مقاله مروری

مجله انفورماتیک سلامت و زیست پزشکی
مرکز تحقیقات انفورماتیک پزشکی
دوره دوم شماره اول. ص٥٦-٤٨، ١٣٩٤

مروری جامع بر خطرات تهدید کننده امنیت اطلاعات سلامت در ابزارهای سیار

روح‌الله خارا[1]، مرضیه صارمیان[2]*

• دریافت مقاله: ۹۴/۳/۲ • پذیرش مقاله: ۹۴/۳/۲۴

مقدمه: یکی از جلوه‌های نوین فناوری اطلاعات که به دلیل داشتن قابلیت‌های منحصر به فرد در سازمان‌های سلامت به کار گرفته شده است، ابزار سیار می‌باشد. دانستن این که چه تهدیدات و خطراتی امنیت ابزار سیار و اطلاعات را به خطر می‌اندازد موجب کنترل بهتر و کاهش عواقب منفی در صورت بروز مشکل می‌شود. هدف از انجام این مطالعه شناخت تهدیدات و خطرات امنیتی مربوط به اطلاعات در استفاده از ابزار سیار در حوزه سلامت می‌باشد.

روش: این مقاله نوعی مطالعه مروری- نقلی است، که مقالات حاصل از جستجوی کلمات کلیدی مربوط به امنیت اطلاعات ابزار سیار در حوزه سلامت در پایگاه‌های داده‌های مرتبط و مربوط به سال ۲۰۰۵ لغایت ۲۰۱۵ را در بر می‌گیرد. همچنین مقالات مرتبط با موضوع در فهرست منابع مقالات منتخب نیز مورد بررسی قرار گرفتند. سپس مهم‌ترین تهدیدات، شناسایی و به صورت سازماندهی شده ارائه شد.

نتایج: طبق بررسی مطالعات انجام شده، مهم‌ترین تهدیدات و خطرات امنیت اطلاعات ابزار سیار شامل ۱۹ مورد اصلی بوده است. بعضی از این موارد شامل: به سرقت رفتن یا گم شدن ابزار سیار، حملات هدف‌دار توسط هکرها، بد افزارها و مواردی از این قبیل هستند.

نتیجه‌گیری: سازمان‌های سلامت باید کلیه چالش‌های مربوط به استفاده از ابزار سیار به خصوص چالش‌های مربوط به امنیت را مورد توجه قرار دهند تا با آگاهی از این چالش‌ها بتوانند از این ابزار بهره گیری کامل را به عمل آورند.

کلید واژه‌ها: تهدید امنیتی، ابزار، سیار، امنیت، اطلاعات سلامت

•ارجاع: خارا روح‌الله، صارمیان مرضیه. مروری جامع بر خطرات تهدید کننده امنیت اطلاعات سلامت در ابزارهای سیار. مجله انفورماتیک سلامت و زیست پزشکی ۱۳۹۴؛ ۲(۱):۵۶-۴۸.

۱. کارشناس ارشد فناوری اطلاعات سلامت، بیمارستان فیروزگر، تهران، ایران

۲. کارشناس ارشد فناوری اطلاعات سلامت، دانشگاه علوم پزشکی لرستان، خرم‌آباد، ایران

* **نویسنده مسؤول:** لرستان، خرم آباد، دانشگاه علوم پزشکی لرستان

• **شماره تماس:** ۰۹۱۶۳۶۹۰۵۹۷

• **Email:** marziehsaremian@gmail.com

مقدمه

امروزه فناوری اطلاعات به عنوان مؤثرترین عامل در افزایش کارایی و اثربخشی سازمان‌ها محسوب می‌شود [۲،۱]. همراستا با پیشرفت‌های علم و فناوری، مراقبت سلامت نیز به سرعت در حال پیشرفت است، به گونه‌ای که فناوری‌های جدید، جنبه‌های جدیدی از خدمات مراقبت سلامت را شکل داده‌اند [۳]. یکی از جلوه های نوین فناوری اطلاعات که به دلیل داشتن قابلیت‌های منحصر به فرد، تقریباً در تمامی سازمان‌ها، از جمله سازمان‌های مراقبت سلامت به کار گرفته شده است، فناوری ابزار سیار است [۱]. چنان که، تلفن‌های هوشمند و دیگر ابزارهای سیار نقش مهم و محوری در چگونگی برقراری ارتباط، اتصال به شبکه و انجام فعالیت‌های روزمره مانند، کارهای بانکی، خرید و فروش و غیره را در صنایع مختلف و همچنین در زندگی روزمره مردم انجام می‌دهند [۴]. صنعت سلامت نیز به دلیل مشکلات فراوان از جمله محدودیت منابع، افزایش هزینه‌های بهداشتی و درمانی، نیاز به دسترسی فوری به اطلاعات بهداشتی و درمانی به ویژه در وضعیت‌های اورژانسی، تصادفات و مناطق روستایی و صعب العبور، سعی در به کار گیری هرچه بیشتر این نوع ابزار دارد [۵،۱]. همچنین قابلیت‌های منحصر به فرد ابزار سیار از جمله حمل آسان و دسترسی سریع به اطلاعات، نرم افزارهای کاربردی فراوان، ارزان بودن، استفاده آسان و دسترسی به شبکه جهانی اینترنت در هر زمان و مکان، از یک طرف و سیار بودن دائمی متخصصان و کارکنان سازمان‌های سلامت از طرف دیگر دلیل دیگر استفاده از ابزارهای سیار در صنعت سلامت است [۷،۶،۱]. تا آنجایی که وجود ابزارهای پرتابل به عنوان یکی از الزامات آمادگی سازمان‌ها برای پیاده سازی پرونده الکترونیک سلامت به حساب می‌آید [۸].

