مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۱، بهار ۱۳۹۶، ص ۱۸-۹

یک طرح تعمیم‌یافته برای استخراج کلید بیومتریک از الگوی تایپ

امیر بیدختی[1*]، سیدمرتضی پورنقی[2]، امیرحسین خلیلی تیرانداز[3]

۱- دانشجوی دکتری، دانشگاه صنعتی شریف، ۲- دانشجوی دکتری، دانشگاه قم، ۳- دانشجوی دکتری، دانشگاه علم و صنعت ایران
(دریافت: ۹۴/۱۱/۱۲، پذیرش: ۹۵/۰۸/۱۰)

چکیده

در این مقاله، یک طرح تعمیم‌یافته برای استخراج کلید بیومتریک از روی نمونه‌های الگوی تایپ کاربر (بیومتریک رفتاری) پیشنهاد شده و امنیت آن نشان داده می‌شود. در طرح پیشنهادی، ابتدا ویژگی‌های مناسبی از الگوی تایپ کاربر استخراج می‌شود. سپس به کمک یک طرح تسهیم راز مناسب، بسته به میزان یکتا بودن هر ویژگی تعدادی سهم مجاز برای بازسازی کلید مخفی به آن تخصیص داده می‌شود. این سهم‌ها در میان اعداد تصادفی پنهان می‌شوند. در صورت نیاز به احراز اصالت، پس از این که کاربر کلمه عبور خود را وارد کرد، مجدداً ویژگی‌های الگوی تایپ استخراج شده و در صورت صحت هر ویژگی، یک سهم درست به دست خواهد آمد. اگر این تعداد از حدی که در طرح تسهیم راز مقاوم مشخص شده است، بیشتر باشد بازسازی کلید مخفی امکان خواهد داشت. طرح دارای دو پارامتر است که بر خلاف طرح‌های پیشین به آن قابلیت تنظیم رابطه خطای رد نادرست و خطای پذیرش نادرست را می‌دهد. طرح پیشنهادی قادر است ۲۵ الی ۵۰ بیت کلید را بسته به نوع صفحه‌کلید (صفحه‌کلیدهای سنتی یا صفحه‌کلیدهای لمسی) با نرخ EER[1]=۰,۰۴ استخراج نماید. نشان می‌دهیم که استفاده از این طرح به عنوان عامل تکمیلی در کنار کلمه عبور، امنیت طرح مبنا را ۲ تا ۳ برابر افزایش می‌دهد. این طرح در کنترل دسترسی، حفاظت از دستگاه‌های حساس و ... قابل استفاده است.

واژه‌های کلیدی: رمزنگاری بیومتریک، الگوی تایپ، مدیریت کلید، آنتروپی، تسهیم راز

۱- مقدمه

تقریباً در تمام سامانه‌های رمزنگاری امروزی امنیت نهایی مبتنی بر کلید مخفی است. از همین رو مدیریت کلید یکی از مهم‌ترین بخش‌های یک سامانه امنیتی به حساب می‌آید. ضعف در مدیریت کلید یک سامانه امنیتی، می‌تواند تمام نقاط قوت الگوریتم‌ها و پروتکل‌های به‌کار رفته در طراحی سامانه را بی‌فایده سازد. یکی از مهم‌ترین بخش‌های مدیریت کلید، تولید تصادفی و توزیع آن در میان کاربران سامانه است. به طور سنتی این کلید در قالب یک کلمه عبور کاربر که کلید رمزنگاری از روی آن قابل بازتولید است، یا یک تراشه حاوی کلید تصادفی در اختیار کاربران قرار داده می‌شود. در رویکرد اول، انتخاب کلمات عبور ساده و یا امکان فراموش کردن آن از اهمیت سامانه می‌کاهد. در بخش ۴ بیشتر به این موضوع خواهیم پرداخت. در رویکرد دوم نیز، امنیت نهایی، منوط به حفاظت فیزیکی از تراشه خواهد بود. علاوه بر مسائل مربوط به امنیت، در بسیاری از کاربردهای عملی مسئله حریم خصوصی مطرح می‌شود. این نگرانی‌ها به ویژه بر اثر گسترش استفاده از بیومتریک‌ها در سامانه‌های مختلف به وجود آمده است. به عنوان مثال اگر اطلاعات بیومتریک در یکی از این سامانه‌ها افشا شود، امکان حملات تکرار[2] و جعل هویت[3] به سامانه‌های دیگر وجود خواهد داشت.

رمزنگاری بیومتریک به رفع این اشکالات کمک می‌کند. در این حالت کلید مخفی در هر بار استفاده از سیستم به طور یکتا از روی بیومتریک‌های کاربر ایجاد می‌شود و لذا نیازی به حفظ کردن آن وجود ندارد. همچنین چون در مکانی ذخیره نمی‌شود، نگرانی‌ها در خصوص حریم خصوصی و نیز احتمال دستبرد نیز منتفی می‌شود.

در مقاله حاضر یک طرح رمزنگاری بیومتریک به کمک الگوی تایپ کاربر پیشنهاد می‌گردد. این طرح در حقیقت تعمیم یک طرح ساده است که قبلاً از سوی مونروز[4] و همکاران [۱] پیشنهاد شده است. به کمک چند ایده ابتکاری، تعمیمی از این

* رایانامه نویسنده مسئول: amirbidokhti@yahoo.com

1 -Equal Error Rate

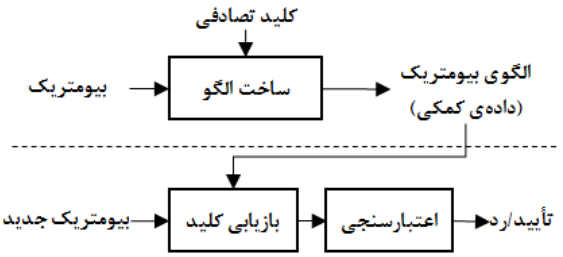
2 -Replay Attack
3 -Spoofing Attack
4 -Monrose

طرح به دست می‌دهیم که قادر است بیت‌های تصادفی بیشتری (آنتروپی بیشتری) از الگوی تایپ استخراج کند. نشان داده شد که با استفاده از طرح پیشنهادی امنیت سامانه‌های مبتنی بر کلمه عبور دو تا سه برابر افزایش خواهد یافت. مزیت طرح حاضر بر طرح [۱] قابلیت انعطاف آن در تعیین خطای نوع اول (پذیرش نادرست) و نوع دوم (رد نادرست) است. این قابلیت، طرح پیشنهادی را برای موقعیت‌های عملیاتی متفاوتی مناسب می‌سازد.

بخش ۲، رویکردهای عمده در زمینه رمزنگاری بیومتریک را مرور می‌کند. در بخش ۳ کلیات طرح پیشنهادی ارائه خواهد شد و در بخش‌های ۴ و ۵، جنبه‌های امنیتی و عملیاتی تحلیل می‌شود. این مقاله را با نتیجه‌گیری در بخش ۶ به پایان می‌رسد.

۲- کارهای مرتبط

در حالت کلی طرح‌های رمزنگاری بیومتریک [۲] به دو دسته‌ی طرح‌های تولید کلید[1] و طرح‌های ترکیب کلید[2] تقسیم می‌شوند. این دو دسته در [۲] به طور مفصل بررسی شده‌اند. در دسته اول از روی نمونه بیومتریک کاربر یک کلید تولید می‌شود که تا حدودی خواص شبه‌تصادفی دارد و برای رمزنگاری یا سایر مصارف به کار می‌رود. اما در دسته دوم یک کلید کاملاً تصادفی تولید شده و به نحوی با بیومتریک کاربر ترکیب شده و الگوی بیومتریک (یا داده کمکی[3]) را می‌سازد. این الگوی بیومتریک هیچ اطلاعاتی در مورد بیومتریک یا کلید مخفی فاش نمی‌سازد، اما کاربر با در اختیار داشتن آن و ارائه یک نمونه بیومتریک صحیح قادر است کلید مخفی را بازسازی کند. طرح ارائه شده در مقاله حاضر نیز از دسته دوم است. طرح‌های دسته دوم (ترکیب کلید) از دو الگوریتم تولید الگوی بیومتریک و بازسازی کلید تشکیل می‌شوند. در شکل (۱) نمودار این دو الگوریتم آمده است.



