به نام خدا

جلسه‌ی سخن‌رانی هفتگی آزمایشگاه امنیت داده و شبکه

مبهم‌سازی همسان‌گر: تعریف، ساخت، امنیت و کاربردها

Indistinguishability Obfuscation: Definition, Construction, Security, and Applications

بهنام مومنی

زمان: شنبه ۸ خرداد ماه ۱۳۹۵ ساعت ۹:۱۵

مکان: دانشکده‌ی مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه‌ی چهار، سالن خوارزمی

هدف از مبهم‌سازی نرم‌افزار این است که نرم‌افزار ورودی به گونه‌ای تغییر یابد که نتوان هیچ دانشی از چگونگی کارکرد آن به دست آورد مگر همان دانشی که با ورودی دادن و خروجی گرفتن و بدون نگاه به توصیف داخلی آن قابل کسب است. از آنجا که چنین تغییری همانند قرار دادن برنامه در یک جعبه‌ی سیاه پیش از توزیع آن است، به آن مبهم‌سازی جعبه‌سیاه مجازی هم می‌گویند. هر چند چنین تبدیلی می‌تواند کاربردهای رمزنگارانه‌ی بسیاری داشته باشد، ثابت شده است که چنین کاری ناممکن است. از همین رو گونه‌ی ضعیف‌تری از مبهم‌سازی مورد توجّه قرار گرفته است که در آن اجازه‌ی استخراج دانش از برنامه داده می‌شود. ولی اگر برنامه‌هایی با کارکرد یکسان (خروجی یکسان به ازای ورودی یکسان) به آن تحویل داده شوند، نمی‌توان از روی برنامه‌ی مبهم‌شده به این نکته پی برد که کار از روی کدام یک از برنامه‌های معادل آغازین شروع شده است. به چنین تبدیلی مبهم‌سازی همسان‌گر گفته می‌شود. از آنجا که مبهم‌سازی همسان‌گر بر روی برنامه‌هایی کار می‌کند که پیش از مبهم‌سازی هم کارایی یکسانی داشته‌اند، سودمندی آن در آغاز چندان روشن نبود. تا سال ۲۰۱۳ که نخستین محقّق‌سازی برای یک مبهم‌ساز همسان‌گر معرفی شد و چگونگی کاربرد آن برای ساخت یک رمزنگاری تابعی نشان داده شد. با مشخّص شدن راهی برای به‌کارگیری این مبهم‌سازی ضعیف‌تر در کاربردهای رمزنگارانه، ساخت‌های دیگر رمزنگاری همچون تبدیل رمزنگاری با کلید خصوصی به یک رمزنگاری با کلید عمومی یا انجام رمزنگاری انکارپذیر بر مبنای مبهم‌سازی همسان‌گر معرفی شدند. در این سخن‌رانی، چیستی مبهم‌سازی همسان‌گر و یک محقّق‌سازی برای آن معرّفی شده و با بیان چگونگی اثبات امنیّت آن، به کاربردهای آن پرداخته می‌شود. به طور خاص کاربرد این مبهم‌سازی در رمزنگاری تابعی تشریح می‌شود.

ـ شرکت در این جلسه برای همه‌ی دانشجوهای علاقه‌مند آزاد است ـ