از سوی دیگر رویکردهای جدید حوزه سلامت به گونه‌ای است که بیماران را بیشتر در روند سلامتی و درمان خود درگیر می سازد. در همین راستا، فناوری‌های کاربردی مانند اینترنت، نوت بوک‌ها، تبلت‌ها و گوشی‌های تلفن همراه، بیماران را قادر می‌سازد که به طور فعال در مراحل درمان و دیگر مراحل مربوط به سلامت خود شرکت داشته باشند. از این رو بهداشت و درمان در حال حرکت به سوی ارائه خدمات بهداشتی با استفاده از ابزار سیار و سنسورها و همچنین استفاده از فناوری‌های بی‌سیم در جهت کمک به بهبود ارائه خدمات و اطلاعات بهداشتی است [۱۰،۹].

ابزارهای سیار با وجود همه مزایایی که دارند، با طیف گسترده‌ایی از چالش‌ها و تهدیدها مواجه‌اند [۱۱]. به گونه‌ای که به کارگیری این نوع ابزارها در سازمان‌های مراقبت سلامت ممکن است خطرات زیادی به همراه داشته باشد. یکی از بحرانی‌ترین چالش‌های به وجود آمده، افزایش خطرات مربوط به امنیت و محرمانگی اطلاعات است، که می‌تواند منجر به نقص یا آسیب ناخواسته به بیماران و سازمان‌های مراقبت سلامت شود [۵]. در سیستم اطلاعاتی سازمان‌های مراقبت سلامت، اطلاعات زیادی از منابع متنوع، از جمله بخش اورژانس، آزمایشگاه، داروخانه، بخش مراقبت های ویژه، اتاق عمل، واحد مالی و غیره گرد آوری می شوند [۱۲]. مسائلی که در مورد جوانب امنیتی، حقوقی، اخلاقی و محرمانگی اطلاعات بیماران وجود دارد، علاوه بر زیان‌هایی برای بیمار، باعث بروز مشکلات زیادی در سیستم‌های ارائه دهنده خدمات بهداشتی –درمانی می‌شود [۱۳]. تا آنجا که حتی می‌توان گفت، استفاده از سلامت الکترونیک تنها مشروط بر حفظ حریم خصوصی بیماران و رعایت حقوق محرمانگی، سودمند است [۱۴].

از زمان پیدایش سیستم‌های اطلاعاتی تا کنون امنیت یکی از مهم‌ترین ابعاد هر سیستم اطلاعاتی است و ارتباطات امن و قابل اطمینان از طریق ابزار و رسانه‌های ارتباطی مانند اینترنت، همواره یکی از الزامات اولیه سیستم‌های اطلاعاتی به حساب می‌آید [۱،۷]. مسئله امنیت اطلاعات الکترونیک یکی از مهم‌ترین دغدغه‌های نیم قرن اخیر متخصصین حوزه سلامت بوده است و امروزه نیز امنیت و محرمانگی اطلاعات در بخش مراقبت سلامت یک مسئله مهم و در حال رشد است. پذیرش پرونده‌های دیجیتال، قوانین و افزایش نیاز به تبادل اطلاعات بین بیماران و فراهم کنندگان و پرداخت کنندگان، همگی باعث شده است که امروزه توجه به امنیت اطلاعات بیشتر شود [۱۵،۱]. تا جایی که نگرانی‌های مربوط به محرمانگی اطلاعات ممکن است مانع از به ثمر رسیدن تمامی ابعاد فناوری‌های جدید در حوزه بهداشت و درمان شود [۱۶]. همچنین با کامپیوتری شدن اطلاعات شخصی آنلاین ممکن است، شخصی ترین و حساس ترین اطلاعات بیماران در معرض خطر قرار گیرد [۱۷]. به دلیل ظرفیت رو به رشد فناوری برای جمع آوری، ذخیره و انتقال حجم زیاد اطلاعات، نگرانی بیماران در مورد دسترسی افراد به اطلاعات شخصی آن‌ها افزایش یافته است [۱۸،۱۵].

بنابراین امروزه با ظهور دستاوردهای نوین فناوری در قالب ابزارهای سیار نیاز به فاکتورهای امنیتی جدیدتری نیز احساس می‌شود [۱۹،۹،۱]. از این رو یکی از مهم‌ترین مسائلی که در زمینه امنیت ابزار سیار باید مورد مطالعه دقیق قرار گیرد، مسئله شناخت تهدیدها و خطرات امنیتی است. دانستن این که چه

تهدیدات و خطراتی امنیت ابزار و اطلاعات را به خطر می‌اندازد موجب کنترل بهتر و کاهش عواقب منفی در صورت بروز مشکلاتی می‌شود که ابزار سیار و به تبع آن اطلاعات سلامت را مورد تهدید قرار می‌دهد [۲۰]. هدف از انجام این مطالعه شناخت تهدیدات و خطرات امنیتی مربوط به امنیت ابزار سیار و امنیت اطلاعات این ابزارها در حوزه سلامت می‌باشد.

