

شناسایی ریسک‌های امنیتی در زیست‌بوم توزیع برنامه‌های سامانه‌های هوشمند همراه

سپیده نیک‌منظر و محمد حسام تدین*

پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)، تهران، ایران

s.nikmanzar@aut.ac.ir

tadayon@itrc.ac.ir

چکیده

با توجه به استفاده روزافزون از سامانه‌های هوشمند همراه در بین اقشار مختلف جامعه و قابلیت‌های بسیاری که دستگاه‌های تلفن همراه در اختیار کاربران قرار می‌دهند، تضمین امنیت سامانه‌های هوشمند همراه حائز اهمیت است. یکی از مواردی که امنیت سامانه‌های هوشمند را به خطر می‌اندازد، کانال‌های عرضه و توزیع برنامه‌ها یا «فروشگاه‌های برنامه» هستند. بسیاری از سازمان‌ها به یک روش ارزیابی ریسک جهت حفاظت از دارایی‌های خود نیاز دارند؛ لذا، شناسایی ریسک‌های امنیتی موجود در زیست‌بوم توزیع برنامه ضروری است. هدف این مقاله، شناسایی تهدیدها، آسیب‌پذیری‌ها و مهم‌ترین ریسک‌های امنیتی در حوزه توزیع برنامه‌های سامانه هوشمند همراه است. ابتدا مدلی از زیست‌بوم برنامه ارائه شده و سپس تهدیدات امنیتی براساس تحلیل STRIDE معرفی می‌شوند. در انتها نیز ریسک‌های امنیتی موجود در زیست‌بوم توزیع برنامه‌ها شناسایی خواهند شد.

واژگان کلیدی: سامانه هوشمند همراه، فروشگاه برنامه، توزیع برنامه، مدلسازی تهدید، ریسک امنیتی، درخت حمله

۱- مقدمه

که فروشگاه در اختیار آن‌ها قرار می‌دهد، برنامه‌های خود را منتشر، به‌روزرسانی و مدیریت کنند. تاکنون میلیاردها برنامه از این فروشگاه‌ها بارگیری شده است. طبق آمارهایی که پایگاه Statista منتشر کرده، در سال ۲۰۱۶ تعداد دو میلیون برنامه در فروشگاه اپل برای بارگیری وجود داشته است [1]. بر اساس آمار منتشرشده توسط همان پایگاه، از سال ۲۰۰۸ تا ۲۰۱۶، در مجموع ۱۳۰ میلیارد برنامه از فروشگاه iTunes شرکت اپل دانلود شده است [2]. همچنین، بر اساس آمارهای ارائه‌شده از سوی یکی از فروشگاه‌های برنامه فعال در کشور، در سال ۱۳۹۳ حدود ۲۵ هزار برنامه از طریق این فروشگاه عرضه شده است [3]. هر داندلود یک خطر امنیتی بالقوه برای گوشی‌های هوشمند محسوب می‌شود؛ زیرا برنامه‌های مخرب به‌راحتی از طریق این بازارها روی دستگاه‌های کاربران قابل نصب هستند. فروشگاه‌های برنامه نقش مهمی را در تضمین امنیت گوشی‌های هوشمند ایفا می‌کنند و می‌توانند از کاربران در مقابل توسعه‌دهندگان بدافزارها

با گسترش روزافزون گوشی‌های تلفن همراه هوشمند و برنامه‌های آن‌ها، نیازمندی‌ها و الزامات جدیدی شکل گرفته و نیاز به بازارها و کتابخانه‌هایی جهت توزیع این برنامه‌ها به‌وجود آمده است. در این شرایط، کاربران به سامانه‌هایی نیاز دارند که برنامه‌ها در آن‌ها سازمان‌دهی شده و به‌صورت رایگان یا برای فروش، عرضه شده باشند. به‌منظور دستیابی به این هدف، افراد و شرکت‌ها، بازارهایی را جهت توزیع برنامه‌ها راه‌اندازی کردند که به این بازارها، «فروشگاه برنامه»^۱ گفته می‌شود. استفاده از فروشگاه‌های برنامه، یکی از ویژگی‌های کلیدی در حوزه سامانه‌های هوشمند همراه به‌شمار می‌رود. فروشگاه برنامه، مخزنی مدیریت‌شده از نرم‌افزارهای شخص ثالث است. این فروشگاه‌ها فرصت مناسبی را در اختیار توسعه‌دهندگان قرار می‌دهند تا به بازار برنامه‌های گوشی‌های هوشمند ورود کرده و کسب درآمد کنند. توسعه‌دهندگان می‌توانند با استفاده از پنل مخصوصی

¹ App Store

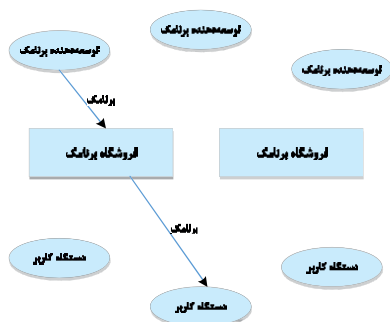
* نویسنده‌عهددار مکاتبات

منجر به وقوع حمله می‌شوند، مشخص می‌شوند. بر مبنای درخت حمله، ریسک‌های مطرح در سطح توزیع‌کنندگان برنامه‌های سامانه‌های هوشمند همراه معرفی خواهند شد. برای هر ریسکی که در این مقاله پوشش داده شده، مشخصات مرتبط با آن ریسک هم بیان شده است. از جمله این مشخصات به تهدیدها، آسیب‌پذیری‌ها و همچنین دارایی‌هایی که تحت تأثیر قرار می‌گیرند، می‌توان اشاره کرد. مطالب کامل‌تر در این خصوص در مستندات موجود در مرکز تحقیقات ایران قابل استفاده است [21].

در مقاله حاضر، در بخش ۲ زیست‌بوم توزیع برنامه‌ها را معرفی خواهیم کرد. دارایی‌ها و آسیب‌پذیری‌های حوزه مورد بحث در بخش ۳ و ۴ ارائه خواهند شد. در بخش پنجم این مقاله، ابتدا تعریفی از تهدیدها STRIDE ارائه، سپس تهدیدهای رایج در زیست‌بوم برنامه‌ها را معرفی خواهیم کرد. پس از آن در بخش ۶، درخت حمله ترسیم می‌شود. در انتها، در بخش ۷ ریسک‌های امنیتی حوزه توزیع برنامه‌ها معرفی خواهند شد.

۲- زیست‌بوم توزیع برنامه

علاوه بر «فروشگاه برنامه‌ها اپل» و «بازار اندروید گوگل»، تعداد بسیار زیادی فروشگاه دیگر نیز وجود دارند که به فعالیت مشغول هستند. برای مثال، «آمازون» فروشگاه خود را برای گوشی‌های هوشمند اندروید راه‌اندازی کرده و «مایکروسافت» فروشگاه‌های را برای تلفن‌های «ویندوز تلفن همراه» ایجاد کرده است. شرکت «سیسکو» نیز فروشگاه‌های برای عرضه برنامه‌های مخصوص تبلت‌های ساخت این شرکت توسعه داده است. بعضی از سازمان‌ها نیز اقدام به راه‌اندازی فروشگاه برنامه‌ها برای کارکنان خود کرده‌اند. در این مقاله، به مجموعه فروشگاه‌های برنامه‌ها با یک پلتفرم یکسان، «زیست‌بوم برنامه‌ها» گفته می‌شود که در شکل (۱) نشان داده شده است.



شکل - ۱: زیست‌بوم برنامه‌ها [6]

محافظت کنند [4]. به همین دلیل، مسائل متعددی از نظر امنیت و حریم خصوصی در حوزه بازارهای توزیع برنامه‌های تلفن همراه هوشمند به وجود آمده است.

این مقاله به توزیع‌کنندگان برنامه‌ها، سازمان‌ها و بخش‌های خصوصی و دولتی کمک می‌کند تا بتوانند ریسک‌های امنیتی این حوزه را شناسایی و تأثیرات آن را به کمینه برسانند. ریسک تابعی از تهدیدها است که از آسیب‌پذیری‌ها سوء استفاده می‌کند تا بتواند به دارایی‌های سیستم دست پیدا کند یا موجب وارد شدن آسیب یا خسارت به دارایی‌ها شود. ارزیابی ریسک یک فرایند نظام‌مند برای تعیین شدت ریسک و بررسی پیامدهای بالقوه ناشی از وقوع حوادث احتمالی در سازمان یا سیستم است. هدف از ارزیابی ریسک این است که به کارشناسان و متخصصان امنیتی درک درستی از مهم‌ترین ریسک‌ها داده شود تا روش‌های کنترلی مؤثری را در زمینه مواجهه با ریسک مشخص کنند و میزان کارآمدی این روش‌ها را مشخص کنند.

روشی که جهت تحلیل ریسک مورد استفاده قرار گرفته، روش ارائه‌شده توسط OWASP است که بر اساس روش‌های استاندارد بوده و برای امنیت برنامه‌ها اختصاصی و سفارشی شده است [5]. نخستین گام در این روش، شناسایی ریسک‌های امنیتی است. برای این منظور، فهرستی از دارایی‌هایی که تحت تأثیر سوء استفاده (در نتیجه رخداد ریسک) قرار خواهند گرفت، مشخص می‌شوند؛ سپس، اطلاعاتی در مورد تهدیدها، آسیب‌پذیری‌ها و تأثیر یک سوء استفاده موفق بر دارایی‌های سامانه هوشمند همراه از طریق کانال عرضه برنامه جمع‌آوری می‌شود. در این مقاله، مهم‌ترین تهدیدها و آسیب‌پذیری‌های امنیتی در حوزه بازارهای توزیع برنامه‌های تلفن همراه هوشمند معرفی می‌شوند. آژانس امنیت اطلاعات و شبکه اروپا (ENISA¹) در گزارش خود در مرجع [6]، به بررسی جامعی در خصوص حفظ امنیت سامانه‌های هوشمند همراه در حوزه بازارهای توزیع برنامه‌ها بر مبنای «مدل‌سازی تهدید» پرداخته است. مدل‌سازی تهدید رویکردی ساخت‌یافته است که به سازمان‌ها و سیستم‌ها این امکان را می‌دهد تا اقدامات متقابل امنیتی برای کاهش اثرات تهدیداتی که دارایی‌ها و منابع آن‌ها را در معرض خطر قرار می‌دهند، طراحی و اعمال کنند؛ سپس، بر اساس ترسیم درخت حمله، تهدیدهایی که

¹ The European Network and Information Security Agency

- مرزهای اعتماد^۵ (به صورت خط چین قرمز رنگ نمایش داده می‌شوند) لبه‌های کنترل را مشخص می‌کنند. برای مثال، مرز اعتماد بین گوشی هوشمند و فروشگاه برنامه ترسیم می‌شود؛ زیرا گوشی هوشمند تحت کنترل کاربر قرار دارد و فروشگاه برنامه توسط مالک فروشگاه کنترل می‌شود.

۲-۲- مدل سازی زیست‌بوم برنامه

نمودار کامل جریان داده برای توزیع برنامه در شکل (۲) نشان داده شده است [6]. در گوشه بالا سمت چپ نمودار در شکل (۲)، نحوه تعامل توسعه‌دهنده برنامه (I1) با فروشگاه نشان داده شده است. توسعه‌دهنده برنامه یک برنامه جدید یا به‌روزرسانی یک برنامه موجود را به چک پذیرش (P1) می‌تواند ارسال کند. چک پذیرش بررسی می‌کند که آیا برنامه برای قرارگیری در فروشگاه مناسب است یا خیر. گوشه بالا سمت راست نمودار، نحوه تعامل کنترل‌کننده فروشگاه برنامه (I2) را نشان می‌دهد. کنترل‌کننده فروشگاه، برنامه‌ها را جهت قرارگیری در فروشگاه تأیید می‌کند (P1). برنامه جدید یا برنامه به‌روزرسانی شده و همچنین تأییدیه تصویب برنامه از سوی کنترل‌کننده فروشگاه برنامه، ورودی‌های فرایند P1 را تشکیل می‌دهند. پس از انجام چک پذیرش، برنامه تأییدشده جهت قرارگیری در فروشگاه بسته‌بندی می‌شود (P2). در فرایند P2، فراداده‌ها به برنامه افزوده می‌شوند. فراداده‌ها شامل توصیفی از برنامه و فهرستی از مجوزهای دسترسی مورد نیاز برنامه روی دستگاه کاربر است. به این فراداده‌ها در اصطلاح «ظهارنامه^۶» گفته می‌شود. فرایند P2 برنامه تأییدشده را به همراه فراداده‌ها در انبار داده فروشگاه (D1) ذخیره می‌کند. علاوه بر این، کنترل‌کننده می‌تواند برنامه‌ها را امحا کند (P3). امحای یک برنامه بر اساس شکایتهای صورت‌گرفته از آن برنامه صورت می‌گیرد. ورودی فرایند P3 دستور ابطال برنامه از سوی کنترل‌کننده فروشگاه است که عملیات امحای برنامه را از انبار داده فروشگاه انجام می‌دهد. در طی فرایند امحا، برنامه‌های نصب‌شده روی دستگاه‌های کاربر از دستگاه‌های کاربر نیز حذف می‌شوند که به این کار kill-switch می‌گویند و با همکاری فرایند P6 این کار انجام می‌گیرد.

