شناسایی ریسک‌های امنیتی در زیست‌بوم توزیع برنامک 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 به‌خطر می‌اندازد، کانال‌های عرضه و توزیع برنامک‌ها یا «فروشگاه‌های برنامک» هستند. بسیاری از سازمان‌ها به یک روش ارزیابی ریسک جهت حفاظت از دارایی‌های خود نیاز دارند؛ لذا، شناسایی ریسک‌های امنیتی موجود در زیست بوم توزیع برنامک ضروری است. هدف این مقاله، شناسایی تهدیدها، آسیب‌پذیری‌ها و مهم‌ترین ریسک‌های امنیتی در حوزه توزیع برنامک‌های سامانه هوشمند همراه است. ابتدا مدلی از زیست‌بوم برنامک ارائه شده و سپس تهدیدات امنیتی براساس تحلیل STRIDE معرفی می‌شوند. در انتها نیز ریسک‌های امنیتی موجود در زیست‌بوم توزیع برنامک‌ها شناسایی خواهند شد.

واژگان کلیدی: سامانه هوشمند همراه، فروشگاه برنامک، نوزیع برنامک، مدلسازی تهدید، ریسک امنیتی، درخت حمله

۱- مقدمه

با گسترش روزافزون گوشی‌های تلفن همراه هوشمند و برنامک‌های آن‌ها، نیازمندی‌ها و الزامات جدیدی شکل گرفته و نیاز به بازارها و کتابخانه‌هایی جهت توزیع این برنامک‌ها به‌وجود آمده است. در این شرایط، کاربران به سامانه‌هایی نیاز دارند که برنامک‌ها 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 برنامک‌ها راه‌اندازی کردند که به این بازارها، «فروشگاه برنامک»[1] گفته می‌شود. استفاده از فروشگاه‌های برنامک، یکی از ویژگی‌های کلیدی در حوزه سامانه‌های هوشمند همراه به‌شمار می‌رود. فروشگاه برنامک، مخزنی مدیریت‌شده از نرم‌افزارهای شخص ثالث است. این فروشگاه‌ها فرصت مناسبی را در اختیار توسعه‌دهندگان قرار می‌دهند تا به بازار برنامک‌های گوشی‌های هوشمند ورود کرده و کسب درآمد کنند. توسعه‌دهندگان می‌توانند با استفاده از پنل مخصوصی که فروشگاه در اختیار آن‌ها قرار می‌دهد، برنامک‌های خود را منتشر، به‌روزرسانی و مدیریت کنند.

تاکنون میلیاردها برنامک از این فروشگاه‌ها بارگیری شده است. طبق آمارهایی که پایگاه Statista منتشر کرده، در سال ۲۰۱۶ تعداد دو میلیون برنامک 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 برنامک از فروشگاه iTunes شرکت اپل دانلود شده است [2]. همچنین، بر اساس آمارهای ارائه‌شده از سوی یکی از فروشگاه‌های برنامک فعال در کشور، در سال ۱۳۹۳ حدود ۲۵ هزار برنامه از طریق این فروشگاه عرضه شده است [3]. هر دانلود یک خطر امنیتی بالقوه برای گوشی‌های هوشمند محسوب می‌شود؛ زیرا برنامک‌های مخرب به‌راحتی از طریق این بازارها روی دستگاه‌های کاربران قابل نصب هستند. فروشگاه‌های برنامک نقش مهمی را در تضمین امنیت گوشی‌های هوشمند ایفا می‌کنند و می‌توانند از کاربران در مقابل توسعه‌دهندگان بدافزارها

[1] App Store

* نویسندهٔ عهده‌دار مکاتبات

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

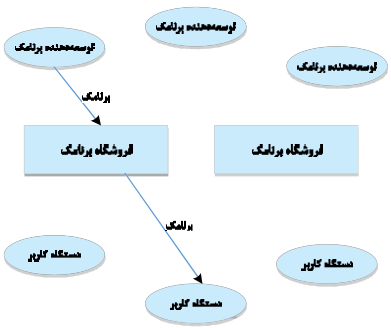
این مقاله به توزیع‌کنندگان برنامک‌ها، سازمان‌ها و بخش‌های خصوصی و دولتی کمک می‌کند تا بتوانند ریسک‌های امنیتی این حوزه را شناسایی و تأثیرات آن را به کمینه برسانند. ریسک تابعی از تهدیدها است که از آسیب‌پذیری‌ها سوء استفاده می‌کند تا بتواند به دارایی‌های سیستم دست پیدا کند یا موجب واردشدن آسیب یا خسارت 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 برنامک‌ها 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 برنامک جمع‌آوری می‌شود. در این مقاله، مهم‌ترین تهدیدها و آسیب‌پذیری‌های امنیتی در حوزه بازارهای توزیع برنامک‌های تلفن همراه هوشمند معرفی می‌شوند. آژانس امنیت اطلاعات و شبکه اروپا (ENISA[1]) در گزارش خود در مرجع [6]، به بررسی جامعی در خصوص حفظ امنیت سامانه‌های هوشمند همراه در حوزه بازارهای توزیع برنامک‌ها 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 منجر به وقوع حمله می‌شوند، مشخص می‌شوند. بر مبنای درخت حمله، ریسک‌های مطرح در سطح توزیع‌کنندگان برنامک‌های 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 جملهٔ 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 برنامک 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 زیست بوم برنامک را معرفی خواهیم کرد. پس از آن در بخش ۶، درخت حمله ترسیم می‌شود. در انتها، در بخش ۷ ریسک‌های امنیتی حوزه توزیع برنامک‌ها معرفی خواهند شد.

۲- زیست‌بوم توزیع برنامک

علاوه‌بر «فروشگاه برنامک 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» فروشگاهی را برای تلفن‌های «ویندوز تلفن همراه» ایجاد کرده است. شرکت «سیسکو» نیز فروشگاهی برای عرضهٔ برنامک‌های مخصوص تبلت‌های ساخت این شرکت توسعه داده است. بعضی از سازمان‌ها نیز اقدام به راه‌اندازی فروشگاه برنامک برای کارکنان خود کرده‌اند. در این مقاله، به مجموعه فروشگاه‌های برنامک با یک پلتفرم یکسان، «زیست‌بوم برنامک» گفته می‌شود که در شکل (۱) نشان داده شده است.



(شکل- ۱): زیست‌بوم برنامک [6]

[1] The European Network and Information Security Agency

در زیست‌بوم برنامک، توسعه‌دهندگان برنامک‌ها را ایجاد و سپس اقدام به فروش یا عرضه رایگان آن‌ها به کاربران می‌کنند. برنامک، نرم‌افزاری است که عملکرد و کارایی دستگاه کاربر (تلفن همراه هوشمند یا مرورگر) را بهبود می‌دهد. این فروشگاه‌ها، برنامک‌ها را از توسعه‌دهندگان دریافت کرده و آن‌ها را به کاربران می‌فروشند (یا توزیع می‌کنند) و در این بین، نقش واسطه[1] را ایفا می‌کنند. به‌طورمعمول فروشگاه‌ها امکان نمایش اعتبار هر برنامک را فراهم می‌کنند (برای نمونه، تعداد دانلودهای انجام‌شده برای هر برنامک، نظرات یا انتقادات کاربران و رأی کاربران). در ادامه این مقاله، به تهدیدهایی که از سوی برنامک‌های ناامن یا بدافزارها به زیست‌بوم برنامک وارد می‌شوند، می‌پردازیم. پیش از آن، ابتدا نمودار جریان داده‌ها را در زیست‌بوم برنامک معرفی می‌کنیم.

