گزارش امنیتی (مستند مرجع)

عنوان گزارش: بررسی چالش‌های امنیتی سیستم‌های مبتنی بر شاخص‌های بیومتریکی

چکیده

امروزه، استفاده از تکنولوژی بیومتریک در راستای احراز هویت و تشخیص اصالت کاربران، امری بسیار رایج است و بسیاری از شرکت‌های سازنده‌ی وسایل دیجیتال، برای تامین مقاصد امنیتی دستگاه‌های تولیدی خود، به جای استفاده از روش‌های قدیمی‌تر مانند گذرواژه‌ها، از شاخص‌های بیومتریک استفاده می‌کنند.

مزایا و راحتی کار این تکنولوژی بر کسی پوشیده نیست. برای مثال، فراموشی رمز عبور از مشکلات رایج مردم است، در حالی‌که چنین مشکلی، در سیستم بیومتریک پیش نخواهد آمد. همچنین، به‌دلیل عدم امکان به اشتراک‌گذاری مشخصات بیومتریک، امنیت این سیستم‌ها بالا می‌رود، اما همانند سایر فناوری‌ها، این سیستم‌ها نیز از حملات هکرها و آسیب‌پذیری‌ها مصون نیستند. برخی معتقدند حملات به این‌گونه سیستم‌ها، در مقایسه با سیستم‌های قدیمی‌تر، مخرب‌تر خواهد بود.

در این گزارش، علاوه بر معرفی سیستم‌های بیومتریک و نگاهی اجمالی به نحوه‌ی فعالیت آنها، خطرات موجود را برشمرده و در صورت امکان، نمونه‌هایی از اتفاقات پیشین در این زمینه را بررسی خواهیم کرد.

بررسی چالش‌های امنیتی سیستم‌های مبتنی بر شاخص‌های بیومتریکی

با پیشرفت روزافزون فناوری در زندگی انسان و ناگزیر بودن وی به انجام برخی اعمال حساس و گاهاً محرمانه در فضای الکترونیک، اهمیت امنیت اطلاعات و احراز هویت صحیح فرد در این فضا نیز در حال افزایش است. یکی از تکنولوژی‌های شناخته‌شده برای احراز هویت، تکنولوژی بیومتریک است که از ویژگی‌های منحصر به‌فرد رفتاری و فیزیکی شخص، برای احراز هویت وی استفاده می‌کند. با وجود مزایای بارز این تکنولوژی در مقایسه با تکنولوژی‌های قدیمی‌تر مانند استفاده از گذرواژه‌ها، خطراتی جدی، امنیت آن را زیر سوال می‌برند. در این گزارش به بررسی این سیستم‌ها، مزایا، و معایب آنها پرداخته شده‌است.

1 معرفی بیومتریک

طبق دسته‌بندی مایکروسافت انکارتا، سه سطح امنیتی احراز هویت و تایید اصالت در کامپیوتر وجود دارد: سطح اول، مربوط به چیزی است که شخص با خود حمل می‌کند، مانند یک کارت الکترونیک که نقش عبوری برای فرد را ایفا می‌نماید؛ سطح دوم، مربوط به چیزی است که فرد می‌داند، مانند رمز عبوری که مشخص نموده‌است؛ سطح سوم، که بالاترین سطح امنیتی است، مربوط به چیزی است که بخشی از ساختار فیزیولوژیکی یا رفتاری شخص است، مانند اثر انگشت، یا امضای شخص. منظور از امنیت بیومتریک، احراز هویت و اصالت فرد به‌وسیله‌ی خصوصیات فیزیولوژیکی و رفتاری وی است [1].

واژه‌ی بیومتریک، از ترکیب واژه یونانی "بیو" به معنای زندگی، و "متریک" به معنای معیار، گرفته شده‌است. ایده‌ی اصلی احراز هویت بیومتریک این است که هر شخص، یکتا است و می‌تواند توسط ویژگی‌های ذاتی یا رفتارهای وی، شناسایی شود [2].

تکنولوژی بیومتریک قادر است افراد را بر اساس ویژگی‌های منحصر به فرد افراد، مانند صورت، اثر انگشت، عنبیه‌ی چشم، یا DNA شناسایی کرده و روش‌های ایمنی را برای احراز هویت آنها از این طریق، فراهم سازد. بنابراین، بیومتریک عبارت است از تحلیل آماری و اندازه‌گیری ویژگی‌های رفتاری و فیزیکی یک شخص. برای نمونه، سیستم‌های تشخیص صوتی، با استفاده از اندازه‌گیری ویژگی‌های سخنرانی یک شخص (مانند هوایی که از ریه‌ها خارج می‌شود، از حنجره می‌گذرد و از طریق دهان و بینی وی خارج می‌شود)، عمل می‌نمایند [3, 4].

امروزه، امنیت بیومتریک، یک صنعت رو به‌رشد است. جالب است بدانید که این علم، یک علم نوظهور نیست. در واقع، شواهدی از نقاشی‌های داخل غارها دال بر ورود افراد از طریق شکل دست، وجود دارد. این شواهد، قدمتی 31 هزار ساله دارند، اما بیومتریک‌های مورد مطالعه در این گزارش، در قرن 19 مورد توجه جدی قرار گرفتند. مطالعات روی تشخیص دستی اثر انگشت، به اواخر قرن نوزدهم بازمی‌گردد و تشخیص عنبیه‌ی چشم نیز از سال 1936 شروع شده‌است. با این‌حال، پیشرفت جدی این موارد، در نیمه‌ی دوم دهه‌ی 1980 بوده‌است [5].

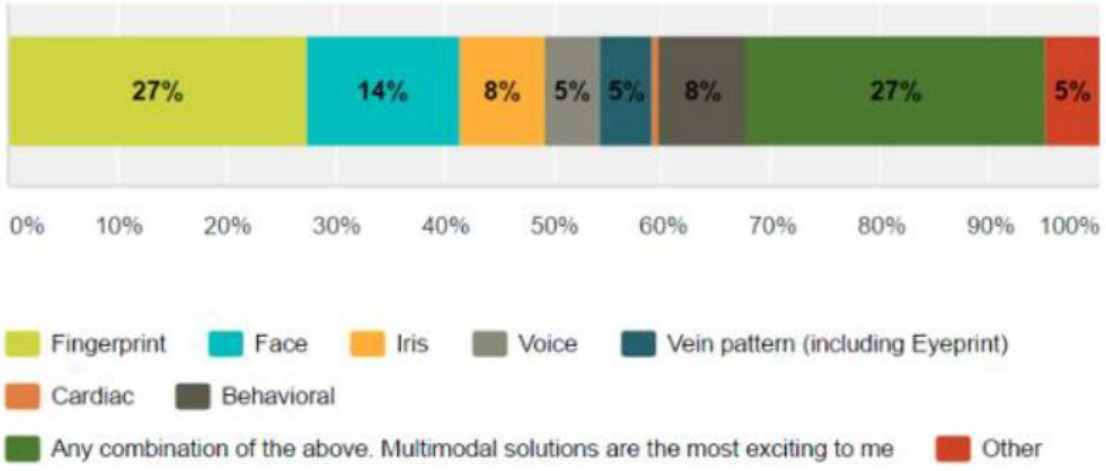
در سیر دقیق‌تری به این وقایع تاریخی، می‌بینیم که در سال 1892، گالتون، طبقه‌بندی اثر انگشت‌ها را توسعه داد. در سال 1959، پلیس لوس آنجلس، کاتالوگی از خالکوبی‌ها و نشانه‌هایی را برای احراز هویت افراد، گردآوری کرد. در سال 1994، اولین الگوریتم شناسایی بر اساس عنبیه‌ی چشم اختراع شد. همچنین، در همین سال، سرویس خودکار مهاجرت با استفاده از ساختار دست معرفی گردید. بین سال‌های 1994 تا 1999، FBI، سیستم یکپارچه‌ی شناسایی خودکار توسط اثر انگشت را توسعه داد و راه‌اندازی نمود. تشخیص چهره طی مسابقات ملی فوتبال آمریکا در سال 2001 آزمایش شد. در سال 2002، یک فیلم گزارش امنیت، عموم مردم را نسبت به بیومتریک‌ها کنجکاو نمود. در سال 2003، سازمان بین المللی هوانوردی آمریکا، از اسناد مسافرتی قابل خواندن توسط ماشین، پشتیبانی کرد. فناوری شناسایی مهاجرین و گردشگران ایالات متحده در سال 2004 راه‌اندازی شد. این روند، تا به امروز رو به پیشرفت بوده‌است و هر روز، محققین بیشتری در عرصه‌ی ایمن‌سازی سیستم‌های دیجیتال از طریق بیومتریک، گام می‌نهند [5].

همانطور که ذکر گردید، در تکنولوژی بیومتریک، افراد بر اساس ویژگی‌های منحصر به فرد خود، تمییز داده می‌شوند. این ویژگی‌ها، عمدتاً به دو دسته‌ی فیزیولوژیکی و رفتاری تقسیم می‌گردند. دسته‌ی نخست، به ساختار و شکل بدن مربوط می‌شود و شامل مواردی مانند اثر انگشت، چهره، و عنبیه‌ی چشم است. قدیمی‌ترین مورد از این دسته، اثر انگشت است که استفاده از آن قدمتی بیش از هزار سال دارد [3].

در شناسایی به‌وسیله‌ی اثر انگشت، ویژگی‌های مربوط به شیارهای سر انگشت، مانند تعداد لبه‌ها، نوع طرح، فاصله‌ی بین لبه‌ها، نقطه‌ی مرکزی، و منافذ، اندازه‌گیری و ثبت می‌شوند و برای احراز هویت، مورد استفاده قرار می‌گیرند. در فناوری تشخیص چهره، فاصله‌ی میان اجزای صورت (چشم‌ها، بینی، دهان و غیره) و در موارد پیشرفته‌تر، وضعیت بافت پوست صورت نیز بررسی می‌گردند. در شناسایی از طریق عنبیه‌ی چشم، بافت قسمت‌های رنگی چشم، اندازه‌گیری و ثبت می‌شود و برای شناسایی فرد به کار می‌رود. با پیشرفت فناوری، شناسایی از طریق ساختار رگ‌ها، ساختار دست، و ساختار انگشت‌ها نیز به این دسته افزوده شده‌اند [3].

دسته‌ی دوم، روی برخی رفتارهای فرد تمرکز دارد. در این دسته‌ی بیومتریک، نحوه‌ی حرکات بدن به‌طور اختصاصی سنجیده می‌شود. ویژگی‌هایی نظیر نحوه‌ی تایپ کردن شخص، صداهای وی، الگوی راه رفتن، امواج مغزی و یا ضربان قلب وی می‌توانند به شکلی تعیین گردند که مانند امضای فرد، منحصر به‌فرد باشند [3].

طبق آمار منتشر شده در سال 2017، بیومتریک رفتاری، سومین فناوری بیومتریک پرطرفدار است و اثر انگشت و چهره، به‌ترتیب، در رده‌های اول و دوم قرار دارند. این تحقیق توسط سایت FindBiometrics.Com روی 165 متخصص بیومتریک و شرکت‌های مرتبط با هویت و شناسه، صورت گرفته‌است [6].



رایج‌ترین مورد از این دسته، امضای فرد است. در این مورد، نحوه‌ی ترسیم امضا توسط فرد، شکل و سرعت ترسیم و مواردی دیگر از قبیل زاویه‌ی قلم یا فشار شخص روی قلم، برای احراز هویت، اندازه‌گیری و ثبت می‌شوند. در تشخیص هویت به‌وسیله‌ی گفتار، تن و آهنگ صدای فرد ذخیره می‌گردد و بر اساس تفاوت تارهای صوتی و اوج‌های صدا، احراز هویت صورت می‌پذیرد [3].

داده‌های بیومتریک نیز مانند سایر داده‌های فضای دیجیتال، از خطرت و رخنه‌های امنیتی در امان نیستند. در بخش بعدی نگاهی دقیق‌تر به امنیت آنها خواهیم داشت.