در زیست‌بوم برنامه، توسعه‌دهندگان برنامه‌ها را ایجاد و سپس اقدام به فروش یا عرضه رایگان آن‌ها به کاربران می‌کنند. برنامه، نرم‌افزاری است که عملکرد و کارایی دستگاه کاربر (تلفن همراه هوشمند یا مرورگر) را بهبود می‌دهد. این فروشگاه‌ها، برنامه‌ها را از توسعه‌دهندگان دریافت کرده و آن‌ها را به کاربران می‌فروشند (یا توزیع می‌کنند) و در این بین، نقش واسطه^۱ را ایفا می‌کنند. به‌طور معمول فروشگاه‌ها امکان نمایش اعتبار هر برنامه را فراهم می‌کنند (برای نمونه، تعداد دانلودهای انجام‌شده برای هر برنامه، نظرات یا انتقادات کاربران و رأی کاربران). در ادامه این مقاله، به تهدیدهایی که از سوی برنامه‌های ناامن یا بدافزارها به زیست‌بوم برنامه وارد می‌شوند، می‌پردازیم. پیش از آن، ابتدا نمودار جریان داده‌ها را در زیست‌بوم برنامه معرفی می‌کنیم.

۲-۱- نمودار جریان داده‌ها در زیست‌بوم

توزیع برنامه

در این بخش، نمودار جریان داده‌ها را برای زیست‌بوم برنامه نمایش می‌دهیم. مدل ارائه‌شده در این بخش، به‌عنوان مبنایی برای تحلیل تهدیدها به روش STRIDE به‌شمار می‌رود که در بخش ۵ به آن پرداخته خواهد شد. به‌طور کلی، نمودار جریان داده‌ها شامل مؤلفه‌های زیر است:

- تعامل‌گران^۲ (با مستطیل نشان داده می‌شوند) ورودی را تولید کرده و خروجی (به یک فرایند) را همانند کاربران مصرف می‌کنند. در نمودار جریان داده کاربر، تعامل‌گران عبارتند از: کاربر دستگاه، توسعه‌دهنده برنامه، کنترل‌کننده فروشگاه برنامه.
- فرایندها^۳ (به شکل دایره نشان داده می‌شوند) تابع خاصی را انجام می‌دهند. یک یا چندین ورودی را دریافت و یک یا چندین خروجی را همانند بسته‌بندی و ذخیره برنامه در انبار داده فروشگاه تولید می‌کنند.
- انبار داده‌ها^۴ (با دو خط موازی نشان داده می‌شوند) برای ذخیره‌ی موقت یا دائمی داده‌ها همانند سیستم فایل و پایگاه داده استفاده می‌شوند.

¹ Broker

² Interactors

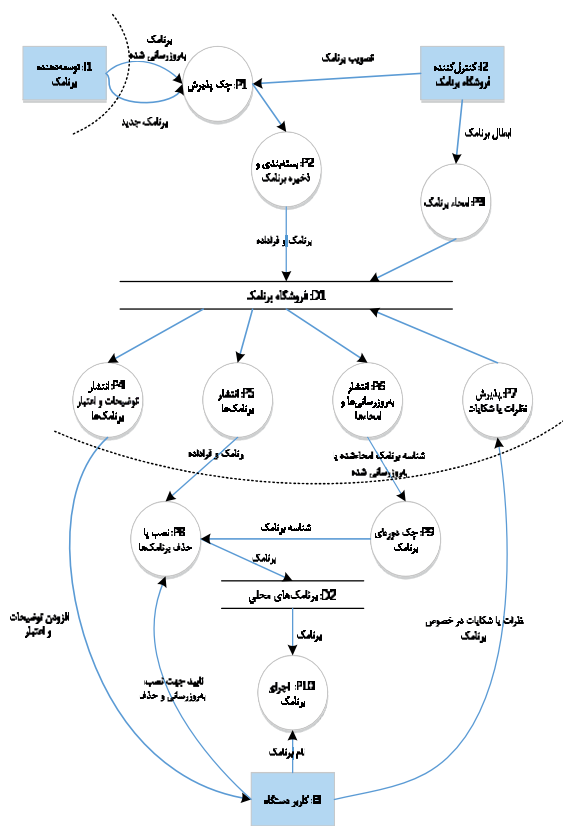
³ Processes

⁴ Datastores

⁵ Trust boundaries

⁶ Manifest

فروشگاه درج شده بود، توسط فرایند P6 خوانده شده و در فروشگاه منتشر می‌شود. فرایند P9 شناسه برنامه‌ی را که بایستی امحا شود از فرایند P6 دریافت کرده و آن را جهت حذف برنامه‌ی از روی انبار داده برنامه‌های محلی ذخیره‌شده روی دستگاه به فرایند P8 ارسال می‌کند. فرایند P8 علاوه بر شناسه برنامه‌ی امحاشده، تأییدیه حذف برنامه‌ی از سوی کاربر است و به این ترتیب، عملیات حذف برنامه‌ی از روی انبار داده دستگاه کاربر انجام گیرد. رویه دریافت به‌روزرسانی‌ها روی دستگاه کاربر نیز مشابه دریافت امحای برنامه‌ی است.



(شکل ۲-): نمودار جریان داده در توزیع برنامه [6]

مدلی که از زیست‌بوم برنامه‌ی در این بخش ارائه شد، یک مدل کلی بر اساس تحلیل بازار اندروید، فروشگاه برنامه‌ی iPhone، و فروشگاه افزونه Mozilla است و خلاصه‌ای از نحوه عملکرد زیست‌بوم‌های برنامه‌ی را بیان می‌کند. در رویکرد «مدل‌سازی تهدید» پس از ارائه نمودار جریان داده‌ها، در مرحله بعد لازم است که تهدیدها شناسایی شوند. برای این منظور از مدل STRIDE جهت شناسایی و طبقه‌بندی تهدیدها استفاده می‌شود [7]. در بخش ۵ به تشریح مدل‌سازی تهدید خواهیم پرداخت.

قسمت پایین نمودار، نحوه تعامل کاربر دستگاه (I3) با فروشگاه را نشان می‌دهد. کاربر دستگاه می‌تواند توصیف و اعتبار هر برنامه‌ی را ببیند (P4). برای این منظور، فرایند P4 به‌ازای هر برنامه‌ی که در انبار داده فروشگاه وجود دارد، توضیحات و اعتبار مربوط به برنامه‌ی را که از سوی سایر کاربران منتشر شده‌اند، به کاربر دستگاه نمایش می‌دهد. امکان انتشار برنامه‌ی منتشرشده توسط فروشگاه (P5) و همچنین تأییدیه نصب از کاربر دستگاه به‌عنوان ورودی فرایند نصب (P8) دریافت می‌شود. فرایند P5 برنامه‌ی ذخیره‌شده را در انبار داده فروشگاه به‌عنوان ورودی دریافت کرده و در ویتترین فروشگاه به نمایش درمی‌آورد. در صورت انتخاب برنامه‌ی از سوی کاربر جهت نصب، فرایند P5 برنامه‌ی را به همراه فراداده‌های جهت قرارگیری روی دستگاه کاربر به فرایند P8 ارسال می‌کند. تأییدیه نصب از سوی کاربر و همچنین برنامه‌ی و فراداده‌های آن، ورودی‌های فرایند P8 را تشکیل می‌دهند. در طی انجام فرایند نصب در فرایند P8، یک برنامه‌ی در انبار داده مربوط به برنامه‌ی محلی نصب‌شده روی دستگاه کاربر (D2) ذخیره می‌شود. بعد از نصب، کاربر دستگاه می‌تواند برنامه‌ی را اجرا کند (P10). مهم‌ترین فرایند انجام‌گرفته در سمت دستگاه کاربر، فرایند اجرای برنامه‌ی نصب‌شده روی دستگاه خود را داشته باشد، بایستی نام برنامه‌ی را به‌عنوان ورودی به فرایند P10 اعلام کند تا فرایند P10 از انبار داده برنامه‌ی محلی (ذخیره‌شده روی دستگاه کاربر) برنامه‌ی انتخابی کاربر را روی سیستم‌عامل اجرا کند. کاربر همچنین می‌تواند نظرات و شکایات خود درباره برنامه‌ی را ثبت کند. این نظرات و شکایات در فروشگاه برنامه‌ی پردازش و ذخیره می‌شوند (P7). برای این منظور نظرات و شکایات از سوی کاربر به‌عنوان جریان داده ورودی به فرایند P7 وارد شده و پس از آن فرایند P7 جریان‌های داده ورودی را در انبار داده فروشگاه ذخیره می‌کند تا قابل رؤیت برای کاربران دیگر فروشگاه باشد.

برای اطمینان از این که دستگاه کاربر به‌روزرسانی‌ها و امحایها را مرتباً دریافت می‌کند، بررسی‌های دوره‌ای برای برنامه‌های به‌روزرسانی‌شده یا امحاشده انجام می‌گیرد (P9). به‌روزرسانی‌ها و هشدارهای امحا به کاربر اعلام می‌کنند که برنامه‌ی به‌روز شده را نصب یا یک برنامه‌ی امحاشده را حذف کند. دستور ابطال برنامه‌ی (صادرشده از سوی کنترل‌کننده فروشگاه) که پیش از این از طریق فرایند P3 در انبار داده

۳- دارایی‌ها

نخستین فعالیت در انجام فرایند ارزیابی ریسک، شناسایی دارایی‌های حوزه مورد بررسی است تا پس از آن بتوان احتمال وقوع یک تهدید را بر اساس تعداد آسیب‌پذیری‌های ممکن و همچنین سهولتی نسبی که یک مهاجم از آن آسیب‌پذیری‌ها می‌تواند سوء استفاده کند یا برای مهاجم جذاب باشد، تعیین کرد. میزان تأثیر یک تهدید را بر اساس ارزش دارایی‌هایی که متأثر از آن تهدید هستند، می‌توان تعیین کرد؛ لذا لازم است فهرستی از دارایی‌هایی که در سامانه هوشمند همراه دارای ارزش و اهمیت هستند و باید در حوزه توزیع برنامه‌ها مورد محافظت قرار گیرند، تهیه شود.

منابع مختلف، دسته‌بندی‌های متفاوتی را برای دارایی‌ها در سامانه‌های هوشمند همراه ذکر کرده‌اند. گزارش ENISA شش دسته دارایی را مشخص کرده است که عبارتند از: داده‌های شخصی، مالکیت معنوی شرکت^۱، اطلاعات (دولتی) طبقه‌بندی‌شده^۲، دارایی‌های مالی^۳، دسترسی‌پذیری^۴ و عملکرد^۵ دستگاه‌ها و سرویس‌ها؛ و اعتبار شخصی و سیاسی [8]. در مطالعه دیگری، دارایی‌های سامانه هوشمند همراه به صورت زیر تعریف شده است [9]:

- دستگاه (دستگاه فیزیکی)
- ارتباطات (ارتباطات صوتی و پیام‌رسانی)
- داده‌های ذخیره‌شده (برنامه‌های کاربردی برون خط^۶ و سایر داده‌های مربوط به کاربر)
- برنامه‌ها (نقشه و جهت‌یابی، شبکه‌های اجتماعی و سایر برنامه‌ها)
- دسترسی به داده‌ها (رایانامه، دسترسی وب، بلوتوث یا مادون قرمز)

همچنین، در ارزیابی ریسک صورت‌گرفته در حوزه سامانه‌های هوشمند همراه، دارایی‌ها به چهار دسته کلی دستگاه، اطلاعات^۷، داده‌ها و برنامه‌ها تقسیم‌بندی شده‌اند [10]. در این مطالعه، دارایی‌های فروشگاه‌های برنامه به پنج دسته کلی (۱) دستگاه، (۲) اطلاعات، (۳) داده‌ها، (۴)

برنامه‌ها و (۵) سرویس‌ها تقسیم‌بندی می‌شوند. فهرست کامل دارایی‌ها به همراه شرح کاملی از هر یک در جدول (۱) مشخص شده‌اند. این دسته‌بندی، جامع و کامل بوده و در بردارنده موارد مشخص شده در دسته‌بندی‌های دیگر نیز است.

