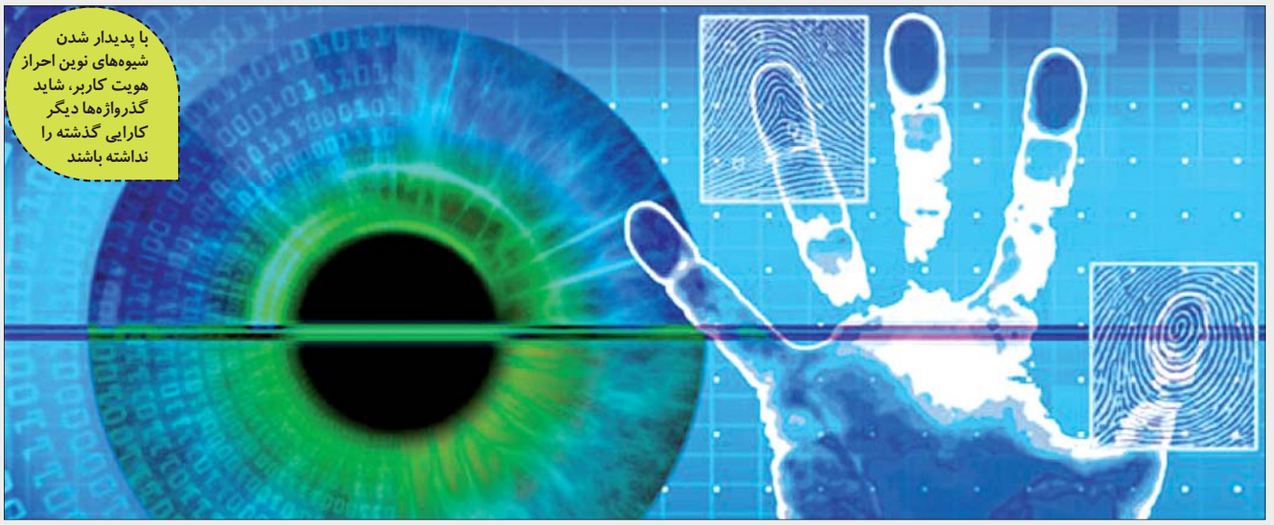

با پدیدار شدن شیوه‌های نوین احراز هویت کاربر، شاید گذرواژه‌ها دیگر کارایی گذشته را نداشته باشند

زمان مرگ گذرواژه فرارسیده است؟

در جست‌وجوی امنیت بیشتر

صالح سپهری‌فر

اگر نگاهی به اخباری که در چند ماه اخیر از دنیای فناوری اطلاعات منتشر شده بیندازیم، حتما باید در کارایی استفاده از گذرواژه به‌عنوان ابزاری برای حفاظت از حریم خصوصی‌مان تردید کنیم. بهار امسال فیسبوک پذیرفت گذرواژه میلیون‌ها کاربر اینستاگرام در قالبی غیررمزنگاری‌شده روی سرورهایش نگهداری می‌شد. یاهو نیز همچنان درگیر تبعات حقوقی افشای داده‌های خصوصی سه میلیارد کاربر است که مواردی نظیر نشانی ایمیل، سؤال امنیتی و نیز گذرواژه‌های آنها را شامل می‌شد. سال پیش هکرها به وب‌سایت کوئرا که یک سامانه پرسش و پاسخ آنلاین است حمله کردند و به این ترتیب، نام و نشانی ایمیل صد میلیون کاربر به دست هکرها افتاد. واقعیت این است که گذرواژه، ساده‌ترین راه به منظور دسترسی غیرمجاز به داده‌ها یا سامانه‌های مختلف است. بیشتر افراد از گذرواژه‌های ساده استفاده می‌کنند تا به‌راحتی آن را به خاطر آورند، اما همین سادگی سبب می‌شود امکان دستیابی هکرها و کاربران غیرمجاز به گذرواژه نیز ساده‌تر شود. به همین دلیل، بسیاری از شرکت‌ها، داده‌های بیومتریک یا دیگر شیوه‌ها را جایگزین استفاده از گذرواژه‌ها کرده‌اند، اما آیا واقعا دوره استفاده از گذرواژه‌ها به پایان رسیده است؟

صرفه‌جویی در هزینه‌ها!

