به نام خدا

جلسه سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

رمزنگاری پنهان داده

Transparent Data Encryption

محمدهاشم حقیقت

زمان: یک شنبه ۱۰ اسفندماه ۱۳۹۳ ساعت ۱۵: ۴ عصر

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

از آنجایی که پایگاه‌داده‌ها به عنوان انباره‌ای برای ذخیره‌سازی داده‌ها و مدیریت آن‌ها بشمار می‌رود، تأمین امنیت آن از نیازمندی‌های اصلی در حوزه‌ی امنیت داده‌ها در ذخیره‌سازی بشمار می‌رود. سرقت رسانه‌ی ذخیره‌سازی مثالی از تهدیدات ممکن است، که می‌تواند امنیت داده‌های مجتمع شده در پایگاه‌داده‌ها را به مخاطره اندازد. بر این اساس رمزگذاری داده‌ها یک مکانیزم ضرروی است که نقش مهمی را در افزایش ضریب امنیتی در سیستم‌های مدیریت پایگاه‌داده‌ها ایفا می‌کند. هدف اصلی رمزگذاری مخفی نگه داشتن داده‌ها از کاربران غیرمجاز است. در این صورت با گذر کاربران غیرمجاز از لایه‌های امنیتی مانند دیوار آتش شبکه و خط‌مشی‌های کنترل دسترسی پایگاه‌داده، همچنان به رمزگشایی داده‌ها برای اطلاع از آن‌ها نیاز خواهد بود.
اما در رمزنگاری پایگاه داده، سطح و ریزدانگی رمزگذاری دو فاکتور اصلی در طراحی یک چارچوب رمزگذاری هستند. در حقیقت رمزگذاری می‌تواند در سطح سیستم فایل، سمپاد، و سطح کاربرد انجام گیرد. رمزگذاری می‌تواند در ریزدانگی‌های مختلفی چون فیلد، ستون، سطر، کل جدول، و پایگاه‌داده‌ها باشد. چارچوب رمزگذاری پنهان داده که رمزگذاری را در ریزدانگی ستون و سطح سمپاد انجام می‌دهد، می‌تواند راهکارهای مناسبی را برای مواجهه با چالش‌های مذکور ارائه کند. در حقیقت این چارچوب از دید برنامه کاربردی پنهان خواهد بود و حتی‌المقدور کارهای مربوط به مدیریت رمزگذاری داده‌ها را خود بر عهده می‌گیرد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.