۲-۱- نمودار جریان داده‌ها در زیست‌بوم توزیع برنامک

در این بخش، نمودار جریان داده‌ها را برای زیست‌بوم برنامک 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[2] (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 برنامک، کنترل‌کننده فروشگاه برنامک.
- فرایندها[3] (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 برنامک در انبار داده فروشگاه تولید می‌کنند.
- انبار داده‌ها[4] (با دو خط موازی نشان داده می‌شوند) برای ذخیره‌ی موقت یا دائمی داده‌ها همانند سیستم فایل و پایگاه داده استفاده می‌شوند.
- مرزهای اعتماد[5] (به‌صورت خط‌چین قرمز رنگ نمایش داده می‌شوند) لبه‌های کنترل را مشخص می‌کنند. برای مثال، مرز اعتماد بین گوشی هوشمند و فروشگاه برنامک ترسیم می‌شود؛ زیرا گوشی هوشمند تحت کنترل کاربر قرار دارد و فروشگاه برنامک توسط مالک فروشگاه کنترل می‌شود.

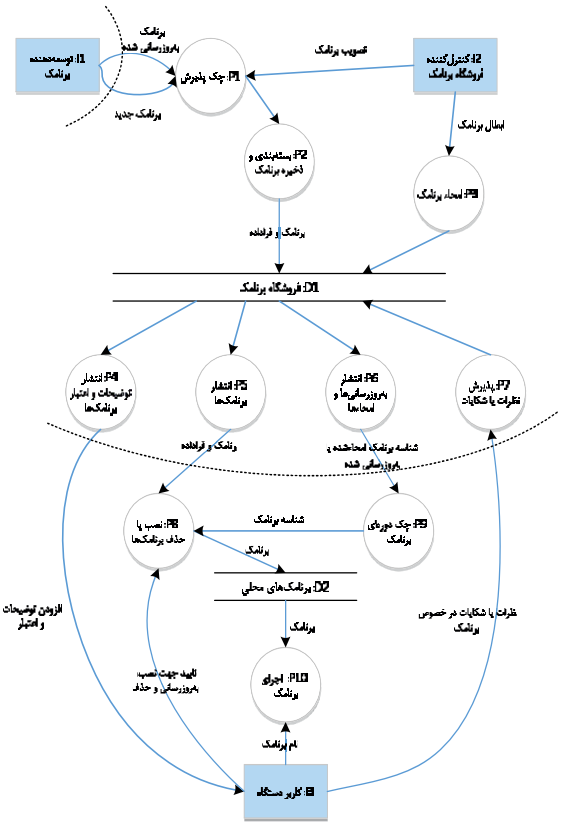
۲-۲- مدل‌سازی زیست‌بوم برنامک

نمودار کامل جریان داده برای توزیع برنامک در شکل (۲) نشان داده شده است [6]. در گوشه بالا سمت چپ نمودار در شکل (۲)، نحوه تعامل توسعه‌دهنده برنامک (I1) با فروشگاه نشان داده شده است. توسعه‌دهنده برنامک یک برنامک جدید یا به‌روزرسانی یک برنامک موجود را به چک پذیرش (P1) می‌تواند ارسال کند. چک پذیرش بررسی می‌کند که آیا برنامک برای قرارگیری در فروشگاه مناسب است یا خیر. گوشه بالا سمت راست نمودار، نحوه تعامل کنترل‌کننده فروشگاه برنامک (I2) را نشان می‌دهد. کنترل‌کننده فروشگاه، برنامک‌ها را جهت قرارگیری در فروشگاه تأیید می‌کند (P1). برنامک جدید یا برنامک به‌روزرسانی شده و همچنین تأییدیه تصویب برنامک از سوی کنترل‌کننده فروشگاه برنامک، ورودی‌های فرایند P1 را تشکیل می‌دهند. پس از انجام چک پذیرش، برنامک تأییدشده جهت قرارگیری در فروشگاه بسته‌بندی می‌شود (P2). در فرایند P2، فراداده‌ها به برنامک افزوده می‌شوند. فراداده‌ها شامل توصیفی از برنامک و فهرستی از مجوزهای دسترسی مورد نیاز برنامه روی دستگاه کاربر است. به این فراداده‌ها دراصطلاح «اظهارنامه[6]» گفته می‌شود. فرایند P2 برنامک تأییدشده را به‌همراه فراداده‌ها در انبار داده فروشگاه (D1) ذخیره می‌کند. علاوه‌بر این، کنترل‌کننده می‌تواند برنامک‌ها را امحا کند (P3). امحای یک برنامک بر اساس شکایت‌های صورت‌گرفته از آن برنامک صورت می‌گیرد. ورودی فرایند P3 دستور ابطال برنامک از سوی کنترل‌کنندهٔ فروشگاه است که عملیات امحای برنامک را از انبار داده فروشگاه انجام می‌دهد. در طی فرایند امحا، برنامک‌های 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.

[1] Broker
[2] Interactors
[3] Processes
[4] Datastores
[5] Trust boundaries
[6] Manifest

