به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

سیستم رمزنگاری با کلید انتخابی مبتنی بر آشوب:
مسیری نو در امن‌سازی شبکه خصوصی مجازی

Chaos-based Selective Key (CSK) Cryptosystem:
A New Direction to Secure VPN

وحید خدابخشی

زمان: شنبه ۱۲ مرداد ماه ۱۳۹۲، ساعت ۹ صبح

مکان: دانشکده‌ی مهندسی کامپیوتر، طبقه‌ی پنجم، آزمایشگاه امنیت داده و شبکه

امروزه، شبکه‌های خصوصی مجازی کاربردهای متنوع و جدیدی یافته‌اند؛ که در این میان می‌توان به «شبکه‌های خصوصی میان-ابری» و «ابر خصوصی مجازی» اشاره کرد. با توجه به رشد روزافزون این نوع کاربردها، امروزه یکی از نیازمندی‌های جدّیِ یک شبکه‌ی خصوصی مجازی، امنیت بالاتر در کنار گذردهی قابل قبول است. یکی از مهم‌ترین مؤلفه‌های امنیتی در اغلب شبکه‌های خصوصی مجازی، «رمز قالبی» است. رمزهای قالبیِ مرسوم، از ضعف‌های ساختاری رنج می‌برند. بنابراین حمله‌کننده با استفاده از این ضعف‌ها می‌تواند رمز قالبی را با توان محاسباتی به مراتب کم‌تر از توان محاسباتیِ مورد نیاز برای حمله‌ی «جست‌وجوی فراگیر» بشکند. یکی از راه‌کارهای ارائه شده برای تقویت رمزهای قالبی، «رمزنگاری آبشاری» است، که سربار محاسباتی بالایی دارد. در این ارائه، یک روش جدید و کارا برای تقویت امنیتِ رمزهای قالبی معرفی می‌گردد، که نسبت به رمزنگاری آبشاری از سربار محاسباتی کمتری برخوردار است. هدف از این روش، پیچیده‌تر کردن دسته‌ای از «تحلیل رمز»های مبتنی بر ضعف‌های ساختاری رمزهای قالبی است. این دسته از تحلیل‌ها، بر اساس جمع‌آوری تعداد مناسب جفت متن رمز- متن آشکار، به منظور دست‌یابی به کلید رمزنگاریِ متقارن است. روش ارائه شده، در واقع جمع‌آوری اطلاعات لازم برای تحلیل رمز را دشوار می‌سازد. تمرکز این ارائه، استفاده از این روش برای طراحی شبکه‌های خصوصی مجازی با امنیت بالاتر و گذردهی قابل قبول است. هچنین چنین شبکه‌های خصوصی مجازی، قادر هستند در بستر پروتکل‌های غیر قابل اطمینان در لایه‌ی انتقال، بدون نیاز به همگامیِ طرفین ارتباط، استقرار یابند. ارزیابی‌های تحلیلی و عملیاتی، صحت ادعاهای مطرح شده را نشان می‌دهد.

شرکت در این جلسه برای عموم دانشجویان علاقه‌مند آزاد است.