روش

مطالعه حاضر به صورت مرور جامع مقالات، پایان‌نامه‌ها، کتب و نیز پایگاه‌های داده از جمله، PubMed، ProQuest، scholar Google، SID، Magiran و IranMedex انجام شده است. در این مطالعه سعی بر آن بود که مهم‌ترین تهدیدات امنیت اطلاعات ابزار سیار در حوزه سلامت، شناسایی شده و به صورت سازماندهی شده ارائه گردند. بدین منظور پژوهشگران از طریق جستجو در پایگاه های داده مرتبط و با استفاده از کلید واژه‌های "تهدید امنیتی"، "ابزار سیار"، "امنیت"، "اطلاعات سلامت" و مترادف انگلیسی آن‌ها، مستندات مربوط به بازه زمانی سال‌های ۲۰۰۵ لغایت ۲۰۱۵ را مورد بررسی قرار دادند و همواره سعی بر این بوده که از مستندات جدیدتر استفاده نمایند.

نتایج

امروزه خطرات امنیتی و راه‌های مقابله با آن، به تکنولوژی به کار رفته در هر سازمان وابسته است [۲۱]. ابزارهای سیار دارای انواع مختلفی از شکل‌ها، قابلیت پردازش و دسترسی بی‌سیم می‌باشند. این ابزارها شامل انواع لپ تاپ‌ها، گوشی‌های هوشمند، شبکه حس‌گرها، حافظه‌های فلش، هاردهای اکسترنال، تبلت‌ها، و حتی ابزار ردیابی می‌باشند، البته ابزار سیار به همین‌ها محدود نمی‌شوند [۱۶،۵]. از آنجایی که استفاده از ابزار سیار روز به روز در حال افزایش است، این ابزارها از طیف وسیعی از نرم‌افزارها و سخت‌افزارها استفاده می‌کنند [۲۲]. آن‌ها اندازه فیزیکی کوچک، حافظه ذخیره‌سازی و قدرت پردازش ضعیفی دارند، همچنین رابط کاربری محدود به دلیل کوچک بودن صفحه نمایش و به خاطر استفاده از باتری، محدودیت استفاده از برق را دارند. این ابزارها می‌توانند به صورت بی‌سیم با استفاده از فناوری‌های ارتباطی مانند بلوتوث (Bluetooth)، فروسرخ یا امواج رادیویی با دیگر ابزارها ارتباط برقرار کنند. همچنین برای انجام بسیاری از فعالیت‌ها از قبیل ارسال و دریافت ایمیل و دسترسی به اینترنت، مدیریت قرار ملاقات‌ها و دسترسی به اطلاعات، بررسی اسناد، پاسخگویی از طریق پست الکترونیک، ارائه و نمایش داده‌ها و دسترسی به داده‌های سازمانی بسیار مفیداند. نکته قابل توجه این که، همه این کارها را با هزینه‌ایی پایین انجام می‌دهند. به طور کلی ابزارهای دستی در محیط‌های مختلفی به صورت سبک و قابل حمل با اهداف و کارایی‌های مختلف استفاده می‌شوند. همین قابلیت‌ها و برنامه‌های کاربردی غنی، آن‌ها را به اهداف جذابی برای مهاجمان تبدیل نموده است. به همین دلیل است که محیط به کارگیری ابزار سیار، نیازهای امنیتی خاص خود را دارد [۲۳،۱۱]. محیط‌های سیار نسبت به محیط‌های ثابت سنتی، تفاوت‌های منحصر به فردی دارند. از این رو روش‌هایی که برای مقابله با تهدیدات و خطرات امنیتی ابزار سیار استفاده می‌شود، تفاوت‌های عمده‌ایی با روش‌های مقابله با تهدیدات برای کامپیوترهای رومیزی و غیره دارد [۲۴].

همواره ابزار سیار نسبت به ابزار ثابت منابع کمتری در اختیار دارند و به همین دلیل، خطرات زیادی آن‌ها را تهدید می‌کند. بسته به هزینه و سطح تکنولوژی و با توجه به وزن، قدرت، اندازه و شکل در بسیاری از موارد منابعی که این ابزار در اختیار دارند مانند منبع برق، قدرت پردازشگر و اندازه حافظه، محدود می‌باشد [۲۵،۱۶]. به همین دلیل ممکن است برنامه‌های محافظتی پیچیده‌ای که نیاز به محاسبات بالایی دارند، قابلیت اجرا بر روی این دستگاه‌ها را نداشته باشند، که این خود به عنوان یک تهدید برای امنیت آن‌ها به حساب می‌آید [۲۵،۱۱].

با توجه به این که، ابزار سیار نسبت به ابزارهای دیگر آسیب پذیری‌های خاص خود را دارند، در این مطالعه تهدیدات مربوط به امنیت ابزار سیار و امنیت اطلاعات در این ابزارها مورد بررسی قرار گرفته است (جدول۱) [۱۶].

