

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه



کریپت دی بی: حفظ محرمانگی، همراه با پردازش پرس و جوی رمز شده (۲)

CryptDB: Protecting Confidentiality with Encrypted Query Processing(2)

سید حسام الدین شاهرخی

زمان: شنبه ۱۸ مرداد ماه ۱۳۹۳ ساعت ۳ عصر

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

کریپت دی بی یک میان افزار است که سرویس محرمانگی را برای نرم افزارهایی که از سمپاد استفاده می کنند، فراهم می کند. این سامانه عملیاتی، به منظور ایجاد محرمانگی عملی و قابل اثبات برای کاربردهایی که داده های حساس خود را در پایگاه داده ذخیره می کنند، استفاده می شود. نکته کلیدی کریپت دی بی که آن را کاربردی هم می کند این است که پایگاه داده ها یکسری اپراتور خوش تعریف دارند که در کریپت دی بی نیز تمامی این اپراتورها به همان صورتی که در پایگاه داده ها هستند، بر روی داده های رمز شده استفاده می شود. کریپت دی بی پرس و جوها را مستقیماً روی داده های رمز شده اجرا می کند و کارپذیر برای اجرا و پاسخ گویی به پرس و جوها، نیاز به رمز گشایی داده ها ندارد. بنابراین مدیر پایگاه داده هیچ گاه به داده های آشکار دسترسی ندارد.

با توجه به ویژگی های منحصر به فرد معماری این سامانه در برون سپاری امن داده، تلاش می شود تا در دو سخنرانی (طی دو هفته) تمامی جزئیات این سامانه تشریح گردد.

شکرک در این جلسه برای تمامی دانشجوین علاقه مند آزاد است.