بسم الله الرحمن الرحیم

کدام روش ورود به گوشی امن ترین است؟

What Is The Best Login Method For Smart Phone?

اکثر تلفن‌های همراه امروز به صورت هوشمند و اتوماتیک هستند و دیگر کمتر در سطح جامعه شاهد استفاده مردم از تلفن‌های قدیمی هستیم از این رو شرکت‌های توسعه دهنده تلفن همراه هروزه با به‌روزرسانی شیوه‌های امن کردن تلفن همراه به روند توسعه امنیت پایا تلفن همراه‌های شخصی کمک می‌کنند.

اما بزرگ‌ترین سوال در بین تمامی شیوه‌های امنیت تلفن همراه هوشمند این است که کدام روش بهترین روش امن کردن پایا تلفن همراه است. در این مقاله ما به بررسی شیوه های امنیت پایا سیستم های تلفن همراه و شیوه عملکرد آن می پردازیم.

برای بررسی انواع تلفن همراه ما آن‌ها را به دو دسته تقسیم کردیم:

۱- تلفن‌های هوشمند

۲-تلفن‌های غیرهوشمند

اینکه چه تفاوتی بین تلفن‌های هوشمند و غیرهوشمند وجود دارد باید گفت که در نوع کاربری و اختیاراتی که کاربر در هر دستگاه (چه هوشمند و چه غیرهوشمند) دارد متفاوت است برای مثال یک تلفن هوشمند به‌صورت خودکار میزان پردازش را کنترل می‌کند و نسبت به میزان استفاده کاربر سخت افزار مورد نیاز را ارائه می‌دهد اما در دستگاه‌های غیرهوشمند اینطور نیست یا در تلفن‌های هوشمند میزان نورصفحه با توجه به محیط تنظیم می‌شود و در مصرف باتری گوشی صرفه‌جویی می‌شود ولی در گوشی‌های غیرهوشمند اینگونه نیست.

با علم بر این موضوع حال برای ورود به هرکدام از این تلفن‌ها راه‌های مختلفی وجود دارد طبیعی است تلفن هوشمند راه‌های هوشمندانه‌ای برای ورود خواهد داشت و تلفن‌های غیرهوشمند راه های ساده‌تری خواهند داشت.

یکی از ساده‌ترین راه‌های ورود به تلفن‌همراه که توسط شرکت نوکیا معرفی شد استفاده از کلید های ترکیبی بود که کاربر به‌صورت پیش فرض با فشار دادن دکمه OK و دکمه ستاره(*) تلفن همراه خود را باز می‌کرد این راه یکی از ساده‌ترین راه‌ها برای امنیت تلفن همراه بود که بعدها می

توانستید کلیدهای پیش‌فرض را تغییر دهید ، اما این روش بسیار راحت هک می شد و به راحتی به اطلاعات داخل گوشی دسترسی پیدا می‌کردید.

تلفن های ساده ۲ وجهی

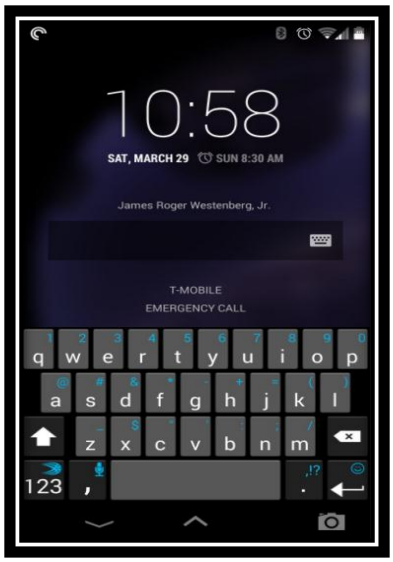
*کاملا غیر ایمن

نسل بعدی رمزنگاری بر روی تلفن های همراه ایجاد یک متد ایجاد پسورد یا رمز عبور به خصوص برای هر کاربر بود به طوری‌که کاربر یک پسورد را از قبل تعیین می‌کند و زمانی که گوشی قفل می‌شود برای ورود باید آن رمز عبور را وارد نماید، این روش تا به امروز بر روی برخی گوشی‌های هوشمند نیز استفاده می شود اما این روش آن چنان کارآمد نیست چرا که این روش رمز نگاری از متد ۴ بایتی استفاده می‌کند و صاحب تلفن باید یک رمز ۴ رقمی تعیین کند از این رو حدس زدن آن برای هکر بسیار ساده است.