شکل (۱). شمای کلی یک طرح بیومتریک. شامل دو الگوریتم ساخت الگو و بازیابی کلید

محققان تلاش کرده‌اند تا ایده رمزنگاری بیومتریک را به کمک بیومتریک‌های مختلف تحقق بخشند. در [۳] یک طرح مبتنی بر صدای کاربر پیشنهاد شده است که در شرایط کم نویز، قادر است کلیدی به طول حدود ۴۶ بیت را به نمونه صدای مرتبط سازد. خطای رد نادرست آن نیز در حد ۲۰٪ گزارش شده‌است. طرح ارائه شده در [۴] نیز طرحی مبتنی بر اثر انگشت کاربر پیشنهاد شده است. این طرح که بایوسکریپت[4] نام دارد، از طریق استخراج مولفه فاز و کدگذاری اکثریت[5]، کلید تصادفی را تولید می‌کند. بدین ترتیب این طرح در دسته نخست طرح‌های رمزنگاری بیومتریک قرار می‌گیرد.

در [۵] یک طرح مبتنی بر چهره افراد پیشنهاد شده است. این طرح قادر است تا ۸۰ بیت را با بیومتریک چهره، ترکیب کند و خطای رد نادرست آن کمتر از ۱٪ گزارش شده است. اساس این طرح تجزیه تصویر به مولفه‌های بنیادی (تجزیه PCA) و سپس اعمال کدینگ اکثریت است.

در [۶] طرحی مبتنی بر تصویر عنبیه چشم ارائه شده است. در این طرح با اعمال فیلترهای گابور در سطوح مختلف و جهت‌گیری‌های مختلف، تصویر عنبیه به یک رشته بیت ۲۵۶ تایی تبدیل می‌شود. این رشته بیت IrisCode نامیده می‌شود و به تغییرات رایج در اندازه‌گیری تصویر عنبیه مقاوم است. سپس کلید تصادفی به طول ۱۴۰ بیت تولید شده و با اعمال کدگذاری هادامارد و سپس Reed-Solomon طول آن به ۲۵۶ بیت می‌رسد. ترکیب کلید کدشده و IrisCode، الگوی بیومتریک را تشکیل می‌دهد.

استفاده از بیومتریک‌های اشاره‌شده تاکنون، معمولاً در عمل با موانعی مواجه است. ذخیره این بیومتریک‌ها معمولاً به حسگرهای خاص احتیاج دارد. این امر از یک سو هزینه بر است و از سوی دیگر در برخی کاربردها قابل اجرا نیست. همچنین در برخی موارد از قبیل سنسور عنبیه چشم، ادعاهایی مبنی بر مضر بودن آن برای سلامت افراد وجود دارد. اشکال دیگر این بیومتریک‌ها مقاومت برخی کاربران در برابر استفاده از این سامانه‌ها به علت نگرانی‌های حریم خصوصی است. بیومتریک الگوی تایپ که در طرح پیشنهادی این مقاله مورد استفاده قرار گرفته است، اشکالات قبلی را ندارد. در زیربخش بعدی به برخی کارهای در حیطه الگوی تایپ اشاره می‌کنیم.

۲-۱- الگوی تایپ به عنوان بیومتریک

الگوی تایپ کاربران به عنوان یک بیومتریک رفتاری مطرح است. نخستین استفاده‌ها از این بیومتریک به سال‌های جنگ دوم جهانی برمی‌گردد [۷]؛ جایی که از نحوه تایپ کدهای نقطه و خط به هویت فرستنده تلگراف پی برده می‌شد. این تکنولوژی

1 -Key Generation
2 -Key Binding
3 -Helper data
4 -Bioscrypt
5 -Majority Coding

بعدها الهام بخش یک پروژه تحقیقاتی در موسسه RAND شد. نتایج این پروژه بنیان‌های آماری روش مورد استفاده برای تشخیص فرستنده تلگراف را مورد تأیید قرار داد و پیشنهاد استفاده از آن به عنوان یک فناوری امنیتی را مطرح کرد [۸]. در سال‌های بعد ایده استفاده از الگوی تایپ برای تعیین هویت کاربران به صورت جدی مورد بررسی قرار گرفت [۱۳-۹]. از آن‌جا که مقاله حاضر به طور خاص به تایید هویت از طریق الگوی تایپ اختصاص ندارد، به جزئیات روش‌های فوق نمی‌پردازیم.

با ارائه شدن مفهوم رمزنگاری بیومتریک، یکی از بیومتریک‌هایی که مورد توجه محققین قرار گرفت، الگوی تایپ بود. Monrose و همکاران [۱] طرحی موسوم به «کلمه عبور تقویت‌شده[1]» ارائه دادند که از نحوه تایپ کاربر برای استخراج کلید استفاده می‌کرد. در این طرح، ویژگی‌های استخراج‌شده از الگوی تایپ، به دو دسته تمایزپذیر و غیرتمایزپذیر تقسیم می‌شوند. دسته اول، ویژگی‌هایی هستند که با احتمال بالایی همواره کمتر یا بیشتر از یک آستانه مشخص قرار می‌گیرند (این آستانه از پارامترهای طرح است). بر این اساس یک جدول با دو ستون و به تعداد ویژگی‌ها سطر، تشکیل می‌شود که هر سطر مربوط به یک ویژگی می‌باشد. برای ویژگی‌های تمایز بخش، بسته به این که مقادیر بالا یا پایین آستانه را اختیار کرده باشد، سهم درست در یکی از خانه‌ها و عددی تصادفی در خانه دیگر قرار می‌گیرد. برای سایر ویژگی‌های نیز در هر دو خانه سهم درست قرار می‌گیرد. در مرحله احراز اصالت، مقدار ویژگی اندازه‌گیری می‌شود و بسته به این که بالاتر یا پایین تر از آستانه باشد، از هر سطر یک سهم انتخاب می‌شود. به کمک این سهم‌ها و یک طرح تسهیم راز، سعی می‌شود کلید مخفی بازیابی شود. برای محافظت از الگوی بیومتریک، این جدول به کمک کلمه عبور رمزگذاری می‌شود.

از آنچه گفته شد، مشخص است که طول کلید ساخته‌شده به اندازه ویژگی‌های تمایز بخش خواهد بود. این طول به طور نوعی حدود ۸ تا ۱۰ بیت می‌باشد. همچنین خطای رد نادرست این طرح نزدیک به ۴۸٪ گزارش شده است که مقدار بالایی است.

این طرح یک ایراد عمده دارد و آن عدم انعطاف است. زیرا حتی اگر یک سهم اشتباه یافت شود، کلید مخفی قابل دست‌یابی نیست. در طرح پیشنهادی به کمک طرح‌های تسهیم راز خاص این ایراد را برطرف خواهیم کرد. همچنین طول کلید استخراج‌شده وابستگی زیادی به پارامتر آستانه دارد. در طرح پیشنهادی ما، با انتخاب صحیح آستانه برای هر الگوی تایپ و ذخیره‌کردن آن در الگوی بیومتریک، این مشکل نیز رفع شده است. علاوه بر این با مدل کردن بهتر تابع توزیع احتمال ویژگی‌ها، توانسته‌ایم آنتروپی بیشتری از آن استخراج نموده و در نتیجه طول کلید را ۲ تا ۳ برابر افزایش دهیم. در بخش پیش‌رو جزئیات طرح پیشنهادی مطرح شده است.

