بخش نخست

خرابکارها اجازه نمی‌گیرند

نگاهی به جایگاه امنیت در فناوری اطلاعات و شیوه‌های جدید جاسوسی

سعید نوری‌آزاد

این که امنیت لازمه زندگی دیروز و امروز بشر است، توضیح واضحات است، اما این‌که زندگی امروز ما در کجای این بازار پرخطر فناوری‌ها قرار دارد، این سوال را در ذهن ما ایجاد می‌کند که چه خطراتی ممکن است ما را تهدید کنند؟

امنیت اطلاعات در محیط‌های مجازی همواره به‌عنوان یکی از زیرساخت‌ها و الزامات اساسی در کاربری توسعه‌ای و فراگیر از فناوری اطلاعات و ارتباطات تاکید شده است. گرچه امنیت مطلق چه در محیط واقعی و چه در فضای مجازی دست‌نیافتنی است، ولی ایجاد سطحی از امنیت که به اندازهٔ کافی و متناسب با نیازها و سرمایه‌گذاری انجام شده باشد، تقریبا در تمام شرایط محیطی امکان‌پذیراست. تنها با فراهم بودن چنین سطح مطلوبی است که اشخاص حقیقی، سازمان‌ها، شرکت‌های خصوصی و ارگان‌های دولتی ضمن اعتماد و اطمینان به طرف‌های گوناگونی که همگی در یک تبادل الکترونیکی دخیل هستند و احتمالا هیچ‌گاه یکدیگر را ندیده ونمی‌شناسند، نقش مورد انتظار خود به‌عنوان گره‌های موثر از این شبکه متعامل و هم‌افزا را ایفا خواهند کرد.

اطمینان از ایمنی سرمایه‌های اطلاعاتی و تجهیزات زیرساختی کشور، گذشته از ابعاد گسترده امنیت ملی، کلید قفل فرصت‌های بی‌شمار تجاری و غیرتجاری جدید اینترنتی است . آنچه مسلم است، چالش امنیتی رودرروی کشور، دسترسی نداشتن به فناوری یا عدم وجود محصولات امنیتی نیست، بلکه سیاست‌گذاری، فرهنگ‌سازی، بهره‌وری مناسب از منابع موجود و نیز سازگاری آن‌ها به‌گونه‌ای است که نیاز منحصربه‌فرد شبکه و فضای دیجیتالی کشور را تامین کند. [نصرالله جهانگرد، مقدمه ترجمه کتاب امنیت و فناوری اطلاعات، نوشته سادوسکای]

سرقت اطلاعات رایانه از طریق پریز برق

پیشرفت تکنولوژی مانند تیغی دولبه‌است که خاصیت‌ها و نمودهای مثبت و گاه منفی دارد. استفاده از شیوه‌های مختلف برای ارسال اطلاعات توانسته آسایش و امکانات بسیاری را برای ما فراهم کند، اما همین نقل‌وانتقال اطلاعات می‌تواند بسیار خطرآفرین باشد، چرا که این محیط دارای خواصی منطقی است که مشکلات امنیتی بسیاری نیز دارد.

یکی از جدیدترین شیوه‌های سرقت اطلاعات از ارتعاش نوسانی برق در دستگاه رایانه فرد است که می‌تواند روی برق ورودی دستگاه تاثیر بگذارد و به‌نوعی واکنش انعکاسی به‌وجود آورد. همین واکنش کافی است تا در آن سوی کابل برق ورودی کسی بتواند اطلاعات شما را بدون اطلاع‌تان دریافت کند و به‌گفته پژوهشگران در امر امنیت اطلاعات، از پریز برق می‌توان برای شنود آنچه مردم روی صفحه‌کلید کامپیوتر تایپ می‌کنند، استفاده کرد.

پژوهشگران موسسه Inverse Path دریافته‌اند که فقدان لایه‌های حفاظتی کافی برای جلوگیری از انتشار نویز در کابل برخی صفحه کلیدها، باعث می‌شود که هنگام تایپ هر حرف، اطلاعاتی حساس از طریق این سیم نشت کند و روی جریان های داخلی رایانه تاثیر بگذارد. این پژوهشگران با تحلیل اطلاعاتی که از طریق پریز برق به‌دست‌آمد، دریافتند که فرد مورد شنود قرار گرفته، چه چیزی روی صفحه‌کلید کامپیوتر خود تایپ می‌کند؟

در این پژوهش مشخص شده است که اطلاعات منتقل شده از طریق سیم صفحه‌کلید، از ۱۵متری نقطه اتصال کامپیوتر به یک پریز برق و حتی از نقاطی مانند لوله های آب نیز قابل شنود است.

آندریا باریسانی و دانیل بیانکو، از پژوهشگران موسسه Inverse Path در یک مقاله علمی به‌تشریح یافته‌های خود پرداختند و نوشتند: «هدف ما این است که نشان دهیم اطلاعات را از غیرمنتظره‌ترین راه‌ها می‌توان شنود کرد.»