مایکروسافت سال گذشته اعلام کرد قصد دارد گذرواژه را به‌طور کلی از همه محصولات و خدماتش حذف کند و در عوض، از داده‌های بیومتریک یا یک کلید ویژه امنیتی برای ارائه دسترسی کاربر به خدمت یا محصول مورد نظرش استفاده کند.

موسسه معتبر گارتنر که در زمینه آینده‌پژوهشی در حوزه فناوری فعالیت می‌کند، پیش‌بینی کرده که تا سال ۲۰۲۲ حدود ۶۰درصد از شرکت‌های بزرگ و تقریبا همه شرکت‌های متوسط نیمی از نیاز خود به گذرواژه را به شیوه‌هایی دیگر (نظیر داده‌های بیومتریک) تامین کنند.

تردیدی نیست که حذف گذرواژه از سازوکار دسترسی کاربران نه تنها می‌تواند امنیت آنها را به شکل قابل توجهی افزایش دهد، بلکه دیگر وقت ارزشمند کاربران صرف انجام فرآیند بازیابی گذرواژه‌های فراموش‌شده نمی‌شود.

جالب است بدانید میزان هزینه استفاده از گذرواژه در شرکت‌ها نیز محاسبه شده است! کارشناسان تخمین می‌زنند استفاده از گذرواژه توسط هر کارمند حدود ۲۰۰ دلار هزینه روی دست یک سازمان می‌گذارد. این هزینه در واقع هزینه هدر رفتن زمان به خاطرآوری و وارد کردن گذرواژه یا انجام فرآیند بازیابی آن است. این رقم در یک سازمان بزرگ، بسیار چشمگیر خواهد بود.

گذرواژه‌ای برای همه چیز

همه ما در زندگی، برای خدمات مختلف نیاز به گذرواژه داریم. شاید تعیین و استفاده از یک گذرواژه مشخص برای کارت بانکی، دسترسی به اینترنت بانک، ایمیل، حساب در شبکه‌های اجتماعی و موارد دیگر، کار دشواری باشد، زیرا دیگر به‌راحتی نمی‌توان آنها را به خاطر آورد. به همین دلیل بیشتر افراد، یک یا چند گذرواژه ثابت را برای اغلب کارهای خود استفاده می‌کنند. اما این مساله دقیقا پاشنه آشیل امنیت دیجیتال آنها خواهد بود، زیرا در صورت لو رفتن یکی از آنها، حساب‌های دیگرشان نیز به‌شدت در برابر دسترسی غیرمجاز آسیب‌پذیر خواهد بود.

مدتی پیش، اتحادیه اروپا قوانین جدیدی را برای حل این مساله تدوین کرد. بر این اساس، شرکت‌های مختلف ملزم هستند برای احراز هویت مشتری خود از شیوه دو مرحله‌ای استفاده کنند.

در شیوه احراز هویت دو مرحله‌ای معمولا از توکن، گذرواژه یک‌بار مصرف یا کد ارسالی توسط پیامک استفاده می‌شود. با این وجود، به نظر می‌رسد توجه‌ها از این شیوه به سمت داده‌های بیومتریک جلب می‌شود. آمارهای یک موسسه امنیت مالی نشان می‌دهد حدود ۶۷درصد از بانک‌ها به سرمایه‌گذاری روی داده‌های بیومتریک فیزیکی نظیر اثرانگشت، الگوی صدا یا تشخیص چهره روی آورده‌اند.

بیومتریک را دریاب!

شرکت ناتوست که در زمینه ارائه کارت‌های اعتباری فعالیت می‌کند، دست به نوآوری جالبی زده است. این شرکت، یک اسکنر کوچک اثرانگشت را به‌صورت مستقیم روی کارت‌های اعتباری مشتریان قرار داده است. هرگاه مشتری بخواهد از این کارت استفاده کند، باید با اثرانگشت خود، درستی تراکنش مورد نظر را تایید کند. از آنجا که سرقت هویت و استفاده غیرمجاز از کارت اعتباری از مهم‌ترین دردسرهای موسسات مالی به شمار می‌رود، این روش می‌تواند تا حد زیادی جلوی سوءاستفاده‌های رایج را بگیرد.