۳- طرح پیشنهادی

در این بخش جزئیات طرح پیشنهادی را شرح می‌دهیم. توجه داریم که هر چند توضیحات ارائه‌شده در این مقاله بیشتر بر کاربرد کنترل دسترسی متکی است، اما تعمیم آن به کاربردهای دیگر از قبیل رمزگذاری فایل‌ها نیز سرراست است. در این طرح آنتروپی کلید از دو منبع تأمین می‌شود؛ منبع اول همان کلمه عبور سنتی و منبع دوم اطلاعات مربوط به نحوه تایپ این کلمه عبور است.

این طرح، به عنوان یک طرح رمزنگاری بیومتریک، شامل دو مرحله ثبت‌نام و احراز اصالت است. در مرحله ثبت‌نام، کاربر کلمه‌ی عبور خود را انتخاب کرده و آن را در یک جلسه یا جلسات متفاوت چندین بار وارد می‌کند. از روی اطلاعات جمع‌آوری‌شده در این مرحله، یک الگوی[2] بیومتریک برای کاربر ایجاد می‌شود. با توجه به نگرانی‌های مربوط به امنیت و حریم شخصی افراد که در بخش ۱ به آن اشاره کردیم، این الگو به نحوی ساخته می‌شود که اطلاعاتی در مورد بیومتریک مدنظر (در اینجا نحوه تایپ)، افشا نکند.

سپس در مرحله احراز اصالت، کاربر کلمه عبور خود را وارد می‌کند. سامانه از طریق ترکیب عبارت کلمه عبور و اطلاعات مربوط به نحوه تایپ آن، اجازه دسترسی به سامانه را می‌دهد و یا مانع آن می‌شود. شمای کلی طرح پیشنهادی در شکل (۲) آمده است. در زیربخش‌های آینده جنبه‌های مختلف این طرح را بیشتر توضیح می‌دهیم.

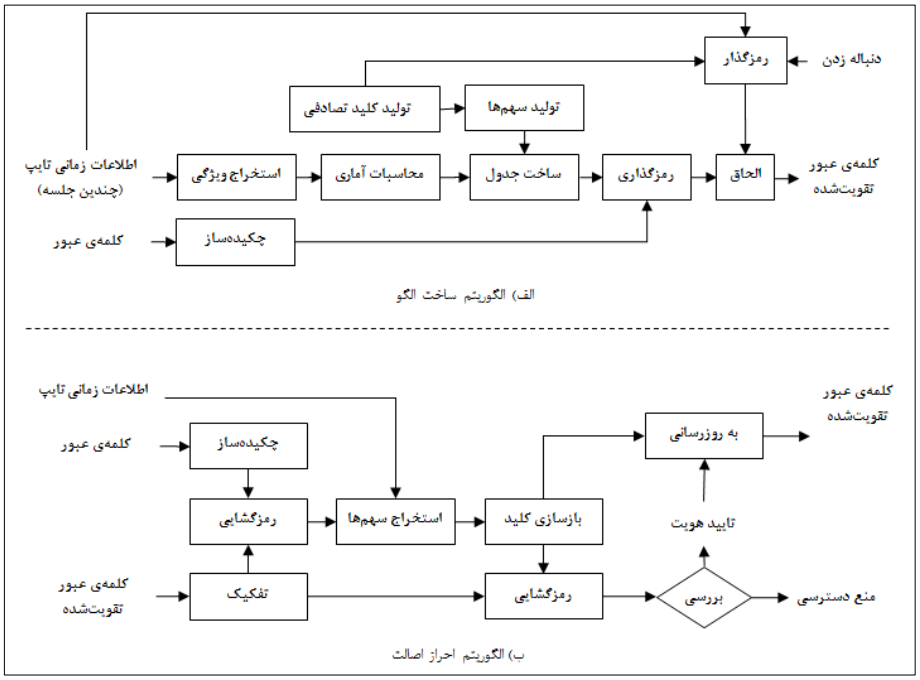
۳-۱- استخراج ویژگی

هر چند طرح پیشنهادی بر اساس انواع ویژگی‌های قابل استخراج از نحوه تایپ قابل پیاده‌سازی است، اما در مقاله حاضر از دو دسته ویژگی استفاده کرده‌ایم. این ویژگی‌های تقریباً به کمک تمام صفحه‌کلیدهای رایج قابل استخراج هستند.

الف) زمان نگه‌داشت کلید: برای هر یک از کلیدهایی که در حین تایپ کلمه عبور فشرده می‌شود، زمان بین فشردن و رها کردن آن کلید به عنوان یک ویژگی در نظر گرفته می‌شود. اگر کلمه عبور دارای N حرف باشد، N ویژگی از این جنس قابل استخراج است.

1 -Hardened Password

2 -Template



شکل (۲). شمای کلی الگوریتم‌های ساخت الگو و احراز اصالت در طرح پیشنهادی

ب) تاخیر بین فشردن دو کلید متوالی: زمان بین فشردن هر کلید تا فشردن کلید بعدی، به عنوان یک ویژگی در نظر گرفته می‌شود. اگر کلمه عبور دارای N حرف باشد، $N-1$ ویژگی از این جنس قابل استخراج است.

با این حساب، طول بردار ویژگی استخراج‌شده برابر است با: $L=2N-1$ که هر یک از این ویژگی‌ها یک عدد بر حسب میلی‌ثانیه خواهد بود. در [۱۴] اعلام شده است که دقت سیستم‌عامل ویندوز برای تفکیک رویدادهای مربوط به صفحه کلید، ۱۵٫۶۲۵ ms است (۶۴ بار در ثانیه). آزمایش‌های انجام شده در حین پژوهش جاری نیز این مطلب را تایید می‌کند.

در صورت استفاده از بردارهای ویژگی بزرگ‌تر، طرح پیشنهادی به سادگی قابل تعمیم است. به عنوان مثال، در تلفن‌های همراه هوشمند که از صفحه کلید لمسی استفاده می‌کنند، اغلب ویژگی‌هایی از قبیل میزان فشار دست بر صفحه، سطح تماس انگشت با صفحه، مختصات دقیق تماس نیز قابل اندازه‌گیری است. در بخش ۲-۴ به برخی نکات در خصوص این تعمیم و اثرات آن بر مشخصات امنیتی طرح پیشنهادی اشاره شده است.

۳-۲- ساخت الگو

برای ساخت الگوی بیومتریکِ کاربر، ابتدا از او می‌خواهیم h بار کلمه عبور خود را وارد کند. h یکی از پارامترهای طرح است و در ساخت الگوی بیومتریک کاربر، تنها آخرین h ورود موفق او دخالت دارد. اطلاعات این ورودهای موفق در یک ماتریس تاریخچه $H: L \times h$ ذخیره می‌شود. هر ستون این ماتریس بردار ویژگی مربوط به یک ورود موفق را در خود دارد. پس از h بار ورود کلمه عبور و تکمیل ماتریس تاریخچه، محدوده تغییرات هر دسته ویژگی محاسبه می‌شود. در طرح حاضر دو دسته ویژگی داریم، لذا:

$$[LL_i \quad UL_i] = \left[\min\{\text{ویژگی‌های دسته‌ی نام}\ i\} \quad \max\{\text{ویژگی‌های دسته‌ی نام}\ i\}\right] \qquad (۱)$$
$$i = 1,2$$

سپس با تقسیم این بازه به K قسمت، $K-1$ عدد به عنوان مرز مقادیر این بازه‌ها (برای هر دسته ویژگی) به دست می‌آوریم، این مرزها عبارتند از:

$$L_{i,j} = j\frac{ul_j - LL_i}{K} \quad i = 1.2 \quad j = 1. \ldots . K-1 \qquad (۲)$$

علت محاسبه مقادیر مرزی و دامنه تغییرات برای هر دسته ویژگی به صورت مجزا، این است که دامنه تغییرات این دسته‌ها تفاوت قابل توجهی با یکدیگر دارد. توضیح بیشتر در این خصوص در قسمت تحلیل‌های امنیتی آمده است.