قسمت پایین نمودار، نحوه تعامل کاربر دستگاه (I3) با فروشگاه را نشان می‌دهد. کاربر دستگاه می‌تواند توصیف و اعتبار هر برنامک را ببیند (P4). برای این منظور، فرایند P4 به‌ازای هر برنامک که در انبار داده فروشگاه وجود دارد، توضیحات و اعتبار مربوط به برنامک را که از سوی سایر کاربران منتشر شده‌اند، به کاربر دستگاه نمایش می‌دهد. امکان انتشار برنامک منتشرشده توسط فروشگاه (P5) و همچنین تأییدیه نصب از کاربر دستگاه به‌عنوان ورودی فرایند نصب (P8) دریافت می‌شود. فرایند P5 برنامک ذخیره‌شده را در انبار داده فروشگاه به‌عنوان ورودی دریافت کرده و در ویترین فروشگاه به نمایش درمی‌آورد. در صورت انتخاب برنامک از سوی کاربر جهت نصب، فرایند P5 برنامک را به همراه فراداده‌هایش جهت قرارگیری روی دستگاه کاربر به فرایند P8 ارسال می‌کند. تأییدیه نصب از سوی کاربر و همچنین برنامک و فراداده‌های آن، ورودی‌های فرایند P8 را تشکیل می‌دهند. در طی انجام فرایند نصب در فرایند P8، یک برنامک در انبار داده مربوط به برنامک‌های محلی نصب‌شده روی دستگاه کاربر (D2) ذخیره می‌شود. بعد از نصب، کاربر دستگاه می‌تواند برنامک را اجرا کند (P10). مهم‌ترین فرایند انجام‌گرفته در سمت دستگاه کاربر، فرایند اجرای برنامک است. کاربر در هر زمانی که تصمیم به اجرای برنامک نصب‌شده روی دستگاه خود را داشته باشد، بایستی نام برنامک را به‌عنوان ورودی به فرایند P10 اعلام کند تا فرایند P10 از انبار داده برنامک‌های محلی (ذخیره‌شده روی دستگاه کاربر) برنامک انتخابی کاربر را روی سیستم‌عامل اجرا کند. کاربر همچنین می‌تواند نظرات و شکایات خود درباره برنامک را ثبت کند. این نظرات و شکایات در فروشگاه برنامک 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 امحاها را مرتباً دریافت می‌کند، بررسی‌های دوره‌ای برای برنامه‌های به‌روزرسانی‌شده یا امحاشده انجام می‌گیرد (P9). به‌روزرسانی‌ها و هشدارهای امحا به کاربر اعلام می‌کنند که برنامک به‌روز شده را نصب یا یک برنامه امحاشده را حذف کند. دستور ابطال برنامک (صادرشده از سوی کنترل‌کننده فروشگاه) که پیش از این از طریق فرایند P3 در انبار داده فروشگاه درج شده بود، توسط فرایند P6 خوانده شده و در فروشگاه منتشر می‌شود. فرایند P9 شناسه برنامکی را که بایستی امحا شود از فرایند P6 دریافت کرده و آن را جهت حذف برنامک از روی انبار داده برنامک‌های محلی ذخیره‌شده روی دستگاه به فرایند P8 ارسال می‌کند. ورودی فرایند P8 علاوه بر شناسه برنامک امحاشده، تأییدیه حذف برنامک از سوی کاربر است و به این ترتیب، عملیات حذف برنامک از روی انبار داده دستگاه کاربر انجام گیرد. رویه دریافت به‌روزرسانی‌ها روی دستگاه کاربر نیز مشابه دریافت امحای برنامک است.



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

مدلی که از زیست‌بوم برنامک در این بخش ارائه شد، یک مدل کلی بر اساس تحلیل بازار اندروید، فروشگاه برنامک iPhone، و فروشگاه افزونه Mozilla است و خلاصه‌ای از نحوه عملکرد زیست‌بوم‌های برنامک 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.

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 برنامک‌ها 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[1]، اطلاعات (دولتی) طبقه‌بندی‌شده[2]، دارایی‌های مالی[3]، دسترسی‌پذیری[4] و عملکرد[5] دستگاه‌ها و سرویس‌ها؛ و اعتبار شخصی و سیاسی [8]. در مطالعه دیگری، دارایی‌های سامانه هوشمند همراه به‌صورت زیر تعریف شده است [9]:

- دستگاه (دستگاه فیزیکی)
- ارتباطات (ارتباطات صوتی و پیام‌رسانی)
- داده‌های ذخیره‌شده (برنامه‌های کاربردی برون‌خط[6] و سایر داده‌های مربوط به کاربر)
- برنامک‌ها (نقشه و جهت‌یابی، شبکه‌های اجتماعی و سایر برنامک‌ها)
- 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، اتصالات[7]، داده‌ها و برنامک‌ها تقسیم‌بندی شده‌اند [10]. در این مطالعه، دارایی‌های فروشگاه‌های برنامک به پنج دسته کلی (۱) دستگاه، (۲) اتصالات، (۳) داده‌ها، (۴) برنامک‌ها و (۵) سرویس‌ها تقسیم‌بندی می‌شوند. فهرست کامل دارایی‌ها به‌همراه شرح کاملی از هر یک در جدول (۱) مشخص شده‌اند. این دسته‌بندی، جامع و کامل بوده و دربردارنده موارد مشخص‌شده در دسته‌بندی‌های دیگر نیز است.

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

دارایی	توضیحات
A1: دستگاه	دارایی‌های از نوع دستگاه شامل دستگاه فیزیکی و منابع آن (همانند باتری، حافظه اصلی[8]، 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. سرورهای پردازش و ذخیره اطلاعات در فروشگاه‌های برنامک نیز در این دسته قرار دارند.
A2: اتصالات	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[9] می‌تواند GPRS، HSDPA، UMTS، LTE و هر شبکه سلولی نسل آینده باشد) ارائه می‌دهد.
A3: داده‌ها	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[10] را به دنبال داشته باشند.

[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

	• 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 شناسه[1]های اتصال همانند Wi-Fi MAC، IMSI یا IMEI و کلیه داده‌هایی که جهت برقراری ارتباط مورد نیاز هستند، می‌شوند.
A4: برنامک‌ها	برنامک‌ها به عنوان سرویس‌های قابل ارائه به کاربر تلقی می‌گردد.
A5: سرویس‌ها	سرویس‌هایی که توسط فروشگاه برنامک مورد استفاده قرار می‌گیرند (مثالی در این زمینه تحلیل‌گرهای 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[2] 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 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 توزیع‌کنندگان 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 تلفن‌همراه که بر سیستم‌عامل، برنامه‌های کاربردی، نرم‌افزار و سخت‌افزار تأثیر می‌گذارند، معرفی کرده است [12]. پایگاه آسیب‌پذیری‌های تلفن همراه (MVD[3]) نیز منبعی دیگری است که آسیب‌پذیری‌های گزارش‌شده را در سراسر جهان برای پلتفرم‌های تلفن‌همراه جمع‌آوری می‌کند [13]. این پایگاه به کاربران این امکان را می‌دهند تا آسیب‌پذیری‌های خاص پلتفرم تلفن‌همراه 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 (NIST[4]) 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 تلفن‌همراه 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 ناامن داده‌ها (Insecure data storage)
- ارتباطات ناامن (Insecure communication)

[1] Identifier

[2] Assurance

[3] Mobile Vulnerability Database

[4] National Institute of Standards and Technology

- 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 برنامک 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 و 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 برنامک را مورد پوشش کامل قرار دهند. در ادامه، به معرفی آسیب‌پذیری‌هایی می‌پردازیم که ممکن است در فروشگاه‌های برنامک سامانه‌های هوشمند همراه وجود داشته باشد.

V1- آسیب‌پذیری‌های منجر به نصب بدافزار: در این مورد، دسته‌ای از آسیب‌پذیری‌ها مطرح هستند که به موارد زیر می‌توان اشاره کرد:

V1-1- ضعف در عملیات وصله‌کردن[1]

در فروشگاه برنامک با مدل walled-garden[2]، هر وصله پیش از آن که برای استفاده روی یک دستگاه به‌کار گرفته شود، از فرایند بازنگری[3] فروشگاه برنامک عبور داده می‌شود. به‌رغم بهبودهای امنیتی که فرایند بازنگری به دنبال دارد، روش‌های بازنگری برنامه کاربری در توزیع وصله‌ها نوعی گلوگاه[4] محسوب می‌شوند. این امر یک مانع جدی در عرضه به‌موقع برنامک‌ها تلقی می‌شود.