(جدول-۱): انواع دارایی‌های تحت تأثیر در ارزیابی ریسک فروشگاه‌های برنامه [10]

توضیحات	دارایی
دارایی‌های از نوع دستگاه شامل دستگاه فیزیکی و منابع آن (همانند باتری، حافظه اصلی ^۸ ، پردازنده، کارت‌های حافظه و سیم‌کارت و کلیه متعلقات مربوط به دستگاه تلفن همراه) هستند. لازم به ذکر است که داده‌های ذخیره‌شده جزو این نوع دارایی محسوب نمی‌شوند. سرویس‌های پردازش و ذخیره اطلاعات در فروشگاه‌های برنامه نیز در این دسته قرار دارند.	A1: دستگاه
سامانه‌های هوشمند همراه از چهار کانال اتصالی استفاده می‌کنند که عبارتند از: (۱) سرویس‌های GSM همانند ارسال پیام (SMS)، EMS و کلیه سرویس‌های مشابه) و تماس‌های صوتی (۲) واسط PAN: کانال‌های داده با برد کوتاه و رایگان (همانند بلوتوث، IrDA، و سایر واسط‌های PAN) (۳) WLANs کانال داده پرسرعت (همانند Wi-Fi و WiMAX و کلیه شبکه‌های محلی بی‌سیم) (۴) شبکه سلولی که ارتباط اینترنت را در سرعت‌های متغیر (بسته به فناوری حامل ^۹ می‌تواند GPRS، HSDPA، UMTS، LTE و هر شبکه سلولی نسل آینده باشد) ارائه می‌دهد.	A2: اتصالات
داده‌ها در سامانه هوشمند همراه انواع متنوعی می‌توانند داشته باشند که عبارتند از: • داده‌های شخصی: که مربوط به فردی با هویت مشخص هستند. این نوع داده‌ها خصوصی بوده و نباید در اختیار عموم قرار گیرند (همانند تصاویر و ویدیوها). • داده‌های سازمانی (یا مالکیت معنوی شرکت): به داده‌هایی گفته می‌شوند که دارای اهمیت تجاری و اقتصادی برای سازمان هستند. مثال‌هایی از این نوع داده‌ها می‌توانند اطلاعات بازار یا اطلاعات محصولات (زیر نظر طراحی سازمان) باشند. افشای ناخواسته این داده‌ها به عموم مردم و یا رقبا ممکن است عواقبی همچون نقض کپی‌رایت و از بین رفتن حسن نیت ^{۱۰} را به دنبال داشته باشد.	A3: داده‌ها

¹ Corporate intellectual property

² Classified

³ Financial assets

⁴ Availability

⁵ Functionality

⁶ Offline

⁷ Connectivity

⁸ RAM

⁹ Carrier

¹⁰ Loss of Goodwill

برنامک و کاربران دستگاه تشکیل شده است. به همین منظور باید آسیب‌پذیری‌های مربوط به هر سه ناحیه اعتماد معرفی شوند تا از این طریق بتوان ریسک‌های امنیتی مربوط به سامانه‌های هوشمند همراه را در حوزه توزیع کنندگان برنامک‌ها استخراج کرد.

منابع متعددی به جمع‌آوری اطلاعات در مورد آسیب‌پذیری‌ها در حوزه سامانه‌های هوشمند همراه پرداخته‌اند. یکی از این منابع، پایگاه vulnerability-lab است که فهرستی از آسیب‌پذیری‌های تلفن همراه که بر سیستم‌عامل، برنامه‌های کاربردی، نرم‌افزار و سخت‌افزار تأثیر می‌گذارند، معرفی کرده است [12]. پایگاه آسیب‌پذیری‌های تلفن همراه (MVD³) نیز منبعی دیگری است که آسیب‌پذیری‌های گزارش‌شده را در سراسر جهان برای پلتفرم‌های تلفن همراه جمع‌آوری می‌کند [13]. این پایگاه به کاربران این امکان را می‌دهد تا آسیب‌پذیری‌های خاص پلتفرم تلفن همراه خود و نسخه خاص آن جستجو کنند. پلتفرم‌های گوشی‌های هوشمند یا تبلت‌هایی که توسط این پایگاه داده پوشش داده می‌شوند شامل اندروید، iOS، ویندوز فون و بلک‌بری هستند. مؤسسه ملی فناوری و استانداردها (NIST⁴) نیز در گزارش خود به توصیف آسیب‌پذیری‌های برنامک مختص پلتفرم‌های iOS و اندروید پرداخته است [14]. نکته قابل ذکر این است که آسیب‌پذیری‌ها مطرح‌شده توسط این منابع مختص پلتفرم یا تولیدکننده سخت‌افزار و سیستم‌عامل هستند.

پروژه امنیت برنامه کاربردی وب باز (OWASP) در راستای ایمن‌سازی طراحی، پیاده‌سازی، توسعه و آزمایش پروژه‌های نرم‌افزاری فعالیت می‌کند. مستندات، ابزارها و چک‌لیست‌های لازم OWASP در جهت برطرف کردن آسیب‌پذیری‌های امنیتی متداول توسعه داده شده‌اند. این سازمان در پروژه امنیت تلفن همراه خود فهرستی از شاخص‌ترین آسیب‌پذیری‌های رایج در زمینه برنامک‌های تلفن همراه را در سرتاسر جهان را ارائه می‌دهد. آخرین آسیب‌پذیری‌های منتشرشده در سال ۲۰۱۶ توسط OWASP عبارتند از [15]:

- استفاده نادرست از پلتفرم (Improper platform usage)
- ذخیره نامن داده‌ها (Insecure data storage)
- ارتباطات نامن (Insecure communication)

³ Mobile Vulnerability Database

⁴ National Institute of Standards and Technology

- داده‌های دولتی: این داده‌ها بر روی نظم عمومی، روابط بین‌الملل یا کارایی سازمان‌های ارائه‌دهنده سرویس‌های عمومی تأثیر می‌گذارند. این نوع از داده‌ها با داده‌های کسب‌وکار متفاوت بوده زیرا دارای اهمیت ملی و بین‌المللی هستند.
- داده‌های مالی: به اطلاعات ثبت‌شده مربوط به تراکنش‌های مالی و منابع مالی فعلی اشاره دارند. تغییر غیرمجاز، افشا یا عدم دسترسی‌پذیری این نوع از داده‌ها ممکن است منجر به خسارات مالی یا نقض قرارداد شوند.
- داده‌های احراز اصالت: به اعتبارنامه‌های کاربر همانند رمز عبور، PINs، بیومتریک‌ها و داده‌های مربوط به احراز اصالت گفته می‌شوند. دسترسی غیرمجاز به این اطلاعات تأثیراتی همچون خسارت مالی، افشای اطلاعات شخصی و عواقب حقوقی را به دنبال دارد.
- داده‌های ارتباطی / سرویس: به داده‌هایی اشاره دارند که در برقراری ارتباطات شبکه موردنیاز هستند. این داده‌ها شامل شناسه‌های اتصال همانند Wi-Fi MAC، IMSI یا IMEI و کلیه داده‌هایی که جهت برقراری ارتباط مورد نیاز هستند، می‌شوند.

A4: برنامک‌ها به عنوان سرویس‌های قابل ارائه به کاربر تلقی می‌گردد.

A5: سرویس‌هایی که توسط فروشگاه برنامک مورد استفاده قرار می‌گیرند (مثالی در این زمینه تحلیل گره‌های برخط هستند).

۴- آسیب‌پذیری‌ها

طبق توصیه RFC 2828، آسیب‌پذیری یک رخنه یا ضعف در طراحی، پیاده‌سازی، عملکرد و مدیریت سیستم است که در جهت نقض سیاست امنیتی سیستم مورد سوء استفاده می‌تواند قرار گیرد [11]. بر اساس تعریفی که از آسیب‌پذیری در امنیت سیستم‌های رایانه‌ای شده است، آسیب‌پذیری یک ضعف است که به مهاجم اجازه می‌دهد ضمانت^۲ اطلاعاتی یک سیستم را به مخاطره بیندازد. همانند سیستم‌های رایانه‌ای، آسیب‌پذیری‌های متعددی در سامانه‌های هوشمند همراه وجود دارند که آن‌ها را مستعد وقوع یک حمله هستند. با توجه به اینکه هدف این مقاله، شناسایی ریسک‌های امنیتی در زیست‌بوم برنامک است، لذا باید آسیب‌پذیری‌های مربوط به این زیست‌بوم شناسایی شوند. همان‌گونه که در شکل (۲) قابل مشاهده است، زیست‌بوم برنامک از سه ناحیه اعتماد فروشگاه برنامک، توسعه‌دهنده

¹ Identifier

² Assurance

بهبودهای امنیتی که فرایند بازنگری به دنبال دارد، روش‌های بازنگری برنامه کاربری در توزیع وصله‌ها نوعی گلوگاه^۴ محسوب می‌شوند. این امر یک مانع جدی در عرضه به‌موقع برنامه‌ها تلقی می‌شود.

انجام ارزیابی جامع و کامل که در آن تک‌تک برنامه‌های یک وصله آزمایش شوند (حتی برای تعداد کمی از محصولات) دشوار است. مدیریت در یک سامانه به‌روزرسانی امنیتی برای ده‌ها محصول مختلف (که با توجه به نوع پلتفرم و سیستم‌عامل متفاوت هستند و یا در حال حاضر بسیار قدیمی شده‌اند) بسیار دشوار خواهد بود. اگر وصله‌های امنیتی برای تمام مدل‌ها به‌طور کامل آزمایش نشده باشند، به‌روزرسانی‌های خودکار می‌توانند آسیب بیشتری را برای گوشی‌های تلفن همراه به دنبال داشته باشند؛ لذا استقرار چنین زیرساختی می‌تواند برای بسیاری از تولیدکنندگان محصولات نرم‌افزاری چالش برانگیز باشد.

2-1-7- قابلیت‌های محدود در راه‌کارهای امنیتی

شخص ثالث (مدیریت امنیتی متمرکز^۵)

بسیاری از پلتفرم‌ها، امکانات عملکردی محدودی را برای سرویس‌های امنیتی شخص ثالث ارائه می‌دهند. به‌عنوان مثال، در برخی از پلتفرم‌ها، برنامه‌ها اجازه دسترسی به فرایندها را ندارند، مگر این‌که توسط گواهی‌نامه توسعه‌دهنده امضا شده باشند. برخی از پلتفرم‌ها نیز اجازه اجرا به انواع خاصی از برنامه‌ها را در پس‌زمینه^۶ نمی‌دهند. این امر موجب می‌شود که ارائه سرویس‌های امنیتی (که مبتنی بر نظارت بر فعالیت‌های برنامه‌ها هستند) دشوار شود. این مسأله، مسئولیت بیشتری را بر عهده ارائه‌دهندگان سیستم‌عامل و فروشگاه برنامه قرار می‌دهد.

3-1-7- آسیب‌پذیری‌های اعتبار

وجود آسیب‌پذیری‌ها در سامانه‌های اعتبار که برای برنامه‌ها به کار گرفته می‌شوند، ممکن است به یک مهاجم این امکان را دهد که اعتبار یک برنامه را به صورت جعلی (با اعتبار بیشتر) نمایش دهد و در نتیجه اعتماد بی‌مورد را از سوی کاربران کسب کند. این آسیب‌پذیری‌ها عبارتند از عدم احراز اصالت برای رأی‌دهندگان، امکان رأی دادن‌های متعدد و رأی‌هایی که با توجه به اهمیت برنامه مدنظر وزن‌دهی نشده‌اند و سایر موارد.

⁴ Bottleneck

⁵ Centralized

⁶ Background

- احراز اصالت ناامن (Insecure Authorization)
- رمزنگاری ناکافی (Insufficient cryptography)
- صدور مجوز ناامن (Insecure Authorization)
- کیفیت کد مشتری (Client code quality)
- دستکاری کد (Code tampering)
- مهندسی معکوس (Reverse Engineering)
- عملکرد خارج از قلمرو (Extraneous functionality)

همان‌گونه که مشاهده می‌شود، آسیب‌پذیری‌های مطرح‌شده توسط OWASP دربردارنده ناحیه اعتماد توسعه‌دهنده و دستگاه کاربر بوده و اشاره‌ای به آسیب‌پذیری‌های حوزه فروشگاه برنامه ندارند. آژانس امنیت اطلاعات و شبکه اروپا (ENISA) با کمک افراد خبره فعال در حوزه سامانه‌های هوشمند همراه و با بهره‌گیری از اطلاعات منتشرشده توسط OWASP، آسیب‌پذیری‌های متعددی را که ممکن است در این سامانه‌ها وجود داشته باشند، استخراج و معرفی کرده است [8]. این آسیب‌پذیری‌ها مختص سامانه‌های هوشمند همراه هستند و فارغ از پلتفرم فروشنده و تولیدکننده سخت‌افزار سیستم‌عامل معرفی شده‌اند. پس از مطالعات بررسی‌های به‌عمل آمده، تشخیص داده شد که آسیب‌پذیری‌های مطرح‌شده برای سامانه‌های هوشمند همراه در مرجع [8] قادرند آسیب‌پذیری‌های مربوط به هر سه ناحیه اعتماد زیست‌بوم یعنی دستگاه کاربر، توسعه‌دهنده و فروشگاه برنامه را مورد پوشش کامل قرار دهند. در ادامه، به معرفی آسیب‌پذیری‌هایی می‌پردازیم که ممکن است در فروشگاه‌های برنامه سامانه‌های هوشمند همراه وجود داشته باشد.