اما داده‌های بیومتریک، دردسرهای خاص خود را دارند. استفاده از این داده‌ها برای دسترسی به محصول یا خدمت موردنظر به مراتب ساده‌تر از وارد کردن یک گذرواژه است. با این وجود، استفاده از این داده‌ها نیازمند سخت‌افزار ویژه و البته پرهزینه است، اما شاید بتوان از یک میانبر برای حل این مساله استفاده کرد؛ این میانبر هم چیزی نیست جز گوشی هوشمند. بسیاری از شهروندان یک گوشی هوشمند دارای قابلیت شناسایی اثرانگشت دارند و تعداد این گوشی‌ها نیز درحال افزایش است. به این ترتیب شاید بتوان سامانه یا محصول مورد نظر را به شکلی طراحی کرد که بخش احراز هویت مبتنی بر اثرانگشت آن با استفاده از گوشی هوشمند انجام شود.

حتی داده‌های بیومتریک نیز ممکن است سرقت شوند. یکی دو ماه پیش، پژوهشگران چینی در یک کنفرانس امنیت سایبری در شانگهای نشان دادند که چطور می‌توان الگوی اثرانگشت یک فرد را با استفاده از چند تصویر که با فاصله چند متری از او گرفته شده، بازسازی کرد. همچنین در شماره‌های پیشین کلیک هم توضیح دادیم که هکرها چطور می‌توانند حتی از تصاویر سلفی به اشتراک‌گذاشته‌شده در شبکه‌های اجتماعی، تصویر اثرانگشت کاربر را به دست آورند.

اگر گذرواژه‌مان لو برود، شاید به‌راحتی بتوانیم گذرواژه‌ای دیگر را انتخاب کنیم. حال سؤال اینجاست که اگر تصویر اثرانگشت‌مان فاش شود چه؟

احراز هویت چندمرحله‌ای

شاید بهترین راه این باشد که از شیوه احراز هویت چندمرحله‌ای استفاده کنیم. هر قدر تعداد مراحل احراز هویت کاربر بیشتر باشد، احتمال دسترسی غیرمجاز هکرها و کاربران دیگر به حساب یا محصول مورد نظر نیز کاهش می‌یابد.

احراز هویت چندمرحله‌ای الزاما به وارد کردن گذرواژه یا اسکن اثرانگشت خلاصه نمی‌شود و شاید بتوان از اطلاعات دیگری که از کاربر موجود است برای اطمینان از هویت واقعی کاربر درخواست‌دهنده استفاده کرد. برای نمونه، موقعیت مکانی معمول برای دسترسی، سابقه خرید، سرعت تایپ، هویت گوشی و حتی شیوه در دست گرفتن گوشی، همگی مواردی است که می‌توانند به شناسایی بهتر هویت کاربر واقعی کمک کنند.

با در نظر گرفتن همه موارد ذکر شده، شاید جایگزین‌کردن داده‌های بیومتریک به جای گذرواژه معمولی، اقدام چندان عاقلانه‌ای نباشد. در واقع بهتر است به سمت استفاده از ترکیبی از همه تدابیر موجود، اعم از گذرواژه، ارسال پیامکی رمز موقت، اسکن اثرانگشت و موارد دیگر برویم.

ترکیبی از بهترین شیوه‌ها

احراز هویت چندمرحله‌ای نسبت به دیگر شیوه‌ها امن‌تر محسوب می‌شود، اما این روش نیز یک ایراد بزرگ دارد و آن هم زمان‌بر بودن است. به هر حال به نظر می‌رسد در آینده برای برخی موارد ضروری و حساس (مثل حساب‌های بانکی) از شیوه‌های احراز هویت چند مرحله‌ای بیشتر استفاده شود و برای موارد کم‌اهمیت‌تر نیز شیوه‌های تک‌مرحله‌ای، ولی امن‌تری نظیر اسکن اثرانگشت به کار گرفته شود.

خرده‌بین

اگر مطالب این صفحه را می‌پسندید، عدد ۲ ۷۳۰ را به شماره ۳۰۰۰۱۱۲۲۶ پیامک کنید