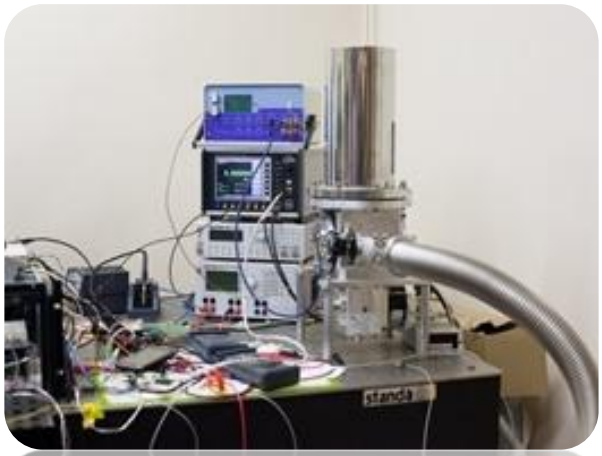
جدیدترین متد سرقت صدا در دنیای کامپیوتر



گروه شرکت های آرک

نرم افزارهایی مطمئن، هوشمند و کارآمد

جدیدترین متد سرقت صدا در دنیای کامپیوتر

تشخیص کلیدهای رمزنگاری مخفی در کامپیوتر و گجت های مختلف چیز جدیدی نیست، اگرچه اغلب تکنیک‌های به‌کار رفته غیرعملی است.

مقاله‌ای جدید از محققان دانشگاه تل‌آویو نشان می‌دهد که این نظارت دست‌یافتنی شده و در چند متری ما و جاسوسان رخ می‌دهد. در جریان الکتریکی در طول رمزگذاری روتین نوسانات جزئی داریم یا حتی صداهایی توسط سیستم ساخته می‌شوند. کلیدهای به‌کاررفته در جریان بی‌سیم قابل‌برداشت است، اما نیاز به تجهیزات بسیار گران و مدت زمان زیادی برای این کار است و این دقیقاً همان چیزی است که در برنامه جاسوسی سازمان NSA به نام TEMPESTانجام شده است.

در مقاله منتشرشده در مجله ACM Journal متعلق به انجمن ماشین‌های حسابگر Association for/ Computing Machinery (بزرگ‌ترین جامعه علوم آکادمیک کامپیوتر در جهان تأسیس ۱۹۴۷) محققان دانشگاه تل آویو جزییات کیت ارزان‌قیمتی را منتشر کردند که قادر به برداشت کلیدهای رمزنگاری ۴۰۹۶ بیتی در کمتر از چند ثانیه از فاصله ۱۰ متری سوژه است.

کار آنها مشابه کاری است که سال گذشته از طریق دانگل یو اس بی رادیویی (سیگنال‌های رادیویی منتشرشده از طریق لپ‌تاپ) داخل یک حلقه نان انجام شد. این گروه از محققان موفق شدند تا این کار را از طریق آکوستیک انجام دهند. آکوستیک یا صداشناسی یکی از شاخه‌های علم فیزیک است و موضوع آن بررسی موج‌های مکانیکی در گازها، مایع‌ها و جامدها، ازجمله نوسان‌ها، صدا، فراصوت و فروصوت است. کاربردهای آکوستیک در بسیاری از جنبه‌های زندگی امروز دیده می‌شوند و ساده‌ترین نمونه آن صنایع صوتی و نیز کنترل نویز مکانیکی است. مانند پردازنده کامپیوتری که محاسبات رمزنگاری خود را انجام می‌دهد، این کار از طریق فرکانس بالای دستگاه و صداهای سیم‌پیچ در جریان الکتریکی انجام می‌گیرد.

جدیدترین متد سرقت صدا در دنیای کامپیوتر

تیم مذکور در تحقیقات خود با استفاده از میکروفون سهمی‌وار قادر به برداشت صداهای سیم‌پیچ از فاصله ۱۰ متری شد. تنها مشکل به وجود آمده دیده شدن میکروفون مذکور حین انجام عملیات است و به همین خاطر آنها از میکروفون یک موبایل استفاده کرده و آن را در فاصله ۳۰ سانتی‌متری لپ‌تاپ قراردادند تا بتوانند صداهای سیم را به راحتی شنود کنند .در هر دو مورد آنها توانستند کلیدهای RSA 4096 بیتی را به‌راحتی شنود کرده و بخوانند.

البته برای ممانعت از این روش، نیاز به زدن تریک نرم‌افزاری است. اگر تقلیل‌گر صوتی داخل رایانه قرار دهیم جلوی انتشار الکترومغناطیس گرفته می شود و یک عایق برای لپ‌تاپ ایجاد می‌شود .این تیم به دانشمندان علوم کامپیوتری توصیه کردند با ساخت محاسبات ساختگی برای عملیات رمزگذاری جلوی این ترفند را بگیرند. تیم اکادمیک همچنین ایجاد محافظ سخت‌افزاری روی میکروفون لپ‌تاپ یا گجت خود را نیز پیشنهاد داده‌اند تا جلوی هر احتمالی گرفته شود.