انجام ارزیابی جامع و کامل که در آن تک‌تک برنامک‌های 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 چالش‌برانگیز باشد.

V1-2- قابلیت‌های محدود در راه‌کارهای امنیتی شخص ثالث (مدیریت امنیتی متمرکز[5])

بسیاری از پلتفرم‌ها، امکانات عملکردی محدودی را برای سرویس‌های امنیتی شخص ثالث ارائه می‌دهند. به‌عنوان مثال، در برخی از پلتفرم‌ها، برنامک‌ها اجازه دسترسی به فرایندها را ندارند، مگر این که توسط گواهی‌نامه توسعه‌دهنده امضا شده باشند. برخی از پلتفرم‌ها نیز اجازه اجرا به انواع خاصی از برنامک‌ها را در پس‌زمینه[6] نمی‌دهند. این امر موجب می‌شود که ارائه سرویس‌های امنیتی (که مبتنی بر نظارت بر فعالیت‌های برنامک‌ها هستند) دشوار شود. این مسأله، مسئولیت بیشتری را بر عهده ارائه‌دهندگان سیستم‌عامل و فروشگاه برنامک قرار می‌دهد.

V1-3- آسیب‌پذیری‌های اعتبار

وجود آسیب‌پذیری‌ها در سامانه‌های اعتبار که برای برنامک‌ها به کار گرفته می‌شوند، ممکن است به یک مهاجم این امکان را دهد که اعتبار یک برنامک 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 برنامک مدنظر وزن‌دهی نشده‌اند و سایر موارد.

[1] Patching

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

[3] Vetting

[4] Bottleneck

[5] Centralized

[6] Background

V1-4- عدم وجود فرایندهای بررسی کد / برنامک

به‌دلیل فشارهای وارده از سوی بازار، پلتفرم‌های تلفن همراه تمایل دارند که به‌صورت باز[1] عرضه شوند و توسعه‌دهندگان را نیز تشویق می‌کنند تا به سوی توسعه باز حرکت کنند؛ لذا توسعه‌دهندگان برنامک شخص ثالث نقش مهمی را در زیست‌بوم‌های دستگاه تلفن همراه ایفا می‌کنند. علاوه‌بر این، «زیرساخت‌های امضای برنامک» و «چارچوب‌های امنیتی سطح سیستم‌عامل» نیز به‌عنوان یک مانع بزرگ برای توسعه برنامک‌ها توسط اشخاص ثالث در نظر گرفته می‌شوند. با توجه به موارد گفته‌شده، امکان تعریف فرایندهای مشخص و دقیق برای بررسی کد/برنامک در این پلتفرم‌ها دشوار خواهد بود.

V1-5- امضای برنامک

ممکن است کاربران این تصور را به غلط داشته باشند که برنامک‌های امضاشده در مقایسه با برنامک‌هایی که امضا نشده‌اند قابل اعتمادتر هستند؛ در حالی که ممکن است چنین استنباطی درست نباشد. واضح است که در برخی موارد، امضای برنامک فقط یک اظهارنامه است که نشان می‌دهد برنامک بر اساس معیارهای خاصی بررسی شده است؛ اما در مواردی دیگر، امضای برنامک یک سازوکار برای ایجاد منبع[2] برنامک است. ریسک‌های ناشی از بدافزارها و جاسوس‌افزار[3]ها نسبت به تلفن‌های همراه قدیمی‌تر افزایش یافته است؛ زیرا امکان سوء استفاده و سوءتعبیر در سازوکارهایی که به کاربران اجازه می‌دهند برنامک‌های قابل اعتماد[4] را از برنامک‌های غیر قابل اعتماد[5] تشخیص دهند (همانند سامانه‌های اعتباردهی و امضای دیجیتالی) وجود دارد.

V1-6- قابلیت باز کردن قفل سامانه هوشمند

در این آسیب‌پذیری، کاربر اقدام به غیرفعال‌کردن برخی از تنظیمات امنیتی دستگاه خود می‌کند. دستگاه تلفن همراه که قفل آن باز شده است به کاربر اجازه می‌دهد تا برنامک‌هایی 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 هیچ‌گونه فرایند بررسی روی آن صورت نگرفته است و یا از اجرای کد با مجوزهای ریشه[6] اطلاع ندارند.

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

در برخی از پلتفرم‌های گوشی‌های هوشمند، داده‌های مکانی در نام فایل[7]های عکس یا فراداده‌های فایل افزوده می‌شوند. اگر این تصاویر در اختیار سایر برنامک‌ها قرار گیرند یا در شبکه‌های اجتماعی بارگزاری شوند، از کاربران خواسته می‌شود که موافقت خود را برای دسترسی به گالری تصاویر اعلام کنند؛ درحالی‌که 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؛ به‌عنوان 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 تأئید مجوزهای دسترسی توسط کاربر: بسیاری از پلتفرم‌های سامانه هوشمند همراه، برای دسترسی برنامک‌ها به داده‌ها و پیام‌های مختلف (همانند پیام‌های هشدار[8]) در زمان نصب روی تلفن همراه موافقت[9] کاربر را از او درخواست می‌کنند. مشکلات متعددی در این زمینه وجود دارند که در ادامه به آن‌ها اشاره می‌کنیم.

[1] Open
[2] Origin
[3] Spyware
[4] Trusted
[5] Untrusted
[6] Root privileges
[7] Filename
[8] Push notification
[9] Consent

در مقایسه با رایانه‌های شخصی و لپ‌تاپ‌ها، واسط‌های کاربر به‌طورمعمول بسیار محدودتر هستند؛ به این معنا که ذخیره‌سازی اعتبارنامه‌ها روی دستگاه با احتمال بیشتری انجام می‌شود و احراز اصالت کاربر نیز نمی‌تواند به طور 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 رایانهٔ 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.

به‌طورمعمول 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 برنامکی را که برای اهداف بازاریابی تهیه شده است و اجازه دسترسی به داده‌های مکانی را درخواست می‌کند، نصب نکنید).

V4- 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[1] سازوکارهای رمزنگاری به‌شدت به رویه‌های فنی که برای مدیریت کلیدهای رمزنگارانه[2] استفاده می‌شوند، وابسته هستند.

V5- ضعف در احراز اصالت توسعه‌دهنده و توزیع‌کننده برنامک: جعل هویت[3] یک نام تجاری قابل اعتماد مانند برنامک بانکداری (و قراردادن در فروشگاه برنامک جهت عرضه) یا جعل وب‌سایت یک فروشگاه برنامک به‌سادگی امکان‌پذیر است. به‌منظور جلوگیری از جعل هویت، لازم است، توسعه‌دهندگان و توزیع‌کنندگان برنامک‌ها احراز اصالت شوند. ممکن است هیچ PKI یا زیرساخت قابل اعتماد دیگری برای تضمین هویت توسعه‌دهندگان وجود نداشته باشد.

V6- 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.