سپس برای هر ویژگی منفرد، میانه مقادیر آن را به‌دست آورده و به کمک آن، انحراف معیار نیمه بالا و پایین داده‌ها را برای آن محاسبه می‌کنیم:

$m_j =$ میانه مقادیر ویژگی نام j

$\sigma_j =$ انحراف معیار تمام مقادیر ویژگی نام j

$\sigma_{j.L} =$ انحراف مقادیر کوچکتر از میانه ویژگی نام j

$\sigma_{j.H} =$ انحراف مقادیر بزرگتر از میانه ویژگی نام j

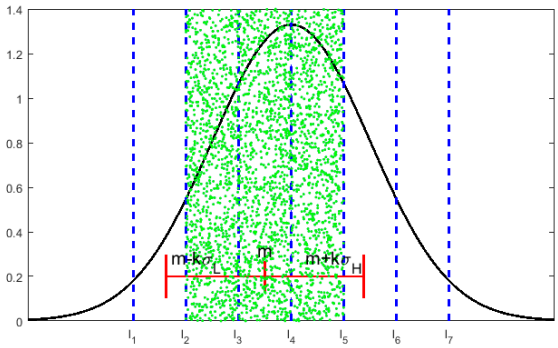
در مرحله بعد، جدول $S: L \times K$ را به صورتی که در ادامه می‌آید می‌سازیم. این جدول بخش اصلی الگوی بیومتریک را تشکیل می‌دهد. هر سطر این جدول مربوط به یک ویژگی

جداگانه، و هر خانه آن سطر، مربوط به یکی از K بازه آن ویژگی است و در آن یک عدد قرار می‌گیرد. بعضی از این اعداد سهم‌های صحیح برای ساختن کلید مخفی هستند و سایر اعداد، به صورت تصادفی انتخاب می‌شوند. برای این که خانه‌های دارای سهم‌های مجاز مشخص شود، ابتدا بازه زیر را برای ویژگی jام به دست می‌آوریم (در اینجا k یک پارامتر طرح است):

$$[m_j - k\sigma_{j.L} \quad m_j + k\sigma_{j.H}] \qquad (۳)$$

سپس بررسی می‌کنیم که کدام یک از سطوح مشخص شده برای این دسته ویژگی، در این بازه می‌گنجند. به شکل (۳) نگاه کنید. در این شکل، برای یک متغیر خاص کل دامنه‌ی تغییرات به هشت ناحیه تقسیم شده‌است (خطوط آبی خط‌چین). میانه مقادیر ویژگی و همچنین بازه مجاز برای متغیر در شکل نشان داده شده است (خطوط قرمز). بر این اساس سه ناحیه از کل هشت ناحیه که در این بازه واقع هستند، مجاز شمرده می‌شوند. در خانه‌های متناظر این بازه‌ها، در سطر jام جدول S سهم‌های درست قرار می‌دهیم.

حال جدول S و مقادیر مرزی برای هر دسته ویژگی را به کمک چکیده کلمه عبور و جدول H را به کمک کلید تصادفی مخفی رمز می‌نماییم. برای این‌که در فرآیند احراز اصالت بتوانیم از صحت یا عدم صحبت کلید بازیابی‌شده مطمئن شویم، قبل از انجام عملیات رمزگذاری، یک رشته بیت ثابت را به جدول H می‌افزاییم. برای عملیات رمزنگاری می‌توان از انواع مختلف الگوریتم‌های رمزنگاری قالبی استفاده کرد. با توجه به استاندارد بودن و امنیت بالای الگوریتم AES [۱۵] در پژوهش حاضر از این الگوریتم استفاده شده است.



شکل (۳). نحوه انتخاب سطوح مجاز و غیرمجاز هر ویژگی

الگوریتم ۱ مراحل ساخت الگو را به صورت خلاصه در خود دارد. شکل (۲- الف) نیز این مراحل را به صورت گرافیکی نشان می‌دهد.

۳-۳- احراز اصالت

در فرآیند احراز اصالت، ابتدا از کاربر خواسته می‌شود تا کلمه عبور خود را وارد کند و سپس اطلاعات زمانی آن را ثبت می‌کنیم. ابتدا به کمک چکیده کلمه عبور کاربر، جدول S و مقادیر مرزی برای سطوح ویژگی‌ها را رمزگشایی می‌کنیم. سپس با توجه به مقدار ویژگی jام، سطح مربوط به آن راتعیین می‌کنیم و سهم مربوطه را از سطر jام جدول S برمی‌گزینیم. این کار را برای تمام L ویژگی انجام می‌دهیم. حال به کمک L سهم به‌دست آمده و به کمک الگوریتم آشکارسازی کلیدِ مخفی در طرح تسهیم راز، کلید مخفی را به‌دست می‌آوریم. به کمک این کلید مخفی جدول H را رمزگشایی می‌کنیم و مقدار رشته بیت افزوده را بررسی می‌کنیم. در صورتی که مقدار صحیح (درج شده در هنگام ساخت الگو) به‌دست آید، هویت فرد تایید می‌شود و در غیر این صورت، هویت او رد و از دسترسی او جلوگیری خواهد شد.

تغییرات تدریجی در الگوی تایپ کاربر، از موانع مهم در عملکرد سامانه‌های مبتنی بر الگوی تایپ به شمار می‌رود. در این طرح برای غلبه بر این تغییرات، پس از هر بار ورود موفق، الگوی بیومتریک به‌روزرسانی می‌شود. به این منظور، اگر اصالت فرد احراز شده باشد، لازم است چند کار دیگر انجام شود. نخست این که جدول H به روز می‌شود: قدیمی‌ترین ستون آن حذف شده و ستون جدیدی از مقادیر بردار ویژگی استخراج شده در این مرحله جای آن را می‌گیرد. سپس همه گام‌هایی که برای ساخت الگو برداشتیم (تعیین سطوح، تهیه سهم‌های مربوط به هر سطر، رمزگذاری)، مجدداً اجرا شده و الگوی جدید ذخیره می‌شود. در الگوریتم ۲، مراحل احراز اصالت به صورت خلاصه ذکر شده است.

الگوریتم (۱) ساخت الگو

ورودی	کلمه عبور pwd، ماتریس تاریخچه $H: L \times h$
خروجی	الگوی بیومتریک
۱	دامنه تغییرات هر دسته ویژگی را به کمک رابطه ۱ به‌دست آور. $[LL_i \quad UL_i] \quad i = 1.2$
۲	مقادیر مرزی را برای هر دسته ویژگی به کمک رابطه ۲ به‌دست آور. $l_{i.j} \qquad i = 1.2 \quad j = 1. \ldots . K-1$
۳	مقادیر میانه و انحراف معیار بالا و پایین را برای هر ویژگی به‌دست آور. $m_j \,.\, \sigma_j \,.\, \sigma_{j.L} \,.\, \sigma_{j.H} \quad j = 1. \ldots . L$
۴	برای هر ویژگی طبق رابطه ۳ سطوح مجاز و غیرمجاز ویژگی را تعیین کن. تعداد سطوح مجاز برای هر ویژگی را c_j و مجموع این سطوح را $C = \sum_{j=1}^{L} c_j$ بنام.
۵	یک کلید تصادفی ایجاد و به کمک یک طرح تسهیم راز، C سهم مجاز تولید کن که بتوانند آن کلید مخفی را آشکار سازند. این سهم‌ها را در خانه‌هایی از جدول S که متناظر با سطوح مجاز هر یک از ویژگی‌ها هستند، قرار بده. بقیه خانه‌های جدول را با اعداد تصادفی پر کن.
۶	چکیده کلمه عبور را محاسبه کن و از آن به عنوان کلید الگوریتم AES برای رمزگذاری مقادیر $l_{i.j}$ و جدول S استفاده کن.
۷	یک رشته‌بیت ثابت و از قبل تعیین‌شده را به جدول H اضافه کن و از کلید تصادفی تولید شده در گام ۵ به عنوان کلید الگوریتم AES برای رمزگذاری این جدول افزوده، استفاده کن.
۸	این جداول رمزگذاری‌شده را به عنوان الگوی بیومتریک ذخیره کن.