جدول۱: تهدیدات مربوط به امنیت ابزار سیار و امنیت اطلاعات در این ابزارها

تهدیدهای امنیتی		مربوط به امنیت ابزار سیار	مربوط به امنیت اطلاعات
به سرقت رفتن یا گم شدن ابزار سیار		✓	
محدودیت منابع		✓	
حملات هدفدار هکرها	دستکاری اطلاعات		
	جعل هویت		✓
	استراق سمع		
	پاسخ دادن		
امنیت شبکه سیار		✓	
بد افزارها		✓	✓
تنوع تولید ابزار سیار		✓	
پیش فرض مسیریاب بی‌سیم			✓
قابلیت نصب خود سر نقطات دسترسی			✓
ساختاربندی ضعیف شبکه بی سیم			✓
سوء استفاده از بلوتوث			✓
نقاط ضعف پروتکل WEP			✓
گذرواژه هایی که متن مخفی شان رمزگشایی شده			✓
کد های مخرب		✓	
راه انداز خودکار		✓	✓
حملات Voice Over IP چندگانه			✓
باز بودن شبکه وای فای و دسترسی از مکان های مختلف			✓
سیاست های نامشخص سازمان		✓	
جلوگیری از برقراری ارتباط		✓	
بهره‌کشی یا سوء استفاده رفتاری از ابزار		✓	

لازم به ذکر است که با توجه به جدول ۱، خطرات امنیتی مربوط به امنیت ابزار سیار می‌تواند، به طور غیر مستقیم، خطرات مربوط به امنیت اطلاعات را نیز در پی داشته باشد. در ادامه به توضیح هر کدام از تهدیدات و خطرات مربوط به امنیت ابزار سیار پرداخته شده است:

۱- به سرقت رفتن یا گم شدن ابزار سیار:

خطر شماره یک و رایج مرتبط با ابزار سیار، گم شدن یا به سرقت رفتن دستگاه است که می‌تواند منجر به نقص یا آسیب ناخواسته به بیمار شود، به عنوان مثال تحقیقات نشان می‌دهد که سرقت لپ‌تاپ نسبت به سرقت کامپیوترهای خانگی حدوداً سه برابر بیشتر است [۲۳].

۲- محدودیت منابع

یکی از واضح ترین چالش‌ها برای توسعه مکانیسم‌های امنیتی ابزار سیار، محدود بودن منابع آن‌ها است. برخلاف ابزار کامپیوتری ثابت، ابزار سیار به دلیل اندازه کوچک خود معمولاً منابع برق و حتی قدرت محاسباتی کمتری دارند. به همین دلیل ممکن است برنامه‌های محافظتی پیچیده که نیاز به محاسبات بالایی دارند قابلیت اجرا بر روی این دستگاه‌ها را نداشته باشند و این خود به عنوان یک تهدید برای امنیت آن‌ها به حساب می‌آید. محدودیت منابع ممکن است باعث ضعف در مواردی مثل، کشف بد افزارها و قدرت دفاع در مقابل حملات شود [۱۱]. محدود بودن ابزار سیار به استفاده از انرژی باتری، باعث محدودیت به کارگیری نرم افزار و سخت افزارهای خیلی قوی در این وسایل می‌شود [۲۵].

۳- حملات هدفدار هکرها

مهاجمین می‌توانند با سوء استفاده از سهل انگاری کاربران یا شناسایی ضعف‌های سیستم، باعث ایجاد تهدیدهایی از بیرون و درون سازمان شوند. اولین هدف این حملات دزدیدن داده‌های با ارزش شخصی است، ولی این حملات می‌توانند برای دستیابی به اهداف دیگر نیز انجام شود، در ادامه به برخی از این اهداف اشاره شده است [۱۶]:

الف) دستکاری اطلاعات

مهاجمین می‌توانند همه یا از بخشی از اطلاعاتی را که به آن دسترسی پیدا کرده‌اند، حذف یا تغییر دهند و یا آن‌ها را برای مقاصد غیر قانونی به جای دیگر ارسال نمایند. با توجه با حیاتی بودن اطلاعات سلامت، دستکاری آن‌ها ممکن است باعث نقصان و همچنین بروز فاجعه برای فرد شود.

ب) جعل هویت

اگر یک مهاجم از طریق استراق سمع، به اطلاعات شناسایی یک گره از شبکه، دست پیدا کند، می‌تواند به وسیله آن اطلاعات، سایر گره‌ها را فریب دهد، و خود را به جای یکی از گره‌های آن شبکه به دیگران بشناساند.

ج) استراق سمع

به دلیل استفاده از تکنولوژی بی‌سیم و امواج برای تبادل اطلاعات بین ابزار سیار، هر شبکه باز دیگر به راحتی می‌تواند ارتباط آن‌ها را قطع کند، اطلاعات ارسالی را دریافت کرده و داده‌های به سرقت رفته را برای اهداف سوء به کار گیرد.

د) پاسخ دادن

ممکن است مهاجمین یکسری از اطلاعات معتبر را از طریق استراق سمع به دست آورده، و این اطلاعات یا پاسخ آن‌ها را دوباره به یک دریافت کننده اصلی بفرستند، و به برخی از اهداف دست پیدا کند.

۴- امنیت شبکه سیار

ابزارهای دستی مدرن شامل انواع مختلفی از تکنولوژی‌های بی-سیم مانند بلوتوث، امواج رادیویی، امواج فروسرخ و غیره هستند که به آن‌ها اجازه می‌دهد با دیگر ابزارها ارتباط برقرار کنند. بنابراین راه‌هایی که یک ابزار سیار می‌تواند از طریق آن‌ها مورد حمله قرار گیرد بیشتر هستند. همچنین در برخی از موارد این قابلیت‌ها باعث انتقال ویروس‌ها، نرم افزارهای تروجان (Damping)، و کرم‌های کامپیوتری به دیگر ابزارها می‌شوند. بسیاری از برنامه‌های ضد ویروس ارتباط فروسرخ بین سیستم‌ها را مورد پایش قرار نمی‌دهند. علاوه بر این‌ها، بلوتوث یک تکنولوژی قدرتمند ارتباطی است که ارتباط را بین فاصله‌های کوتاه برقرار می‌کند و اگر به درستی ساختار بندی نشده باشد، ممکن است بسیاری از ابزارها، بدون پایش به آن متصل شوند [۲۳].