V7- 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 برنامک 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 بارگیری یا نصب برنامک‌ها کرده‌اند) را مورد هدف قرار می‌دهند. تمرکز اصلی روی حملاتی است که از طریق برنامک یا فروشگاه برنامک، بدافزار را روی دستگاه قرار می‌دهند. بین بدافزار مستقل و بدافزاری که به سایر برنامک‌ها 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)
- نگه‌داشتن کد مخرب روی دستگاه کاربر

مهم‌ترین وظیفه فروشگاه‌های برنامک 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 برنامک‌های مخرب به دستگاه‌های کاربران، بتواند این اهداف را برآورده

[1] Effectiveness

[2] Cryptographic

[3] Impersonate

کند، سایر تهدیدها و حملات جانبی از قبیل سرقت اطلاعات نیز پوشش داده می‌شود. برنامک‌هایی که مبادرت به سرقت داده‌های کاربر می‌کنند، نیز یک بدافزار با هدف ثانویه دزدی اطلاعات کاربران است. برای جلوگیری از رسیدن به این هدف لازم است فروشگاه‌های برنامک از نصب و استقرار هرگونه بدافزار روی دستگاه‌های کاربران ممانعت کنند. در اینجا، حملاتی را که هدف آن‌ها توسعه‌دهندگان یا فروشگاه‌های برنامک 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[1]، محرمانگی[2]، دسترسی‌پذیری[3] و صدور مجوز قرار دارند. نام STRIDE از ترکیب حروف نخست شش دسته تهدید زیر به دست می‌آید [4].

جعل هویت[4] (S): در این تهدید، یک فرد یا سامانه با موفقیت خود را به جای فرد یا سامانهٔ 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[5] (T): تهدید دستکاری به ایجاد تغییر مخرب در داده‌ها گفته می‌شود. مثال‌هایی از این تهدید شامل تغییرات غیرمجاز بر روی داده‌های مانا[6] همانند داده‌های ذخیره‌شده در حافظه دائمی، تغییر داده‌هایی که بین دو دستگاه تلفن همراه از طریق یک شبکه باز مثل اینترنت منتقل می‌شوند، می‌باشد.

انکار[7] (R): تهدید انکار زمانی اتفاق می‌افتد که کاربر با ازبین‌بردن 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[8] است.

افشای اطلاعات[9] (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[10] 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 به‌وقوع می‌پیوندد که با اعمال سربار[11] روی یک خدمت، عملکرد عادی آن تحت‌الشعاع قرار می‌گیرد.

ارتقای مجوزهای دسترسی[12] (E): در این نوع تهدید، فرد غیرمجاز به مجوزها دسترسی پیدا می‌کند و به این ترتیب، دسترسی کافی برای به‌مخاطره‌انداختن[13] 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:

[1] Availability
[2] Non-repudiation
[3] Authorization
[4] Spoofing
[5] Tampering
[6] Persistent
[7] Repudiation
[8] Prohibited
[9] Information disclosure
[10] Intruder
[11] Overload
[12] Elevation of Privileges
[13] Compromise

(جدول-۲): تهدیدات STRIDE [7]

نام تهدید	ویژگی تهدیدشده	تعریف تهدید	مؤلفه‌های در معرض تهدید
جعل هویت (S)	احراز اصالت	وانمود کردن یک فرایند یا تعامل‌گر به شخص/ چیز دیگری	فرایند، تعامل‌گر
دستکاری (T)	تمامیت	تغییر یک فرایند، جریان داده یا انبار داده	انبار داده، جریان داده، فرایند
انکار (R)	عدم انکار	از بین بردن شواهد مربوط به یک عمل انجام‌شده توسط یک فرایند یا یک تعامل‌گر	فرایند، تعامل‌گر
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)	دسترسی‌پذیری	اعمال سربار بیش از ظرفیت نرمال روی یک جریان داده، انبار داده یا یک فرایند به‌گونه‌ای که عملکرد عادی را تحت‌الشعاع قرار دهد.	فرایند، انبار داده، جریان داده
ارتقای مجوزهای دسترسی (E)	صدور مجوز	استفاده از یک فرایند برای انجام فعالیت‌های غیرمجاز	فرایندها

۲-۵- تحلیل تهدیدات به روش STRIDE

مدل جریان داده که در بخش ۲ معرفی شد، دارای سه تعامل‌گر، 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 مرز اعتماد کاربر دستگاه) به فرایند (P10) یعنی «اجرای برنامک»[1] 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 برنامک توسط یک مهاجم جعل می‌شود و مهاجم (با نام توسعه‌دهنده) یک برنامک مخرب را ثبت می‌کند.
	T2: مهاجم یک برنامک مخرب را ثبت می‌کند و بعدها انجام آن را انکار می‌کند.
جریان‌های داده بین توسعه‌دهنده برنامک (I1) و فروشگاه برنامک (P1)	T3: مهاجم یک برنامک یا به‌روزرسانی را به منظور اضافه کردن کد مخرب به آن دستکاری می‌کند.
	T4: مهاجم اطلاعات حساس (همانند اعتبارنامه‌های احراز اصالت توسعه‌دهنده برنامک) را به دست می‌آورد.
	T5: مهاجم با ارسال تعداد بسیار زیادی برنامک به چک پذیرش (با اعمال سربار)، مانع ثبت برنامک‌ها یا به‌روزرسانی‌ها توسط توسعه‌دهندگان می‌شود.
چک پذیرش (P1)	T6: مهاجم چک پذیرش را جعل می‌کند و باعث می‌شود توسعه‌دهنده اعتبارنامه‌های احراز اصالت را فاش کند.
	T7: مهاجم کاری می‌کند که برنامک مخرب، چک پذیرش را با موفقیت بگذراند.
	T8: فروشگاه برنامک دریافت یک برنامک یا به‌روزرسانی برای چک پذیرش را انکار می‌کند.
	T9: مهاجم اطلاعات حساس در مورد فروشگاه برنامک یا سایر توسعه‌دهندگان برنامک را از طریق چک پذیرش به دست می‌آورد.
	T10: مهاجم با ارسال تعداد بسیار زیادی برنامک به چک پذیرش (با اعمال سربار)، مانع ثبت برنامک‌ها یا به‌روزرسانی‌ها توسط توسعه‌دهندگان می‌شود.
	T11: مهاجم یک برنامک مخرب را تصویب می‌کند و یا یک برنامک را از طرف فرد دیگری ثبت می‌کند.
تعامل‌گر I3 (کاربر دستگاه)	T12: مهاجم خود را به جای کاربر دستگاه جا می‌زند و بازخورد[2] نادرست را برای یک برنامک پست می‌کند یا تعداد دانلودهای برنامک‌ها را تحریف می‌کند.
	T13: مهاجم ارسال یک بازخورد غلط را انکار می‌کند.
انتشار توضیحات و اعتبار	T14: مهاجم رابط فروشگاه برنامک را جعل می‌کند تا کاربران توضیحات غلط و مقادیر نادرستی را برای اعتبار برنامک‌ها ببینند.