2 چالش‌های امنیتی سیستم‌های بیومتریک

یک سیستم بیومتریک، شامل کل سخت‌افزار، نرم‌افزار مربوطه، و زیرساخت‌های اتصالات داخلی برای اجرای فرآیند بیومتریک انتها به انتها است. اگر فرآیند بیومتریک را بخشی تفکیک‌ناپذیر از یک سیستم بزرگتر درنظر بگیریم، آن‌گاه، این تعریف را می‌توان به هر بخشی از سیستم‌های بزرگتر که اطلاعات کاربری را نگهداری می‌کند (برای مثال گزارشات تراکنش‌ها) تعمیم داد. به‌علاوه، در چنین سیستمی، فرآیند، تا زمان بعد از تکمیل احراز هویت و جایی‌که دیگر نیازی به کارکرد سیستم بزرگتر نیست، تعمیم می‌یابد [7].

در اینجا، منظور از آسیب‌پذیری، امکان به خطر افتادن سیستم بیومتریک و داده‌های مرتبط با آن از طریق طراحی (به‌عبارت دیگر عمل جعل)، خطای کارکردی، تصادف (اتفاقی که موجب فرصتی برای جعل شود)، خرابی سخت‌افزار، و یا شرایط محیطی خارجی است. به‌علاوه، باید درنظر داشت که این موارد، منجر به در خطر قرار گرفتن منافع محافظت‌شده توسط فرآیند بیومتریک خواهند شد [7].

پایداری فیزیکی ابزارهایی که کاربر با آنها مواجه است، از جمله چالش‌های امنیتی این سیستم‌ها به‌شمار می‌رود. دستگاه بیومتریک، به‌همراه هر تجهیزات دیگری در رابط کاربری، باید به‌نحوی طراحی و پیاده‌سازی شود که در مقابل هرگونه حمله‌ی فیزیکی و یا وخامت شرایط محیطی، مقاوم باشد. اگر دستگاه و تجهیزات همراه آن در رابط کاربری مورد حمله قرار گیرند، در حالت ایده‌آل، نباید این امکان وجود داشته‌باشد که بتوان داده‌های بیومتریک یا پروتکل‌های انتقال مربوطه را به‌دست آورد. همین‌طور، دستگاه باید بتواند در حالت ایده‌آل، هر فعالیت تهاجمی را تشخیص داده و آن را مستقیماً به بخش کنترل مرکزی اطلاع دهد. میزان باز بودن دستگاه و ارتباطات داخلی آن برای حمله، به‌همراه امکان به‌دست آوردن اطلاعات و داده‌های مربوطه، درجه‌ای از آسیب‌پذیری را نشان می‌دهند. لازم است عواقب خرابی بخشی یا همه‌ی قسمت‌های دیگر سیستم، در اندازه‌گیری میزان خطر، درنظر گرفته شوند [7].

مورد دیگری از چالش‌های امنیتی بیومتریک، امنیت ارتباط فیزیکی بین نقاط احراز هویت و سیستم میزبان است. این مورد می‌تواند شامل یک لینک مستقیم ساده بین یک دستگاه بیومتریک و یک کنترل‌گر میزبان، مانند یک کامپیوتر شخصی، باشد و یا می‌تواند شامل یک شبکه‌ی اختصاصی پیچیده‌تر باشد که در آن چندین دستگاه مستقیماً به یک کنترل‌گر میزبان متصل هستند. حالت دوم می‌تواند با حضور گره‌های تکرارکننده یا ابزارهای شبکه مشابه، پیچیده‌تر نیز شود. اگر هریک از این ارتباطات سیمی یا ابزارهای شبکه مربوطه، در مقاطعی میان دستگاه بیومتریک و میزبان عمداً قطع گردند، احتمال این‌که نفوذگری بتواند به اطلاعات و داده‌های شخصی دسترسی یابد، میزان آسیب‌پذیری را نشان خواهد داد. اگر همه‌ی این اطلاعات در منبع رمزنگاری شوند، میزان پایداری این رمزنگاری نیز باید مستقیماً دخالت داده‌شود. بر اساس نوع برنامه و محیط فیزیکی موجود، محافظت فیزیکی از این لینک‌های تبادل داده نیز درنظر گرفته می‌شود [7].

یکی دیگر از چالش‌های امنیتی، امنیت شبکه‌های شخص سوم[1] است. اگر یک شبکه‌ی شخص سوم به‌عنوان بخشی از یک سیستم بیومتریک به‌کار برده‌شود (برای مثال استفاده از اینترنت برای اتصال از راه دور به شبکه‌های شرکتی)، در این‌صورت، باید ارتباط انتها به انتهای بین کنترل‌کننده‌ی میزبان و سرور برنامه، به دقت مورد توجه قرار گیرد. برای نمونه، اگر احراز هویت در کنترل‌کننده‌ی میزبان صورت پذیرد، چه اطلاعاتی از طریق مسیر عبوری به سرور برنامه بازمی‌گردد؟ احتمال به‌دست آوردن این اطلاعات از طریق نظارت بر این ارتباط، چقدر است؟ اگر احراز هویت در سمت سرور صورت پذیرد، آن‌گاه، اطلاعات بیومتریک چگونه بین کنترل‌کننده‌ی میزبان و موتور احراز هویت منتقل می‌شوند؟ شاید ترکیبی از متدهای عمومی امنیت اطلاعات و پروتکل‌ها (SSL، IPSEC، VPNs، و غیره) به‌همراه متدهای امنیت اطلاعات اختصاصی سیستم بیومتریک، بتواند معیاری برای آسیب‌پذیری مربوطه را نشان دهد. اگرچه، محاسبه‌ی این میزان، بدون تجارب صحیح، کار دشواری است. شاید بتوان توانایی یا تمایل ISPها برای تضمین یکپارچگی و امنیت اطلاعات را نیز عامل موثری در برابر آسیب‌پذیری دانست. شبکه‌های بی‌سیم نیز باید در این دسته قرار گیرند، مخصوصاً پیامدهای شنود اطلاعاتی که مخابره می‌شوند [7].

امنیت موتور احراز هویت و رابط‌های مربوط به آن نیز از چالش‌های مذکور به‌شمار می‌رود. احتمال این‌که فرآیند احراز هویت در یک موقعیت شبکه‌ای، به‌وسیله‌ی تصویب داده‌های غیرمجاز تحت خطر قرار گیرد، می‌تواند نشانه‌ای از میزان آسیب‌پذیری باشد. این دسته می‌تواند شامل رابط‌های میان موتور احراز هویت و دایرکتوری‌ها، پایگاه‌های داده و سایر اجزایی باشد که مستقیماً با نتایج تصمیمات کار می‌کنند و آنها را می‌پذیرند. برای نمونه، آیا ممکن است بتوان از فرآیند احراز هویت با استفاده از تصرف کنترل چنین رابط‌هایی رد شد؟ به‌طور مشابه، چگونه موتور احراز هویت تایید می‌کند که داده‌های تراکنش واقعی را دریافت می‌نماید و این داده‌ها از جریان داده‌ی منبعی دیگر نیستند؟ احتمال این‌که موتور احراز هویت و رابط‌های مربوطه‌ی آن بتوانند از این طریق گمراه شوند، می‌تواند معیاری از آسیب‌پذیری را نشان دهد [7].

امنیت فرآیندها در کنترل‌کننده‌ی میزبان نیز باید مورد توجه قرار گیرد. با فرض این‌که دستگاه بیومتریک از طریق یکی از باس‌های عمومی به کنترل‌کننده‌ی میزبان متصل شده‌باشد، احتمال این‌که بتوان داده‌ها را بطور مخفیانه از طریق باس به‌دست آورد، چقدر است؟ برای نمونه، می‌توان کدی نوشت که بافرهای FIFO را در یک پورت سریالی تحت نظارت قرار دهد و جریان‌های داده را، بدون این‌که برنامه‌ی

[1] Third party

میزبان و یا کاربر متوجه شوند، به برنامه‌ی دیگری برای تحلیل بیشتر ارسال کند. اگر این اتفاق بیفتد، احتمال این‌که بتوان داده‌های بیومتریک و پروتکل‌های انتقال را به‌دست آورد، چقدر است؟ کجا می‌توان داده‌های رمزنگاری‌شده را بازیابی کرد و خواند؟ اگر جریان داده‌ها به‌طور مخفیانه از این طریق به‌دست آیند، شخص نفوذگر زمان کافی را برای تحلیل داده‌های به‌دست‌آمده در اختیار خواهد داشت [7].

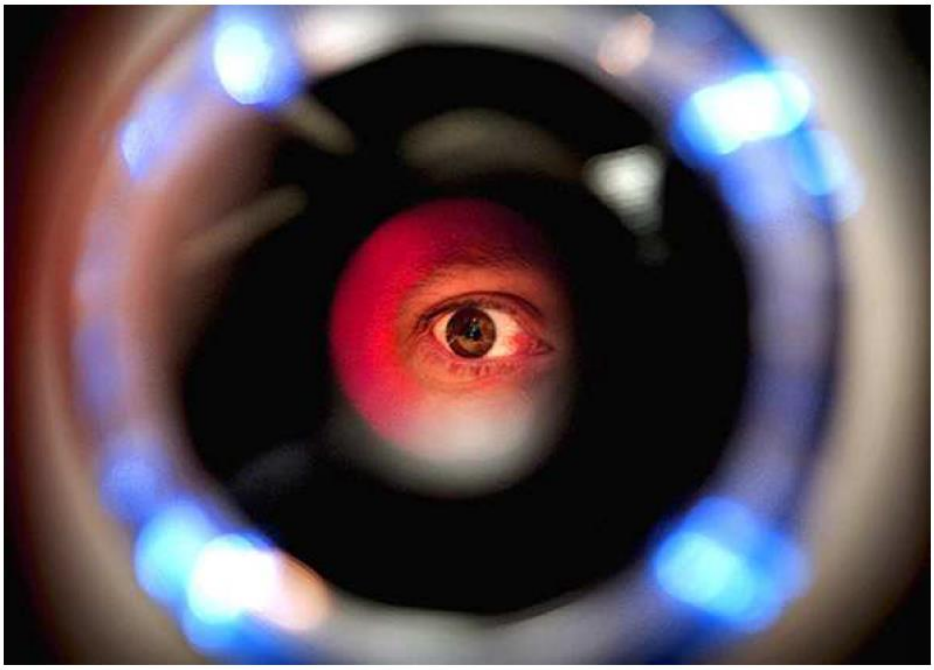
عملکرد دستگاه بیومتریک اصلی، از عوامل مهم امنیتی این سیستم‌ها محسوب می‌شود. احتمال این‌که دستگاه بیومتریک بتواند توسط شخص نفوذگری گمراه شود، مستقیماً در میزان آسیب‌پذیری، موثر است. شاید چنین تلاش‌های نفوذگرانه‌ای، از طریق نمونه‌های زنده از افراد نادرست، و یا دستگاه‌های فرعی گمراه‌شده، مانند انگشت اشتباهی، دست، و یا غیره، صورت پذیرند. دقت ادعای تولیدکنندگان درباره‌ی ارقام مربوط به عملکرد و مواردی از این‌دست، می‌تواند میزانی از آسیب‌پذیری را نشان دهد. اما محاسبه‌ی میزان آسیب‌پذیری در دنیای واقعی و شرایط اجرایی واقعی، کار دشوارتری است و به عوامل متعددی، مانند تنظیمات سیستم، بستگی دارد [7].

یکی دیگر از چالش‌های روبه‌روی امنیتی بیومتریک، امنیت کلیه‌ی رویه‌های احراز هویت است. در بسیاری از نمونه‌ها، ارائه و تایید یک نمونه‌ی بیومتریک، تنها یکی از اعضای فرآیند کلی احراز هویت را نشان می‌دهد. اگر فرآیند شامل چند مرحله باشد (برای مثال شناسه‌ی کاربری، رمز عبور و بیومتریک)، آن‌گاه، آسیب‌پذیری ضعیف‌ترین لینک نیز باید درنظر گرفته شود. برای نمونه، آیا امکان استفاده از رمز عبور به‌عنوان جایگزینی برای بیومتریک به کاربران داده شده‌است یا خیر. بسیاری از سیستم‌ها به‌صورت پایه‌ای، این امکان را به کاربران خود می‌دهند. خود مجموعه نرم افزاری بیومتریک می‌تواند در صورتی‌که شخصی دارای دسترسی سطح مدیر بتواند تنظیمات را تغییر دهد، و یا تظیمات در یک دایرکتوری یا پایگاه داده ذخیره شوند، تحت خطر باشد. بنابراین، رویه‌های احراز هویت باید به تنهایی و صرف‌نظر از عملکرد احراز هویت بیومتریک، از نظر آسیب‌پذیری سنجیده شوند. امکان پیکربندی و نیز پیکربندی مجدد حساب‌های کاربری تقلبی می‌تواند نشان‌گر معیاری از آسیب‌پذیری باشد. همچنین، بسته به نوع فناوری به‌کار رفته، می‌تواند در زمره‌ی آسیب‌پذیری‌های خاص‌منظوره قرار گیرد [7].