جدول (۱). یک نمونه از جدول S در الگوی بیومتریک، در هر سطر از این الگو، K عدد وجود دارد ولی تنها برخی از آن‌ها سهم مجاز برای بازیابی کلید مخفی هستند.

s_{11}	s_{12}	...	s_{1K}
s_{21}	s_{22}	...	s_{2K}
⋮	⋮		⋮
s_{L1}	s_{L2}	...	s_{LK}

الگوریتم (۲) احراز اصالت

ورودی	کلمه عبور pwd، بردار ویژگی‌ها، الگوی بیومتریک
خروجی	تأیید و الگوی بیومتریک به‌روزشده یا عدم تأیید
۱	چکیده کلمه عبور را محاسبه کن و به کمک آن، جدول S را رمزگشایی کن.
۲	مقدار هر یک از ویژگی‌ها را با سطوح دسته ویژگی مربوطه مقایسه کن و سهم متناظر را از جدول S انتخاب کن.
۳	به کمک طرح تسهیم راز و سهم‌های انتخاب‌شده، کلید مخفی را بازسازی کن.
۴	به کمک کلید مخفی تولیدشده در گام ۳، جدولِ افزوده H را رمزگشایی کن. در صورتی که رشته‌بیت از پیش تعیین‌شده در انتهای این جدول به‌دست آمد، هویت فرد را تأیید و در غیر این‌صورت رد کن.
۵	اگر هویت فرد تأیید شد، ابتدا قدیمی‌ترین ستون جدول H را با بردار ویژگی جدید جایگزین کن و سپس طبق الگوریتم (۱) الگوی بیومتریک را به روز کن.

۳-۴- نکات تکمیلی

با توجه به توضیحاتی که تا کنون ارائه کردیم، در مرحله احراز اصالت حتی اگر سهم مربوط به یک ویژگی به درستی انتخاب نشده باشد، قادر به بازیابی کلید مخفی نخواهیم بود. این مسئله باعث می‌شود نرخ رد نادرست[1] بسیار بالا باشد. همان‌طور که در بخش ۱-۲ گفتیم این مسئله یک اشکال مهم طرح [۱] نیز بود. برای رفع این مسئله لازم است بتوانیم با تنظیم پارامتر یا پارامترهایی اجازه بدهیم برخی از سهم‌های استخراج‌شده در فرآیند احراز اصالت اشتباه باشند. بدین‌ترتیب انعطاف بیشتری در تنظیم رابطه بین خطای نوع اول و دوم خواهیم داشت.

طرح‌های تسهیم راز بر اساس ورودی که به آن‌ها داده می‌شود قادر هستند، کلید مخفی را بازسازی کنند یا اعلام نمایند که این کار امکان‌پذیر نیست. دسته‌ی خاصی از این طرح‌ها موسوم به طرح‌های تسهیم راز مقاوم[2]، قادر هستند حتی در حضور تعدادی سهم اشتباه نیز عمل بازسازی کلید مخفی را انجام دهند. البته تعداد سهم‌های اشتباه انعطاف کافی را ندارد. مثلاً در طرح ارائه‌شده در [۱۶]، بازسازی در صورت خطا بودن یک چهارم سهم‌ها امکان‌پذیر است. مثلا اگر تعداد کل سهم‌های استخراج‌شده از الگوی بیومتریک ۳۸ سهم باشد، با داشتن حداقل ۲۹ سهم، امکان بازسازی کلید مخفی وجود خواهد داشت. به کمک این قابلیت طرح‌های تسهیم راز، در طرح پیشنهادی انعطاف ایجاد می‌کنیم.

در بخش ۲-۳ کل دامنه تغییرات هر دسته ویژگی را به K بازه تقسیم کردیم و برای هر ویژگی بر اساس پراکندگی مقادیر آن، بازه‌های مجاز را تعیین کردیم. تا کنون به همه بازه‌های مجاز را با یکدیگر معادل فرض کردیم. ولی همان‌طور که از شکل (۳) قابل درک است، سطح زیر تابع توزیع احتمال در این بازه‌ها با یکدیگر مساوی نیست و لذا منطقی به نظر می‌رسد که اهمیت متفاوتی به آن‌ها بدهیم. به این ترتیب طرح پیشنهادی، مدل بهتری از تابع توزیع احتمال (البته به صورت چندی‌شده[3]) به دست خواهد داد. طرح پیشنهادی را با افزایش تعداد سهم‌های هر ورودی جدول S به ۲ سهم، اصلاح می‌کنیم. همچنین به جای یک پارامتر k از دو پارامتر $k_1 < k_2$ استفاده می‌کنیم. برای ورودی‌هایی که بازه متناظر آن‌ها در ناحیه $[m_j - k_1\sigma_{j.L} \quad m_j + k_1\sigma_{j.H}]$ قرار گیرد، هر دو سهم، مجاز خواهند بود. همچنین برای سایر بازه‌هایی که در ناحیه $[m_j - k_2\sigma_{j.L} \quad m_j + k_2\sigma_{j.H}]$ قرار گیرند، یکی از سهم‌ها مجاز خواهد بود. برای سایر بازه‌ها هر دو سهم، غیرمجاز (اعداد تصادفی) خواهند بود. تعمیم این ایده به مراتب بالاتر نیز سرراست است ولی چون حجم الگو را بالا می‌برد و از سوی دیگر فایده قابل توجهی ندارد، از آن چشم می‌پوشیم.

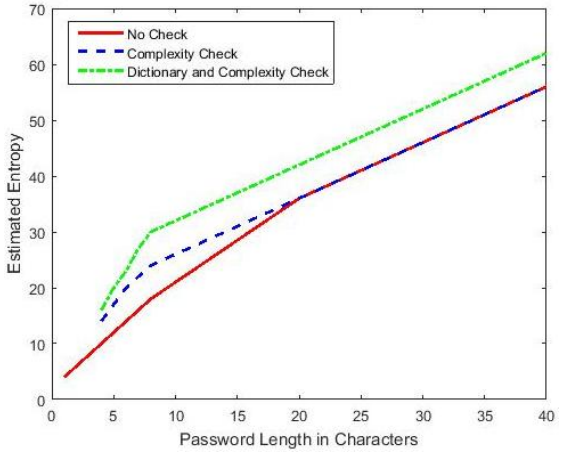
همان‌طور که قبلاً بیان شد، طرح‌های تسهیم راز مقاوم، انعطاف کمی دارند و اگر سهم‌های درست از تعداد خاصی بیشتر باشد، بازسازی رمز موفق خواهد بود. این تعداد معمولاً کسری از تعداد کل سهم‌هاست و نمی‌توان آن را تغییر داد. از این رو برای ایجاد توازن بین خطای نوع اول و دوم، از تغییر پارامترهای k_1 و k_2 بهره می‌گیریم. جزئیات بیشتر در این خصوص را در بخش ۲-۴ می‌آوریم.