[1] Execute

[2] Feedback

برنامک (P4)	T15: مهاجم رابط فروشگاه برنامک را با هدف تغییر توضیحات و اعتبارهای برنامک‌ها دستکاری می‌کند.
	T16: مهاجم توضیحات و اعتبارها را جستجو می‌کند اما بعدها انجام آن را انکار می‌کند.
	T17: مهاجم اطلاعات حساس (همانند اطلاعاتی در مورد این که کدام کاربران می‌خواهند کدام برنامک‌ها را نصب کنند) را به دست می‌آورد.
	T18: مهاجم از طریق اعمال سربار روی فروشگاه برنامک، مانع کاربران در جستجوی توضیحات مربوط به برنامک می‌شود.
	T19: مهاجم اقدام به انجام فعالیت‌های غیرمجاز همانند تغییر توضیحات و اعتبارهای برنامک‌ها می‌کند.
جریان داده‌ها بین P4 و I3: توضیحات و اعتبار برنامک	T20: مهاجم توضیحات و اعتبار برنامک‌ها را تغییر می‌دهد.
	T21: مهاجم اطلاعاتی را در مورد این که کدام کاربران، کدام برنامک‌ها را نصب کرده‌اند، به دست می‌آورد.
	T22: مهاجم با اعمال سربار، مانع کاربران در جستجوی توضیحات برنامک می‌شود.
انتشار برنامک (P5)	T23: مهاجم فروشگاه برنامک را جعل می‌کند تا دستگاه برنامک‌های مخرب را نصب کند.
	T24: مهاجم فروشگاه برنامک را دستکاری می‌کند تا دستگاه برنامک‌های مخرب را نصب کند.
	T25: مهاجم یک برنامک را برای نصب دانلود می‌کند و بعدها انجام آن را انکار می‌کند.
	T26: مهاجم اطلاعات حساس (همانند اطلاعاتی در مورد این که کدام برنامک‌ها روی کدام دستگاه‌ها نصب شده‌اند) را از فروشگاه برنامک به دست می‌آورد.
	T27: مهاجم دسترسی به فروشگاه برنامک را انکار می‌کند تا مانع دستگاه‌ها برای دانلود برنامک‌ها و به‌روزرسانی‌ها جهت نصب شود.
	T28: مهاجم اقدام به انجام فعالیت‌های غیرمجاز همانند افزودن برنامک‌های (مخرب) بیشتر به فروشگاه می‌کند.
جریان داده‌ها بین P5 و P8: برنامک و فراداده‌ها	T29: مهاجم برنامک را دست‌کاری می‌کند تا دستگاه یک برنامک مخرب را نصب کند.
	T30: مهاجم اطلاعاتی در مورد اینکه کدام برنامک‌ها روی کدام دستگاه‌ها نصب شده‌اند را به دست می‌آورد.
	T31: مهاجم مانع دستگاه برای دانلود برنامک‌ها یا به‌روزرسانی‌ها جهت نصب می‌شود.
انتشار به‌روزرسانی‌ها و امحاء (P6)	T32: مهاجم فروشگاه برنامک را جعل می دستگاه نتواند تمامی امحاءها و به‌روزرسانی‌ها را دریافت کند.
	T33: مهاجم رابط فروشگاه برنامک را دستکاری می‌کند تا دستگاه نتواند کل امحاءها و به‌روزرسانی‌ها را دریافت کند.
	T34: مهاجم اخطار مربوط به به‌روزرسانی یا امحاء را دریافت می‌کند و بعدها دریافت اخطار را انکار می‌کند.
	T35: مهاجم اطلاعات حساس (همانند کدام برنامک‌ها روی کدام دستگاه‌ها نصب شده‌اند) را از رابط فروشگاه برنامک به دست می‌آورد.
	T36: مهاجم دسترسی به رابط فروشگاه برنامک را انکار می‌کند تا مانع دریافت به‌روزرسانی‌ها و امحاءها توسط کاربران شود.
	T37: مهاجم فعالیت‌های غیرمجاز همانند تغییر یا حذف به‌روزرسانی‌ها و امحاءها را انجام می‌دهد.
جریان داده‌ها بین P6 و P9: شناسه برنامک‌های امحاءشده یا به‌روزرسانی شده	T38: مهاجم به‌روزرسانی‌ها و امحاءها را از دستگاه دستکاری می‌کند، به طوری که دستگاه تمامی به‌روزرسانی‌ها و امحاءها را دریافت نکند.
	T39: مهاجم اطلاعاتی در خصوص این که کدام برنامک‌ها روی کدام دستگاه‌ها نصب شده‌اند را به‌دست می‌آورد.
	T40: مهاجم مانع دستگاه‌ها در دریافت به‌روزرسانی‌ها یا امحاها جهت نصب می‌شود.
پذیرش نظرات یا شکایات (P7)	T41: مهاجم فروشگاه برنامک را جعل می‌کند، به طوری که کاربر نظرات و شکایات خود را در مکان نادرستی اعلام کند.
	T42: مهاجم رابط فروشگاه برنامک را با هدف تغییر یا حذف شکایات دستکاری می‌کند.
	T43: مهاجم اطلاعات مربوط به بازخورد مثبت را ثبت می‌کند و بعدها این اقدام را انکار می‌کند.
	T44: مهاجم اطلاعات حساس (همانند اطلاعاتی که مشخص می‌کنند کدام برنامک‌ها روی کدام دستگاه‌ها نصب شده‌اند) را به دست می‌آورد.
	T45: مهاجم مانع کاربران دستگاه در ثبت نظرات و شکایات توسط می‌شود؛ این کار را از طریق ارسال تعداد بسیار زیادی نظر به فروشگاه برنامک و اعمال سربار انجام می‌دهد.
	T46: مهاجم فعالیت‌های غیرمجاز همانند حذف نظرات یا شکایات در مورد یک برنامک را انجام می‌دهد.
جریان داده‌ها بین P7 و I3: نظرات یا شکایت درباره برنامک	T47: مهاجم نظرات و شکایات ارسالی از سوی کاربر دستگاه را تغییر می‌دهد.
	T48: مهاجم اطلاعات حساس در مورد کاربران دستگاه (همانند اطلاعات در مورد این که کدام برنامک‌ها توسط کدام کاربران نصب شده‌اند یا جزئیات اطلاعات شخصی درباره کاربران دستگاه) را به دست می‌آورد.