پژوهشگران تحقیق خود را روی سیم‌هایی متمرکز کردند که صفحات کلید با درگاه معمولی PS/2 را به کامپیوترهای رومیزی متصل می‌کند و درگاه‌های USB در این تحقیق مدنظر نبوده است.

این ۲محقق گفته‌اند که ۶سیم داخل یک کابل PS/2 معمولا نزدیک به یکدیگر هستند و حفاظ نویزگیر مناسبی ندارند. این مساله باعث می‌شود اطلاعاتی که از طریق سیم داده (Data) که رابط صفحه‌کلید و رایانه است به‌شکل تغییر ولتاژ در حال انتقال است به سیم متصل زمین (Earth) در همان کابل القا شود.

سیم اتصال به زمین در نهایت از طریق منبع تغذیه کامپیوتر به پریز برق و از آن‌جا هم به کل مدارهایی که برق اتاق را تامین می کنند متصل می‌شود.

طرح: worldpress

در حال حاضر بیش از ۹۵درصد از مبادلات اطلاعات با پست الکترونیکی از طریق سایت‌های خارجی یا سرورهای خارج از مرزهای کشور انجام می‌شود

آنچه شرایط را برای این القای ناخواسته اطلاعات فراهم می‌کند، سرعت پایین انتقال اطلاعات صفحه‌کلید است که سرعت آن به‌مراتب کمتر از سرعت عملکرد دیگر قطعات کامپیوتر مانند کارت گرافیکی و پردازنده مرکزی است.

در این مقاله آمده است: « موج مربعی سیگنال PS/2 را که با کیفیت خوب به سیم ارت منتقل می‌شود، می‌توان به اطلاعات اصلی صفحه‌کلید تبدیل کرد.» یعنی همان کاری که دریافت‌کننده اطلاعات در داخل رایانه انجام می‌دهد، می‌توان دوباره انجام داد و اطلاعات را بازسازی کرد.

پژوهش این افراد نشان داد که حتی اگر محلی که تلاش برای دزدی اطلاعات از آن صورت می‌گیرد تا ۱۵متر از پریز برق فاصله داشته باشد، اطلاعات بدون مشکل منتقل می‌شود و در نتیجه چنین روش شنودی اطلاعات در اتاق هتل یا دفتر کار نیز قابل استفاده است.

این ۲ پژوهشگر اعلام کرده‌اند که تحقیقات آن‌ها در این زمینه کماکان ادامه دارد و قرار است نحوه انجام چنین حمله‌ای در کنفرانس مسائل امنیتی Black Hat که از روز ۲۵ تا ۳۰ژوئیه در لاس‌وگاس برگزار می‌شود، به‌نمایش گذاشته شود.

این روش به‌علت دارا بودن خاصیت حمله به سیستم‌های سیمی اهمیت بسیاری دارد چراکه سیستم‌های قبلی تماما روی سیستم‌های بی‌سیم تکیه داشتند.

صفحه‌کلیدهای بی‌سیم که اکثرا با سیستم بلوتوث هماهنگ شده است، هیچ‌گونه امنیتی ندارد و اطلاعات به‌آسانی از آن‌ها نشت پیدا می‌کند. اطلاعاتی که فرد در هنگام تایپ روی صفحه‌کلید بی‌سیم وارد می‌کند، از فاصله چندین متری و حتی از پشت درهای بسته نیز قابل دریافت است. در کنفرانس IEEE که برای امنیت تشکیل شده بود، روی موضوع امنیت این سیستم‌ها تاکید خاصی شده است. استفاده از این نوع سیستم‌ها در ادارات امنیتی و جاهایی که اطلاعات حساس مبادله می‌کنند، به‌هیچ عنوان توصیه نمی‌شود.

امنیت اطلاعات ایرانی

موضوع «شبکه داده ملی» یا همان «اینترنت ملی» سال‌های زیادی است که زبان، فکر و وقت متخصصان را به‌خود مشغول کرده و از دیدگاه درست این شبکه باید شبکه انتقال اطلاعات کشور باشد که در تمام مواقع نیاز ارتباط ما با میزبانی سرورهای خارجی مرتفع نشود.

این شبکه که در حال حاضر وضعیت نامعلومی دارد، قرار است امسال ۱۰۰هزار مدرسه و دانشگاه و بسیاری مراکز درمانی را به‌هم متصل کند. شبکه الکترونیک سلامت و شبکه ملی مدارس همچنین شبکه علمی کشور، قرار است روی این بستر پیاده‌سازی شوند. منفعت اصلی این شبکه امنیت آن است که می‌تواند برای مواقع حساس و امور زیربنایی کشور به‌کار رود. داشتن ایمیل امن و یک تبادل اطلاعات کاملا ایمن بر بسترهای غیر از این شبکه، امری بسیار پرهزینه و پرخطر است.

در حال حاضر بیش از ۹۵درصد از مبادلات اطلاعات با پست الکترونیکی از طریق سایت‌های خارجی یا سرورهای خارج از مرزهای کشور انجام می‌شود.

منابع

Linda McCarthy, IT Security: Risking the Corporation, Prentice Hall, 2003.

http://www.bbc.co.uk/digitalrevolution/

http://www.gateprotect.com/