۴- تحلیل امنیت

مؤسسه استاندارد و فناوری آمریکا (NIST[4]) در گزارشی [۱۷] به بررسی امنیت کلمه‌های عبور انتخاب‌شده از کاربران در شرایط مختلف پرداخته است. به این منظور آنتروپی کلمه‌های عبور انتخابی به کمک یک صفحه‌کلید با ۹۴ کاراکتر، در سه حالت مختلف محاسبه شده است. حالت اول وقتی است که انتخاب کلمه عبور آزادانه باشد. در حالت دوم کلمه عبور حتماً باید شامل کاراکترهای خاص، حروف بزرگ و کوچک و اعداد باشد. در حالت

1 -False Rejection Ratio (FRR)
2 -Robust Secret Sharing Schemes
3 -Quantized
4 -National Institute of Standards and Technology

سوم، علاوه بر شرایط حالت قبل، اجزای کلمه انتخاب‌شده نباید در یک لغت‌نامه شامل بیش از ۶۵۰۰۰ کلمه وجود داشته باشد. شکل (۴) تخمینی از میزان آنتروپی این کلمات عبور را نشان می‌دهد. مشاهده می‌شود که برای کلمات رایج که طولی حدود ۱۰ کاراکتر دارند، این آنتروپی حداکثر حدود ۳۰ بیت خواهد بود. در حالی که حداکثر آنتروپی ممکن برابر است با: $H_{max} = 10\log_2 94 \approx 65.54$ و اگر رشته بیت لازم برای نمایش این تعداد حرف در استاندارد Unicode را در نظر بگیریم، حداکثر آنتروپی قابل دست‌یابی به ۱۶۰ بیت هم می‌رسد. به این ترتیب طرح‌های رایج که بر اساس کلمه عبور عمل می‌کنند، بخش زیادی از امنیت قابل دست‌یابی را به هدر می‌دهند. در زیربخش‌های بعد خواهیم دید که به کمک طرح پیشنهادی قادر هستیم تا استفاده بیشتری از این امنیت قابل دسترس بکنیم.



شکل (۴). تخمین میزان آنتروپی کلمه‌های عبور رایج در سه شرایط مختلف: انتخاب آزادانه، آزمون پیچیدگی، آزمون پیچیدگی و لغت‌نامه (باز تولید از روی [۳])

۴-۱- حداقل امنیت معادل کلمه عبور ساده

نکته اول در مورد طرح پیشنهادی این است که امنیت آن حداقل به اندازه استفاده از کلمه عبور به تنهایی است. نشان دادن این مطلب ساده است؛ فردی که کلمه عبور را در اختیار نداشته باشد، قادر به رمزگشایی از جدول S نخواهد بود. در نتیجه نخواهد توانست به سهم‌های صحیح دست یابد و به همین دلیل نخواهد توانست به کمک طرح تسهیم راز به کلید مخفی دست یابد.

علاوه بر این، طرح پیشنهادی، در برابر حملات پیوندی نیز مقاومت بیشتری دارد (نسبت به طرح‌های سنتی مدیریت کلید مبتنی بر کلمه عبور)؛ زیرا اگر کلمه عبور یک فرد در دو سامانه با یکدیگر برابر باشد، مهاجمی که به چکیده کلمه عبور کاربران در دو سامانه دسترسی داشته باشد، به سادگی خواهد توانست بفهمد که کلمه عبور کاربر در سامانه دوم چیست. این فرض منطقی است زیرا چکیده کلمه عبور یک مقدار عمومی است و به سادگی در حافظه دستگاه ذخیره می‌شود. در طرف مقابل، در طرح پیشنهادی چکیده کلمه عبور ذخیره نمی‌شود و تنها چکیده کلید مخفی در الگوی بیومتریک نگه داشته می‌شود. این کلید نیز در هر سامانه به صورت تصادفی تعیین می‌شود و احتمال مشابهت آن ناچیز است.

استفاده از الگوی تایپ در کنار کلمه عبور، امنیت بیشتری نیز ایجاد می‌کند. در این‌بخش فرض می‌کنیم از طرح ساده استفاده شده باشد، یعنی برای بازسازی کلید مخفی لازم است تمام سهم‌ها به درستی استخراج شوند. حالت انعطاف‌پذیر طرح که در عمل توصیه می‌شود، در زیربخش بعد بررسی خواهد شد.

اگر فرض کنیم، مهاجم کلمه عبور کاربر را در اختیار داشته باشد و آن را به درستی وارد کند، می‌خواهیم آنتروپی الگوی بیومتریک را محاسبه نماییم. در این‌صورت مهاجم خواهد توانست جدول S را به درستی رمزگشایی کند. حال برای دست‌یابی به کلید تصادفی، باید از بین هر K سهم موجود در هر ردیف، یک سهم را انتخاب کند. چون در سطر jام جدول S تعداد n_j سهم صحیح وجود دارد، آنتروپی کل الگوی بیومتریک برابر خواهد بود با:

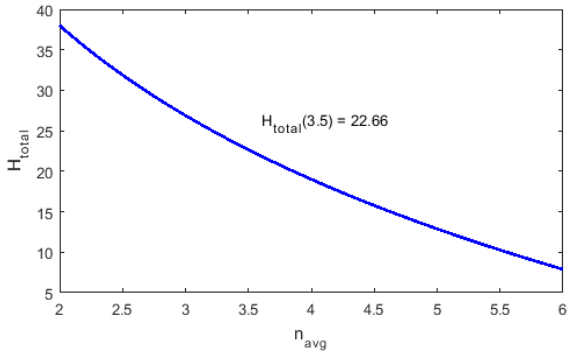
$$H_{total} = -\sum_{j=1}^{L} \log_2\left(\frac{n_j}{K}\right) = Llog_2(K) - \log_2 \prod_{j=1}^{L} n_j$$
$$= L(\log_2 K - \log_2 \bar{n}) \qquad (۵)$$

اگر مقدار L را برای یک کلمه عبور ده حرفی، برابر با ۱۹ بگیریم، از $K = 8$ استفاده کنیم و فرض کنیم متوسط تعداد سهم‌های درست در هر سطر $\bar{n}$ سهم باشد، خواهیم داشت:

$$H_{total} = 19(3 - \log_2 \bar{n}) \qquad (۶)$$

در شکل (۵) مقدار H_{total} بر حسب $\bar{n}$ رسم شده است.

همان‌طور که در بخش ۱-۳ اشاره کردیم، دستگاه‌های همراه هوشمند، قادر هستند ویژگی‌هایی از قبیل فشار و سطح تماس دست با صفحه لمسی را نیز اندازه بگیرند. به این ترتیب به‌ازای یک کلمه عبور با طول ثابت تعداد ویژگی‌ها دوبرابر می‌شود. با فرض ثابت ماندن میانگین تعداد سهم‌های درست در هر سطر، آنتروپی به‌دست‌آمده دو برابر خواهد شد. از این رو انتظار داریم طرح پیشنهادی در این دستگاه‌های امنیت بیشتری نسبت به دستگاه‌های سنتی در اختیار ما قرار دهد.



شکل (۵). آنتروپی کل الگوی بیومتریک بر اساس میانگین تعداد سهم درست در هر سطر جدول S. فرض $K = 8$ و $L = 19$

۴-۲- محاسبه احتمال خطا

در این قسمت امنیت طرح پیشنهادی در حالت انعطاف‌پذیر با سهم‌های نامساوی را بررسی می‌کنیم. به این منظور احتمال خطای نوع اول و دوم را به صورت روابط بسته به‌دست می‌آوریم. این روابط مبتنی بر توزیع آماری ویژگی‌های استخراج‌شده از الگوی تایپ هستند. به همین منظور به کمک یک بانک داده این توزیع‌ها را تخمین می‌زنیم و نتایج نهایی را ارائه می‌کنیم.