بسیاری از حس‌گرهایی که در حوزه مراقبت سلامت مورد استفاده قرار می‌گیرند، امکان استراق سمع، یا حتی خارج شدن از شبکه را دارند. برخی نگرانی‌ها در مورد خطرات این ابزار وجود دارد و این تهدیدات و حملات می‌تواند مشکلات جدی برای زندگی اجتماعی و شخصی افراد داشته باشد [۱۶]. هکرها نیز می‌توانند در نزدیکی مکان یک تلفن هدف، با به وجود آوردن یک ترافیک سنگین و جعلی موجب اختلال جریان داده‌ها در ابزار مورد نظر شوند. به وسیله سرویس پیام کوتاه نیز می‌توان بد افزارهایی را به تلفن‌های هوشمند ارسال نموده که این خود یکی از ضعف‌های امنیتی آن‌ها به حساب می‌آید. اتصال با IPهای (ProtocolInternet) مختلف به شبکه نیز خود یکی از چالش‌های امنیتی است [۲۴].

۵- بد افزارها (Malware)

دیگر خطر بزرگ امنیتی، آلوده شدن به وسیله ویروس است. بد افزارها می‌توانند از طریق یکی از نقطه ضعف‌های ابزار سیار به آن‌ها وارد شده و کنترل برنامه‌های آن را به دست گیرد یا باعث به وجود آوردن ایراد در برنامه شوند. چند نمونه از بد افزارهای ابزار سیار:

- ویروس Mabir/Cabir: می‌تواند از طریق بلوتوث و یا پیامک آلوده به سیستم عامل سیمبیان(Symbian) وارد شود.
- Dampig تروجان: باعث خرابی تنظیمات سیستم می‌شود.
- Commwarrior: باعث غیر فعال کردن نرم افزار های ضد ویروس می‌شود.
- Frontal virus: باعث از کار افتادن کامل تلفن همراه می‌شود.

بد افزارها از راه‌های مختلفی مانند بلوتوث، حافظه‌های SD (Secure Digital memory)، پیام کوتاه و پیام تصویری و غیره وارد سیستم می‌شوند [۲۴،۲۳].

۶- تنوع تولید ابزار سیار

وجود انواع مختلفی از پلت فرم‌های موبایل با سیستم عامل های متفاوت که بر روی سخت افزارهای مختلف نصب شده‌اند، سطح وسیع و متنوعی از ابزارها را به وجود آورده است که خود یک چالش به حساب می‌آید و موجب می شود که سطح دفاعی بسیار وسیع، متنوع و در نتیجه ضعیف و کم عمق به وجود آید. تغییرات مداوم در سخت افزار و ساختار بندی‌های ابزار سیار نیز، یک چالش امنیتی نسبت به عرصه کامپیوترهای ثابت و رومیزی به حساب می‌آید [۲۴].

۷- پیش فرض مسیریاب بی‌سیم (Default Wi-routers Fi)

مسیریاب بی‌سیم دستگاهی است که بسته‌های داده را بر روی یک شبکه بی‌سیم برای رسیدن به مقصدشان، هدایت می‌کند. این مسیریابی توسط آدرس آی پی مقصد و الگوریتم طراحی شده در نرم افزار مسیریاب انجام می‌شود [۲۶]. مسیریاب‌های بی‌سیمی که به فروش می‌رسند، به طور پیش فرض، ناامن

هستند، در نتیجه مهاجمان به راحتی می‌توانند از طریق مسیریابی که امنیتش تأمین نشده به سیستم اطلاعات نفوذ کنند [۲۷].

۸- قابلیت نصب خود سر نقطات دسترسی (Access Points Rogue)

نقاط دسترسی بی‌سیم به راحتی نصب می‌شوند. در نتیجه بسیاری از افراد در سازمان بدون اطلاع مدیر شبکه، اقدام به نصب نقاط دسترسی می‌کنند. این نقاط ممکن است از نظر امنیت ضعف‌هایی داشته باشند، که باعث حمله مهاجمین به آن-ها شود و موجب نفوذ آن‌ها به سیستم اطلاعات شود [۲۷].

۹- ساختاربندی ضعیف شبکه بی‌سیم

هنگامی که یک دستگاه در محدوده یک نقطه دسترسی، به شبکه بی‌سیم وصل می‌شود، آن نقطه دسترسی مشخصات دستگاه را ذخیره می‌کند و دفعه بعد که کامپیوتر دوباره روشن شود به صورت خودکار و بدون مداخله کاربر به شبکه متصل می‌شود. این قابلیت ممکن است در مواقعی موجب ناامن شدن دستگاه شود [۲۷].

۱۰- سوء استفاده از بلوتوث

یکی از روش‌های سوء استفاده از بلوتوث، Blue Snarfing می‌باشد. پروتکل (Object Exchange Protocol) OBEX، پروتکل انتقال است که داده‌ها را تعریف کرده و پروتکلی ارتباطی برای تبادل داده بین دو ابزار به حساب می‌آید [۲۸]. سوء استفاده از پروتکل OBEX باعث می‌شود که یک هکر بدون اطلاع مالک یک ابزار سیار به آن نفوذ کند. همچنین Blue Bugging قابلیتی است که هکرها با استفاده از آن می‌توانند با ارسال پیام کوتاه به ابزار آسیب برسانند [۲۰].