در یک جمع‌بندی از چالش‌های گفته‌شده، می‌توان مشاهده نمود که آسیب‌پذیری واقعی یک فرآیند سیستم بیومتریک، معمولاً متشکل از چند ناحیه‌ی تحت خطر است. اگر هر یک از این نواحی از فرآیند ارزیابی میزان آسیب‌پذیری حذف شوند، نتایج غیرقابل استنادی به‌دست خواهد آمد. دشواری امر، وجود

تعداد زیاد متغیرهای درگیر در محاسبه‌ی این مقدار است، که تنها تعدادی از آنها در اینجا ذکر گردیدند. اندازه‌گیری دقیق آنها نیز خود امری مهم و دشوار به‌شمار می‌رود [7].

با وجود این‌که به‌نظر می‌رسد امنیت بیومتریک در سطح بالایی قرار دارد، اما مقابل هک، ایمن نیست. برای نمونه، در صورت هک این اطلاعات، نمی‌توان اثر انگشت جدیدی جایگزین نمود. پس شاید برخلاف



تصور عموم، امنیت بیومتریک‌ها در حد انتظار آنها بالا نباشد [8].

همان‌گونه که در تصویر بالا مشاهده می‌شود، شخصی در حال استفاده از اسکنر عنبیه‌ی چشم جهت تشخیص هویت است. این رویه متعلق به سال 2004 است. اسکنرهای بیومتریکی که در فیلم‌های جاسوسی/جنایی هالیوود می‌بینیم، قادرند کاملاً دوست را از دشمن تشخیص دهند. شاید به‌همین‌دلیل است که مردم فکر می‌کنند این سیستم‌های احراز هویت بیومتریک، همواره درست و موثر عمل می‌کنند و شکست خوردن آنها غیر ممکن است. همچنین، آنها را آینده‌ی احراز هویت می‌دانند [8].

تا کنون، استفاده از بیومتریک برای احراز هویت، در مراکز بسیاری مورد استقبال قرار گرفته است. برای نمونه، در برخی باشگاه‌های ورزشی، برای احزار هویت ورزشکاران عضو باشگاه، از سیستم بیومتریک استفاده می‌شود. همچنین، در مرکز پزشکی دانشگاه نیویورک، بیماران نیازی به همراه داشتن کارت بیمه ندارند. زیرا

اطلاعات و پرونده‌ی آنها در سیستم امنیتی بیماران این مرکز ذخیره شده‌است و تنها با تایید هویت آنها از طریق بیومتریک، می‌توانند به این پرونده‌ها دسترسی یابند [8].

امنیت بیومتریک در مقایسه با انواع دیگر، از مزایایی برخوردار است. برای نمونه، درحالی‌که فراموش شدن گذرواژه، امری طبیعی است، اما اثر انگشت همواره همراه فرد است. از بسیاری جهات دیگر نیز استفاده از بیومتریک، ایمن‌تر از چند کاراکتری الفبایی ضعیف عمل می‌کند. اما عیب اصلی آنها، عدم قابلیت بازیابی و جایگزین نمودن آنها است. اگر اطلاعات بیومتریک شخصی به دست نفوذگری بیفتد، برای همیشه کنترل آن از دست فرد خارج می‌شود [8].

یکی از محققین امنیتی از دانشگاه ملی یاکوهاما، به نام تسومو متس، برای اثبات آسیب‌پذیری سیستم‌های بیومتریک، روشی پیشنهاد داد که از تصویر پنهان یک اثر انگشت روی یک لیوان عکس گرفته و آن را با قالب ژلاتین بازسازی کرده‌است. این تکنیک، در 80 درصد موارد، اسکنرهای بیومتریک را گمراه می‌کند. هکرهای دیگری نیز برای ساختن قالب اثر انگشت، از خمیر بازی کودکان استفاده کردند که نتیجه‌ی آن، توانایی گمراه کردن 90 درصد اسکنرهای اثر انگشت بوده‌است [8].

در سال 2008، کنفرانسی عمومی در آلمان برگزار شد که طی آن، وزیر داخلی آلمان به‌شدت از استفاده از بیومتریک پشتیبانی نمود. در پاسخ طرفداری وی، گروهی هکر پس از برگزاری سخنرانی عمومی جناب وزیر در دانشگاهی محلی، اثر انگشت وی را از روی یک لیوان آب برداشتند و آن را با قالب پلاستیکی بازسازی کردند. از این اثر انگشت، 4000 مرتبه کپی گرفته شد و به‌همراه مجله‌ی هکرها، بین آنها منتشر گردید. همین موضوع، راهی به سوی وجود اثر انگشت وزیر در صحنه‌های جرم گشود [8].

طرفداران ایمنی بیومتریک، با این استدلال که اثر انگشت یک ویژگی فیزیکی تغییرناپذیر است، از ایمنی آن دفاع می‌کنند. اما در سال 2009، این ادعا توسط فرد 27 ساله‌ی چینی نقض شد. این فرد، از دکتران خواست اثر انگشت وی را عوض کنند تا بتواند از سنسورهای بیومتریک احراز هویت در فرودگاه‌ها عبور نماید. او به جراحان چینی پول هنگفتی داد تا اثر انگشت‌های دست چپ و راست وی را با هم جابه‌جا نمایند و اثر انگشت‌های یکی از دست‌ها را به دیگری پیوند دهند. این حقه‌ی وی موفقیت آمیز بود و توانست از احراز هویت اداره‌ی مهاجرت در فرودگاه عبور کند. اما چند هفته بعد، زمانی‌که قصد داشت با مردی ژاپنی ازدواج نماید، مقامات محلی متوجه زخم‌های عجیبی روی نوک انگشتان وی شدند و پلیس را در جریان امر

قرار دادند. به گزارش پلیس ژاپن، این فرد، که لین نام داشت، نهمین نفری بوده که به‌خاطر جعل بیومتریک از طریق جراحی، دستگیر شده‌بود [8].

سپتامبر 2016، آژانس امنیت مناطق مرزی کانادا اخطار داد که یک حمله‌ی سایبری روی پایگاه‌داده‌های مربوط به اثر انگشت‌ها و چهره‌نگاری‌ها، توانسته‌است مانع خروج مسافران بی‌گناه از کانادا شود و یا به افراد غیرمجاز، اجازه‌ی ورود دهد. مقامات مربوطه اعلام کردند که باید رسیدگی به آسیب‌پذیری‌های سیستم‌های عبور و مرور کشوری را تسریع بخشند. روند رو به‌رشد استفاده از اطلاعات بیومتریک، مانند اثر انگشت، چهره‌نگاری و عنبیه‌ی چشم، نمونه‌های ذکرشده‌ی این فرآیند هستند. رابرت کپس، معاون توسعه‌ی خدمات در شرکت امنیتی NuData اذعان داشت: " زمانی‌که شخص موردنظر به‌صورت فیزیکی به محل احراز هویت مراجعه کند، بیومتریک‌های فیزیکی بسیار مناسب هستند و گمراه شدن آنها تقریباً غیرممکن است. اما در تعاملات غیرحضوری، استفاده از تنها یک نوع داده بیومتریک برای احراز هویت یک کاربر، تفاوت چندانی با اضافه کردن یک رمز عبور جدید نخواهد داشت. حتی در برخی موارد، شرایط بدتر نیز خواهد بود، زیرا می‌توان رمزهای عبور به سرقت‌رفته را بازیابی کرد اما اثر انگشت و یا عنبیه‌ی چشم، از چنین قابلیت بازیابی مجدد بی‌بهره‌اند [9].

تصاویر با کیفیت بالا از اثر انگشت‌ها، و یا نوع ریتم ضربان قلب افراد می‌توانند دزدیده و مجددا به‌کار گرفته شوند، مانند 5.6 میلیون اثر انگشتی که سال پیش از دفتر مدیریت پرسنل به سرقت رفتند. حتی روش‌هایی با سطوح پایین تکنولوژی نیز می‌توانند به نتیجه برسند. برای نمونه، با تعقیب فیزیکی شخص می‌توان اثر انگشت وی را برای فعالیت‌های جعلی به‌دست آورد. گستره‌ی وسیع آسیب‌هایی که تنها با داشتن یکی از اطلاعات بیومتریک فیزیکی می‌تواند وارد شود، پیچیدگی عملیات هکر امروزه و نیز مواردی را که باید تیم‌های امنیتی در نظر گیرند، نشان می‌دهد [9].

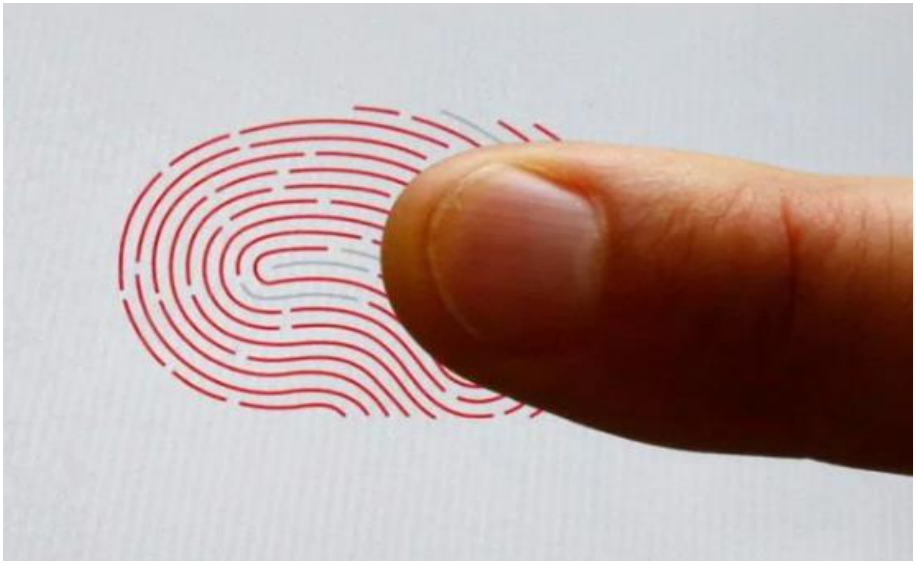
اگر یک آژانس خدمات بین مرزی مورد نفوذ قرار گرفته‌باشد و ما نشانه‌ای از این رخنه نداشته‌باشیم، پس حتماً خطری وجود دارد. مجرمان سایبری می‌توانند با ترکیب اطلاعات دزدیده‌شده در چنین نفوذهایی، قطعات هویت حساب‌های کاربری را کنار هم بچینند. به‌عنوان یک نمونه‌ی ترسناک، می‌توان Facebook of Everything را نام برد. سرویس اطلاعاتی کشور چین، درحال اجرای این طرح متشکل از اطلاعات شخصی به سرقت‌رفته از چندین رخنه‌ی امنیتی عظیم و مهم مانند سازمان مدیریت پرسنل است. مقامات چین اعلام کرده‌اند که هدف آنها، ارائه‌ی این اطلاعات در شبکه‌ای گسترده‌تر از فیسبوک و با اطلاعات و جزئیات

بیشتری نسبت به فیسبوک است. به‌عبارت دیگر، آنها هم اکنون پایگاه‌داده کاملی در اختیار دارند که شامل اطلاعاتی است که می‌تواند برای اهداف کلاهبرداری و جعل به‌کار برده‌شود. آنها قادرند با استفاده از این اطلاعات و اثر انگشت‌های دزدیده‌شده، هویت‌های به سرقت رفته و جعلی ایجاد کنند و با ارزش زیادی، به هکرها بفروشند. اگر اطلاعات بیشتری از افراد در دسترس باشد، سطح خطر کلاهبرداری‌های ممکن نیز بالاتر خواهد رفت. با وجود قابلیت تغییر و بازیابی رمزهای عبور، نمی‌توان اثر انگشت را تغییر داد و یا بازیابی نمود. پس، به سرقت رفتن آن، تبعات خطرناک‌تری را به همراه خواهد داشت [9].

