جلسه هفتگی آزمایشگاه امنیت داده و شبکه

سخنران: محمد علی کارگر

m_kargar@ce.sharif.edu

چگونه یک پروتکل هویت‌شناسی کارا تولید کنیم؟

یکی از مسائل قابل توجه در عرصه امنیت اطلاعات، پروتکل‌های هویت‌شناسی می‌باشند. هدف این پروتکل‌ها نشان دادن اصالت یک شخص به شخص دیگر است. در نظریه اطلاعات، قدرت حمله کننده بینهایت تصور می‌شود، و منظور از شکستن پروتکل پیدا کردن هر نوع راه حل برای نقض پروتکل، مستقل از زمان و همچنین قدرت حمله کننده است. این نوع تفکر ما را از فضای واقعی دور می‌سازد و در عمل مشاهده می‌کنیم که بسیاری از پروتکل‌ها در پیاده‌سازی از نظر زمانی عملیاتی نمی‌باشند. باتوجه به محدودیت زمان/حافظه در عمل، کارایی پروتکل‌ها اهمیت بسزایی دارد. علاوه بر کارایی، امن بودن پروتکل نیز یکی دیگر از چالشهای پیش روی ما است. پروتکل‌های هویت‌شناسی بر اساس فرض سخت بودن برخی از مسائل نظیر تجزیه اعداد یا لگاریتم گسسته بنا شده‌اند. برای طراحی یک پروتکل امن و در عین حال کارآمد، آشنایی قبلی طراح با مسائل پیاده‌سازی و همچنین تنگناهای کارایی اهمیت فراوانی دارد. استفاده از اعداد تصادفی امن و همچنین توان رسانی پیمانه‌ای از جمله تنگناهای پروتکل‌های هویت‌شناسی در پیاده‌سازی محسوب می‌شود.

در این ارائه به بررسی مسائل اصلی در پیاده‌سازی کارای پروتکل‌های هویت‌شناسی می‌پردازیم، و عوامل مقایسه پروتکل‌ها از نظر امنیت را بر می‌شماریم. در نهایت ابزارهایی که برای پیاده‌سازی این پروتکل‌ها و جزئیات مربوط به پیاده‌سازی آنها را بیان می‌کنیم.

زمان: شنبه ۲۷ آبان ماه، ساعت ۹ صبح

مکان: دانشکده مهندسی کامپوتر، طبقه‌ی پنجم، آزمایشگاه امنیت داده و شبکه، اتاق ۵۰۱