انواع دیگر روش‌های سوء استفاده از بلوتوث BlueJacking ، BlueTooth DoS attacks می‌باشند که هکرها با استفاده از هر کدام می‌توانند به ابزار سیار نفوذ کرده و تنظیمات آن را دستکاری کنند [۲۷].

۱۱- نقاط ضعف پروتکل (Wired Equivalent WEP(Privacy

WEP روشی است که برای امنیت شبکه‌های بی‌سیم، از آن استفاده می‌شود که خود دارای ضعف‌هایی است که به راحتی برای هکرها قابل نفوذ است.

۱۲- گذرواژه هایی که متن مخفی شان رمزگشایی شده

رمزهای عبور ابزار سیار به راحتی قابل پاک کردن و نفوذ به این ابزار پس از به سرقت رفتن بسیار آسان است [۲۷].

۱۳- کدهای مخرب

کدهای مخرب باعث آسیب به یک سیستم یا شبکه می‌شوند. این کدها به راحتی و یا از طریق ضد ویروس‌ها قابل کنترل نیستند [۲۹]. کدهای مخربی برای ابزار سیار نوشته می‌شوند به شدت در حال پیچیده‌تر شدن هستند به گونه‌ایی که پیچیدگی بدافزارهای مخصوص ابزار سیار در یک سال برابر با پیچیده تر شدن بد افزارهای کامپیوترهای میزی طی ۲۰ سال است [۲۷].

۱۴-راه انداز خودکار (Auto run)

برخی سیستم عامل‌های ابزار سیار شامل ویژگی‌های کمتر شناخته شده راه اندازی خودکار هستند که یک مهاجم می‌تواند به وسیله آن‌ها به سرعت یک دستگاه پرتابل را آلوده کند [۲۷].

۱۵- حملات Voice Over IP چندگانه

VOIP، فناوری برقراری ارتباط با استفاده از پروتکل اینترنت، به جای سیستم‌های آنالوگ قدیمی است. بعضی از خدمات VOIP به اتصال تلفن‌های معمولی نیاز دارند، در حالی که دیگر خدمات، اجازه برقراری تماس تلفنی را با استفاده از اتصال اینترنت نیز می‌دهند. برخی از خدمات VOIP امکان تماس تلفنی با هر شماره‌ای از جمله: محلی، راه دور، بی‌سیم و شماره بین المللی را فراهم می‌سازند [۳۰].

VOIP بر روی بسیاری از ابزارهای دستی قابل حمل، قابل نصب است. مکالمات از طریق VOIP به صورت رمزگذاری نشده ارسال می‌شوند، در نتیجه دیگران می‌توانند، به مکالمات دسترسی داشته باشند و یا آن ها را ضبط کنند [۲۷].

۱۶- باز بودن شبکه وای‌فای و دسترسی از مکان‌های مختلف:

مطالعات اخیر نشان می‌دهند که حملات از طریق شبکه بی‌سیم وای فای در حال افزایش است، امروزه به دلیل طبیعت باز شبکه‌های وای‌فای هکرها به راحتی می‌توانند به سیستم‌های اطلاعات نفوذ کنند.

بسیاری از کاربران از خطرات اتصال به شبکه از طریق سیستم وای‌فای عمومی آگاه نیستند. به عنوان مثال در یک گزارش آمده است که میزبان شبکه وای‌فای در یک فرودگاه به تمامی اطلاعات کارت‌ها اعتباری و ایمیل مشتریانی که به شبکه وای-فای آن وصل می‌شدند، دست پیدا می کرد و از آن‌ها بهره برداری تبلیغاتی و تجاری می‌نمود [۲۷].

۱۷- سیاست‌های نامشخص سازمان

سیاست‌های نامشخص سازمان در مورد تکنولوژی‌های جدید و عدم وجود ضمانت اجرایی برای سیاست‌های امنیتی تدوین شده باعث شده است که سازمان‌ها در تأمین امنیت ابزار سیار دچار مشکل شوند [۲۷،۲۳].

۱۸- جلوگیری از برقراری ارتباط

جلوگیری از برقراری ارتباط یک تهدید برای هر وسیله‌ای است که قابلیت اتصال به شبکه را داشته باشد. البته مکانیسمی در تلفن‌های هوشمند وجود دارد که ارتباط را رمزگزاری می‌کند ولی این مکانیسم‌ها توسط هکرها قابل خنثی شدن هستند.

۱۹- بهره کشی یا سوء استفاده رفتاری از ابزار

عنصر انسانی نقشی غالب در امنیت دستگاه‌های تلفن همراه ایفا می‌کند. کاربران ابزار سیار در هر سازمان می‌توانند با انگیزه های مختلف از این ابزار سوء استفاده کنند [۲۷].

