به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

پروتکل اصالت سنجی یکبار ورود مبتنی بر رمزنگاری قابل راستی آزمایی امضاء

Single Sign-on Protocol Based on Verifiable Encryption of Signature

داوود سالاری‌پناه

زمان: شنبه ۳۰ آذرماه ۱۳۹۲ ساعت ۹ صبح

مکان: دانشکده مهندسی کامپیوتر، طبقه پنجم، آزمایشگاه امنیت داده و شبکه

هم‌زمان با گسترش شبکه اینترنت و فناوری وب، اصالت‌سنجی کاربران در این شبکه به موضوعی حیاتی تبدیل شده است. خدمات متنوع و فراوان ارائه شده و نیاز به اصالت‌سنجی در هر یک، کاربران را با مشکل نگهداری اعتبارنامه‌ها (نام‌کاربری/کلمه‌عبور) مواجه ساخته است. اصالت‌سنجی یکبار ورود، راه حلی برای این مشکل است. پروتکل‌های مبتنی بر رمزنگاری متقارن نظیر کربروس، این مشکل را تا حدودی برای سازمان‌ها مرتفع کرده‌اند، اما این پروتکل‌ها، در محیط‌های ناامن همچون اینترنت با مخاطرات بسیاری روبه‌رو هستند. در مقابل، استفاده از رمزنگاری نامتقارن، هزینه‌های زیرساختی و عملیاتی زیادی را به کارپذیران و کارخواهان تحمیل می‌کند. در این ارائه، رمزنگاری نامتقارن قابل راستی‌آزمایی امضا برای اصالت‌سنجی یکبار ورود تشریح خواهد شد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.