7-1-7- آسیب‌پذیری‌های منجر به نصب بدافزار: در این مورد، دسته‌ای از آسیب‌پذیری‌ها مطرح هستند که به موارد زیر می‌توان اشاره کرد:

1-7-1- ضعف در عملیات وصله‌کردن^۱

در فروشگاه برنامه با مدل walled-garden^۲، هر وصله پیش از آن که برای استفاده روی یک دستگاه به کار گرفته شود، از فرایند بازنگری^۳ فروشگاه برنامه عبور داده می‌شود. به‌رغم

¹ Patching

^۲ مدل walled garden یا «زیست‌بوم بسته» یا «پلتفرم بسته» به سیستمی گفته می‌شود که در آن سرویس‌دهنده کنترل کامل روی برنامه، محتوا و رسانه دارد و دسترسی به برنامه‌ها یا محتواهای تأییدنشده را محدود می‌کند. این مفهوم در مقابل مفهوم «پلتفرم باز» قرار دارد.

³ Vetting

V1-4- عدم وجود فرایندهای بررسی کد / برنامه

به دلیل فشارهای وارده از سوی بازار، پلتفرم‌های تلفن همراه تمایل دارند که به صورت باز^۱ عرضه شوند و توسعه‌دهندگان را نیز تشویق می‌کنند تا به سوی توسعه باز حرکت کنند؛ لذا توسعه‌دهندگان برنامه‌های خاص ثالث نقش مهمی را در زیست‌بوم‌های دستگاه تلفن همراه ایفا می‌کنند. علاوه بر این، «زیرساخت‌های امضای برنامه» و «چارچوب‌های امنیتی سطح سیستم‌عامل» نیز به عنوان یک مانع بزرگ برای توسعه برنامه‌ها توسط اشخاص ثالث در نظر گرفته می‌شوند. با توجه به موارد گفته شده، امکان تعریف فرایندهای مشخص و دقیق برای بررسی کد/برنامه در این پلتفرم‌ها دشوار خواهد بود.

V1-5- امضای برنامه

ممکن است کاربران این تصور را به غلط داشته باشند که برنامه‌های امضا شده در مقایسه با برنامه‌هایی که امضا نشده‌اند قابل اعتمادتر هستند؛ در حالی که ممکن است چنین استنباطی درست نباشد. واضح است که در برخی موارد، امضای برنامه فقط یک اظهارنامه است که نشان می‌دهد برنامه بر اساس معیارهای خاصی بررسی شده است؛ اما در مواردی دیگر، امضای برنامه یک سازوکار برای ایجاد منبع^۲ برنامه است. ریسک‌های ناشی از بدافزارها و جاسوس‌افزار^۳ها نسبت به تلفن‌های همراه قدیمی‌تر افزایش یافته است؛ زیرا امکان سوء استفاده و سوءتعبیر در سازوکارهایی که به کاربران اجازه می‌دهند برنامه‌های قابل اعتماد^۴ را از برنامه‌های غیر قابل اعتماد^۵ تشخیص دهند (همانند سامانه‌های اعتباردهی و امضای دیجیتال) وجود دارد.

V1-6- قابلیت باز کردن قفل سامانه هوشمند

در این آسیب‌پذیری، کاربر اقدام به غیرفعال کردن برخی از تنظیمات امنیتی دستگاه خود می‌کند. دستگاه تلفن همراه که قفل آن باز شده است به کاربر اجازه می‌دهد تا برنامه‌هایی را نصب کند که فرایند بازنگری فروشگاه روی آن‌ها انجام نگرفته است. این موضوع منجر به موقعیت‌هایی می‌شوند که کاربران در اغلب موارد در مورد اجرای کدی که

¹ Open

² Origin

³ Spyware

⁴ Trusted

⁵ Untrusted

هیچ‌گونه فرایند بررسی روی آن صورت نگرفته است و یا از اجرای کد با مجوزهای ریشه^۶ اطلاع ندارند.

V2- کانال‌های مخفی / جعبه شنی ضعیف: راه‌های گریز متعددی در طرح جعبه شنی وجود دارند. به عنوان نمونه، اگر cache صفحه‌کلید (پایگاه داده‌ای از کلمات که به طور مکرر توسط کار تایپ شده است) در دسترس عموم قرار گیرد (که در اغلب موارد این امر اتفاق می‌افتد)، به برنامه‌ها این امکان را می‌دهد که به داده‌های شخصی کاربران دسترسی داشته باشند و از داده‌های مربوط به سایر برنامه‌ها نیز استفاده کنند. به بسیاری از برنامه‌ها نیز اجازه دسترسی به کتابچه نشانی کاربر که به طور معمول حاوی اطلاعات بسیار حساس است (به عنوان مثال، کاربران جزئیات حساب بانکی خود را به عنوان یک ورودی در دفترچه نشانی ذخیره و پنهان می‌کنند) اعطا می‌شود. برای انتقال مخفیانه داده‌های خصوصی بین برنامه‌ها یا انتقال به یک مهاجم نیز ممکن است از واسط‌های شبکه استفاده شود (به عنوان مثال backdoor در برنامه پیامک به سادگی قابل پیاده‌سازی است).

در برخی از پلتفرم‌های گوشی‌های هوشمند، داده‌های مکانی در نام فایل^۷های عکس یا فراداده‌های فایل افزوده می‌شوند. اگر این تصاویر در اختیار سایر برنامه‌ها قرار گیرند یا در شبکه‌های اجتماعی بارگزاری شوند، از کاربران خواسته می‌شود که موافقت خود را برای دسترسی به گالری تصاویر اعلام کنند؛ در حالی که این مجوز برای دسترسی به داده‌های مکانی نبوده است (در صورتی که کاربر این اجازه را صادر کرده است). این امر به منزله یک کانال مخفی تلقی می‌شود؛ به عنوان مثال، یک کاربر ممکن است بدون این که متوجه باشد نام فایل، حاوی داده‌های مکانی است، عکسی را در یک وبلاگ عمومی قرار دهد.

V3- ضعف در تأیید مجوزهای دسترسی توسط کاربر:

بسیاری از پلتفرم‌های سامانه هوشمند همراه، برای دسترسی برنامه‌ها به داده‌ها و پیام‌های مختلف (همانند پیام‌های هشدار^۸) در زمان نصب روی تلفن همراه موافقت^۹ کاربر را از او درخواست می‌کنند. مشکلات متعددی در این زمینه وجود دارند که در ادامه به آن‌ها اشاره می‌کنیم.

⁶ Root privileges

⁷ Filename

⁸ Push notification

⁹ Consent

در مقایسه با رایانه‌های شخصی و لپ‌تاپ‌ها، واسطه‌های کاربر به‌طور معمول بسیار محدودتر هستند؛ به این معنا که ذخیره‌سازی اعتبارنامه‌ها روی دستگاه با احتمال بیشتری انجام می‌شود و احراز اصالت کاربر نیز نمی‌تواند به‌طور مکرر انجام شود (یک راهکار ممکن در این زمینه احراز اصالت بیومتریک است). به‌عنوان نمونه، درخواست برای احراز اصالت کاربر بر روی یک تلفن همراه هوشمند در مقایسه با یک رایانه شخصی مخاطره‌آمیزتر است.

کاربران زمان و تعهد کافی برای ارزیابی درخواست‌های مجوز دسترسی را ندارند؛ حتی اگر آن را به بررسی یک درخواست (و آن هم در زمان نصب) محدود کنند.

مجوزهای دسترسی حاوی جزئیات کافی درخصوص ریسک‌های ناشی از اعلام موافقت کاربر نیستند. به‌عنوان مثال، اعطای دسترسی به فهرست کلماتی که به‌دفعات تایپ می‌شوند (در Cache صفحه‌کلید) ممکن است از نظر بسیاری از کاربران بی‌ضرر باشد، درحالی‌که این کار رمزهای عبور را فاش می‌کند.

به‌طور معمول برای کاربران دشوار است که مجوزهای دسترسی که آن‌ها پس از درخواست اولیه اعطا کرده‌اند را مجدداً بررسی کنند و/یا تغییر دهند. این امکان که بتوان سیاست‌های کلی برای مجوزهای دسترسی اعطاشده تنظیم کرد، وجود ندارد (به‌عنوان مثال، هر برنامه‌ای را که برای اهداف بازاریابی تهیه شده است و اجازه دسترسی به داده‌های مکانی را درخواست می‌کند، نصب نکنید).

۷۴- ضعف در رمزنگاری: در برخی از پیاده‌سازی‌های رمزنگاری سامانه‌های هوشمند همراه نقاط ضعف متعددی یافت شده است که این امر موجب می‌شود حفاظت از داده‌های دستگاه به‌شکل مطلوبی انجام نگیرد. این نقاط ضعف زمانی خود را نشان می‌دهند که یک مهاجم دسترسی فیزیکی به دستگاه (دستگاهی که گم شده یا به سرقت رفته است) پیدا می‌کند. علاوه‌براین، اثربخشی^۱ سازوکارهای رمزنگاری به‌شدت به رویه‌های فنی که برای مدیریت کلیدهای رمزنگارانه^۲ استفاده می‌شوند، وابسته هستند.

۷۵- ضعف در احراز اصالت توسعه‌دهنده و توزیع‌کننده برنامه: جعل هویت^۳ یک نام تجاری قابل

^۱ Effectiveness

^۲ Cryptographic

^۳ Impersonate

اعتماد مانند برنامه بانکداری (و قراردادن در فروشگاه برنامه جهت عرضه) یا جعل وب‌سایت یک فروشگاه برنامه به‌سادگی امکان‌پذیر است. به‌منظور جلوگیری از جعل هویت، لازم است، توسعه‌دهندگان و توزیع‌کنندگان برنامه‌ها احراز اصالت شوند. ممکن است هیچ PKI یا زیرساخت قابل اعتماد دیگری برای تضمین هویت توسعه‌دهندگان وجود نداشته باشد.

۷۶- عدم وجود بهروشهایی برای حفاظت از حریم خصوصی: این آسیب‌پذیری به‌خصوص برای توسعه‌دهندگان مطرح می‌شود؛ زیرا بهروشهایی در زمینه حریم خصوصی در اختیار توسعه‌دهندگان گوشی‌های هوشمند وجود ندارند. با توجه به ریسک‌های حریم خصوصی، بسیاری از این ریسک‌ها به ویژگی‌های خاص سامانه‌های هوشمند همراه وابسته هستند که یک مسأله مهم تلقی می‌شود.

۷۷- عدم آگاهی کاربر: این آسیب‌پذیری فارغ از نوع پلتفرم است؛ اما به‌عنوان یک عامل در برخی از سناریوهای ریسک محسوب می‌شود. یکی از عوامل اصلی در افشای غیرعمدی اطلاعات، عدم آگاهی کاربران از پیامدهای موافقت با انواع خاصی از افشای اطلاعات است.

۵- تهدیدهای امنیتی

در این بخش تهدیدهای امنیتی، حملات و مهاجمانی را که در زیست‌بوم برنامه وجود دارند، معرفی می‌کنیم. در این مقاله فرض شده است که مهاجمان سایبری، کاربران، مشتریان یا متخصصین در سازمان‌های دولتی و خصوصی (که اقدام به بازرسی یا نصب برنامه‌ها کرده‌اند) را مورد هدف قرار می‌دهند. تمرکز اصلی روی حملاتی است که از طریق برنامه یا فروشگاه برنامه، بدافزار را روی دستگاه قرار می‌دهند. بین بدافزار مستقل و بدافزاری که به سایر برنامه‌ها وابسته است، تفاوتی قائل نمی‌شویم. مهاجمان دو هدف فنی زیر را به‌عنوان اهداف سطح بالا دنبال می‌کنند:

- دریافت کد مخرب روی دستگاه کاربر (اگر بتوانند این کار را انجام دهند)
- ننگ‌داشتن کد مخرب روی دستگاه کاربر

مهم‌ترین وظیفه فروشگاه‌های برنامه در راستای تأمین امنیت سامانه‌های هوشمند همراه، جلوگیری از نصب یا استقرار یک بدافزار بر روی دستگاه‌های تلفن همراه کاربران است. اگر فروشگاه به‌عنوان مدخل ورود برنامه‌های مخرب به دستگاه‌های کاربران، بتواند این اهداف را برآورده

انکار^۷ (R): تهدید انکار زمانی اتفاق می‌افتد که کاربر با از بین بردن شواهد مربوط به یک عمل، منکر انجام آن عمل شود. برای مثال، کاربر یک عمل غیرقانونی را در یک سامانه‌ای انجام می‌دهد که فاقد توانایی برای ردیابی عملیات غیرقانونی^۸ است.