طرح انعطاف‌پذیر با دو پارامتر k_1 و k_2 را در نظر بگیرید. احتمالات زیر را برای یک ویژگی نوعی تعریف می‌کنیم:

$$P_1^{usr} = P\{m^{usr} - k_1\sigma_L^{usr} \le x \le m^{usr} + k_1\sigma_H^{usr} | user\} \quad (۷)$$

$$P_1^{usr} = P\{m^{usr} - k_2\sigma_L^{usr} \le x \le m^{usr} + k_2\sigma_H^{usr} | user\} - P_1^{usr} \quad (۸)$$

$$P_1^{imp} = P\{m^{usr} - k_1\sigma_L^{usr} \le x \le m^{usr} + k_1\sigma_H^{usr} | impostor\} \quad (۹)$$

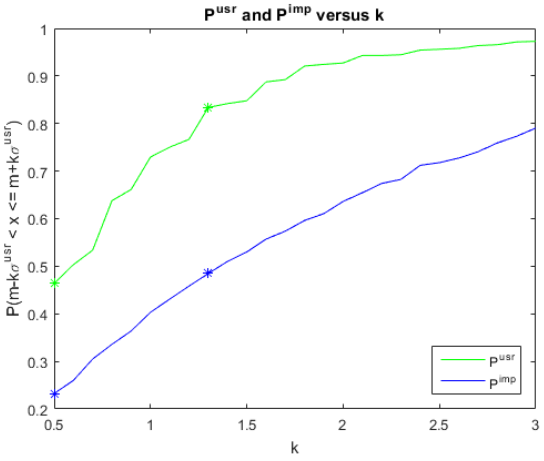
$$P_1^{imp} = P\{m^{usr} - k_2\sigma_L^{usr} \le x \le m^{usr} + k_2\sigma_H^{usr} | impostor\} - P_1^{imp} \quad (۱۰)$$

که در آن، P_1^{usr} و P_2^{usr} به ترتیب احتمال آن هستند که کاربر مجاز بتواند به یک یا دو سهم صحیح دست پیدا کند. P_1^{imp} و P_2^{imp} نیز به ترتیب احتمال دست‌یابی کاربر غیرمجاز به یک یا دو سهم صحیح است. اگر تابع جرم احتمال مربوط به تعداد سهم‌های صحیح استخراج‌شده از هر سطر را به صورت PMF_i برای $i = 1, \dots, N$ نشان دهیم، با فرض استقلال تعداد سهم‌های استخراج‌شده از هر سطر، تابع جرم احتمال مجموعه سهم‌های صحیح را می‌توان برحسب کانولوشن توابع جرم احتمال نوشت.

در اینجا برای بررسی بیشتر فرض می‌شود کلمه عبور ۱۰ حرف داشته باشد و در مجموع ۱۹ ویژگی ($L = 19$) (۱۰ تا مربوط به زمان فشردن کلید و ۹ تا مربوط به فاصله زمانی بین فشردن کلیدها) استخراج شود. برای تخمین احتمالات نیاز به محاسبه P_1 و P_2 برای کاربر مجاز و مهاجم داریم. این احتمالات را از روی یک بانک داده تخمین می‌زنیم.

بانک داده مورد استفاده توسط دانشگاه Carnegie Melon تهیه شده است [۱۸]. در این بانک داده ۵۱ نفر در ۸ جلسه جداگانه که حداقل فاصله بین آن‌ها ۲۴ ساعت بوده است، یک کلمه عبور ثابت را ۴۰۰ بار (هر جلسه ۵۰ بار) تایپ کرده‌اند. ویژگی‌های استخراج شده عبارتند از مدت زمان فشدن کلید، فاصله بین رها کردن کلید تا فشردن کلید بعدی و فاصله بین فشردن کلید تا فشردن کلید بعدی. در شکل (۶) مقدار نوعی احتمالات مورد نیاز را نشان داده‌ایم.

همان‌طور که در بخش ۳-۴ اشاره کردیم، با تغییر مقادیر k_1 و k_2 می‌توان تابع چگالی احتمال تعداد کل سهم‌های صحیح را برای کابرد مجاز و غیرمجاز به نحوی تنظیم کرد که نرخ خطای نوع اول و دوم به مقادیر خواسته شده نزدیک شود. در جدول (۲) چند مقدار نوعی برای این دو پارامتر را آورده‌ایم. همچنین در شکل (۷) تابع چگالی احتمال سهم‌های درست یافته شده را برای کاربر مجاز و مهاجم به ازای $k_1 = 1$ و $k_2 = 2$ رسم شده‌اند. در این حالت مرز تصمیم‌گیری را $38 - \left\lfloor \frac{38-1}{4} \right\rfloor = 29$ نظر گرفته شده است. با تغییر مقادیر k_1 و k_2، نمودار DET[1] را در شکل (۸) رسم می‌کنیم. مشاهده می‌شود که نرخ EER برابر با ۴ درصد به دست می‌آید که بسیار بهتر از طرح [۱] می‌باشد (در آن طرح خطای رد نادرست ۴۸٪ گزارش شده بود).

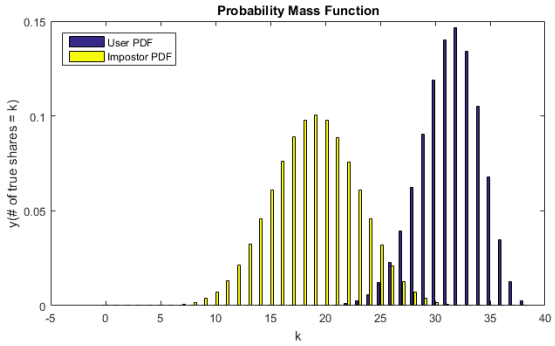


شکل (۶). سطح زیر تابع احتمال کاربر مجاز و مهاجم در بازه $m^{usr} - k\sigma_L^{usr} \le x \le m^{usr} + k\sigma_H^{usr}$ به‌ازای مقادیر مختلف k

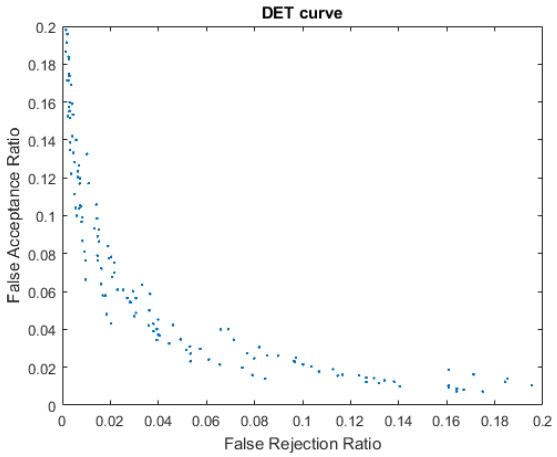
جدول (۲). مقادیر نوعی برای احتمالات P_1 و P_2 برای ویژگی‌ها

k_1	k_2	FRR %	FAR %
۰/۸	۲/۴	۱۳/۸	۱/۱
۰/۸	۲/۵	۱۳/۴	۱/۳
۱/۰	۲/۱	۱۲/۶۵	۱/۴
۱/۲	۱/۷	۱۳,۲	۱/۲
۱/۲	۱/۸	۸	۱/۴

1 -Detection Error Trade-off



شکل (۷). تابع چگالی احتمال تعداد سهم‌های مجاز قابل کشف کاربران. مهاجم به رنگ زرد و تابع کاربر اصلی به رنگ آبی نمایش داده شده است.



شکل (۸). نمودار DET برای طرح پیشنهادی به ازای پارامترهای نوعی. در نمودار مشخص است که $EER \approx 0.04$.

۴-۳- حفاظت حریم خصوصی

در طرح پیشنهادی، اگر مهاجم کلمه عبور را نداند، قادر به استفاده از جداول S و H نخواهد بود. به این ترتیب هیچ اطلاعاتی در مورد الگوی تایپ کاربر نشت نخواهد کرد.

