یکشنبه 21 مهر 1387 - 08:18

کوانتوم و امنیت شبکه‌های کامپیوتری

تکامل امنیت شبکه‌های کامپیوتری با معرفی کدگذاری کوانتومی در کنفرانسی در وین وارد مرحله جدیدی شده است.

این شبکه، شش مرکز در اطراف شهر وین را با 200 کیلومتر خطوط فیبر نوری به هم متصل می‌کند و توسط اتحادیه اروپا پشتیبانی می‌شود و SECO-QC نام دارد.

کدگذاری کوانتومی اساساً با کدگذاری‌ها و سیستم‌های امنیتی که در خانه و محل کار از آن‌ها استفاده می‌کنیم تفاوت دارد. کدهای این شبکه محاسبات و معادلات پیچیده ریاضی هستند که تقریباً غیر قابل نفوذ هستند ولی نفوذ به آن‌ها با در دست داشتن دانش ریاضی کافی و ابزار پیشرفته ممکن است. کلیدهای شبکه (Network Keys) نیز از همین کدها استخراج می‌شود و کاربران برای دسترسی به قسمت‌های مختلف این شبکه نیاز به نوعی شناسه کاربری خاص دارند.

ایده پشت این سیستم مربوط به 25 سال پیش است. زمانی که چارلز بنت از شرکت IBM و گیلز براسارد از دانشگاه مونترال این طرح را به صورت مشترک به پایان رساندند و سپس در این کنفرانس شاهد معرفی این سیستم بودند.

گیلز براسارد می‌گوید:«تمامی سیستم‌های امنیتی کوانتومی بر اساس اصل عدم قطعیت هایزنبرگ بنا شده‌اند. با این ایده که دسترسی به اطلاعات کد گذاری بدون دستکاری و تغییر فوتون‌ها عملی نیست. این نفوذ بدون به جا گذاشتن هیچ‌گونه اثر غیر قابل انجام است.»

در عمل این به معنی شناسایی شعاع‌های نوری و فوتون‌هایی است که میلیون‌ها بار در هر ثانیه بین گره‌های این شبکه بین ساختمان‌های شرکت زیمنس (شبکه فیبر نوری این پروژه توسط زیمنس ساخته شده است) حرکت می‌کنند.

از شناسایی فوتون‌های مشخصی که در این شبکه در حال حرکت هستند، ترکیبی پیچیده از ارقام بوجود می‌آید. از این قسمت به بعد بیشتر شبیه کد گذاری عادی است. مزیت این کار این است که برای دسترسی به کدها باید هر کدام از فوتون‌ها را شناسایی کرد و این کار به دلیل وجود میلیون‌ها فوتون در شبکه برای افرادی که محل دقیق آن‌ها را نمی‌دانند غیر ممکن است.

حتی اگر کسی به درون شبکه نفوذ کند و اقدام به شناسایی فوتون‌ها بکند، نظم فوتون‌ها به هم می‌خورد و شبکه به صورت خودکار از کار می‌افتد ولی این قطع موقتی شبکه به ارتباط گره‌ها با هم مشکلی وارد نمی کند زیرا ارتباط گره‌ها با یکدیگر از طریق خطوط دیگر نیز امکان پذیر است و تنها قسمتی که به آن نفوذ شده است دچار قطع می‌شود.

دکتر هانس هوبل از دانشگاه وین مه یکی از تست کنندگان این شبکه است در این مورد می‌گوید:«ما در حال حاضر با بانک‌ها و موسسات مالی و بیمه در ارتباط هستیم. برای آن‌ها از بین رفتن 10میلیون یورو بسیار کم ضررتر از از کار افتادن کار شبکه برای چند ساعت است. به همین دلیل باید به آن‌ها تضمین بدهیم که قفل‌ها و کدگذاری‌ها شبکه ما برای چندین هفته و بدون خطا کار می‌کند.»

برای اینکه از فوتون در کدگذاری استفاده شود چندین راه وجود دارد. یکی اینکه با قطبی کردن و منحرف کردن آن‌ها، کدها را شناسایی کرد و دیگری اینکه با استفاده از زمانی که طول می‌کشد تا درون شبکه حرکت کنند و از نقطه‌ای به نقطه‌ای دیگر بروند، آن‌ها را شناسایی کرد.

مدیر این پروژه، کریستیان مونیک در این باره می‌گوید:«همان طور که در یک شبکه تلفن همراه، باید وجود صدها گوشی تلفن از صدها سازنده را انتظار داشت، در کدگذاری کوانتومی نیز باید به مشتریان اجازه انتخاب روش کار شبکه را داد.»