افشای اطلاعات^۹ (I): تهدید افشای اطلاعات شامل دستیابی شخص غیرمجاز به اطلاعاتی است که اجازه دسترسی به آن‌ها را نداشته است. برای مثال، توانایی کاربران برای خواندن اطلاعات حساس که اجازه دسترسی به آن اطلاعات را ندارند یا توانایی یک مزاحم^{۱۰} برای خواندن داده‌های در حال انتقال بین دستگاه‌های تلفن همراه را نمونه‌هایی از افشای اطلاعات می‌توان دانست.

ممانعت از ارائه خدمت (D): این حمله، مانع از ارائه خدمات به کاربران مجاز می‌شود. این حمله در زمانی به وقوع می‌پیوندد که با اعمال سربرار^{۱۱} روی یک خدمت، عملکرد عادی آن تحت‌الشعاع قرار می‌گیرد.

ارتقای مجوزهای دسترسی^{۱۲} (E): در این نوع تهدید، فرد غیرمجاز به مجوزها دسترسی پیدا می‌کند و به این ترتیب، دسترسی کافی برای به‌مخاطره‌انداختن^{۱۳} یا تخریب کل سامانه را دارد. تهدیدهای ارتقای مجوز دسترسی، شامل موقعیت‌هایی هستند که در آن‌ها یک مهاجم به‌طور مؤثر به تمامی قابلیت‌های تدافعی سامانه نفوذ می‌کند و بخشی از سامانه قابل اعتماد می‌شود.

در جدول (۲)، تهدیدهای STRIDE به‌همراه ویژگی مطلوبی که مورد تهدید قرار می‌گیرند، تعریفی از تهدید (بر اساس نمودار جریان داده) و مؤلفه‌های نمودار جریان داده که در معرض تهدید قرار دارند، بیان شده است. مدل STRIDE روی تهدیدهایی که روی مرزهای اعتماد مدل جریان داده و همچنین تهدیدهایی که درون مرزهای اعتماد مدل جریان داده به‌وقوع می‌پیوندد، تمرکز می‌کند. در ادامه، این دو دسته از تهدیدها را معرفی می‌کنیم:

کند، سایر تهدیدها و حملات جانبی از قبیل سرقت اطلاعات نیز پوشش داده می‌شود. برنامه‌هایی که مبادرت به سرقت داده‌های کاربر می‌کنند، نیز یک بدافزار با هدف ثانویه دزدی اطلاعات کاربر است. برای جلوگیری از رسیدن به این هدف لازم است فروشگاه‌های برنامه‌ها از نصب و استقرار هرگونه بدافزار روی دستگاه‌های کاربران ممانعت کنند. در اینجا، حملاتی را که هدف آن‌ها توسعه‌دهندگان یا فروشگاه‌های برنامه‌ها بوده و هیچ تأثیری بر کاربر نهایی ندارند، در نظر نمی‌گیریم (همانند click-fraud، سرقت ادبی و رقابت غیرمنصفانه). همچنین حملات مهندسی اجتماعی نیز در نظر گرفته نشده‌اند.

۱-۵- مقدمه‌ای بر STRIDE

STRIDE مدلی است که توسط شرکت مایکروسافت با هدف طبقه‌بندی تهدیدهای امنیتی توسعه یافته است [4]. در ابتدا STRIDE به‌منظور مدل‌سازی تهدیدها در تجزیه و تحلیل امنیت نرم‌افزار به کار گرفته می‌شد؛ ولی اکنون از این مفهوم در حوزه‌های مختلف استفاده می‌شود. تهدیدهای STRIDE در مقابل ویژگی‌های مطلوب امنیتی همانند احراز اصالت، تمامیت، عدم انکار^۱، محرمانگی^۲، دسترسی‌پذیری^۳ و صدور مجوز قرار دارند. نام STRIDE از ترکیب حروف نخست شش دسته تهدید زیر به دست می‌آید [4].

جعل هویت^۴ (S): در این تهدید، یک فرد یا سامانه با موفقیت خود را به جای فرد یا سامانه دیگری می‌تواند تظاهر کند. به‌عنوان مثالی از تهدید جعل هویت به دسترسی غیرقانونی و استفاده از اطلاعات احراز اصالت کاربران مانند نام کاربری و رمز عبور می‌توان اشاره کرد.

دستکاری^۵ (T): تهدید دستکاری به ایجاد تغییر مخرب در داده‌ها گفته می‌شود. مثال‌هایی از این تهدید شامل تغییرات غیرمجاز بر روی داده‌های مانا^۶ همانند داده‌های ذخیره‌شده در حافظه دائمی، تغییر داده‌هایی که بین دو دستگاه تلفن همراه از طریق یک شبکه باز مثل اینترنت منتقل می‌شوند، می‌باشد.

⁷ Repudiation

⁸ Prohibited

⁹ Information disclosure

¹⁰ Intruder

¹¹ Overload

¹² Elevation of Privileges

¹³ Compromise

¹ Availability

² Non-repudiation

³ Authorization

⁴ Spoofing

⁵ Tampering

⁶ Persistent

(جدول-۲): تهدیدات STRIDE [7]

نام تهدید	ویژگی تهدید شده	تعریف تهدید	مؤلفه‌های در معرض تهدید
جعل هویت (S)	احراز اصالت	وانمود کردن یک فرایند یا تعامل گر به شخص/ چیز دیگری	فرایند، تعامل گر
دستکاری (T)	تمامیت	تغییر یک فرایند، جریان داده یا انبار داده، فرایند	انبار داده، جریان داده، فرایند
انکار (R)	عدم انکار	از بین بردن شواهد مربوط به یک عمل انجام شده توسط یک فرایند یا یک تعامل گر	فرایند، تعامل گر
افشای اطلاعات (I)	محرمانگی	فاش شدن داده‌های حساس توسط یک فرایند، جریان داده یا انبار داده	فرایند، انبار داده، جریان داده
ممانعت از ارائه خدمت (D)	دسترسی پذیری	اعمال سربرار بیش از ظرفیت نرمال روی یک جریان داده، انبار داده یا یک فرایند به گونه‌ای که عملکرد عادی را تحت الشعاع قرار دهد.	فرایند، انبار داده، جریان داده
ارتقای مجوزهای دسترسی (E)	صدور مجوز	استفاده از یک فرایند برای انجام فعالیت‌های غیرمجاز	فرایندها

مرز اعتماد کاربر دستگاه) به فرایند (P10) یعنی «اجرای برنامه» مورد توجه قرار می‌گیرند؛ زیرا در اغلب موارد رفتار مخرب در زمان اجرا پدیدار می‌شود.

(جدول-۳): تهدیدات ممکن روی مرزهای اعتماد [6]

شماره تهدید	شرح تهدید
T1	هویت توسعه‌دهنده برنامه توسط یک مهاجم جعل می‌شود و مهاجم (با نام توسعه‌دهنده) یک برنامه مخرب را ثبت می‌کند.
T2	مهاجم یک برنامه مخرب را ثبت می‌کند و بعدها انجام آن را انکار می‌کند.
T3	مهاجم یک برنامه یا به روزرسانی را به منظور اضافه کردن کد مخرب به آن دستکاری می‌کند.
T4	مهاجم اطلاعات حساس (همانند اعتبارنامه‌های احراز اصالت توسعه‌دهنده برنامه) را به دست می‌آورد.
T5	مهاجم با ارسال تعداد بسیار زیادی برنامه به چک پذیرش (با اعمال سربرار)، مانع ثبت برنامه‌ها یا به روزرسانی‌ها توسط توسعه‌دهندگان می‌شود.
T6	مهاجم چک پذیرش را جعل می‌کند و باعث می‌شود توسعه‌دهنده اعتبارنامه‌های احراز اصالت را فاش کند.
T7	مهاجم کاری می‌کند که برنامه مخرب، چک پذیرش را با موفقیت بگذراند.
T8	فروشنگاه برنامه دریافت یک برنامه یا به روزرسانی برای چک پذیرش را انکار می‌کند.
T9	مهاجم اطلاعات حساس در مورد فروشنگاه برنامه یا سایر توسعه‌دهندگان برنامه را از طریق چک پذیرش به دست می‌آورد.
T10	مهاجم با ارسال تعداد بسیار زیادی برنامه به چک پذیرش (با اعمال سربرار)، مانع ثبت برنامه‌ها یا به روزرسانی‌ها توسط توسعه‌دهندگان می‌شود.
T11	مهاجم یک برنامه مخرب را تصویب می‌کند و یا یک برنامه را از طرف فرد دیگری ثبت می‌کند.
T12	مهاجم خود را به جای کاربر دستگاه جا می‌زند و بازخورد ^۲ نادرست را برای یک برنامه پست می‌کند یا تعداد دانلودهای برنامه‌ها را تحریف می‌کند.
T13	مهاجم ارسال یک بازخورد غلط را انکار می‌کند.
T14	مهاجم رابط فروشنگاه برنامه را جعل می‌کند تا کاربران توضیحات غلط و مقادیر نادرستی را برای اعتبار برنامه‌ها ببینند.

۲-۵- تحلیل تهدیدات به روش STRIDE

مدل جریان داده که در بخش ۲ معرفی شد، دارای سه تعامل گر، ده فرایند، دو انبار داده و بیست جریان داده است. با توجه به نحوه تأثیر تهدیدهای STRIDE بر اجزای مختلف مدل جریان داده که در جدول (۲) نشان داده شده است، STRIDE کامل تعداد ۱۳۲ تهدید را مشخص می‌کند. در ابتدا، ۶۷ تهدیدی را که روی مرزهای اعتماد وجود دارند، معرفی می‌کنیم [6]. این تهدیدها در جدول (۳) نشان داده شده‌اند. در این مقاله، تمام تهدیدهای درون مرزهای اعتماد مورد بررسی قرار نمی‌گیرند و فقط تهدیدهای داخلی (درون

¹ Execute
² Feedback

T33: مهاجم رابط فروشگاه برنامه را دستکاری می کند تا دستگاه نتواند کل امحاءها و به روزرسانیها را دریافت کند.	
T34: مهاجم اخطار مربوط به به روزرسانی یا امحاء را دریافت می کند و بعدها دریافت اخطار را انکار می کند.	
T35: مهاجم اطلاعات حساس (همانند کدام برنامه ها روی کدام دستگاهها نصب شده اند) را از رابط فروشگاه برنامه به دست می آورد.	
T36: مهاجم دسترسی به رابط فروشگاه برنامه را انکار می کند تا مانع دریافت به روزرسانیها و امحاءها توسط کاربران شود.	
T37: مهاجم فعالیت های غیرمجاز همانند تغییر یا حذف به روزرسانیها و امحاءها را انجام می دهد.	
T38: مهاجم به روزرسانیها و امحاءها را از دستگاه دستکاری می کند، به طوری که دستگاه تمامی به روزرسانیها و امحاءها را دریافت نکند.	
T39: مهاجم اطلاعاتی در خصوص این که کدام برنامه ها روی کدام دستگاهها نصب شده اند را به دست می آورد.	
T40: مهاجم مانع دستگاهها در دریافت به روزرسانیها یا امحاءها جهت نصب می شود.	جریان دادهها بین P6 و P9: شناسه برنامه های امحاء شده یا به روزرسانی شده
T41: مهاجم فروشگاه برنامه را جعل می کند، به طوری که کاربر نظرات و شکایات خود را در مکان نادرستی اعلام کند.	
T42: مهاجم رابط فروشگاه برنامه را با هدف تغییر یا حذف شکایات دستکاری می کند.	
T43: مهاجم اطلاعات مربوط به بازخورد مثبت را ثبت می کند و بعدها این اقدام را انکار می کند.	
T44: مهاجم اطلاعات حساس (همانند اطلاعاتی که مشخص می کنند کدام برنامه ها روی کدام دستگاهها نصب شده اند) را به دست می آورد.	
T45: مهاجم مانع کاربران دستگاه در ثبت نظرات و شکایات توسط می شود؛ این کار را از طریق ارسال تعداد بسیار زیادی نظر به فروشگاه برنامه و اعمال سربر انجام می دهد.	
T46: مهاجم فعالیت های غیرمجاز همانند حذف نظرات یا شکایات در مورد یک برنامه را انجام می دهد.	
T47: مهاجم نظرات و شکایات ارسالی از سوی کاربر دستگاه را تغییر می دهد.	جریان دادهها بین P7 و P3: نظرات یا شکایات درباره برنامه
T48: مهاجم اطلاعات حساس در مورد کاربران دستگاه (همانند اطلاعات در مورد این که کدام برنامه ها توسط کدام کاربران نصب شده اند یا جزئیات اطلاعات شخصی درباره کاربران دستگاه) را به دست می آورد.	