در ادامه‌ی این گزارش، نمونه‌هایی شهودی از رخنه‌های امنیتی دستگاه‌ها و نیز اتفاقات امنیتی که در رابطه با سیستم‌های بیومتریک اتفاق افتاده‌اند، بررسی خواهند شد.

3 امنیت اثر انگشت (پرکاربردترین شناسه‌ی بیومتریک)

سالیان متمادی است که سنسورهای اثر انگشت، جایگزین رمزهای عبور شده‌اند. این سنسورها به‌طور گسترده‌ای در لپ‌تاپ‌ها دیده می‌شوند و اخیراً، کاربرد آنها در گوشی‌های هوشمند نیز مشهود است. اما



ادعای این سنسورها، مبنی بر رمزگشایی ایمن دستگاه، نقض شده‌است [10].

استفاده از اثر انگشت برای تشخیص هویت کاربر، در مقایسه با رمزعبور، دارای دو نقطه ضعف است [10]:

- اگر اثر انگشتی دزدیده شود، هیچ راهی برای باطل کردن و تعویض آن وجود ندارد. برای جبران این مشکل امنیتی خطیر، باید انگشت را سرقت نمود، که کار بسیار سختی است [10].
- پخش شدن ساده‌ی اطلاعات و کپی‌های اثر انگشت توسط فرد، حتی روی خود دستگاه گوشی، باعث ایجاد امکان جعل اثر انگشت وی می‌شود [10].

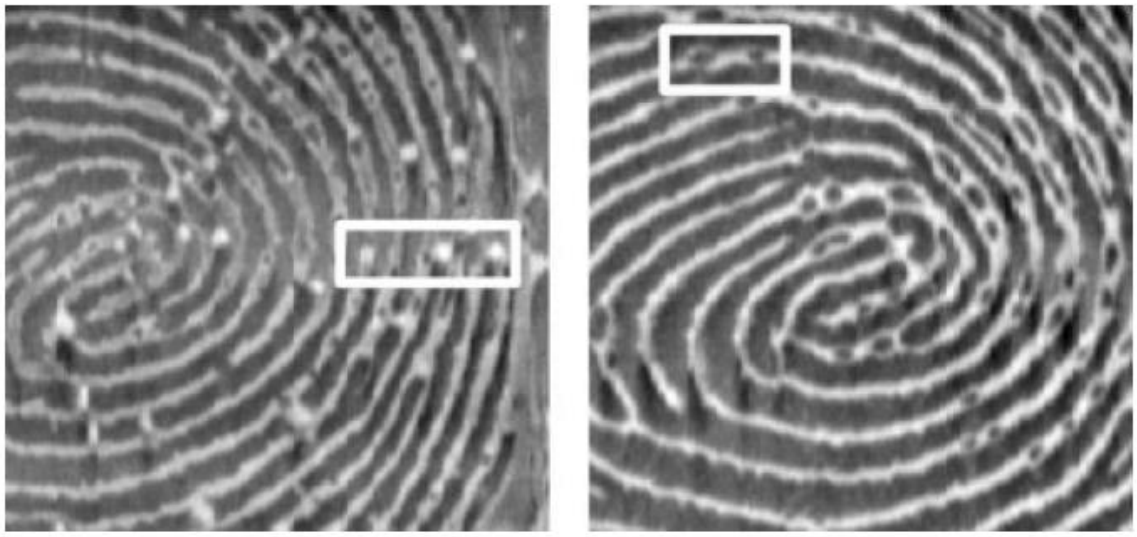
سنسورهای اثر انگشت، ایده‌ای برای حفاظت قوی دارند و آن، فراهم نمودن یک فاکتور احراز هویت دوم است. با این‌وجود، باز هم امکان اقداماتی از طرف نفوذگران وجود دارد. گوشی آیفون S5، از قابلیت‌های لمسی اولیه، کمی فراتر رفته‌است. این دستگاه، عکسی با وضوح بالاتر فراهم می‌آورد و از این وضوح برای

تطابق بر اساس ساختارهای ظریف‌تر استفاده می‌کند [10].

در سمت چپ از شکل فوق، تصویری با وضوح پایین از اثر انگشت مشاهده می‌شود. این تصویر، برای ساختن نسخه‌های جعلی در سنسورهای قدیمی مناسب بود. در سمت راست، تصویری با وضوح بالاتر از اثر انگشت را می‌توان دید. در این تصویر، شیارها واضح و روشن هستند که سنسورهای جدیدتر آنها را شناسایی می‌کنند [10].

این ساختارهای ظریف‌تر نیز می‌توانند جعل شوند: مثلاً، بر اساس عکسی از دوربین یک گوشی هوشمند با وضوح بالا، که با این وضوح برابری کند. این واقعیت نشان می‌دهد که استراتژی‌های دفاعی باید با شرکت تکنیک‌های حملات مربوطه، بهبود یابند [10].

برای پیشگیری از جعل اثر انگشت، بهتر است روی خطاهای اصلی در فرآیند ایجاد نسخه‌ی جعلی، و یا ویژگی‌های ظاهری اثر انگشت تمرکز کرد. می‌توان از حباب‌های هوای موجود در نوار چسبی که برای جعل به‌کار می‌رود به‌عنوان مثالی از این ویژگی‌ها یاد کرد. این حباب‌ها در تصویر سمت چپ عکس زیر، به شکل نقاط سفید رنگی مشهود هستند. همچنین، جزئیات ریزی که در یک سنسور اثر انگشت قابل دیدن هستند



ولی در اثر انگشت پنهانی دیده نمی‌شوند، به شکل نقاط سیاه در تصویر سمت راست، مشهود هستند [10].

هکرها می‌توانند از آسیب‌پذیری‌های موجود در اسکنرهای اثر انگشت در گوشی‌های هوشمند اندرویدی، برای جمع‌آوری از راه دور مقادیر وسیعی از اطلاعات درباره‌ی کاربران، بهره ببرند. این آسیب‌پذیری‌ها، سال 2015 توسط دو تن از محققین FireEye، به نام‌های تائو وی و یولانگ ژنگ، در کنفرانس هک کلاه سیاه در لاس وگاس، گزارش شد [11].

مشکلات امنیتی، مربوط به روشی است که این دستگاه‌ها، داده‌های بیومتریک را مدیریت می‌کنند. در خلاصه‌ای از نکات این سخنرانی می‌توان گفت که نقص‌های موجود، ناشی از موارد زیر هستند [11]:

- ابهام در فرآیندهای تایید اصالت اسکنرها، که می‌تواند به هکرها اجازه دهد بدافزارهایی را نصب کرده و در پرداخت‌های الکترونیک، از ویژگی‌های امنیتی اثر انگشت عبور کنند [11].
- نقص‌های ایمنی موجود در طراحی نطقه‌ی ایمن هسته اندروید (TrustZone) در سنسورهای اثر انگشت، که امکان حملات جاسوسی را فراهم می‌سازد تا هکرها بتوانند اثر انگشت افراد را از راه دور، به‌دست آورند [11].
- درهای پشتی[2] از پیش تعبیه‌شده‌ی اثر انگشت، که می‌توانند برای ربودن پرداخت‌های همراه محافظت‌شده توسط اثر انگشت، به‌کار برده شوند و برای جمع‌آوری اطلاعات کاربر گوشی هوشمند، استفاده گردند [11].

سخن محققین، حاکی از خطرناک بودن این حملات است، زیرا با مقاصد مختلفی، از قبیل سرقت هویت، از جانب هکرها اعمال می‌شوند. همچنین، بیان کرده‌اند که بر خلاف رمزهای عبور، اثر انگشت در طول عمر شخص، ثابت می‌ماند و با هویت قطعی و خاصی، گره می‌خورد. بنابراین، افشا و ایجاد و رخنه‌ی امنیتی در آن، عارضه‌ای جبران‌ناپذیر است [11].

گوشی‌های آیفون شرکت اپل، که از ویژگی TouchID برخوردارند، از این نقص‌ها مبرا هستند. این حملات، روی گوشی‌های وان مکس HTC و سامسونگ گلکسی S5 آزمایش شده‌بودند، اما محققین می‌گویند که این حملات روی اکثر گوشی‌های هوشمند اندرویدی که اسکنر اثر انگشت دارند، موثرند. تعداد دستگاهای اندرویدی که تا کنون مورد حمله قرار گرفته‌اند محدود مانده‌است، زیرا تولیدکنندگان کمی، به‌جز

[2] Backdoors

سامسونگ، هواوی، و اچ‌تی‌سی، اسکنرهای اثر انگشت را به گوشی‌های تولیدی خود اضافه نموده‌اند. با این‌حال، تعداد گوشی‌های اندرویدی مجهز به سنسورهای اثر انگشت، رو به افزایش است. گوگل اعلام کرده‌است که پشتیبانی از اسکنر اثر انگشت را مستقیماً در نسخه‌ی جدید اندروید قرار خواهد داد. این نسخه، که در حال حاضر با عنوان اسم رمز Android M از آن نام برده می‌شود، اواخر سال جاری در کنفرانس توسعه‌ی I/O منتشر خواهد شد. پشتیبانی از این اسکنرها داخل خود اندروید، کار شرکت‌های فناوری را برای اضافه کردن این قابلیت بیومتریک در گوشی‌های هوشمند، راحت‌تر خواهد نمود [11].

تائو وی و یولانگ ژنگ، از تولیدکنندگان گوشی‌های هوشمند به‌خاطر تعداد مراحلی که برای بهبود امنیت اسکنرهای اثر انگشت دستگاه‌های خود انجام داده‌اند، انتقاد کرده‌اند. همچنین، به کاربران این دستگاه‌ها پیشنهاد کردند که برای پیشگیری از قربانی شدن در این حملات، از تولیدکنندگانی گوشی هوشمند خریداری نمایند که سریعاً به آخرین نسخه‌های نرم‌افزاری مجهز و به‌روز می‌شوند. به‌علاوه، افزودند که نصب برنامه‌ها از منابع امن و قابل اعتماد، قدم مهمی در راستای پیشگیری از قربانی شدن است [11].

اکنون، شرکت امنیتی FireEye درنظر دارد در کنفرانس RSA پیش رو، هکی را نشان دهد که داده‌های بیومتریک را قبل از ورود به منطقه‌ی ایمن دستگاه، به سرقت می‌برند. طبق تحقیقات این شرکت، اندروید در تلاش برای غیرقابل دسترس کردن اطلاعات اثر انگشت از سایر برنامه‌ها، با ایزوله کردن آنها در یک ناحیه‌ی امن، موفق نبوده‌است. نفوذگران، به جای تلاش برای ورود به ناحیه‌ی امن، به‌سادگی روی خواندن اطلاعاتی تمرکز می‌کنند که پیش از آن‌که به ناحیه‌ی امن برسد، مستقیماً از سنسور اثر انگشت آمده‌است. محققین بر این باورند که با استفاده از این اطلاعات، ساختن مجدد اثر انگشت و استفاده از آن برای قفل‌گشایی گوشی هوشمند، غیر ممکن نیست [12].

طبق گفته‌ی یکی از محققین امنیتی به نام یولانگ ژنگ، اگر نفوذگر بتواند هسته را بشکند، اگرچه نمی‌تواند به اطلاعات ذخیره‌شده‌ی اثر انگشت در ناحیه‌ی امن دسترسی پیدا کند، اما می‌تواند مستقیماً در هر زمانی، اطلاعات سنسور اثر انگشت را بخواند. یعنی، هربار که شخص سنسور اثر انگشت را لمس کند، نفوذگر می‌تواند اثر انگشت وی را به سرقت برد. سپس، می‌تواند با در دست داشتن داده‌های مذکور، تصویری از اثر انگشت ایجاد کرده و از آن برای مقاصد خود استفاده کند [12].

