به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

مروری بر روش‌های انتساب داده در کشف شواهد جرائم شبکه‌ای

A Review on Payload Attribution Techniques in Network Forensics

زینب ساسان

زمان: شنبه ۱۷ مردادماه ۱۳۹۴ ساعت ۹:۱۵

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

امروزه حوزه جرائم اینترنتی و پیچیدگی‌های حملات به سرعت در حال گسترش است. بررسی‌ها نشان می‌دهد که مکانیزم‌های دفاعی موجود نظیر دیواره آتش و سیستم‌های تشخیص نفوذ به تنهایی جهت حفاظت از شبکه‌ها در برابر حملات مختلف کافی نبوده و قابلیت‌های جدیدی همچون کشف شواهد جرائم شبکه‌ای برای ردیابی حملات در شبکه‌های گسترده نیاز است. در این روش نگهداری تاریخچه‌ای از ارتباطات و داده‌های تبادل شده به منظور تحلیل و بررسی آن‌ها امری مهم و اجتناب‌ناپذیر است. از سوی دیگر نگهداری سوابق و داده‌های ارتباطات شبکه‌های امروزی به طور خام، به فضای ذخیره‌سازی بسیار بزرگی نیاز دارد. برای رفع این مشکل، روش‌های انتساب داده معرفی شده‌اند. در این روش‌ها میزان داده‌های ذخیره شده به نسبت مشخصی کاهش پیدا می‌کند در حالی‌که پاسخ‌های دریافتی با مقداری خطا همراه خواهد بود. در این روش‌ها با پرس‌وجوهایی می‌توان بررسی کرد که آیا بسته‌ای شامل داده‌ی خاص، پیش از این در شبکه مبادله شده است یا خیر.

تاکنون روش‌های انتساب داده‌ی مختلفی معرفی شده که هریک نسبت کاهش حجم و مقدار خطای مثبت-نادرست را بهبود داده‌اند. در این ارائه به معرفی الگوریتم‌های انتساب داده، مشکلات هر یک از الگوریتم‌ها و چالش‌های پیش‌رو هنگام پیاده‌سازی این تکنیک‌ها بر روی شبکه‌های واقعی خواهیم پرداخت.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.