T15: مهاجم رابط فروشگاه برنامه را با هدف تغییر توضیحات و اعتبارهای برنامه ها دستکاری می کند.	برنامه (P4)
T16: مهاجم توضیحات و اعتبارها را جستجو می کند اما بعدها انجام آن را انکار می کند.	
T17: مهاجم اطلاعات حساس (همانند اطلاعاتی در مورد این که کدام کاربران می خواهند کدام برنامه ها را نصب کنند) را به دست می آورد.	
T18: مهاجم از طریق اعمال سربر روی فروشگاه برنامه، مانع کاربران در جستجوی توضیحات مربوط به برنامه می شود.	
T19: مهاجم اقدام به انجام فعالیت های غیرمجاز همانند تغییر توضیحات و اعتبارهای برنامه ها می کند.	جریان دادهها بین P4 و P3: توضیحات و اعتبار برنامه
T20: مهاجم توضیحات و اعتبار برنامه ها را تغییر می دهد.	
T21: مهاجم اطلاعاتی را در مورد این که کدام کاربران، کدام برنامه ها را نصب کرده اند، به دست می آورد.	
T22: مهاجم با اعمال سربر، مانع کاربران در جستجوی توضیحات برنامه می شود.	
T23: مهاجم فروشگاه برنامه را جعل می کند تا دستگاه برنامه های مخرب را نصب کند.	انتشار برنامه (P5)
T24: مهاجم فروشگاه برنامه را دستکاری می کند تا دستگاه برنامه های مخرب را نصب کند.	
T25: مهاجم یک برنامه را برای نصب دانلود می کند و بعدها انجام آن را انکار می کند.	
T26: مهاجم اطلاعات حساس (همانند اطلاعاتی در مورد این که کدام برنامه ها روی کدام دستگاهها نصب شده اند) را از فروشگاه برنامه به دست می آورد.	
T27: مهاجم دسترسی به فروشگاه برنامه را انکار می کند تا مانع دستگاهها برای دانلود برنامه ها و به روزرسانیها جهت نصب شود.	
T28: مهاجم اقدام به انجام فعالیت های غیرمجاز همانند افزودن برنامه های (مخرب) بیشتر به فروشگاه می کند.	
T29: مهاجم برنامه را دستکاری می کند تا دستگاه یک برنامه مخرب را نصب کند.	
T30: مهاجم اطلاعاتی در مورد اینکه کدام برنامه ها روی کدام دستگاهها نصب شده اند را به دست می آورد.	
T31: مهاجم مانع دستگاه برای دانلود برنامه ها یا به روزرسانیها جهت نصب می شود.	جریان دادهها بین P5 و P8: برنامه و فرادادهها
T32: مهاجم فروشگاه برنامه را جعل می کند تا دستگاه نتواند تمامی امحاءها و به روزرسانیها را دریافت کند.	

T64: مهاجم می‌تواند یک برنامه را بدون بر جای گذاشتن ردپا (همانند log) اجرا کند.	
T65: مهاجم اطلاعات حساس را از فرایند اجرا (همانند اطلاعات مربوط به کاربر دستگاه یا اطلاعات حساس روی دستگاه) به دست می‌آورد.	
T66: مهاجم روی فرایند اجرا سربرار اعمال می‌کند تا مانع کاربر در اجرای برنامه‌های دیگر شود.	
T67: مهاجم فعالیت‌های غیرمجاز همانند دستکاری برنامه‌های دیگر، خواندن داده‌های ذخیره‌شده توسط سایر برنامه‌ها یا خواندن اطلاعات حساس را انجام می‌دهد.	

۶- درخت حمله

تحلیل STRIDE انواع متفاوتی از تهدیدات را از دیدگاه تهاجمی می‌تواند مشخص کند. پس از شناسایی تهدیدها لازم است از درخت حمله به‌منظور مدل‌سازی گرافیکی حمله علیه سامانه استفاده شود. تمرکز اصلی در مدل‌سازی تهدید بر چگونگی به وقوع و به نتیجه رسیدن حمله است. درخت حمله ابزاری است که بر اساس تهدیدهای مختلف، هدف حمله و مراحل انجام آن را نشان می‌دهد. روش درخت حمله توسط Bruce Schneier به‌منظور تحلیل تمامی روش‌های مختلف حمله به یک سامانه پیشنهاد شده است [16]. جهت ترسیم درخت حمله ابتدا لازم است، تمامی اهداف ممکن را شناسایی و سپس راه‌های مختلف برای رسیدن به اهداف را متصور شد و آن‌ها را به بدنه درخت اضافه کرد.

ریشه درخت حمله، یک رویداد² امنیتی را نشان می‌دهد که به‌صورت بالقوه می‌تواند به یک دارایی آسیب برساند. تمامی راه‌های محتمل و مراحل مختلف جهت نفوذ به سامانه در زیرگره‌ها مشخص می‌شوند. هر درخت حمله، روش‌ها و راه‌های متعددی را که یک مهاجم از طریق آن‌ها موجب بروز یک رویداد امنیتی می‌تواند شود، مورد بررسی قرار می‌دهد. هر مسیر در درخت حمله نشان‌دهنده یک حمله بالقوه (ریسک) منحصر به فرد است [17]. آنچه که مسیر را منحصر به فرد می‌کند، زیرگره انتهایی هر مسیر است؛ لذا این زیرگره مشخص‌کننده هر حمله بالقوه خواهد بود. این حملات بالقوه همان ریسک‌ها هستند که در صورت وجود یک مهاجم و پیاده‌سازی آن، به حملات بالفعل تبدیل خواهند شد. به این ترتیب، می‌توان ریسک‌ها را شناسایی کرد و قبل از وقوع حملات احتمالی ناشی از این ریسک‌ها،

T49: مهاجم از طریق ارسال تعداد بسیار زیادی نظر به فروشگاه برنامه، مانع کاربران دستگاه در ثبت نظرات و شکایات می‌شود.	
T50: مهاجم دستگاه را جعل می‌کند تا بتواند اطلاعات آماری در خصوص این که کدام کاربران اقدام به نصب کدام برنامه‌ها یا به‌روزرسانی‌ها کرده‌اند را تحریف کند.	نصب یا حذف برنامه (P8)
T51: مهاجم نصاب ¹ را با هدف نصب برنامه‌های مخرب دستکاری می‌کند.	
T52: مهاجم یک برنامه را نصب می‌کند (و بعدها انجام آن را انکار می‌کند) تا بتواند اطلاعات آماری در خصوص این که کدام کاربران اقدام به نصب کدام برنامه‌ها یا به‌روزرسانی‌ها کرده‌اند را تحریف کند.	
T53: مهاجم اطلاعات حساس درباره کاربر (همانند دستگاهی که کاربر مورد استفاده قرار می‌دهد) را به دست می‌آورد.	
T54: مهاجم با اعمال سربرار بر نصاب، مانع کاربران در نصب به‌روزرسانی‌ها یا حذف برنامه‌های امحاء شده می‌شود.	
T55: مهاجم اقدام به انجام فعالیت‌های غیرمجاز همانند نصب برنامه‌های مخرب و rootkit می‌کند.	چک دوره‌ای برنامه (P9)
T56: مهاجم دستگاه کاربر را جعل می‌کند تا بتواند اطلاعات آماری در خصوص این که کدام کاربران هشدارهای مربوط به به‌روزرسانی یا امحاء را دریافت کرده‌اند را تحریف کند.	
T57: مهاجم مانع دستگاه کاربر در دریافت به‌روزرسانی‌های یا امحاءها می‌شود.	
T58: مهاجم هشدار مربوط به به‌روزرسانی یا امحاءها را دریافت می‌کند (و بعدها دریافت این هشدارها را انکار می‌کند) تا بتواند اطلاعات آماری در مورد تعداد کاربرانی که به‌روزرسانی‌ها یا امحاءها را دریافت کردند را تحریف کند.	
T59: مهاجم اطلاعات حساس را از طریق رابط کاربری فروشگاه برنامه به دست می‌آورد (به عنوان مثال، کدام برنامه‌ها روی کدام دستگاه‌های کاربر نصب شده‌اند).	
T60: مهاجم روی فرایند سربرار اعمال می‌کند تا مانع دریافت اطلاعات به‌روزرسانی‌ها و امحاءها در دستگاه کاربر شود.	اجرای برنامه (P10)
T61: مهاجم اقدام به انجام فعالیت‌های غیرمجاز به منظور حذف امحاءها می‌کند.	
T62: مهاجم فرایند اجرا را جعل می‌کند تا کاربران (به اشتباه) تصور کنند که یک برنامه در حال اجرا است.	
T63: مهاجم فرایند اجرا را دستکاری می‌کند تا توابع مخرب عمل کنند.	

² Event

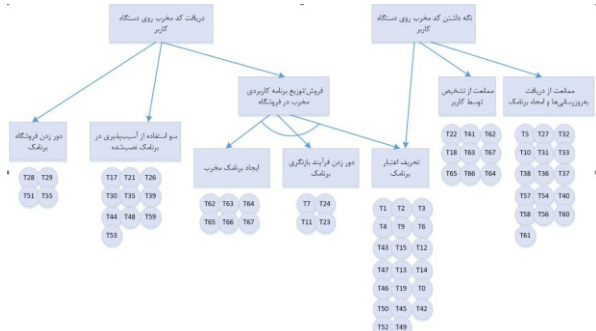
¹ Installer

۱-۷- ریسک R1: دورزدن فروشگاه برنامه

در این ریسک، مهاجم اقدام به دورزدن فروشگاه برنامه رسمی کرده و برنامه‌های خود را از طریق یک فروشگاه برنامه غیررسمی عرضه می‌کند. پس از آن فعالیت‌های غیرمجاز همانند افزودن برنامه‌های مخرب و rootkit به فروشگاه غیررسمی را انجام می‌دهد. مهاجم، یک برنامه یا فرایند نصب در فروشگاه را دستکاری می‌کند تا دستگاه کاربر آن برنامه مخرب را نصب کند. در این ریسک مهاجم از آسیب‌پذیری‌های منجر به نصب بدافزار، ضعف در تأیید مجوزهای دسترسی توسط کاربر و عدم آگاهی کاربر سوء استفاده می‌کند تا کاربر اقدام به نصب برنامه‌های مخرب کند. مشخصات این ریسک که شامل تهدیدها، آسیب‌پذیری‌ها و دارایی‌ها می‌شود، در جدول (۴) ارائه شده است. مثالی از این ریسک، برنامه Financial Times (FT) است که فروشگاه iTunes اپل و بازار اندروید گوگل را دور زد تا بتواند به‌طور مستقیم با خوانندگان ارتباط برقرار کند. برنامه FT یک برنامه مبتنی بر جستجو برای گوشی‌ها و تبلت‌ها است که خودکار به‌روزرسانی می‌شود و به خوانندگان این امکان را می‌دهد تا در تبلت‌ها و گوشی‌های هوشمند خود به محتوای سرمقالات دسترسی پیدا کنند [18].

به مقابله با آن‌ها پرداخت و امکان نفوذ به سیستم را برای مهاجم از بین برد.

در شکل (۳)، درخت حمله مربوط به حمله بدافزارها به دستگاه نشان داده شده است. گره‌های بالای درخت، اهداف فنی و سطح بالای مهاجم را مشخص می‌کنند: «دریافت کد مخرب روی دستگاه کاربر» و «نگه‌داشتن کد مخرب روی دستگاه کاربر». در این درخت، هم برنامه‌های مخرب و هم سوء استفاده از برنامه‌های آسیب‌پذیر را در نظر می‌گیریم. اهدافی همچون سرقت پول یا سرقت داده‌های حساس در نظر گرفته نشده‌اند. بخش پایینی درخت حمله، تهدیدهای حاصل از تحلیل STRIDE را (که در بخش ۵ عنوان شده‌اند) نشان می‌دهد.