ممکن است این سوال مطرح شود که چرا برای هر ویژگی سطوح جداگانه محاسبه نشده است؟ در جواب باید گفت که یکی از مهم‌ترین خواص الگوریتم‌های رمزنگاری بیومتریک این است که از روی الگوی بیومتریک اطلاعاتی در خصوص بیومتریک مورد بررسی نشت نکند. اگر سطوح مربوط به هر ویژگی جداگانه در نظر گرفته شود، مهاجمی که به کلمه عبور دسترسی داشته باشد (و طبعاً بتواند S را رمزگشایی کند) اطلاعاتی در خصوص دامنه تغییرات هر ویژگی به‌دست خواهد آورد که می‌تواند به نوعی الگوی تایپ کاربر را فاش سازد.

۵- کاربردهای عملی

به طور کلی طرح پیشنهادی در اغلب کاربردهای فعلی کلمات عبور قابل استفاده است. به دلیل عدم نیاز به تجهیزات و حسگرهای خاص (برخلاف سایر بیومتریک‌ها) این طرح به سادگی قابل پیاده‌سازی است و نسبت هزینه به امنیت آن بسیار پایین است.

تنها نکته در این خصوص وابستگی اطلاعات زمان به نوع صفحه‌کلید مورد استفاده می‌باشد. از این رو استفاده از این طرح به طور خاص در مواردی از قبیل احراز دستگاه‌های همراه از قبیل تلفن هوشمند، تبلت، لپ‌تاپ، تلفن بی‌سیم و ... پیشنهاد می‌شود. چرا که در این دستگاه‌ها صفحه‌کلید اغلب ثابت بوده و به ندرت تغییر می‌کند. از آن‌جا که امروزه این دستگاه‌ها اطلاعات بسیار زیادی در مورد حریم شخصی افراد در خود دارند و از طرف دیگر بسیار در معرض دستبرد هستند، این کاربرد اهمیت دو چندان می‌یابد.

از مزیت‌های طرح فعلی آن است که به صورت پویا الگوی تایپ کاربر و تغییرات آن را یاد می‌گیرد و خود را با آن تطبیق می‌دهد. به این ترتیب بر یکی از مهمترین مشکلات موجود در استفاده از الگوی تایپ بیومتریک (و به طول کلی بیومتریک‌های رفتاری[1])، یعنی تغییرات تدریجی در گذر زمان، غلبه خواهد شد.

۶- نتیجه‌گیری

در این مقاله یک طرح تعمیم‌یافته برای استفاده از الگوی تایپ کاربران به منظور تولید یک کلید بیومتریک استفاده شد. در این طرح با استفاده از توزیع آماری ویژگی‌های استخراج‌شده از الگوی تایپ کاربر و یک طرح تسهیم راز، یک الگوی بیومتریک محافظت‌شده ساخته شد. نشان دادیم که طرح پیشنهادی برای کلمات عبور معمول قادر است امنیت کلید سامانه‌های مبتنی بر کلمه عبور را ۲ تا ۳ برابر افزایش دهد. همچنین مشخص شد که طرح پیشنهادی هیچ اطلاعاتی در خصوص کلمه عبور یا الگوی تایپ کاربر نشت نمی‌دهد.

از نقطه نظر خطای تایید و رد نادرست نیز، به‌ازای مقادیر مختلف برای دو پارامتر طرح نشان داده شد که دست‌یابی به EER = 0.04 امکان‌پذیر است. در عین حال مشاهده کردیم که اگر FAR=0.01 مدنظر طراح سامانه میزبان باشد، FRR<0.1 قابل دست‌یابی است.

با استفاده از طرح‌های تسهیم راز مقاوم، توانستیم قابلیت تنظیم بین خطای نوع اول و دوم را فراهم سازیم و بدین ترتیب، به عملی شدن این طرح کمک نماییم. همچنین به کمک این ایده توانستیم تابع توزیع احتمال هر ویژگی را به صورت بهتری مدل کنیم و در نتیجه از میزان آنتروپی در اختیار استفاده بیشتری ببریم.

1- Behavioral Biometrics

۷- مراجع

[1] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," International Journal of Information Security, pp. 69-83, 2002.

[2] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," Advances in cryptology-Eurocrypt 2004, Springer Berlin Heidelberg, 2004.

[3] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," Proc. of the 2001 IEEE Symposium on Security and Privacy, 2001.

[4] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and V. Kumar, "Biometric Encryption," ICSA Guide to Cryptography, McGrow-Hill, 1999.

[5] A. Goh and D. C. L. Ngo, "Computation of cryptographic keys from face biometrics," International Federation for Information Processing 2003, Springer-Verlag, LNCS2828, pp. 1–13, 2003.

[6] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," Computers, IEEE Transactions on, pp. 1081-1088, 2006.

[7] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by Keystroke Timing: Some Preliminary Results," Santa Monica, CA: RAND Corporation, 1980.

[8] BioPassword, "Authentication Solutions through Keystroke Dynamics," BioPassword Whitepaper, 2007.

[9] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," Future Generation computer systems, pp. 351-359, 2000.

[10] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," Applied Soft Computing, pp. 1565-1573, 2011.

[11] S. Hwang, S. Cho, and S. Park, "Keystroke dynamics-based authentication for mobile devices," Computers & Security, pp. 85-93, 2009.

[12] P. Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation," Information Security Technical Report, pp. 36-43, 2012.

[13] Y. Zhong, Y. Deng, and A. K. Jain, "Keystroke dynamics for user authentication," Computer Vision and Pattern Recognition Workshops (CVPRW), 2012 IEEE Computer Society Conference on. IEEE, 2012.

[14] K. Killourhy and R. Maxion, "The effect of clock resolution on keystroke dynamics," Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, 2008.

[15] J. Daemen and V. Rijmen, "The Rijndael block cipher: AES proposal," First Candidate Conference (AES1), 1999.

[16] A. Cevallos, S. Fehr, R. Ostrovsky, and Y. Rabani, "Unconditionally-secure robust secret sharing with compact shares," In David Point cheval and Thomas Johansson, editors, Eurocrypt 2012, Springer, pp. 195–208, 2012.

[17] W. E. Burr, D. F. Dodson, and W. T. Polk, "Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology," NIST Special Publication 800-63, Version 1.0.2, National Institute of Standards and Technology, 2006.

[18] K. S. Killourhy and R. S. Maxion, "Comparing Anomaly Detectors for Keystroke Dynamics," In Proc. of the 39th Ann. Int. Conf. on Dependable Systems and Networks (DSN-2009), Estoril, Lisbon, Portugal, pp. 125-134, 2009.

Journal Of Electronical & Cyber Defence
Vol. 5, No. 1, 2017, Serial No. 17

A Generalized Scheme for Extracting Biometric Keys from Keystroke Dynamics

A. Bidokhti*, S. M. Pournaghei, A. H. Khalili Tirandaz

*Sharif University of Technology

(Received: 22/01/2016 , Accepted: 31/10/2016)

ABSTRACT

In this paper, a generalized scheme is proposed for extracting biometric keys from keystroke dynamics of the user. In the proposed scheme, first some features of are extracted from keystroke patterns of the user. Then, using a secret sharing scheme, a number of true shares are assigned to each feature to reproduce the secret key based on its discriminatory power. This true shares are hidden among random shares. When a user wants to be authenticated, the same features are extracted from his or her keystroke pattern and if its value is in the proper region, a true share is extracted. If the total number of true shares are extracted, and exceeds a threshold, reproduction of the secret key will be possible. Otherwise no information about the key will be leaked. Two parameters are used in the scheme, through which FAR and FRR can be balanced.

The proposed scheme is able to extract 20 to 50 bits of secret key (besides the intrinsic entropy of the password itself). The equal error rate (ERR) of the scheme is nearly 4%. Besides, on top of a traditional password-based system, using the proposed scheme increases the security by a factor of 2 or 3 (in number of bits).

Keywords: Biometric Encryption, Keystroke Pattern, Key Management, Entropy, Secret Sharing

* Corresponding Author Email: amirbidokhti@yahoo.com