آنها

فرشته رزمی

زمان: شنبه ۱۲ اسفند، ساعت ۹:۰۰

مکان: دانشکده کامپیوتر، آزمایشگاه امنیت داده و شبکه

چکیده

روند صعودی تعداد بدافزارهای ایجاد شده و افزایش پیچیدگی آن‌ها سبب شده است تا متخصصان حوزه امنیت به دنبال ارائه راهکارهای نوین برای مقابله هرچه کاراتر با بدافزارها باشند. مقابله با بدافزارها اغلب به صورت تشخیص و حذف آنها بر روی سیستم قربانی صورت می‌گیرد. راهکارهای تشخیصی با وجود روش‌های چندریختی و مبهم‌سازی با چالش‌های بسیاری مواجه شده است، از این رو اتخاذ روش‌های دفاعی جدید ضروری به نظر می‌رسد. در برخی موارد عملکرد مشترک بین بدافزارها می‌تواند مبنای راهکارهای دفاعی قرار گیرد. این عملکرد مشترک توسط تحلیلگران آگاه از شیوه رفتار بدافزارها تغییر داده شده و به عنوان راهکار دفاعی مورد استفاده قرار می‌گیرد. در واقع بدافزار خود می‌تواند شیوه مقابله با خود را نیز ارائه دهد. در این ارائه برخی از روش‌های دفاعی برگرفته از عملکرد بدافزارها معرفی خواهند شد.

شرکت در این ارائه برای تمامی دانشجویان علاقه‌مند آزاد است.