به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

نشت اطلاعات در اثر فشرده سازی متن، با بررسی حمله BREACH

Compression and Information Leakage of Plain text, BREACH Attack Story

سید حیدر جوادی، سعید شیروی

زمان: شنبه ۲۵ آذر ماه ۱۳۹۶ ساعت ۹:۱۵

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

در این ارایه به بحث برروی فشرده‌سازی و خلاهای امنیتی ایجاد شده براثر آن بر روی کانال‌های امن SSL/TLS خواهیم پرداخت. افشای اطلاعات محرمانه در اثر اطلاعاتی که از روی نتیجه فشرده‌سازی، برای مهاجمان آشکار می‌شود، از مدت‌ها قبل مورد توجه محققان بوده است که در سال‌های اخیر در عمل نیز حملات موفقی بر مبنای آن طراحی و اجرا شده‌اند. پس از بررسی مختصر مبانی فشرده‌سازی و خلاهای امنیتی ناشی از آن، به معرفی و بررسی حمله کانال جانبی BREACH که کاراترین حمله کانال جانبی مبتنی برفشرده‌سازی هست خواهیم پرداخت.

شرکت در این جلسه برای تمامی علاقه‌مندان آزاد است.