رمز ۴ رقمی

*ایمن

نسل بعدی این نوع رمز نگاری ها را پسورد(password) می‌نامیم به طوری که شخص به جای استفاده از نوع ۴ رقمی رمز از ۸تا ۲۵۴ کاراکتر می‌تواند وارد کند به غیر از کاراکترهای رزرو شده مثل (!~<>"Ø"و...) این شیوه بسیار ایمن تر از روش ۴ بیتی است اما همچنان دارای مشکلاتی است مثل کیلاگر ها که با خواندن محل کلیک کاربر می توانند پسورد قربانی را پیدا کنند.



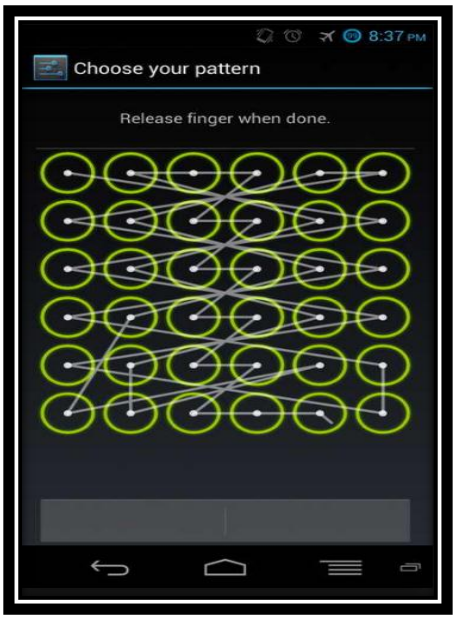
نمونه رمز ورود یک تلفن اندرویدی

*بسته به نوع رمز میتواند بسیار ایمن باشد

بعد از پسورد نسل جدید از نوع رمزنگاری به نام الگو (pattern) وارد بازار رقابت امنیتی تلفن همراه شد. البته این نوع رمز نگاری برای تلفن‌های هوشمند شروع به کار کرد به طوری که برای استفاده از این نوع روش رمزنگاری شما نیاز به صفحه لمسی بر روی تلفن خود هستید که برای اولین بار در PDA ها استفاده شد و استقبال شدیدی از سوی کاربران دستگاه‌های شخصی شد، از این رو شرکت‌های تلفن همراه، این نوع متد را به همراه تلفن‌های نسل جدید خود با ظاهر گرافیکی و کاربر پسند وارد بازار کردند.

این نوع الگوها که از قبل توسط کاربر تنظیم می‌شود بسیار ضریب امنیت بالاتری نسبت به نسخه های قبل دارد چرا که نوع الگو می‌تواند بسیار پیچیده باشد و محدودیتی در ایجاد الگو وجود ندارد

زیرا با ایجاد رابط گرافیکی ایجاد یک الگوی شخصی بسیار راحت‌تر شده است و شخصی که بخواهد نفوذ را انجام دهد به راحتی نمی تواند عمل هک را انجام دهد.



نمونه الگوی مورد استفاده در گوشی اندرویدی

*نسبتاً ایمن

استفاده از الگوها تا به امروز در تمامی تلفن‌های هوشمند استفاده می‌شود اما این روش به علت ماندن اثر الگو بر روی صفحه همچنان روش امن و مطمن نیست چرا که بسیاری از کاربران پس از استفاده تلفن خود را تمیز نمی‌کنند پس میتوان همچنان رمز را حدس زد!

*نکته: پس از استفاده از تلفن صفحه خود را تمیز کنید تا از سوءاستفاده آن جلوگیری کنید!

پس از الگو و همزمان در همان نسل نوع رمزگذاری نسبتا غیر ایمنی وارد تنظیمات تلفن همراه شرکت ها شد که حس هوشمندی تلفن همراه را چند برابر می کرد اما امنیت چندانی نداشت این روش به‌صورتی بود که تلفن یک متن را از قبل توسط کاربر با استفاده میکروفن های تلفن ذخیره می‌کرد و هر زمان که کاربر آن جمله را تکرار می‌کرد تلفن باز می شد.