این آسیب‌پذیری، در نسخه جدیدتر اندروید (لالی‌پاپ) برطرف شد و کاربرانی که امکان ارتقای سیستم گوشی هوشمند خود را دارند، بهتر است این کار را انجام دهند. اما برخی دستگاه‌های اندرویدی که از نسخه‌های قبل از لالی‌پاپ استفاده می‌کنند، تحت خطر حملات هستند [12].

اما آیا باز هم می‌توانیم در عصر پایگاه‌داده‌های بیومتریک انبوه، از ورود از طریق اثر انگشت استفاده کنیم؟ شخصی به تنهایی طی 5 دقیقه توانست اثر انگشتی را جعل کند و وارد گوشی یک قربانی شود. کار ساده‌ای بود، حقه‌ای که شرکت بیومتریک Vkansee، چند ماه پیش در یک برنامه تجاری اجرا کرد. تنها چیزی که لازم بود، یک قالب و کمی خمیر بازی برای پر کردن آن بود. این‌کار، مجددا روی گوشی آیفون 6 و گلکسی S6 اج انجام داده‌شد و باز کردن قفل آنها، تنها کمی سخت‌تر از باز کردن یک نامه بود. البته، این روش خاص، تنها زمانی موثر است که خود شخصی که قصد دارید از اثر انگشت وی استفاده نمایید، حاضر باشد به شما کمک کند [13].

محققین مرکز تحقیقات فناوری تشخیص هویت (به اختصار CITER) ترفندی مشابه با روش ذکرشده انجام دادند. آنها از یک عکس ذخیره‌شده، به جای اثر انگشت، با خمیر به‌طور سه بعدی پرینت گرفته بودند. در کنفرانس CCC سال 2014، یک محقق امنیت به نام استاربوگ، با استفاده از یک عکس با وضوح بالا از دست وزیر خارجه‌ی آلمان و با به‌کارگیری این تکنیک‌ها، اقدام به ساخت یک مدل از اثر انگشت وزیر نمود. این، حقه‌ی خوبی است و برای کاربران این دستگاه‌ها می‌تواند نگران‌کننده باشد. امروزه اثرانگشت‌خوان‌ها، بخشی اساسی از یک گوشی هوشمند مدرن به‌شمار می‌روند و در اکثر موارد، شامل بالا رفتن سطح ایمنی برنامه‌ها می‌شوند. اکثر خوانندگان بیومتریک، با سخت‌افزار خاص و پروتکل دانایی صفر کار می‌کنند. پس‌گرفتن داده‌ی رد و بدل‌شده برای جعل کردن یک ورود، کافی نیست. بلکه، برای وارد شدن، به خود اثر

انگشت احتیاج دارید. اما خبر بد این است که اثر انگشت‌ها می‌توانند به سرقت روند و خبر بدتر این‌که برخلاف رمزهای عبور، نمی‌توان اثر انگشت را تغییر داد و اثر انگشت جدیدی جایگزین کرد! پس، تنها یک‌بار سرقت این اعتبار، آسیب‌پذیری شگرفی، به مدت طول عمر فرد، ایجاد خواهد کرد. بنابراین، آن‌چه که به‌نظر می‌رسید یک ارتقای امنیتی به‌شمار رود، بسیار پیچیده‌تر و چالش‌برانگیزتر است. اثر انگشت پلاستیکی ساخته‌شده توسط CITER را در شکل زیر مشاهده می‌کنید [13].

در جریان اتفاقات تیراندازی در سال 2016 در سن برناردینو، مامورین دولتی در تلاش بودند تا قفل یک گوشی آیفون را، که به یک حادثه‌ی تیراندازی عظیم مرتبط بود، بازگشایی کنند. گوشی مذکور، آیفون S5 (آخرین گوشی آیفون فاقد اثر انگشت‌خوان) بود. اما اگر یک گوشی جدیدتر با اثر انگشت قفل شده‌بود، وارد شدن به آن برای مامورین دولتی چندان کار پیچیده‌ای نبود [13].

قالب‌های سه بعدی چاپ‌شده، باعث می‌شوند که هر عکسی از یک اثر انگشت، به یک مدل کارا از همان اثر انگشت تبدیل شود. پلیس امنیت محلی آمریکا، اثر انگشت افراد غیربومی با سن بین 14 تا 79 سال و همچنین مهاجرین غیرقانونی را جمع‌آوری کرده‌است [13].

سازمان FBI، یک پایگاه‌داده برای سیستم خودکار شناسایی اثر انگشت جمع‌آوری می‌کند که بالای صد میلیون رکورد اثر انگشت در آن موجود است. این تعداد، شامل 34 میلیون اثر انگشت افراد مدنی است که

به هیچ مورد جنایی، مرتبط نیستند. وزارت دفاع، یک پایگاه‌داده‌ی سومی دارد که حتی تعداد هویت بیشتری نسبت به پایگاه‌داده‌ی مذکور قبلی، توسط افسران نظامی از سراسر دنیا در آن گردآوری شده‌است. از این رکوردها معمولاً برای شناسایی هویت استفاده می‌شود، اما دلیلی ندارد که برای باز کردن قفل اثرانگشت‌خوان‌ها نیز به‌کار برده نشوند [13]!

حتی با رایج‌تر شدن این مجموعه، ممکن است اثر انگشت‌ها نیز به شکل دیگری از اطلاعات لو رفته، مانند رمزهای عبور، کارت‌های اعتباری، و شماره‌ی تامین اجتماعی، درآیند. به‌عنوان نمونه‌ای از این اتفاق، می‌توان به رخنه‌ی امنیتی در دفتر مدیریت پرسنل (به اختصار OPM) اشاره کرد، که باعث به‌خطر افتادن اثر انگشت 14 میلیون مامور فدرال شد. همین رخنه‌ی امنیتی می‌تواند در مقیاس کوچکتر نیز صورت پذیرد. بدین‌صورت که شخص نفوذگر، اثر انگشت افراد را از روی مبلمان و وسایل، و یا حتی از روی عکس‌های با وضوح بالا بردارد [13].

برای یک شخص نفوذگر، یافتن و دیدن اثر انگشت، ساده‌تر از یافتن رمز عبور است، زیرا همیشه در بدن شما مشخص و قابل رؤیت است و فرد قربانی، هر بار با لمس کردن سطوح صاف، یک کپی از آن در اختیار نفوذگر قرار می‌دهد. هنگامی‌که نفوذگر عکسی از یک اثر انگشت در اختیار داشته‌باشد، ساختن مدل، کار بسیار راحتی است. علاوه بر چاپگرهای سه بعدی، که به‌راحتی در دسترس هستند، متخصصین امنیتی، راه‌های دیگری را نیز برای جعل اثر انگشت یافته‌اند [13].

با وجود تعبیه اثر انگشت‌خوان‌ها روی اکثر گوشی‌ها، بیومتریک‌ها راه درازی پیش رو دارند تا ورودی اصلی دستگاه‌ها شوند. تحلیل‌گران برآورد کرده‌اند که کمتر از 15 درصد ورود به گوشی‌های آیفون، از طریق اثر انگشت صورت می‌گیرد و اکثر گوشی‌ها، اثر انگشت کاربر را ندارند. برای این گوشی‌ها، پایگاه‌داده‌ها و رکوردهای اثر انگشت ذخیره‌شده‌ی افراد توسط دولت، کاربردی ندارد، اما در مورد کاربرانی که با اثر انگشت وارد گوشی خود می‌شوند، پلیس راه ساده‌ای برای ورود به گوشی آنها خواهد داشت. البته، این مشکل، تنها متوجه خلافکارها نیست، بلکه در ارتباط با بیومتریک نیز صادق است، زیرا اثر انگشت‌های جمع‌آوری‌شده توسط سازمان فدرال، هرگز نمی‌توانند محرمانه باقی بمانند. جمع‌آوری آنها می‌تواند مانند ماجرای دفتر مدیریت پرسنل، به یک رخنه‌ی امنیتی بینجامد. در ادامه، اتفاقات مربوط به رخنه‌ی امنیتی در سازمان مدیریت پرسنل تشریح خواهد شد [13].

4 بزرگترین دزدی اطلاعات شخصی حساس در تاریخ

بالاخره دولت فدرال، پس از چندین ماه از بیانیه‌ی آژانس مدیریت پرسنل مبنی بر مورد حمله قرار گرفتن توسط هکرها، در ماه اکتبر سال 2015 شروع به اطلاع‌رسانی به 21.5 میلیون نفری کرد که اطلاعات شخصی آنها از طریق یک رخنه‌ی امنیتی عظیم در این دفتر به سرقت رفته بود [14].

بث کوبرت، رئیس اداره‌ی مدیریت پرسنل، در بیانیه‌ای در یک وبلاگ اظهار داشت: "دیروز شروع به ارسال نامه‌ها و اطلاع‌رسانی‌ها به افرادی کردیم که اطلاعات آنها در یک حمله‌ی سایبری علیه دولت فدرال، به سرقت رفته بود. این اطلاع‌رسانی، از طریق خدمات پستی آمریکا خواهد بود و از پست الکترونیکی استفاده نخواهد شد." نخستین‌بار، این اداره در اوایل ماه ژوئن متوجه شد که اسناد مربوط به تحقیقات درمورد میلیون‌ها تن از کارمندان پیشین یا فعلی فدارل و یا پیمانکاران آنها، در یک حمله‌ی سایبری در اوایل سال 2014، به سرقت رفته‌است. در اواسط ماه ژوئن، این آژانس، حمله‌ی بزرگتری را اعلام کرد که اطلاعات میلیون‌ها آمریکایی دیگر را که برای تایید امنیت ثبت‌نام کرده‌بودند، هدف قرار داده‌بود. اعتراضات مبنی بر این اخبار، موجب استعفای کاترینا آرچولتا، رئیس این سازمان، شد [14].

پس از آن، این سازمان اعلام کرد که در یک حمله‌ی سایبری، 5.6 میلیون اثر انگشت افراد به سرقت رفته‌است، که 5 برابر بیشتر از مقدار اعلام‌شده‌ی پیشین بود. کوبرت اظهار داشت: "گروهی از متخصصین در حال بررسی راه‌هایی هستند که ممکن است مجرمان از آنها برای سرقت اطلاعات اثر انگشت استفاده کرده‌باشند و طی نتایجی که تا کنون به‌دست آمده‌است، این متخصصین بر این باورند که راه‌های مذکور، محدود هستند [15, 14]."

مظنون اصلی این رخنه‌ها و حملات، کشور چین است، اما دولت آمریکا تا کنون از اتهام این ملت به انجام این حملات خودداری کرده‌است. رئیس جمهور چین نیز در دیداری از ایالات متحده اذعان داشت که کشور وی شدیداً حامی امنیت سایبری است و خود نیز قربانی حملات هک قرار می‌گیرد [15].

این حمله‌ی سایبری به دفتر مدیریت پرسنل، نشانی از مشکلات سیستمی در بخش فناوری اطلاعات دولت بود. تیم‌های فناوری اطلاعات به هنگام مواجهه با حمله‌ی سایبری، باید به‌طور سریع و قاطع، پاسخگو باشند. اما علی‌رغم این نکته، کمیته‌ی نمایندگان نظارت و اصلاحات دولتی، اخبار حملات سایبری علیه دفتر مدیریت پرسنل را بسیار دیر علنی کردد. این حملات به مدت چند سال در جریان بوده و باعث افشای

اطلاعات شخصی 21.5 میلیون نفر، از جمله کارمندان دولتی، شده‌است. این اتفاق حاکی از مشکل سیستمی در بخش فناوری اطلاعات دولت است [16].

در اثبات این ادعا می‌توان به اخطار امنیتی سربازرس در سال 2005 و سپس، ارائه‌ی گزارش نقص‌های امنیتی این سازمان در سال 2014 اشاره کرد. این نقص‌ها شامل مواردی، همچون عدم رمزنگاری، عدم احراز هویت دو مرحله‌ای برای دست‌یابی از راه دور به سیستم، عدم ایجاد فهرستی از سرورها و پایگاه‌های داده، و عدم آگاهی از تمامی سیستم‌های مرتبط با شبکه‌های این سازمان است. اولین افکاری که با دیدن این اخبار به ذهن می‌رسد، این است که میزان پول موردنیاز برای جلوگیری از این اتفاقات، بسیار ناچیز است، مخصوصاً برای یک سازمان دولتی! اما سوال اینجاست که چرا کسی این هزینه را تقبل نکرده‌است؟ به‌نظر می‌رسد پاسخ این سوال، از عدم مسئولیت‌پذیری حکایت دارد، زیرا این سازمان تا سال 2013 حتی یک تیم امنیت فناوری اطلاعات نیز نداشته‌است. همچنین، علی‌رغم تعدادی از اتفاقات و رخنه‌های امنیتی که طی دهه‌ی پیشین رخ داده، هیچ‌کس از سِمت خود در این سازمان برکنار نشده و عواقبی نیز متوجه این سازمان نگردیده‌است [16].