	T49: مهاجم از طریق ارسال تعداد بسیار زیادی نظر به فروشگاه برنامک، مانع کاربران دستگاه در ثبت نظرات و شکایات می‌شود.
نصب یا حذف برنامک (P8)	T50: مهاجم دستگاه را جعل می‌کند تا بتواند اطلاعات آماری در خصوص این که کدام کاربران اقدام به نصب کدام برنامک‌ها یا به‌روزرسانی‌ها کرده‌اند را تحریف کند.
	T51: مهاجم نصاب[1] را با هدف نصب برنامک‌های مخرب دستکاری می‌کند.
	T52: مهاجم یک برنامک را نصب می‌کند (و بعدها انجام آن را انکار می‌کند) تا بتواند اطلاعات آماری در خصوص این که کدام کاربران اقدام به نصب کدام برنامک‌ها 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 سربار بر نصاب، مانع کاربران در نصب به‌روزرسانی‌ها یا حذف برنامک‌های امحاءشده می‌شود.
	T55: مهاجم اقدام به انجام فعالیت‌های غیرمجاز همانند نصب برنامک‌های مخرب و rootkitها می‌کند.
چک دوره‌ای برنامک (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 امحاء 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 برنامک به دست می‌آورد (به عنوان مثال، کدام برنامک‌ها روی کدام دستگاه‌های کاربر نصب شده‌اند).
	T60: مهاجم روی فرایند سربار اعمال می‌کند تا مانع دریافت اطلاعات به‌روزرسانی‌ها و امحاءها در دستگاه کاربر شود.
	T61: مهاجم اقدام به انجام فعالیت‌های غیرمجاز به منظور حذف امحاءها می‌کند.
اجرای برنامک (P10)	T62: مهاجم فرایند اجرا را جعل می‌کند تا کاربران (به اشتباه) تصور کنند که یک برنامک در حال اجرا است.
	T63: مهاجم فرایند اجرا را دستکاری می‌کند تا توابع مخرب عمل کنند.
	T64: مهاجم می‌تواند یک برنامک 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 سربار اعمال می‌کند تا مانع کاربر در اجرای برنامک‌های دیگر شود.
	T67: مهاجم فعالیت‌های غیرمجاز همانند دستکاری برنامک‌های دیگر، خواندن داده‌های ذخیره‌شده توسط سایر برنامک‌ها یا خواندن اطلاعات حساس را انجام می‌دهد.

[1] Installer

۶- درخت حمله

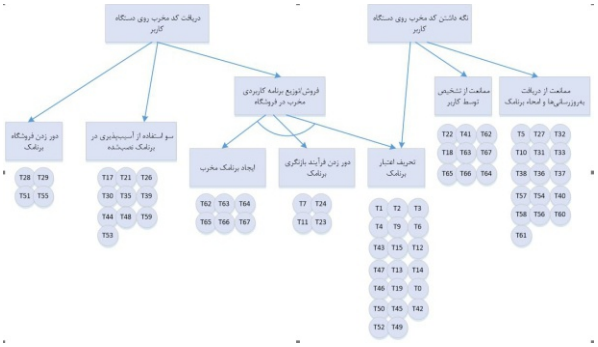
تحلیل STRIDE انواع متفاوتی از تهدیدات را از دیدگاه تهاجمی می‌تواند مشخص کند. پس از شناسایی تهدیدها لازم است از درخت حمله به‌منظور مدل‌سازی گرافیکی حمله علیه سامانه استفاده شود. تمرکز اصلی در مدل‌سازی تهدید بر چگونگی به وقوع و به نتیجه‌رسیدن حمله است. درخت حمله ابزاری است که بر اساس تهدیدهای مختلف، هدف 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 رویداد[2] 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) منحصربه‌فرد است [17]. آنچه که مسیر را منحصربه‌فرد می‌کند، زیرگرهٔ 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،

[2] Event

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

در شکل (۳)، درخت حمله مربوط به حملهٔ 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 برنامک‌های مخرب و هم سوء استفاده از برنامک‌های 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 حاصل‌ضرب «احتمال وقوع تهدید» در «تأثیر یک تهدید» علیه دارایی‌های یک سازمان یا یک فرد به‌دست 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 برنامک‌های 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.

۷-۱- ریسک R1: دورزدن فروشگاه برنامک

در این ریسک، مهاجم اقدام به دورزدن فروشگاه برنامک رسمی کرده و برنامک‌های خود را از طریق یک فروشگاه برنامک غیررسمی عرضه می‌کند. پس از آن فعالیت‌های غیرمجاز همانند افزودن برنامک‌های مخرب و rootkit به فروشگاه غیررسمی را انجام می‌دهد. مهاجم، یک برنامک یا فرایند نصب در فروشگاه را دستکاری می‌کند تا دستگاه کاربر آن برنامک 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 برنامک‌های مخرب کند. مشخصات این ریسک که شامل تهدیدها، آسیب‌پذیری‌ها و دارایی‌ها می‌شود، در جدول (۴) ارائه شده است. مثالی از این ریسک، برنامک Financial Times (FT) است که فروشگاه iTunes اپل و بازار اندروید گوگل را دور زد تا بتواند به‌طورمستقیم با خوانندگان ارتباط برقرار کند. برنامک FT یک برنامک 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].

(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 برنامک و نصب برنامک‌ها از فروشگاه‌های غیرمجاز (یا منابع تأییدنشده) توسط کاربر، احتمال مخرب بودن برنامک 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 تائید 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: برنامک‌ها

۲-۷- ریسک R2: سوء استفاده از آسیب‌پذیری‌های موجود در برنامک نصب‌شده

در این ریسک، مهاجم از آسیب‌پذیری‌های موجود در برنامک نصب‌شده سوء استفاده کرده و پس از آن، اطلاعات حساس همانند مشخصات کاربرانی که اقدام به نصب برنامک کرده‌اند و همچنین اطلاعات مربوط به برنامک‌های نصب‌شده روی دستگاه‌ها را از طریق رابط کاربری فروشگاه یا برنامک نصب‌شده به دست می‌آورد. برای این که مهاجم بتواند به اطلاعات حساس (در مورد کاربران و برنامک‌های نصب‌شده روی دستگاه) از طریق فروشگاه دست پیدا کند، از آسیب‌پذیری‌های اعتبار که در فروشگاه برنامک 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 برنامک‌های نصب‌شده از سوی فروشگاه سوء استفاده می‌کنند، برآورده می‌شود. تأثیر وقوع این تهدیدها بر دارایی‌های سازمان‌ها (به‌دلیل دستیابی به داده‌های حساس سازمانی، دولتی و مالی) و در فروشگاه‌های برنامک‌ها رسمی به‌دلیل این که اعتبار فروشگاه زیر سؤال می‌رود، زیاد است.

(جدول-۵): مشخصات ریسک شماره دو

تهدیدها	- T17، T21، T26، T30، T35، T39، T44، T48، T53، T59 توضیح: با توجه به تهدیدات T17، T21، T26، T30، T35، T39، T44، T48، T53 و T59 در صورت وجود آسیب‌پذیری در انباره داده و یا رابط فروشگاه برنامک، مهاجم اطلاعات حساس (همانند مشخصات کاربرانی که اقدام به نصب برنامک کرده‌اند، اطلاعاتی که مشخص می‌کنند کدام برنامک‌ها روی کدام دستگاه نصب‌شده است و همچنین اطلاعات مربوط به دستگاهی که کاربر مورداستفاده قرار می‌دهد) را به دست می‌آورد.
آسیب‌پذیری‌ها	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.
	V4- ضعف در رمزنگاری. تهدیدات T21 و T59 و T39 توسط این آسیب‌پذیری رخ می‌دهند.
دارایی‌ها	A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامک‌ها

۳-۷- ریسک R3: ایجاد برنامک‌های مخرب

در این ریسک فقط تهدیدها مربوط به اجرای برنامک مورد توجه قرار می‌گیرند؛ زیرا در اغلب موارد، رفتار مخرب در زمان اجرا پدیدار می‌شود. در این نوع تهدیدها، مهاجم فرایند اجرای برنامک 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 Rufraud دریافت شده‌اند [19]. مجموعه آسیب‌پذیری‌هایی که منجر به نصب بدافزار می‌شوند، کانال‌های مخفی/ جعبه شنی ضعیف، ضعف در تأئید مجوزهای دسترسی توسط کاربر، عدم وجود بهروش‌هایی برای حفاظت از حریم خصوصی و عدم آگاهی کاربر در بروز ریسک ایجاد و اجرای برنامک مخرب دخیل هستند. مشخصات ریسک ایجاد برنامک‌های مخرب در جدول (۶) قابل مشاهده است.