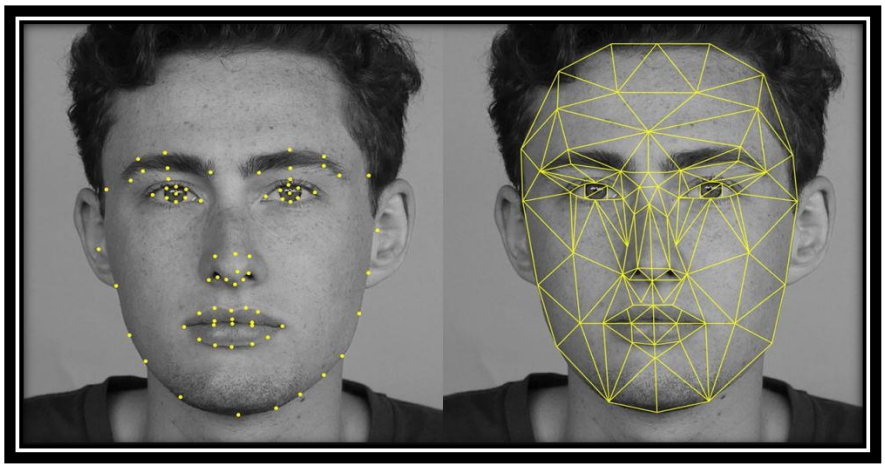
این روش خیلی زود از روی تلفن‌های هوشمند جدید حذف شد چرا که اگر صدای کاربر را در تلفن دیگری پخش کنید تلفن متوجه صدای زنده و غیر زنده را متوجه نمی‌شود پس تلفن را باز می‌کند.(این روش اکنون کاربرد تفریحی دارد) این روش را نمی‌توان ضریب امنیتی برای تلفن همراه دانست!

نمونه صفحه ورود با voice password

*بسیار غیر ایمن

همزمان با ارائه رمز کلامی که توضیح دادیم نوع دیگری از رمزنگاری در تلفن‌های همراه به وجود آمد.از طرفی توسعه دهنده‌های تلفن همراه تصمیم گرفتند که دوربین جلویی تلفن‌های هوشمند خود را قوی‌تر کنند از این رو شرکت‌های امنیتی از این پیشرفت استفاده کردند و نوع جدید از باز کردن تلفن همراه را معرفی کردند و نام آن را face recognition یا تشخیص چهره گذاشتند

به صورتی که تلفن همراه مولفه‌هایی را در سورت کاربر پیدا می‌کند که معمولاً خیلی سخت می توان تمام آن‌ها را در یک فرد پیدا کرد برای مثال: فاصله بین ابروها، فاصله بین چشم‌ها، اندازه بینی ،فاصله بین بینی تا لب، نوع لب ،فاصله بین لب تا فک، رنگ پوست و غیره... که با این تفاسیر این روش را بی‌نقص نشان دهند اما این روش هم به‌راحتی تمام هک شد به صورتی که اگر ما از صاحب گوشی یک عکس بگیریم وآن را جلوی گوشی بگیریم تلفن توانایی شناسایی عکس زنده و غیره زنده را ندارد پس فکر می‌کند صاحب اصلی جلوی دوربین است و تلفن را باز می کند. سال هاست که توسعه دهنده های تلفن همراه سخت در تلاش هستند که این روش را به صدر بازار امنیت برگرداند اما همچنان ناموفق هستند.

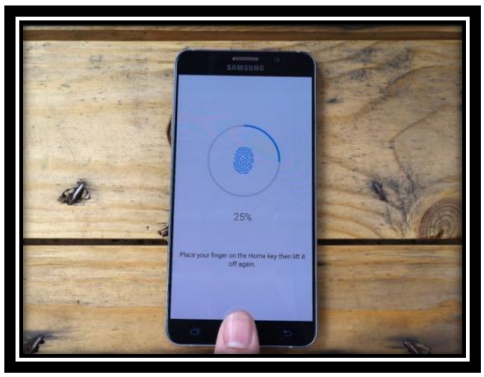


تشخیص چهره

*نا ایمن

پس از ناکامی های به وجود آمده در روش‌های رمزنگاری شرکت‌های بزرگ تولید تلفن تصمیم گرفتند گوشی‌های هوشمند خود را کمی هوشمندتر کنند به صورتی که با استفاده از چیپ‌های بسیار خاص و با ضریب امنیت بالا اقدام به اضافه کردن حسگر اثر انگشت finger print در تلفن‌های خود کردند، این روش یکی از بهترین روش‌های رمزنگاری در عرصه رمزنگاری ورود به تلفن همراه است که تاکنون کرکی برای نفوذ به این روش گزارش نشده است مگر با خطای انسانی چرا که هیچ سیستم امنیتی به طور کامل امن نیست و همیشه یک راه نفوذ وجود دارد.