اگر این گزارش موردی را به ما نشان دهد، آن، محافظت مقابل رخنه‌های اطلاعاتی و حملات سایبری نیست، بلکه این است که اگر کسی در مقابل رخنه‌های اطلاعاتی پاسخگو نباشد، کسی انگیزه‌ای برای محافظت در مقابل آنها نخواهد داشت و یا حتی تلاشی برای کاهش تلفات آنها پس از انجام حملات صورت نخواهد گرفت [16].

هک سازمان مدیریت پرسنل، بدتر از آن چیزی است که تصور می‌شود! رخنه‌ی امنیتی اطلاعات در دفتر مدیریت پرسنل، بزرگترین دزدی اطلاعات شخصی حساس در تاریخ را به خود اختصاص داده‌است. اما تا به امروز، هیچ اطلاعاتی درباره‌ی مقیاس و دامنه‌ی این رخنه، یا پیامدها و یا حتی واکنش‌ها و محافظت‌های شخصی درباره‌ی آن، به‌طور دقیق و کامل بیان نشده‌است. مقیاس این رخنه، بزرگتر و مخرب‌تر از میزان متصور است. نحوه‌ی پاسخگویی به آن، باعث بدتر شدن اوضاع امنیتی قربانیان شده، و دولت به‌طور نامطلوبی درباره‌ی عواقب این اتفاق، اخبار مبهمی ارائه می‌دهد. هر چند ما نمی‌توانیم بفهمیم که برای کاهش عواقب این رخنه، چه اقداماتی مخفیانه‌ای از جانب دولت در حال انجام است، اما با توجه به آن‌چه در عموم می‌توان دید، میلیون‌ها قربانی این ماجرا، دلیل راسخی برای وحشت‌زدگی دارند. در ادامه، مقیاس این اتفاق را بررسی می‌کنیم [17].

اوایل ژوئن سال 2015 میلادی، برای نخستین‌بار، اخبار نقض امنیتی سازمان مدیریت پرسنل پخش شد. چندی پس از آن، در اواسط ماه ژوئن، مقامات، رخنه‌ی دیگری را، که شامل پرونده‌های امنیتی کارکنان فعلی و پیشین و نیز پیمانکاران این سازمان بود، اعلام کردند. اطلاعات تحت خطر، شامل فرم‌های SF-86 بودند که حاوی اطلاعات و جزئیات دقیق درباره‌ی زندگی شخصی، اعضای خانواده و سایر اطلاعات کارمندان شرکت است. اما وسعت محدوده‌ی این رخنه امنیتی، حتی بیشتر از این نفوذهای عظیم اعلام شده‌است. برای نمونه، در ماه دسامبر سال 2015، روزنامه‌ی واشنگتن پست گزارش داد که دولت، اطلاعیه‌هایی به روزنامه‌نگارانی که به ساختمان‌های فدرال دسترسی داشته‌اند و یا دارند، ارسال کرد تا به آنها اخطار دهد که ممکن است اطلاعات شخصی آنها در معرض خطر قرار گرفته‌باشد. این اطلاعیه می‌گوید که این رخنه، به تنهایی می‌تواند شامل حال صدها و هزاران گزارش‌گر، عکاس، و فیلمبردار زن و مرد باشد [17].

اولین سخنرانی مقابل کمیته‌ی نظارت و اصلاحات، در تاریخ 16 ژوئن 2015، نشانه‌ی دیگری از وسعت این نفوذ بود. در آن‌جا، دونا سیمور، رئیس اطلاعات این سازمان اعلام کرد که اطلاعات به خطرافتاده، شامل اطلاعات فرم‌های SF-86 و نیز تصمیم‌گیری‌ها و احکام سازمان است. این اخبار، بسیار تکان‌دهنده بود. اگرچه، اکثر رسانه‌ها توجه خود را روی اطلاعات فرم‌های FS-86 متمرکز کردند، اما اطلاعات مربوط به حکم‌ها بسیار مهم‌تر و پیچیده‌تر هستند. راهنمای حکم‌ها، که مختص افرادی هستند که به اطلاعات طبقه‌بندی‌شده دسترسی دارند، بسیار گسترده است. برای نمونه، اطلاعات جمع‌آوری‌شده برای تصمیم‌گیری درباره‌ی یک تحقیق محرمانه، شامل مصاحبه شخصی، مصاحبه با همسایگان، کارفرمایان، مربیان، و همسران است. همچنین، مکان‌های زندگی پیشین شخص و یا محل‌های آموزش طی ده سال پیش وی را به‌همراه دارد، که هیچ‌یک از این اطلاعات، در فرم‌های استاندارد SF-86 وجود ندارند [17].

اگرچه، به سرقت رفتن اطلاعات اثر انگشت به‌طور گسترده گزارش شد، اما بخش مهمی از مجموعه‌ی داده وجود دارد که نادیده گرفته شده‌است. انواع خاصی از تاییدیه‌های امنیتی به تحقیقات و آزمایشات با دستگاه دروغ‌سنج نیاز دارند. با وجود این‌که نمی‌دانیم این داده‌ها به‌صورت کامل در چه محلی ذخیره می‌شوند، اما بخش‌هایی از این اطلاعات، در داده‌هایی که دفاتر با سازمان مدیریت پرسنل به اشتراک می‌گذارند، وجود دارند [17].

هنوز گستره‌ی کامل داده‌های امنیتی تحت خطر مشخص نیست، زیرا برای نمونه، مقامات ایالات متحده هنوز این مورد را که پایگاه‌داده‌ی سازمان مدیریت پرسنل با پایگاه‌داده‌ی سازمان اطلاعاتی Scattered

Castles در ارتباط است را تایید یا تکذیب نکرده‌اند. پایگاه‌داده مذکور این سازمان اطلاعاتی، در سال 2008، با هدف استفاده‌ی انحصاری توسط انجمن اطلاعات، ایجاد شده‌بود. با وجود جدا بودن پایگاه‌داده‌ی سازمان مدیریت پرسنل از برخی سازمان‌های وابسته، اشتراک برخی اطلاعات فوق‌العاده حساس در آنها، کاملاً مشهود است. در گزارشی از سازمان تحقیقات در ماه جولای سال 2015 آمده‌است که اگر پایگاه‌داده‌ی سازمان اطلاعات به پایگاه‌داده‌ی سازمان مدیریت پرسنل مرتبط شده‌بود، هکرها می‌توانستند به اطلاعات پرسنل سازمان اطلاعات و نیز هویت مامورین مخفی دسترسی پیدا کنند. حتی اگر اطلاعات محرمانه‌ی این سازمان تحت خطر نبود، باز هم هکرها می‌توانستند با استفاده از اطلاعات توانایی‌ها و ضعف‌های مامورین و خویشاوندان آنها، مشکلاتی را برای آنها ایجاد نمایند [17].

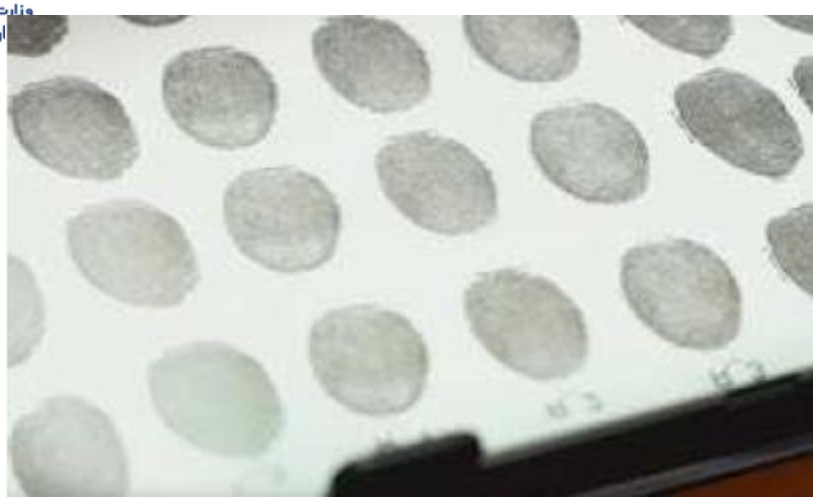
موردی که باعث وخیم‌تر شدن شرایط می‌گردد، این است که ظاهراً سازمان مدیریت پرسنل، پایگاه‌داده‌ای رمزنگاری‌نشده و غیرامن برای نگهداری تاییدیه‌های امنیتی داشته‌است. طبق گزارش این سازمان در سال 2006، داده‌ها به‌صورت داده‌های به اشتراک گذاشته‌شده[3]، ذخیره شده‌اند و دیسک‌های حاوی این اطلاعات، توسط همه‌ی سیستم‌ها قابل دسترسی هستند [17].

فارغ از پایگاه‌داده‌هایی که ذکر شد، سیستم‌های سازمان مدیریت پرسنل، به‌طور الکترونیکی، با سازمان‌ها و پایگاه‌داده‌های دیگری در ارتباط هستند. برای نمونه، شخصی که قادر است وارد سیستم سازمان مدیریت پرسنل شود، به‌دلیل ارتباط سیستم‌های این سازمان با JPAS، به مجموعه کاملی از اطلاعات محرمانه امنیت ملی، مانند اطلاعات وزارت دفاع ایالات متحده و ارتباطات با کشورهای خارجی و ملاقات‌های اعضای NATO، دسترسی خواهد داشت [17].

5 حملات و تهدیدات جدید (MasterPrintها)

اسکنر اثر انگشت گوشی‌های هواوی و سامسونگ را می‌توان با استفاده از یک چاپگر جوهرافشان، گمراه کرد. محققین نشان دادند که می‌توان با استفاده از چاپگر معمولی و کاغذهای مخصوص و جوهر، که برای چاپ مدارها استفاده می‌شوند، سنسورهای اثر انگشت را گمراه کرده و اثر انگشت را جعل کنند [18].

[3] Shared-data



اثر انگشت چاپ شده توسط یک چاپگر جوهرافشان پرشده با جوهر خازنی و کاغذ مخصوص، در تصویر بالا نشان داده شده‌است. با استفاده از این اثر انگشت می‌توان قفل بیومتریک گوشی را بازگشایی کرد [18].

محققین دانشگاه ایالتی میشیگان نشان دادند که سنسورهای اثر انگشت، که به‌منظور ایمن ساختن گوشی‌های هوشمند به‌کار می‌روند، می‌توانند با استفاده از چیزی به سادگی یک چاپگر جوهرافشان، گمراه شوند. کائی کائو و آنیل جین از بخش علوم مهندسی و کامپیوتر توانستند با استفاده از یک اثر انگشت، که با چاپگر جوهرافشان استاندارد و جوهر و کاغذ مخصوص چاپ شده‌بود، یک گوشی سامسونگ گلکسی S6 و هواوی هانر 7 را قفل‌گشایی کنند. این محققین، اسکن‌هایی از چندین انگشت گرفتند و به‌سادگی، آن را به‌صورت دو بعدی، روی کاغذ با جوهر خازنی چاپ نمودند. کاغذ مذکور، مخصوص چاپ مدارهای الکترونیکی و سایر سیستم‌های حامل بار است و جوهر آن نیز بار تولید می‌کند. آنها دریافتند که در زمان کمی می‌توانند همین‌کار را برای افراد و اثر انگشت‌های دیگر انجام دهند. در حالی‌که تلاش‌های پیشین در این زمینه، نیازمند تولید یک مدل از اثر انگشت توسط چوب یا پلاستیک یا چسب بودند، که به حداقل 30 دقیقه زمان و نیز تجهیزات ویژه نیاز داشتند. به گفته‌ی کائی کائو و آنیل جین، این آزمایش، ضرورت تکنیک‌های ضدجعل را برای سیستم‌های تشخیص اثر انگشت، نشان می‌دهد [18].