بحث و نتیجه‌گیری

مزایای استفاده از ابزار سیار در پژوهش‌های مختلف به وضوح قابل رؤیت است و با مطالعه در این زمینه مشخص می‌شود که به کارگیری ابزار سیار برای هر سازمانی ارزشمند است. به دلیل قابلیت‌های منحصر به فردی که این ابزارها دارند، می‌توان از آن‌ها به طور گسترده در سراسر سازمان‌های بهداشتی بهره برد. بررسی مطالعات در این زمینه نشان می‌دهد که کاربرد ابزار سیار در محیط مراقبت سلامت روز به روز در حال افزایش است، از طرف دیگر به دلیل قابلیت‌های زیاد این ابزارها، از جمله استفاده از تکنولوژی‌های مختلف ارتباطی، پردازش‌گرهای قوی و همچنین رشد روز افزن برنامه‌های کاربردی، این ابزار به هدف‌هایی جذاب برای مهاجمان تبدیل شده‌اند و تهدیدهای زیادی متوجه آن‌ها است. به همین دلیل پژوهش‌های بسیاری در زمینه مسائل مربوط به امنیت ابزار سیار و امنیت اطلاعات در این ابزارها به انجام رسیده است [۳،۹،۱۰،۱۳،۱۷،۲۰،۲۱،۲۴-۱]. به عنوان مثال، مطالعات نشان می‌دهد، از میان تهدیدات و خطرات شناسایی شده، گم شدن یا به سرقت رفتن ابزار سیار به خاطر طبیعت ساخت و اندازه آن‌ها به عنوان خطر شماره یک امنیت ابزار سیار محسوب می‌شود، سازمان‌ها با آگاهی از این تهدید می‌توانند سیاست‌ها و خط مشی هایی برای جلوگیری از گم شدن و به سرقت رفتن، ردیابی ابزار گم شده و غیره را قبل از پیش آمدن چنین مشکلی ترسیم نمایند، که این کار خود باعث ساختار منظم فعالیت‌ها و کاهش خسارات به سازمان می‌شود. در مطالعه حاضر، پژوهشگران با بررسی جامع این قبیل پژوهش‌ها، مهم‌ترین تهدیدات امنیت اطلاعات ابزار سیار در حوزه سلامت را شناسایی و به صورت سازماندهی شده‌ایی ارائه نمودند.

با توجه به مطالعات انجام شده و نتایج این پژوهش، نتیجه می‌گیریم که سازمان‌ها باید کلیه چالش‌های مربوط به استفاده از ابزار سیار به خصوص چالش‌های امنیتی را مورد توجه قرار دهند تا با دیدی باز به سوء استفاده از این ابزار حرکت کنند و با آگاهی بتوانند از این ابزار بهره‌گیری کامل را به عمل آورند. همچنین سازمان‌های مراقبت سلامت به دلیل مواجه بودن با مشکلات فراوان از جمله محدودیت منابع، افزایش هزینه‌های بهداشتی و درمانی و نیاز به دسترسی فوری به اطلاعات بهداشتی و درمانی در شرایط ویژه، ناگزیر به استفاده از ابزار سیار هستند و می‌بایست به منظور رسیدن به سطح قابل قبول امنیت اطلاعات سلامت در ابزار سیار، تهدیدات و خطرات امنیتی را شناسایی نموده و پس از مطلع کردن تمامی کارکنان از این خطرات، برحسب نیازهای امنیتی از جنبه‌های مختلف فنی، فیزیکی، فردی و اداری راه حل‌های مناسب برای مقابله با آن‌ها را پیش گیرند. همچنین از آنجایی که تهدیدات همراه با پیشرفت فناوری روز به روز پیچیده‌تر می‌شوند، لازم است که این تهدیدات به صورت دوره‌ای مورد بررسی قرار گیرند.

تهدیدات و خطرات امنیتی ابزار سیار را از دیدگاه‌های دیگر نیز می‌توان تقسیم بندی کرد، مانند فعال و غیر فعال، برون سازمانی و درون سازمانی که به دلیل گستردگی مباحث مربوط به این دیدگاه‌ها، شرح این تقسیم‌بندی‌ها از حیطه این مقاله خارج است.

تشکر و قدردانی

در پایان از کلیه کسانی که به انجام این پژوهش کمک کرده‌اند، سپاسگزاریم.

References

1. Mohammadzade N. Health information security in mobile devices. J Health Adm. 2011;7(11):31-7. Persian.

2. Safdari R, Ghazisaeedi M, Sheikhtaheri A, Saremian M. Prioritizing the factors influencing places of rural health centers equipped with telehealth services using Analytical Hierarchy Process. J Clin Res Paramed Sci 2015; 4(1):24-33.

3. Saremian M. Design a Site Selection Model for Telemedicine Centers for Health Centers Using Geographic Information Systems.[dissertation] Tehran: Tehran University of Medical Sciences; 2015.

4. Juniper Networks, Inc. Mobile device security—emerging threats, essential strategies. 2011.[cited 2014 Aug 24].Available from: http://

