به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

Data and Network Security Laboratory

تشخیص جریان‌های بدخواه در شبکه بر اساس خصوصیت‌های رفتاری کاربران

Malicious Network Flow Detection based on Behavioral Characteristics of Users

ابوالفضل زرگر

زمان: شنبه ۱۵ اسفندماه ۱۳۹۴ ساعت ۹:۱۵

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

امروزه شاهد پیشرفت و گسترش دانش، امکانات، و انگیزه مهاجمان برای دزدی اطلاعات و خرابکاری در شرکت‌های بزرگ و سازمان‌های مهم هستیم. این موضوع موجب شکل‌گیری نسل جدیدی از تهدیدات به نام "تهدیدات پیشرفته پایا" شده است. در این‌گونه تهدیدات، مهاجم سعی دارد برای دستیابی به هدف نهایی خود، در طول اجرای گام‌های حمله، تا حد امکان، هیچ اثری از خود بروز ندهد. لذا در گام‌هایی از حمله که نمود شبکه‌ای دارند، سعی می‌کند که اهداف خود را در قالب جریان‌های قانونی و متداول محقق کند. این رویکرد، معمولا راهکارهای مبتنی بر سوء استفاده را بی‌اثر کرده و راهکارهای مبتنی بر ناهنجاری را با چالش‌های اساسی روبرو می‌کند. در این پایان‌نامه، جریان‌های مشکوک ولی قانونی را که اغلب در تهدیدات پیشرفته پایا مشاهده می‌شوند، از طریق تحلیل برخط داده‌های رفتاری کاربران، که از سطح شبکه و میزبان‌ها استخراج شده، کشف می‌کنیم. حجم بسیار بالای داده‌های مورد استفاده برای تحلیل، ایجاب می‌کندکه روش مورد استفاده باید بتواند با کمینه نوع داده‌های مورد نیاز و بدون نیاز به ذخیره‌سازی داده‌های دریافتی، مدل‌های رفتاری را شکل داده و انواع ناهنجاری-های بافتاری را کشف کند. به نظر می‌رسد بسیاری از رفتارهای مجرمانه که در سطح میزبان یا شبکه عادی و قانونی تلقی می‌شوند، حداقل موجب یک نوع ناهنجاری بافتاری در ترکیب این دو محیط می‌شوند؛ لذا روش ارائه شده در این پایان‌نامه می‌تواند برخی از فن‌روش‌های مخفیانه مهاجمان را که در حوزه جریان‌های شبکه نمودی هر چند قانونی دارند، کشف کند. در نهایت، صورت مسأله‌ای که امروزه، تهدیدات پیشرفته پایا، با فن‌روش‌های مخفیانه و بعضاً غیررایانه‌ای خود برای جامعه‌ی امنیتی گشوده‌است، کشف کارا و برخط انواع ناهنجاری‌های بافتاری در گستره تمام اطلاعات رایانه‌ای و غیررایانه‌ای سازمان است.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.