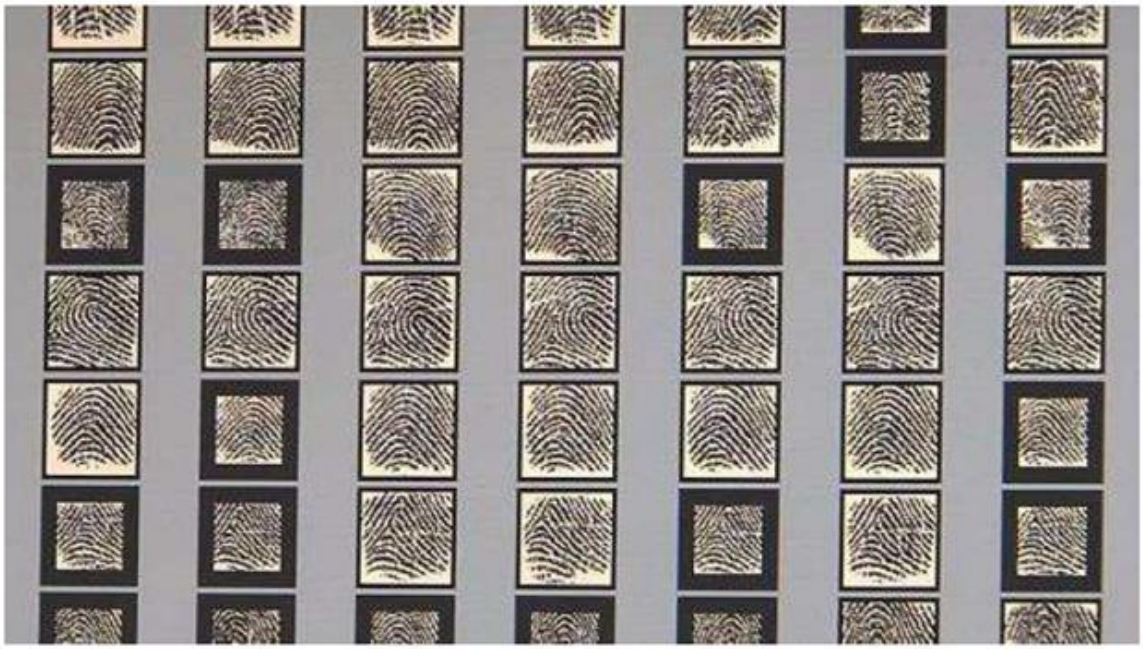
از آنجاکه گوشی‌های گلکسی S6 و هواوی هانر 7، از تکنولوژی اسکن اثر انگشت مشابه اکثر دستگاه‌های دیگر استفاده می‌کنند، می‌توان با استفاده از همین تکنیک، بسیاری از گوشی‌های دیگر را نیز به‌صورت جعلی، قفل‌گشایی نمود [18].

یک سخنگوی شرکت سامسونگ درباره‌ی این موارد اظهار داشت که سامسونگ، امنیت اثر انگشت را بسیار جدی می‌گیرد و به کاربران این اطمینان خاطر را می‌دهد که اثر انگشت‌ها، رمزنگاری‌شده و به‌صورت ایمن، داخل دستگاه‌ها ذخیره می‌شوند. وی افزود، با توجه به مندرجات گزارش، شبیه‌سازی اثر انگشت یک شخص، نیازمند تجهیزات و شرایط خاصی است، و هرگاه یک آسیب‌پذیری موثق وجود داشته‌باشد، این شرکت، بی‌درنگ اقدام به تحقیق و رفع آن خواهد نمود [18].

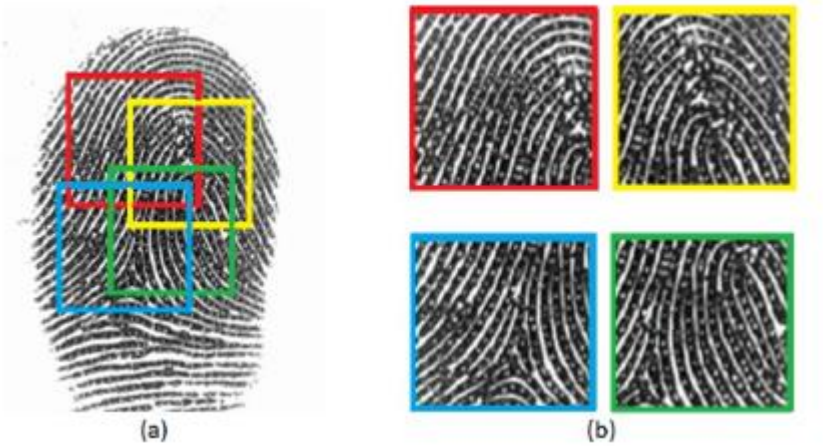
یک سخنگوی شرکت هواوی نیز به تعهد شرکت هواوی برای حفاظت از حریم شخصی افراد اشاره کرد و گفت که از طریق به‌روزرسانی مداوم تکنولوژی‌های جدید، از جمله تکنولوژی اثر انگشت، به این هدف نائل می‌آیند. وی با اشاره به گزارش‌های موجود درباره‌ی آسیب‌پذیری تکنولوژی سنسور اثر انگشت گفت که شرکت هواوی، گوشی هانر 7 را به امنیت سطح چیپ‌ست مجهز نموده که اطلاعات شخصی، مانند عکس اثر انگشت فرد، توسط سخت‌افزار، محافظت می‌شود. روش مذکور، برتری خاصی نسبت به تکنولوژی سایر گوشی‌های اندرویدی دارد. وی در پایان افزود که این شرکت، همچنان به توسعه‌ی فناوری‌های جدید برای بهبود امنیت و حریم خصوصی افراد پایبند است [18].

یک حمله‌ی سایبری گسترده در اوایل سال 2017، 300هزار قربانی در 150 کشور گرفت. اگرچه، سرعت این حمله رو به کاهش است، اما متخصصین هشدار دادند که موارد بیشتری از جمله هک اثرانگشت‌خوان‌ها، پیش رو هستند [19].

در گفتگویی با استیون گراسمن، از معاونین یک شرکت تحلیل امنیت سایبری، موضوع باج‌افزارها مطرح شد. وی در این‌باره گفت که هرگز به کسی پیشنهاد نکرده‌است باج بپردازد، اما زمانی‌که شخصی در حال از دست دادن اطلاعات مالی و یا عکس‌های خانوادگی بوده و نسخه‌ی پشتیبانی نیز از آنها در اختیار نداشته‌باشد، شاید پرداخت باج برای این افراد، گزینه‌ی مناسبی به‌حساب آید [19]!



یک محقق از مدرسه‌ی مهندسی تندن دانشگاه نیویورک نشان می‌دهد که کدام اثرانگشت‌ها می‌توانند همسان شوند. محققین مدرسه‌ی مهندسی تندن دانشگاه نیویورک، MasterPrintها را کشف کردند: اثر انگشت‌هایی که به‌صورت دیجیتال دستکاری شده‌اند و می‌توانند با انگشت‌های افراد بسیاری تطابق یابند. پروفسور نصیر ممون از مدرسه‌ی تندون دانشگاه نیویورک گفت: "اگر من این دستکش یا دست مصنوعی را، که MasterPrint بر آن قرار دارد، داشته‌باشم، قادر به بازگشایی قفل 25 الی 40 درصد گوشی‌ها خواهم بود



".[19]

وی در ادامه‌ی سخنان خود، به طرز کار MasterPrint اشاره کرد: "با وجود یکتا بودن اثر انگشت، محققین بر این باورند که اکثر گوشی‌های هوشمند، تنها از جزئی از اثر انگشت استفاده می‌کنند و همین امر، موجب سادگی امر گمراه کردن سنسورها می‌شود. زمانی‌که تنها از جزئی از اثر انگشت استفاده شود، خاصیت یکتایی و منحصر به‌فرد بودن آن کاهش می‌یابد و یا از دست می‌رود، اما چیزی که به حادتر شدن این مشکل می‌افزاید، ذخیره‌ی چندین اثر انگشت توسط گوشی‌های هوشمند است [19, 20]."

محققین، برای اثبات این ادعا باید آزمایشاتی روی گوشی واقعی انجام دهند، اما فعلاً از شبیه‌سازی

کامپیوتری استفاده کرده‌اند [19].

طبق گفته‌ی محققین مدرسه‌ی مهندسی تندن دانشگاه نیویورک، چهار مورد اثر انگشت نشان‌داده‌شده در تصویر فوق، با تعداد زیادی از اثر انگشت‌ها تطابق خواهند داشت، اما نظر متخصصین سایت امنیتی شرکت اپل، متفاوت است. بنا به‌نظر آنها، به‌دلیل منحصر به‌فرد بودن اثر انگشت‌ها، این‌که بخش کوچکی از دو اثر انگشت مجزا، آنقدر شبیه به هم باشد که بتوان میان آنها تطابقی درنظر گرفت، بسیار نادر است. احتمال

وقوع این رخداد، یک در پنجاه هزار برای هر انگشت ثبت شده‌است، که این احتمال، بسیار بهتر از شانس حدس زدن یک کلمه‌ی عبور چهار رقمی (معادل با یک در ده هزار) است [19, 20].

به گفته‌ی راهنمای آنلاین شرکت گوگل، جدیدترین نرم‌افزار سنسور اثر انگشت، باید نرخ پذیرش کاذبی کمتر از دو هزارم داشته‌باشد [19].

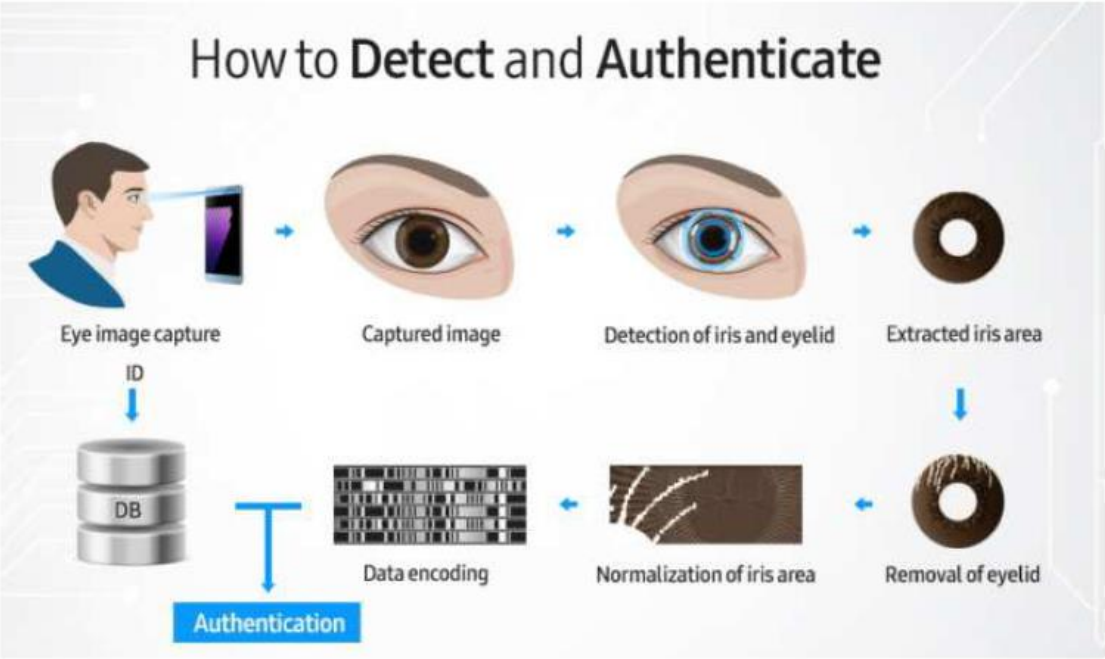
نکته‌ی جالب توجه اینجاست که پروفسور ممون، با وجود تحقیقات صورت‌گرفته، هنوز از اثر انگشت روی گوشی خود استفاده می‌کند، زیرا از نظر وی، مانند اکثر مردم، استفاده از اثر انگشت بسیار راحت است. اما توصیه وی این است که به هنگام انجام عملیاتی حساس، مانند کارهای بانکی، از عواملی ایمن‌تر استفاده کنید [19].

