رمزگذاری کوانتومی، راهکاری برای افزایش ایمنی رایانه ها در مقابل هکرها - دیجیاتو

محسن خوشنود | یکشنبه، ۰۵ آذر ۱۳۹۶

با معرفی کامپیوترهای کوانتومی و اطلاع عموم از سرعت خیره کننده آنها، برخی نگرانی ها بابت احتمال دسترسی هکرها به این سخت افزارهای قدرتمند و سوء استفاده از آنها به وجود آمد که در صورت بروز چنین اتفاقی، سیستم های امنیتی کنونی عملاً شانسی برای مقابله با خرابکاران سایبری نخواهند داشت.

اما پژوهشگران حوزه امنیت نیز بیکار نیستند و با ابداع یک سیستم رمزگذاری بر پایه فناوری رایانش کوانتومی، روشی را به وجود آورده اند که امنیت سیستم های کاربران در مقابل نفوذ هکرها را تا حد بسیار زیادی تضمین می کند.

سیستم مورد بحث که توسط دانشمندان دانشگاه ایالتی اوهایو توسعه یافته، قادر به رمزگذاری داده ها با سرعت های چند مگابیت بر ثانیه است که در مقایسه با روش های موجود بین 5 تا 10 برابر سریع تر بوده، و در مقابل حملات متداول حتی در صورت بروز رخنه های سخت افزاری نیز مقاوم خواهد بود.

روش QKD نخستین بار در سال 1984 معرفی شده بود

همان طور که احتمالاً می دانید، برای ارسال و خوانش داده های رمزنگاری شده، هر دو طرف نیازمند کلید مشابهی هستند تا به محتوای پیام دسترسی پیدا کنند. در این بین روش توزیع کلید کوانتومی یا «QKD» با بهره گیری از خاصیت تغییر دائمی ویژگی های ذراتی مانند الکترون یا فوتون، در هر لحظه وجود شکاف های امنیتی را بررسی کرده و به هر دو طرف ارتباط گزارش می کند.

البته روش QKD نخستین بار در سال 1984 معرفی و به کار گرفته شد، اما تجهیزات مورد نیاز برای بهره مندی گسترده از آن به تازگی توسعه یافته و حتی برخی کمپانی ها در اروپا اقدام به فروش سیستم های QKD مبتنی بر لیزر نموده اند.

لازم به ذکر است که پیش از این امکان رمزنگاری یک بیت داده به وسیله یک فوتون میسر شده بود که حالا با ابداع روش جدید و استفاده از خاصیت «فاز» فوتون، سیستم های موجود توانایی

رمزگذاری 2 بیت داده به ازای هر فوتون را خواهند داشت.

گفتنی است در شرایط ایده آل، نفوذ به سیستم هایی که با روش QKD رمزگذاری شده اند تقریباً غیر ممکن است؛ چرا که هرگونه اقدام برای هک ارتباطات اینچنینی خطاهایی را به ثبت می رساند که توسط طرف گیرنده به راحتی قابل مشاهده و تشخیص خواهند بود.

دیجیاتو