www.bytes.co.uk/files/8913/4399/7443/juniper_mobile_white_paper.pdf
5. Hughes G. Mobile device security(Updated). Journal of AHIMA. 2012; 83(4):50-5.
6. Ammenwerth E, Buchauer A, Bludau B, Haux R.. Mobile information and communication tools in the hospital. Int J Med Inform. 2000;57(1):21-40.
7. Stanford V. Pervasive health care applications face tough security challenges. IEEE. 2002;1(2):8-12.
8. Ajami S, Ketabi S, Isfahani SS, Heidari A. Readiness assessment of electronic health records implementation. Acta Inform Med. 2011;19(4):224-7.
9. Meingast M, Roosta T, Sastry S, editors. Security and privacy issues with health care information technology. Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE ; 2006 Aug -Sep 30 – 3; New York, NY: IEEE; 2006. p. 5453 – 8.
10. Pharow P, Blobel B, Ruotsalainen P, Petersen F, Hovsto A. Portable devices, sensors and networks: wireless personalized eHealth services. Stud Health Technol Inform. 2009;150:1012-6.
11. Oberheide J, Jahanian F. When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments. Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications; New York, NY, USA: ACM; 2010.p. 43-8.
12. Ghazi Saeedi M, Khara R, Hosseiniravandi M. Necessitates of using dashboards in Health Information Management. Health Inf Manage. 2015; 12(2): 245-52. Persian.
13. Mashofi M, Refahi S, Mardi A, Mazaheri E. EHealth vision of medical confidentiality. 2nd International Congress of Medical Ethics in Iran; 2008 Apr 18-16; Tehran Medical Ethics and History of Medicine Research Center; 2008. p. 140.
14. Faghihi M, MemarzadehTehran GR, Rofogar Astaneh H. Patient privacy, necessary for e-health development. Medical Ethics. 2010;4(12): 164-88.
15. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. International Journal of Internet and Enterprise Management. 2010;6(4):279-314.
16. Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. J Med syst. 2012;36(1):93-101.
17. Rindfleisch TC. Privacy, information technology, and health care. Communications of the ACM. 1997;40(8):92-100.
18. Farzandipour M, Ahmady M, Sadoughi F, Karimi I. Designing a model for security requirements of electronic health records in Iran. J Qazvin Univ Med Sci. 2009;13:79-86. Persian.
19. Pharow P, Blobel B. Mobile health requires mobile security: challenges, solutions, and standardization.
Stud Health Technol Inform. 2008;136:697-702.
20. Nunoo EM. Smartphone Information Security Risks: Portable Devices and Workforce Mobility. [dissertation]. Luleå University of Technology: Department of Computer Science, Electrical and Space Engineering; 2013.
21. Blakley B, McDermott E, Geer D. Information security is information risk management. Proceedings of the 2001 workshop on New security paradigms; 2001 Sep 11-13; New York, NY, USA: ACM ; 2001. p.97-104.
22. Pelgrin WF. Cyber Security getting started: a non technical guide Center for Internet Security [cited 2014Aug 26]. Available from: http://msisac.cisecurity.org/resources/toolkit/oct13/documents/securingyourdataonthego.pdf.
23. Nunoo EM. Smartphone Information Security Risks: Portable Devices and Workforce Mobility.[dissertation]. Luleå University of Technology; 2013.
24. Couture E. Mobile Security: Current threats and emerging protective measures SANS Institute InfoSec Reading Room: SANS Institute; 2010.
25. Satyanarayanan M. Fundamental challenges in mobile computing. Proceedings of the 15th annual ACM symposium on Principles of distributed computing; 1996 May 23 – 26; New York, NY, USA: ACM; 1996. p.1-7.
26. Zerfos P, Zhong G, Cheng J, Luo H, Lu S, Li JJ-R, editors. Dirac: a software-based wireless router system. Proceedings of the 9th annual international conference on Mobile computing and networking; 2003 Sep 14 - 19; ACM; 2003. p. 230-44.
27. Association MARs. The Ten Most Critical Wireless and Mobile Security Vulnerabilities. Mobile Antivirus Researcher's Association 2006 [cited 2013 Jul 30].
28. portal bd. Object Exchange (OBEX). Bluetooth SIG; 2013 [cited 2014 Jul 3]; Available from: https://developer.bluetooth.org/TechnologyOverview/Pages/OBEX.aspx.
29. Janssen C. Techopedia explains Malicious Code**;** 2013 [cited 2014 Jul 4]; Available from: http://www.techopedia.com/definition/4014/malicious-code.
30. Federal Communications Commission. Voice Over Internet Protocol (VoIP); 2013 [cited 2014 Jul 3]; Available from: http://www.fcc.gov/guides/voice-over-internet-protocol-voip.

Review Article

Journal of Health and Biomedical Informatics
Medical Informatics Research Center
2015; 2(1): 48-56

Comprehensive Overview of the Health Information Security Risks in Mobile Devices

Rohullah Khara[1], Marzieh Saremian[2]*

• **Received:** 23 May, 2015 • **Accepted:** 14 Jun, 2015

Introduction: One of the innovative aspects of information technology that has been used in health organizations due to its unique capabilities is mobile devices. Knowing the threats and risks of mobile devices and information security leads to a better management and reduction in the negative consequences of problems. The purpose of this study was to identify threats and security risks of information associated with using mobile devices in health domain.

Method: This article is a narrative review. We searched keywords related to information security of mobile devices in the field of health through related databases, in Persian and English language articles published from 2005 to 2015. Also related articles in the selected articles list have been analyzed. Then the most important threats and dangers have been recognized and presented in a systematic way.

Results: According to this survey, the main security risks of mobile devices in the field of health generally included 19 cases. Some of these cases could be the mobile devices being lost or stolen, targeted threats of hackers, and malware.

Conclusion: The health organizations need to consider all security challenges about mobile devices, especially those related to security. Thus they can take full advantage of these tools consciously.

Key words: Security Threat, Devices, Mobile, Security, Health Information

• **Citation:** Khara R, Saremian M. Comprehensive Overview of the Health Information Security Risks in Mobile Devices. Journal of Health and Biomedical Informatics 2015; 2(1): 48-56.

1. M.Sc. in Health Information Technology, Firoozgar Hospital, Tehran, Iran.
2. M.Sc. in Health Information Technology, Lorestan University of Medical Sciences, Khorramabad, Iran.

***Correspondence**: Lorestan University of Medical Sciences, Lorestan, Iran.
• **Tel:** 09163690597 • **Email:** marziehsaremian@gmail.com