این توازن میان امنیت و راحتی کار را می‌توان در سخنی از گراسمن خلاصه کرد: "موضوع اصلی، برقراری تعادل میان راحتی و امنیت است. این‌که روی درب منزل خود می‌خواهید چه تعداد قفل نصب کنید، در مقابل این‌که هنگام ورود به منزل می‌خواهید چه میزان راحت باشید [19]!"

با توجه به اهمیت اثر انگشت و رایج‌تر بودن آن نسبت به سایر سیستم‌های بیومتریک، عمده تمرکز نمونه‌های شهودی بر اتفاقات و رخنه‌های امنیتی متوجه اثر انگشت ذکر شدند. اما در موردی دیگر، اشاره‌ای به آسیب‌پذیری بیومتریک عنبیه چشم خواهیم داشت.

شرکت سامسونگ از فناوری تشخیص عنبیه در گوشی گلکسی S8 رونمایی کرد و آن را یک سیستم امنیتی نفوذناپذیر خطاب نمود. این شرکت، مدعی شده که این سیستم احراز هویت به قدری قدرتمند است که نمی‌توان آن را رمزگشایی کرد [21].

نحوه‌ی کار این سیستم در شکل زیر نشان داده شده‌است. در مرحله‌ی اول، مقادیر اندازه‌ی چشم کاربر پردازش شده، سپس رنگ عنبیه بررسی می‌شود. در مرحله‌ی آخر، میزان انحنای چشم کاربر توسط دستگاه بررسی و ثبت می‌شود. پس به‌نظر می‌رسد تنها راه رمزگشایی آن، در اختیار داشتن چشم کاربر است [21]!



اما محققین شرکتی به نام Chaos Computer Club، با شیوه‌ای بسیار هوشمندانه و با صرف هزینه‌ی اندکی توانستند ادعای شرکت سامسونگ را نقض کنند. آنها در ابتدا به کمک یک دوربین سونی، عکسی با

وضوح بالا از چهره‌ی فرد گرفتند [21].

سپس، با استفاده از یک دستگاه چاپگر لیزری سامسونگ، ناحیه‌ی چشم شخص را چاپ کردند، اما از آنجاکه تصویر دو بعدی، قابلیت نمایش انحنای چشم کاربر را ندارد، هکرها با استفاده از یک لنز طبی توانستند تصویر چشم را حقیقی نشان داده و انحنایی در آن ایجاد کنند و این سیستم بیومتریک را فریب دهند [21].

6 متدهای نوین احراز هویت

امروزه، احراز هویت چندعاملی، یکی از مضامین موردتوجه در صنعت امنیت سایبری است. احراز هویت چندعاملی (به اختصار MFA) یک پروتکل امنیتی است که برای عملیات ورود یا عملیات دیگر، به بیش از یک عامل منحصر به‌فرد از طرف کاربر نیاز دارد. معمولاً این عوامل، سه عدد هستند: یک رمز عبور ایجادشده توسط خود کاربر؛ اطلاعاتی از دستگاه کاربر؛ و شناسه‌های بیومتریک وی [22].

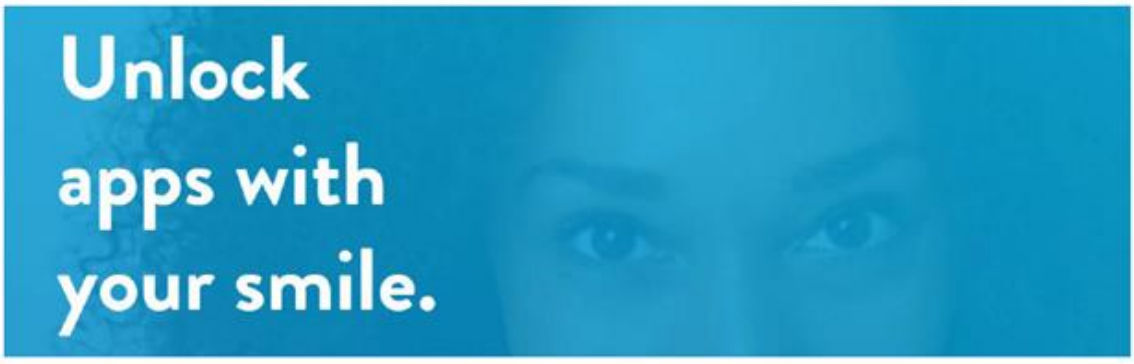
شرکت‌های فناوری، بر انواع جدیدی از بیومتریک‌ها کار می‌کنند که نمونه‌هایی از آنها، در ادامه خواهد آمد [22]:

- شرکت سوناویشین، در حال توسعه‌ی یک فناوری خواندن اثر انگشت با استفاده از سنسورهای فراصوتی است. تمرکز این شرکت روی ایمن‌سازی فعالیت‌ها و تراکنش‌های مالی افراد است [22].

- شرکت سوکیور، با برنامه‌ی بیومتریک اجتماعی، کاربران جعلی و کلاهبردار را با استفاده از الگوریتم‌های یادگیری ماشین، در وب‌سایت‌ها و برنامه‌های گوشی، تشخیص می‌دهد [22].

- شرکت بیبوکچ، بیش از 400 پارامتر بیومتریک رفتاری و فیزیولوژیکی را با هدف ایجاد یک شناسه‌ی یکتا برای کاربر، جمع‌آوری و تحلیل می‌کند [22].

- شرکت سمایل آیدنتیتی، اسناد شناسه را به یک سلفی از کاربر پیوند می‌دهد تا یک تصویر



بیومتریک برای احراز هویت کاربر در هر دستگاه اندرویدی ایجاد نماید [22].

در کنگره‌ی جهانی موبایل (به اختصار MWC) سال 2017 در بارسلونا، توسعه‌دهندگان بسیاری، دستگاه‌ها و سنسورهای هوشمندی ارائه دادند که بسیار ایمن‌تر از سطح انتظار و تصور ما بود. بنا به گفته‌ی شرکت نروژی آیدکس، که سنسورهای اثر انگشت را برای شرکت ال.جی و سایر شرکت‌ها تامین می‌کند، امنیت سنسورهای اثر انگشت به میزان قابل توجهی، بهبود یافته‌است. در ابتدا، اطلاعات خام گرفته‌شده از اسکنر اثر انگشت، رمزنگاری می‌شود، که این عمل موجب رفع آسیب‌پذیری اسکنرهای پیشین می‌گردد و داده‌ی خام برای استفاده مجدد به سرقت می‌رود. سپس، لبه‌های تصویر، تشخیص داده‌شده و رمزنگاری می‌شوند و تمامی این اطلاعات، به حافظه‌ی امن منتقل می‌گردند. همه‌ی عملیات مذکور، در یک محیط قابل اطمینان و ایزوله، که از طرف فرآیندهای دیگر غیرقابل دسترسی است، صورت می‌گیرند [23].

یک شرکت سازنده‌ی بیومتریک با نام کروشال تک، سنسورهای ضربان قلب را به سنسور اثر انگشت اضافه نموده‌است. با این‌کار، کپی‌های سه بعدی از اثر انگشت، انگشت‌های پلاستیکی و حتی انگشت‌های واقعی بریده‌شده، نمی‌توانند از قفل گشایی بیومتریک عبور کنند [23].

تعبیه‌ی اسکنرهای عنبیه‌ی چشم در دستگاه‌های خودپرداز بانکی نیز، می‌تواند نیاز به رمز عبور را از میان بردارد. می‌توانید قدم بردارید و جلوی دستگاه بایستید تا در عرض چند ثانیه، عنبیه‌ی چشم شما اسکن شود و تراکنش مالی خود را انجام دهید. شرکت سی‌تی‌گروپ، اخیراً نمونه‌ای از این دستگاه را با نوعی فناوری که توسط عکس یا ویدیو گمراه نمی‌شود، آزمایش کرده‌است [23].

هر روزه، مرزهای امنیت سایبری و محدوده‌ی آن، جابه‌جا می‌شود. هر دستگاه جدید متصل به شبکه، هدف جدیدی برای نفوذگران است، که باید ایمن شود.

7 مراجع

[1]. E. Emmanuel, Nwabueze, D. Edebatu, N. C. A. Ngozi, "Vulnerability of Biometric Authentication System," International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue 3, Mar 2016.

[2]. "Biometric security systems: a guide to devices, fingerprint scanners and facial recognition access control," https://www.ifsecglobal.com/biometric-security-systems-guide-devices-fingerprint-scanners-facial-recognition/, 2017.

[3]. V. Arulalan, G. Balamurugan, V. Premanand, "A Survey on Biometric Recognition Techniques," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 2, Feb 2014.

[4]. M. Blalock: "Banking Cybersecurity: New Trends in Biometric Security," https://itpeernetwork.intel.com/banking-cybersecurity-new-trends-in-biometric-security/, Mar 2017.

[5]. T. P. Keenan, "Hidden Risks of Biometric Identifiers and How to Avoid Them," Black Hat, 2015.

[6]. BioCatch, "Is 2017 the year for Behavioral Biometrics," http://www.biocatch.com/blog/is-2017-the-year-for-behavioral-biometric, Feb 2017.

[7]. J. Ashbourn, "Vulnerability with Regard to Biometric Systems," http://www.eetimes.com/document.asp?doc_id=1255101, 2002.

[8]. M. Goodman, "You Can't Replace Your Fingerprints," http://www.slate.com/articles/technology/future_tense/2015/02/future_crimes_excerpt_how_hackers_can_steal_fingerprints_and_more.html, 2015.

[9]. R. Capps, "A cyber attack on biometric data could pose significant risks at border- expert comment," https://www.globalsecuritymag.com/A-cyber-attack-on-biometric-data,20160916,65293.html, Sept 2016.
[10]. R. Brandom, "Your phone's biggest vulnerability is your fingerprint," https://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security, May 2016.
[11]. A. Peterson, "OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought," https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/, Sep 2015.
[12]. "Samsung and Huawei fingerprint scanners can be fooled using an inkjet printer," https://www.theguardian.com/technology/2016/mar/08/samsung-and-huawei-fingerprint-scannerscan-be-fooled-using-an-inkjet-printer, Feb 2017.
[13]. J. Schlesinger, "New hacking threats: Fingerprint reader vulnerabilities and sophisticated ransomware,"https://www.google.com/#q=New+hacking+threats:+Fingerprint+reader+vulnerabilities+and+sophisticated+ransomware, May 2017.
[14]. J. Eng, "OPM Hack: Government Finally Starts Notifying 21.5 Million Victims," http://www.nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126, Oct 2015.
[15]. B. I. Koerner: "Inside the Cyberattack That Shocked the US Government," https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/, Oct 2016.
[16]. M. Goodman, "You Can't Replace Your Fingerprints," http://www.slate.com/articles/technology/future_tense/2015/02/future_crimes_excerpt_how_hackers_can_steal_fingerprints_and_more.html, 2015.
[17]. M. Towler, "OPM Cyber Attack Shows Systemic Issues in Government IT," https://blog.ipswitch.com/opm-cyber-attack-proves-systemic-issues-in-government-it, Oct 2016.
[18]. "Fingerprints are not fit for secure device unlocking," https://srlabs.de/bites/spoofing-fingerprints/.
[19]. A. Stevenson, "Hackers can remotely steal your identity using Android fingerprint scanners," http://www.businessinsider.com/android-phones-fingerprint-scanners-have-serious-securityvulnerabilities-2015-8, Aug 2015.
[20]. A. Roy, N. Memon, A. Ross, "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems," IEEE Transactions on Information Forensics and Security, 2017.
[21]. "Yes, Samsung Galaxy S8's iris scanner can be hacked – here's how," http://www.techradar.com/news/samsung-galaxy-s8-iris-scanner-hack, May 2017.
[22]. M. Goodman, "You Can't Replace Your Fingerprints," http://www.slate.com/articles/technology/future_tense/2015/02/future_crimes_excerpt_how_hackers_can_steal_fingerprints_and_more.html, 2015.

[23]. 9 Early-Stage Multi-Factor Authentication Cybersecurity Startups To Watch; https://www.cbinsights.com/research/biometric-cybersecurity-companies-to-watch/, Feb 2017.