

به نام خدا

## سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه



### بهبود روشهای انتساب داده در بررسی شواهد جرایم شبکه

## Improving Payload Attribution Techniques in Network Forensics

### فرهاد آرام‌بام

زمان: شنبه ۲۱ تیرماه ۱۳۹۳ ساعت ۳ عصر

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

امروزه با گسترش حوزه و پیچیدگی جرایم اینترنتی نگهداری تاریخچه‌ای از ارتباطات و داده‌های رد و بدل شده امری مهم و اجتناب ناپذیر است. نگهداری داده‌های ارتباطات شبکه‌های امروزی به طور خام به فضای ذخیره‌سازی بسیار بزرگی نیاز دارد. حجم بالای داده‌ها باعث بروز چالش‌هایی بر روی میزان زمان نگهداری و جستجو بر روی داده‌ها می‌شود. همچنین نگرانی‌های زیادی در زمینه حریم خصوصی داده‌های ذخیره شده وجود دارد بر این اساس روش‌های انتساب داده اصلی پیشنهاد شدند. در این روش‌ها داده‌ها درهم‌سازی شده و به صورت خام در دسترس نیستند. میزان داده‌های ذخیره شده به نسبت مشخصی کاهش پیدا می‌کند و در عوض مقداری خطا به پاسخ‌های دریافتی از سامانه افزوده می‌شود. در این گزارش کارهای مرتبط صورت گرفته در زمینه انتساب داده‌ها مورد بررسی قرار می‌گیرند، چالش‌ها و مشکلات پیش روی آن‌ها بیان خواهند شد و تلاش می‌شود روشی برای بهبود مشکلات پیشنهاد شود.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.