(شکل-۳): درخت حمله مربوط به حمله بدافزارها به سامانه

هوشمند [6]

۷- ریسک‌های امنیتی

ریسک تهدیدی است که از نقاط آسیب‌پذیر سوء استفاده کرده تا بتواند به یک دارایی آسیب وارد کند. در امنیت اطلاعات، شدت ریسک از حاصل ضرب «احتمال وقوع تهدید» در «تأثیر یک تهدید» علیه دارایی‌های یک سازمان یا یک فرد به دست می‌آید. احتمال وقوع یک تهدید بر اساس تعداد آسیب‌پذیری‌های ممکن و همچنین سهولتی نسبی که یک مهاجم می‌تواند از آن‌ها سوء استفاده کند یا برای مهاجم می‌تواند جذاب باشد، تعیین می‌شود. تأثیر وقوع تهدیدهایی که از یک یا چند آسیب‌پذیری بهره‌برداری می‌کنند، بر روی دارایی‌های موجود در آن زیست‌بوم قابل شناسایی است. در ادامه، ریسک‌های مطرح در سطح توزیع‌کنندگان برنامه‌های سامانه‌های هوشمند همراه معرفی خواهند شد. برای هر ریسکی که در این بخش پوشش داده شده، مشخصات مرتبط با آن ریسک هم بیان شده است. از جمله این مشخصات به تهدیدات، آسیب‌پذیری‌ها و همچنین دارایی‌هایی که تحت تأثیر قرار می‌گیرند، می‌توان اشاره کرد.

(جدول-۴): مشخصات ریسک شماره یک

تهدیدها	T28, T29, T51, T55 - توضیح: با توجه به تهدیدات T28, T29, T51 و T55 در صورت دور زدن فروشگاه برنامه و نصب برنامه‌ها از فروشگاه‌های غیرمجاز (یا منابع تأیید نشده) توسط کاربر، احتمال مخرب بودن برنامه نصب‌شده روی گوشی هوشمند وجود دارد و امکان سوء استفاده از آن‌ها فراهم می‌شود.
آسیب‌پذیری‌ها	V1- آسیب‌پذیری‌های منجر به نصب بدافزار. تهدیدات T55, T28 و T29 توسط این آسیب‌پذیری رخ می‌دهند. V3- ضعف در تأیید مجوزهای دسترسی توسط کاربر. تهدید T51 توسط این آسیب‌پذیری رخ می‌دهد. V7- عدم آگاهی کاربر. تهدید T51 توسط این آسیب‌پذیری رخ می‌دهد.
دارایی‌ها	A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامه‌ها

<p>V4- ضعف در رمزنگاری. تهدیدات T21 و T59 و T39 توسط این آسیب‌پذیری رخ می‌دهند.</p>	
<p>A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامه‌ها</p>	<p>دارایی‌ها</p>

۷-۳- ریسک R3: ایجاد برنامه‌های مخرب

در این ریسک فقط تهدیدها مربوط به اجرای برنامه مخرب مورد توجه قرار می‌گیرند؛ زیرا در اغلب موارد، رفتار مخرب در زمان اجرا پدیدار می‌شود. در این نوع تهدیدها، مهاجم فرایند اجرای برنامه را جعل یا دستکاری کرده و یا روی فرایند اجرا سربار اعمال کرده تا اقدام به انجام عملیات مخرب کند. مثالی از این نوع تهدیدها، گزارش‌هایی هستند که درخصوص آلوده‌شدن دستگاه‌ها به بدافزارهایی مثل Ruffraud دریافت شده‌اند [19]. مجموعه آسیب‌پذیری‌هایی که منجر به نصب بدافزار می‌شوند، کانال‌های مخفی / جعبه شنی ضعیف، ضعف در تأیید مجوزهای دسترسی توسط کاربر، عدم وجود بهروشهایی برای حفاظت از حریم خصوصی و عدم آگاهی کاربر در بروز ریسک ایجاد و اجرای برنامه مخرب دخیل هستند. مشخصات ریسک ایجاد برنامه‌های مخرب در جدول (۶) قابل مشاهده است.

جدول (۶): مشخصات ریسک شماره سه

<p>T62, T63, T64, T65, T66, T67 - توضیح: با توجه به تهدیدات T62, T63, T64, T65, T66, T67 و T68 در این ریسک، فقط تهدیدات ناشی از اجرای یک برنامه مخرب در سمت دستگاه تلفن همراه کاربر مورد توجه قرار گرفته است.</p>	<p>تهدیدها</p>
<p>V1- آسیب‌پذیری‌های منجر به نصب بدافزار (قابلیت باز کردن قفل سامانه هوشمند). کلیه تهدیدات T62, T63, T64, T65, T66, T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند. V2- کانال‌های مخفی / جعبه شنی ضعیف. کلیه تهدیدات T62, T63, T64, T65, T66, T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند. V3- ضعف در تأیید مجوزهای دسترسی توسط کاربر. کلیه تهدیدات T62, T63, T64, T65, T66, T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند. V6- عدم وجود بهروشهایی برای حفاظت از حریم خصوصی. کلیه تهدیدات T62, T63, T64,</p>	<p>آسیب‌پذیری‌ها</p>

۷-۲- ریسک R2: سوء استفاده از

آسیب‌پذیری‌های موجود در برنامه

نصب‌شده

در این ریسک، مهاجم از آسیب‌پذیری‌های موجود در برنامه نصب‌شده سوء استفاده کرده و پس از آن، اطلاعات حساس همانند مشخصات کاربرانی که اقدام به نصب برنامه کرده‌اند و همچنین اطلاعات مربوط به برنامه‌های نصب‌شده روی دستگاه‌ها را از طریق رابط کاربری فروشگاه یا برنامه نصب‌شده به دست می‌آورد. برای این که مهاجم بتواند به اطلاعات حساس (در مورد کاربران و برنامه‌های نصب‌شده روی دستگاه) از طریق فروشگاه دست پیدا کند، از آسیب‌پذیری‌های اعتبار که در فروشگاه برنامه وجود دارد بهره می‌گیرد. مشخصات این ریسک که شامل تهدیدها، آسیب‌پذیری‌ها و دارایی‌ها می‌شود، در جدول (۵) ارائه شده است.

هدف بسیاری از مهاجمان در حمله به گوشی‌های تلفن همراه هوشمند از طریق مجموعه تهدیدهایی که از آسیب‌پذیری در برنامه‌های نصب‌شده از سوی فروشگاه سوء استفاده می‌کنند، برآورده می‌شود. تأثیر وقوع این تهدیدها بر دارایی‌های سازمان‌ها (به دلیل دستیابی به داده‌های حساس سازمانی، دولتی و مالی) و در فروشگاه‌های برنامه‌ها رسمی به دلیل این که اعتبار فروشگاه زیر سؤال می‌رود، زیاد است.

جدول (۵): مشخصات ریسک شماره دو

<p>T17, T21, T26, T30, T35 - توضیح: با توجه به تهدیدات T17, T21, T26, T30, T35, T39, T44, T48, T53, T59 در صورت وجود آسیب‌پذیری در انبار داده و یا رابط فروشگاه برنامه، مهاجم اطلاعات حساس (همانند مشخصات کاربرانی که اقدام به نصب برنامه کرده‌اند، اطلاعاتی که مشخص می‌کنند کدام برنامه‌ها روی کدام دستگاه نصب‌شده است و همچنین اطلاعات مربوط به دستگاهی که کاربر مورد استفاده قرار می‌دهد) را به دست می‌آورد.</p>	<p>تهدیدها</p>
<p>V1- آسیب‌پذیری‌های منجر به نصب بدافزار (آسیب‌پذیری‌های اعتبار). تهدیدات T17 و T44 توسط این آسیب‌پذیری رخ می‌دهند. V2- کانال‌های مخفی / جعبه شنی ضعیف. تهدیدات T35 و T39 توسط این آسیب‌پذیری رخ می‌دهند.</p>	<p>آسیب‌پذیری‌ها</p>

V5- ضعف در احراز اصالت توسعه‌دهنده و توزیع‌کننده برنامه. تهدیدات T23 و T24 توسط این آسیب‌پذیری رخ می‌دهند.	
A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامه‌ها	دارایی‌ها

۵-۷- ریسک R5: تحریف اعتبار برنامه‌ها

همان‌گونه در جدول (۸) قابل مشاهده است، در این ریسک، مهاجم چندین هویت مستعار برای خود ایجاد کرده و با به‌دست آوردن نفوذ زیاد، اعتبار برنامه ارائه‌شده در فروشگاه را تغییر یا تحریف می‌کند. به این ترتیب، مهاجم کاری می‌کند که کاربران به‌غلط تصور کنند یک برنامه امن توسط فروشگاه توزیع شده است؛ درحالی‌که، یک برنامه مخرب از طریق فروشگاه روی دستگاه کاربر قابل نصب است.

حمله‌ای که اقدام به تحریف اعتبار برنامه‌ها در فروشگاه می‌کند و در این زمینه گزارش شده است، حمله Sybil نام دارد. باید سازوکارهایی جهت مقابله با حمله Sybil در نظر گرفته شود. نظرات و بررسی جعلی در گوگل پلی و فروشگاه برنامه اپل نیز گزارش شده است [20].

فروشگاه‌های برنامه هر روز رقابتی‌تر می‌شوند و ناشران برنامه به‌دنبال روش‌های هوشمندی هستند تا بتوانند کسب‌وکار پایداری را برای سامانه هوشمند همراه شکل دهند. این مسئله منجر به سرمایه‌گذاری در ابزارهایی همانند MobileDevHQ برای بهینه‌سازی فروشگاه برنامه، اپنتیو برای بازخورد درون برنامه‌ها و ابزارهای نگهداری شده است. متأسفانه در چند سال اخیر، مواردی مشاهده شده‌اند که به‌نظر می‌رسد ناشران برنامه با استفاده از بررسی‌های جعلی سعی می‌کنند تا توجه مردم را جلب کنند، به این امید که این عمل به آن‌ها کمک کند تا نرخ فروش را در فروشگاه افزایش دهند. بررسی‌های جعلی فقط به فروشگاه‌های برنامه محدود نمی‌شود و کاربران نیز این عمل را به‌مدت چندین سال روی آمازون انجام می‌دادند. آمارها نشان می‌دهند که ۵۵ درصد از برنامه‌ها که شامل بررسی‌های جعلی بوده‌اند، مربوط به برنامه‌های iOS بوده و ۴۵ درصد مربوط به برنامه‌های اندروید بوده‌اند.

(جدول ۸): مشخصات ریسک شماره پنج

T1 - T2, T3, T4, T6, T9, T12, T13 - T14, T15, T19, T20, T24, T42, T43, T45	تهدیدها
--	---------

T65, T66, T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند. V7- عدم آگاهی کاربر. کلیه تهدیدات T62, T63, T64, T65, T66, T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند.	
A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامه‌ها	دارایی‌ها

۴-۷- ریسک R4: دور زدن فرایند بررسی برنامه‌ها

برنامه‌ها

در این ریسک مهاجم تهدیدهایی را اعمال کرده تا فرایند بررسی برنامه را دور می‌زند و فروشگاه برنامه را با هدف عرضه برنامه‌ها جعل یا دستکاری می‌کند. به این ترتیب، مهاجم می‌تواند برنامه مخرب را در فروشگاه عرضه کند یا بفروشد و کاربران با فرض این که برنامه‌های عرضه‌شده از سوی فروشگاه قابل اعتماد هستند، برنامه مخرب را روی دستگاه خود نصب می‌کنند؛ علاوه بر این، رفتارهای پرخطر که در زمینه دور زدن فرایند بررسی برنامه‌ها از سوی توسعه‌دهندگان شناخته شده سر می‌زند (و این رفتارها توسط فروشگاه قابل ردیابی است) نیز نشانه‌ای از یک حمله (همانند حمله فیشینگ) می‌تواند باشد. حملات فیشینگ یا XSS که با هدف به‌دست آوردن اعتبارنامه‌های توسعه‌دهندگان برنامه انجام می‌گیرند، نمونه‌ای از خطرانی بوده که در فروشگاه‌های برنامه مشاهده شده است. در صورت وقوع این حملات، دارایی‌های فروشگاه‌ها به‌شدت تحت تأثیر قرار خواهند گرفت. مشخصات ریسک ایجاد دور زدن فرایند بررسی برنامه‌ها در جدول (۶) نشان داده شده است.