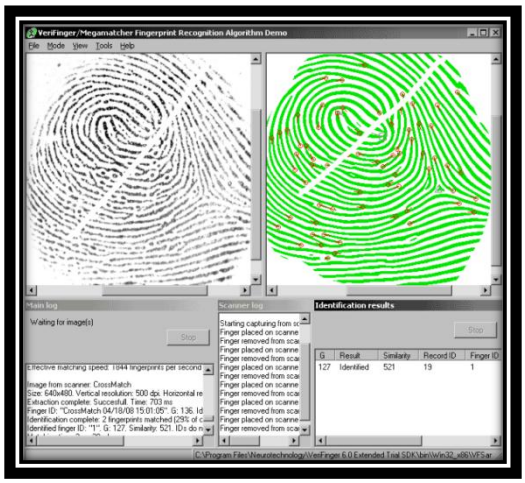
این روش به‌طوری عمل می‌کند که با جمع آوری اطلاعات روی انگشت و خطهای روی آن،آن خطها را به صورت دیتا ذخیره می کند و ضریب خطا را به حداقل می رساند.



حسگر اثر انگشت

*نسبتاً ایمن

تمامی مردم تصور می‌کردند که با وجود حسگر اثر انگشت دیگر تلفن آنها مورد نفوذ قرار نخواهد گرفت اما هک اثر انگشت بسیار ساده‌تر از هک کردن یک پسورد ۴ دیتایی است، تنها لازمه آن یک دستگاه verifinger است کافی است از انگشت صاحب تلفن عکس بگیرید(نتایج عکس های تا فاصله۳ متر هم مثبت بوده و مورد نفوذ قرار گرفته است) عکس گرفته شده با یک دوربین استاندارد بوده است و به راحتی می‌توان اثرانگشت را کپی و توسط دستگاه verifinger شناسایی کرد نسخه جعلی آن را طراحی کرد و به تمامی حساب‌ها و تلفن همراه قربانی تسلط داشت.



Verifinger دستگاه کپی اثر انگشت

*راه حل سرقت اثر انشگت

(این روش معمولی برای کاربران عادی نیست

تنها برای افراد خاص از این روش استفاده می‌شود)

"خب اکنون هیچ روش امنی برای ورود وجود ندارد"

جمله بالا تا سال ۲۰۱۶ صحیح بود اما روش بسیار امنی وجود دارد که کرک آن هزینه بسیار بالا و همچنین ریسک بسیار بالایی نسبت به ارزش انجام آن دارد.

این روش را IRIS می نامند روش نوین با استفاده از سنسورهای جلوی گوشی که با اسکن عنبیه چشم و دریافت کدهای روی عنبیه چشم که مانند اثر انگشت یکتاست انجام می شود، یک روش بسیار خوب برای تلفن همراه است.شاید کمی زیاده روی باشد اما منطقی است چون امروزه همه کاربران اطلاعات حساب بانکی وحساب های شخصی خود را بر روی تلفن هوشمند خود به همراه دارند پس هرچه قدر به این بخش از تلفن همراه امنیت اضافه کنیم به هیچ وجه اضافه کاری انجام نشده است.

شیوه کار این روش بسیار شبیه به اثر انگشت است با این تفاوت که این روش علاوه بر حسگر اثر انگشت روی تلفن همراه که از یک حسگر استفاده می‌کند از دو حسگر اسکن استفاده می‌کند و تمامی سطح چشم را اسکن می‌کند. تا به امروز این روش یکی از امن ترین روش های موجود برای تمامی کاربران است.

حسگر IRIS در تلفن های هوشمند
*بسیار امن

نباید فراموش کرد که هنوز هم امن ترین روش برای باز کردن تلفن همراه پیدا نشده و تلاش برای رسیدن به این روش ادامه دارد، به احتمال زیاد نسل بعدی امنیت ورود به گوشی از طریق رابط طبیعی و از طریق DNA انجام خواهد پذیرفت.

جای تعجبی ندارد برای هربار ورود لازم باشد یک سوزن بسیار ریز وارد بدن شده و با خون بدن شما تلفن شما باز شود.

نویسنده اثر : علی عباسی