به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه


# کریپت دی بی: حفظ محرمانگی همراه با پردازش پرس وجوی رمز شده (۱)

# CryptDB: Protecting Confidentiality with Encrypted Query Processing(1)

**هاشم حبیبی**

زمان: شنبه ۱۱ مردادماه ۱۳۹۳ ساعت ۳ عصر

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

کریپت‌دی‌بی یک میان‌افزار است که سرویس محرمانگی را برای نرم‌افزارهایی که از سمپاد استفاده می‌کنند، فراهم می‌کند. این سامانه عملیاتی، به منظور ایجاد محرمانگی عملی و قابل اثبات برای کاربردهایی که داده‌های حساس خود را در پایگاه‌داده ذخیره می‌کنند، استفاده می‌شود. نکته کلیدی کریپت‌دی‌بی که آن را کاربردی هم می‌کند این است که پایگاه داده‌ها یکسری اپراتور خوش‌تعریف دارند که در کریپت‌دی‌بی نیز تمامی این اپراتورها به همان صورتی که در پایگاه داده‌ها هستند، بر روی داده‌های رمز شده استفاده می‌شود. کریپت‌دی‌بی پرس‌وجوها را مستقیماً روی داده‌های رمز شده اجرا می‌کند و کارپذیر برای اجرا و پاسخ‌گویی به پرس‌وجوها، نیاز به رمزگشایی داده‌ها ندارد. بنابراین مدیر پایگاه‌داده هیچ‌گاه به داده‌های آشکار دسترسی ندارد.

با توجه به ویژگی‌های منحصربه فرد معماری این سامانه در برون‌سپاری امن داده، تلاش می‌شود تا در دو سخنرانی (طی دو هفته) تمامی جزئیات این سامانه تشریح گردد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.