(جدول ۶): مشخصات ریسک شماره چهار

T7, T11, T23, T24 - توضیح: بر اساس تهدیدات T7, T11, T23, T24 به دلیل وجود آسیب‌پذیری در انباره داده یا رابط فروشگاه برنامه، مهاجم اقدام به انجام فعالیت‌های مخرب در راستای دور زدن فرایند بازنگری فروشگاه برنامه کرده و به این ترتیب قادر خواهد بود که برنامه مخرب خود را روی دستگاه کاربر نصب کند.	تهدیدها
V1- آسیب‌پذیری‌های منجر به نصب بدافزار. تهدیدات T7 و T11 توسط این آسیب‌پذیری رخ می‌دهند.	آسیب‌پذیری‌ها

انجام فعالیت‌های مخرب که مانع ثبت مقادیر واقعی برای نظرات، شکایات و توضیحات مربوط به برنامه می‌شود، موجب می‌شود که کاربران اقدام به نصب برنامه‌ها مخرب روی دستگاه خود نمایند.	
V1- آسیب‌پذیری‌های منجر به نصب بدافزار (آسیب‌پذیری‌های اعتبار). تهدیدات T18، T22 و T41 توسط این آسیب‌پذیری رخ می‌دهند. V1- آسیب‌پذیری‌های منجر به نصب بدافزار (قابلیت باز کردن قفل سامانه هوشمند). کلیه تهدیدات T62، T63، T64، T65، T66، T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند. V2- کانال‌های مخفی/ جعبه سنی ضعیف. کلیه تهدیدات T62، T63، T64، T65، T66، T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند. V3- ضعف در تأیید مجوزهای دسترسی توسط کاربر. کلیه تهدیدات T62، T63، T64، T65، T66، T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند. V6- عدم وجود بهروزش‌هایی برای حفاظت از حریم خصوصی. کلیه تهدیدات T62، T63، T64، T65، T66، T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند. V7- عدم آگاهی کاربر. کلیه تهدیدات T62، T63، T64، T65، T66، T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند.	آسیب‌پذیری‌ها
A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامه‌ها	دارایی‌ها

T49، T47، T46 توضیح: بر اساس تهدیدات مطرح‌شده، مهاجم اقدام به جعل هویت توسعه‌دهنده برنامه یا کاربر دستگاه کرده تا بتواند اعتبار برنامه را جعل کرده و کاربران را تشویق به نصب برنامه‌ها مخرب از طریق فروشگاه نماید.	
V1- آسیب‌پذیری‌های منجر به نصب بدافزار (آسیب‌پذیری‌های اعتبار). تهدیدات T14، T15، T19، T20، T42، T43، T45، T46، T47 و T49 توسط این آسیب‌پذیری رخ می‌دهند. V4- ضعف در رمزنگاری. تهدیدات T12 و T13 توسط این آسیب‌پذیری رخ می‌دهند. V5- مکانیسم‌های ضعیف در احراز اصالت توسعه‌دهنده و توزیع‌کننده برنامه. تهدیدات T1، T2، T3 و T4 توسط این آسیب‌پذیری رخ می‌دهند.	آسیب‌پذیری‌ها
A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامه‌ها	دارایی‌ها

۶-۷- ریسک R6: ممانعت از تشخیص توسط کاربر

در این ریسک، مهاجم از طریق اعمال سربرار روی فروشگاه برنامه یا جعل فروشگاه برنامه، از این که کاربران بتوانند نظرات و شکایات خود را ثبت کنند یا توضیحات مربوط به برنامه را مشاهده کنند، ممانعت می‌کنند. در صورتی که کاربر اقدام به نصب کد مخرب روی دستگاه خود کرده باشد، قادر نخواهد بود که از نظرات و شکایات باقی کاربران در خصوص مخرب بودن آن اطلاع حاصل کند. به دلیل عدم دریافت گزارش‌هایی از وقوع حملات ممانعت از تشخیص توسط کاربر در فروشگاه‌های برنامه، پیش‌بینی می‌شود، احتمال وقوع این ریسک برای فروشگاه‌ها پایین باشد. در صورت وقوع این حمله، به دلیل این که مهاجم فرایند اجرا را می‌تواند دستکاری و به اطلاعات حساس دسترسی پیدا کند، تأثیر آن بر دارایی‌های فروشگاه برنامه بالا است. مشخصات ریسک شماره شش در جدول (۹) بیان شده است.

(جدول-۹): مشخصات ریسک شماره شش

T65، T64، T63، T62، T41، T22، T18 - T67، T66 توضیح: با توجه به تهدیدات T18، T22، T41، T62، T63، T64، T65، T66 و T76، مهاجم با	تهدیدها
---	---------

۷-۷- ریسک R7: ممانعت از دریافت

به روزرسانی‌ها و امحاء برنامه

در این ریسک، مهاجم مانع از دریافت به‌روزرسانی‌ها و امحاء‌ها از طرف فروشگاه برنامه در دستگاه کاربران می‌شود. در صورتی که کاربر اقدام به نصب یک کد مخرب روی دستگاه خود کرده باشد، در صورت بالفعل شدن این ریسک، قادر نخواهد بود که کد مخرب را از روی دستگاه خود حذف و از ادامه فعالیت آن جلوگیری کند. مشخصات کامل این ریسک در جدول (۱۰) بیان شده است. فروشگاه باید نسبت به دریافت به‌روزرسانی‌ها و امحاء برنامه در دستگاه‌های کاربر اطمینان حاصل کند. گاهی نیز نیاز است که علاوه بر حذف از روی دستگاه‌های کاربران، فروشگاه نسبت به حذف برنامه از ویتترین خود اقدام کند.

(جدول ۱۰-): مشخصات ریسک شماره هفت

<p>T5, T10, T27, T31, T32, T33, T36, T37, T38, T40, T54, T56, T57, T58, T60, T61</p> <p>توضیح: با توجه به تهدیدات برشمرده شده، مهاجم از طریق انجام فعالیت‌های مخرب مانع از دریافت به‌روزرسانی‌ها یا امحاء مربوط به برنامه‌ها نصب‌شده روی دستگاه کاربر می‌شود.</p>	<p>تهدیدها</p>
<p>V1- آسیب‌پذیری‌های منجر به نصب بدافزار. تهدیدات T5, T10 و T27 و T31 توسط این آسیب‌پذیری رخ می‌دهند.</p> <p>V2- کانال‌های مخفی / جعبه شنی ضعیف. تهدید T54 توسط این آسیب‌پذیری رخ می‌دهد.</p> <p>V3- ضعف در تأیید مجوزهای دسترسی توسط کاربر. تهدیدات T56 و T57 توسط این آسیب‌پذیری رخ می‌دهند.</p> <p>V5- ضعف در احراز اصالت_توسعه‌دهنده و توزیع‌کننده برنامه. تهدیدات T32, T33 و T36 و T37 توسط این آسیب‌پذیری رخ می‌دهند.</p>	<p>آسیب‌پذیری‌ها</p>
	<p>دارایی‌ها</p> <p>A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامه‌ها</p>

۸- نتیجه‌گیری

در این پژوهش، جهت راهنمایی متخصصان امنیتی در حوزه ارائه برنامه‌های مربوط به سامانه‌های هوشمند همراه، ریسک‌های امنیتی مربوط به حوزه توزیع برنامه‌های سامانه‌های هوشمند همراه شناسایی و معرفی شدند. به‌منظور دستیابی به این هدف ابتدا، زیست‌بوم توزیع برنامه استخراج و معرفی و سپس، دارایی‌ها و آسیب‌پذیری‌های این حوزه ارائه شد. براساس «مدل‌سازی تهدید»، مهم‌ترین تهدیدهای امنیتی رایج در زیست‌بوم توزیع برنامه استخراج شدند. در انتها، ریسک‌های امنیتی مطرح در سطح توزیع‌کنندگان برنامه‌های سامانه‌های هوشمند همراه شناسایی شدند. برای هر ریسکی که در این حوزه پوشش داده شده است، تهدیدها، آسیب‌پذیری‌ها و همچنین دارایی‌هایی که تحت تأثیر قرار می‌گیرند، نیز مشخص شد. الگوی ارائه‌شده در این مقاله درصدد بررسی تهدیدها و آسیب‌پذیری‌ها و ریسک‌های محتمل در حوزه ارائه برنامه‌های مربوط به سامانه‌های هوشمند همراه بر پایه ارزیابی ریسک دارایی‌های حیاتی است. این مقاله منبع

ارزشمندی به‌منظور استخراج، پیاده‌سازی و اجرای یک چارچوب امنیتی در کانال‌های عرضه و توزیع برنامه‌ها یا «فروشگاه‌های برنامه» می‌تواند باشد. با این حال برنامه‌ریزی جهت تدوین و اجرای سیاست‌ها و دستورالعمل‌های امنیتی به‌صورت الزامات امنیتی قابل اجرا توسط توزیع‌کنندگان برنامه‌های سامانه‌های هوشمند همراه ضروری به‌نظر می‌رسد.

۹- مراجع

- [1] The Statistics Portal. *Number of available apps in the Apple App Store from July 2008 to June 2016*, 2016, <http://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/>.
- [2] The Statistics Portal. *Cumulative number of apps downloaded from the Apple App Store from July 2008 to September 2016 (in billions)*, 2016, <https://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/>.
- [3] Café bazar. *Peivast*, 1393, http://peivast.com/files/pdf/special%20editions/SE-Caffe_Bazar.pdf.
- [4] D. Knott, *Hands-on Mobile App Testing: A Guide for Mobile Testers and Anyone Involved in the Mobile App Business*, Addison-Wesley Professional, 2015.
- [5] "OWASP Risk Rating Methodology," OWASP, [Online]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology. [Accessed 2016].
- [6] Dekker, M., Hogben, G., *Appstore security: 5 lines of defence against malware*, European Network and Information Security Agency (ENISA) Report, 2011.
- [7] Shostack, A., *Threat Modeling Designing for Security*, John Wiley & Sons Press, 2014.
- [8] Hogben, G., Dekker, M., *Information security risks, opportunities and recommendations for users*, ENISA, 2010.
- [9] T. Lederm and N. L. Clarke, *Risk Assessment for Mobile Devices*, International Conference on Trust, Privacy and Security in Digital Business, 2011.
- [10] M. Theoharidou, A. Mylonas and D. Gritzalis, *A risk assessment method for smartphones*, in *IFIP International Information Security Conference*, 2012.



محمد حسام تدین هیأت علمی دانشیار

در مرکز تحقیقات مخابرات ایران است. وی دارای تجربه چندساله مدیریت گروه‌های پژوهشی و انجام چندین پروژه پژوهشی در زمینه‌های مختلف، منجمله امنیت

اینترنت اشیا و امنیت سامانه‌های هوشمند همراه است. وی علاوه بر انتشار مقالات علمی، کتاب‌هایی را در زمینه امنیت کاربران سامانه‌های هوشمند همراه و برنامه‌نویسی امن برنامه‌های سامانه‌های هوشمند تألیف کرده است. علاقه‌مندی ایشان بر امنیت داده‌ها، رمزنگاری و امنیت فناوری‌های نوین در حوزه فناوری اطلاعات و ارتباطات متمرکز است.

- [11] Shirey, R., *RFC 2828 Internet Security Glossary*, IETF, 2000.
- [12] Vulnerability-lab. *Vulnerability Research, Bug Bounties & Vulnerability Assessments* [Database], Retrieved 2016, Dec. 29 from <https://www.vulnerability-lab.com/index.php>
- [13] VARUTRA. MVD: Mobile Vulnerability Database [Database], Retrieved 2016, Dec. 29 from <http://www.varutra.com/mobile-vulnerability-database-mvd.html>.
- [14] S. Quiroigico, J. Voas, T. Karygiannis, C. Michael and K. Scarfone, *Vetting the Security of Mobile Applications*, NIST Special Publication 800-163, 2015.
- [15] OWASP. *Mobile Top 10 2016-Top 10* [Report], Retrieved 2016, Dec. 29 from https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
- [16] B. Schneier, *Attack tree secrets and lies*, John Wiley and Sons Chichester, 2000.
- [17] A. K. Talukder and M. Chaitanya, *Architecting secure software systems*, Parkway NW: CRC Press., 2008.
- [18] M. Humphries, Available: <http://www.geek.com/apple/the-financial-times-bypasses-the-app-store-by-using-html5-1388119/>.
- [19] E. Mills, "Google boots 'RuFraud' apps from Android market," cnet, 2011. [Online]. Available: <http://www.cnet.com/news/google-boots-rufraud-apps-from-android-market/>. [Accessed 2016].
- [20] E. SIEGEL, "apptentive," 2014. [Online]. Available: <http://www.apptentive.com/blog/fake-reviews-google-play-apple-app-store/>



سپیده نیک منظر مدرک کارشناسی

خود را در رشته مهندسی فناوری اطلاعات از دانشگاه آزاد قزوین در سال ۱۳۸۷ و مقطع کارشناسی ارشد را در رشته مهندسی فناوری اطلاعات گرایش

شبکه‌های کامپیوتری در دانشگاه صنعتی سهند تبریز در سال ۱۳۹۱ اخذ کرده است. وی اکنون دانشجوی دکترا در دانشگاه صنعتی امیرکبیر است و از جمله زمینه‌های پژوهشی مورد علاقه وی شبکه‌های بی‌سیم، امنیت شبکه‌های کامپیوتری و بهینه‌سازی تصادفی است.