(جدول-۶): مشخصات ریسک شماره سه

تهدیدها	- 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 برنامک مخرب در سمت دستگاه تلفن همراه کاربر مورد توجه قرار گرفته است.
آسیب‌پذیری‌ها	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 تائید 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،

	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.
دارایی‌ها	A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامک‌ها

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

در این ریسک مهاجم تهدیدهایی را اعمال کرده تا فرایند بررسی برنامک را دور می‌زند و فروشگاه برنامک را با هدف عرضه برنامک‌ها جعل یا دستکاری می‌کند. به این ترتیب، مهاجم می‌تواند برنامک مخرب را در فروشگاه عرضه کند یا بفروشد و کاربران با فرض این که برنامک‌های عرضه‌شده از سوی فروشگاه قابل اعتماد هستند، برنامک مخرب را روی دستگاه خود نصب می‌کنند؛ علاوه بر این، رفتارهای پرخطر که در زمینه دورزدن فرایند بررسی برنامک‌ها از سوی توسعه‌دهندگان شناخته‌شده 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 به‌دست‌آوردن اعتبارنامه‌های توسعه‌دهندگان برنامک انجام می‌گیرند، نمونه‌ای از خطراتی بوده که در فروشگاه‌های برنامک مشاهده شده است. درصورت وقوع این حملات، دارایی‌های فروشگاه‌ها به‌شدت تحت تأثیر قرار خواهند گرفت. مشخصات ریسک ایجاد دورزدن فرایند بررسی برنامک‌ها در جدول (۶) نشان داده شده است.

(جدول-۷): مشخصات ریسک شماره چهار

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

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

۵-۷- ریسک R5: تحریف اعتبار برنامک‌ها

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

حمله‌ای که اقدام به تحریف اعتبار برنامک‌ها 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 برنامک اپل نیز گزارش شده است [20].

فروشگاه‌های برنامک هر روز رقابتی‌تر می‌شوند و ناشران برنامک 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 برنامک، apptentive برای بازخورد درون‌برنامه ای و ابزارهای نگهداری شده است. متأسفانه در چند سال اخیر، مواردی مشاهده شده‌اند که به‌نظر می‌رسد ناشران برنامک 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 برنامک محدود نمی‌شود و کاربران نیز این عمل را به‌مدت چندین سال روی آمازون انجام می‌دادند. آمارها نشان می‌دهند که ۵۵ درصد از برنامک‌ها که شامل بررسی‌های جعلی بوده‌اند، مربوط به برنامک‌های iOS بوده و ۴۵ درصد مربوط به برنامک‌های اندروید بوده‌اند.

(جدول-۸): مشخصات ریسک شماره پنج

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

	T46، T47، T49 توضیح: بر اساس تهدیدات مطرح‌شده، مهاجم اقدام به جعل هویت توسعه‌دهنده برنامک یا کاربر دستگاه کرده تا بتواند اعتبار برنامک را جعل کرده و کاربران را تشویق به نصب برنامک‌ها مخرب از طریق فروشگاه نماید.
آسیب‌پذیری‌ها	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 برنامک. تهدیدات T1، T2، T3 و T4 توسط این آسیب‌پذیری رخ می‌دهند.
دارایی‌ها	A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامک‌ها

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

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

(جدول-۹): مشخصات ریسک شماره شش

تهدیدها	T18 -، T22، T41، T62، T63، T64، T65، T66، T67 توضیح: با توجه به تهدیدات T18، T22، T41، T62، T63، T64، T65، T66 و T76، مهاجم با انجام فعالیت‌های مخرب که مانع ثبت مقادیر واقعی برای نظرات، شکایات و توضیحات مربوط به برنامک می‌شود، موجب می‌شود که کاربران اقدام به نصب برنامک‌ها مخرب روی دستگاه خود نمایند.
آسیب‌پذیری‌ها	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 شنی ضعیف. کلیه تهدیدات T62، T63، T64، T65، T66، T67 و T68 توسط این آسیب‌پذیری رخ می‌دهند. V3- ضعف در تائید 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، 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.
دارایی‌ها	A1: دستگاه A2: اتصالات A3: داده‌ها A4: برنامک‌ها

۷-۷- ریسک R7: ممانعت از دریافت به‌روزرسانی‌ها و امحاء برنامک

در این ریسک، مهاجم مانع از دریافت به‌روزرسانی‌ها و امحاءها از طرف فروشگاه برنامک در دستگاه کاربران می‌شود. درصورتی‌که کاربر اقدام به نصب یک کد مخرب روی دستگاه خود کرده باشد، درصورت بالفعل‌شدن 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 برنامک در دستگاه‌های کاربر اطمینان حاصل کند. گاهی نیز نیاز است که علاوه‌بر حذف از روی دستگاه‌های کاربران، فروشگاه نسبت به حذف برنامک از ویترین خود اقدام کند.

(جدول-۱۰): مشخصات ریسک شماره هفت

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

۸- نتیجه‌گیری

در این پژوهش، جهت راهنمایی متخصصان امنیتی در حوزه ارائه برنامک‌های مربوط به سامانه‌های هوشمند همراه، ریسک‌های امنیتی مربوط به حوزه توزیع برنامک‌های سامانه‌های هوشمند همراه شناسایی و معرفی شدند. به‌منظور دستیابی به این هدف ابتدا، زیست‌بوم توزیع برنامک استخراج و معرفی و سپس، دارایی‌ها و آسیب‌پذیری‌های این حوزه ارائه شد. براساس «مدل‌سازی تهدید»، مهم‌ترین تهدیدهای امنیتی رایج در زیست‌بوم توزیع برنامک استخراج شدند. در انتها، ریسک‌های امنیتی مطرح در سطح توزیع‌کنندگان برنامک‌های 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 برنامک‌های 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 برنامک‌ها یا «فروشگاه‌های برنامک» می‌تواند باشد. با این حال برنامه‌ریزی جهت تدوین و اجرای سیاست‌ها و دستورالعمل‌های امنیتی به‌صورت الزامات امنیتی قابل اجرا توسط توزیع‌کنندگان برنامک‌های 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.

[11] Shirey, R., *RFC 2828 Internet Security Glossary*, IETF, 2000.

[12] Vulnerability-lab. *Vulnerability Research, Bug Bounties & Vulnerability Assesments* [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. Quirolgico, 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/

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

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.