پیوست

شورای اجرایی (عالی) فناوری اطلاعات کشور

کمیسیون توسعه دولت الکترونیکی

چارچوب معماری سازمانی ایران

معماری مرجع امنیت

استانداردهای امنیتی حوزه تلفن همراه

نسخه ۱,۰ – اردیبهشت ماه ۱۳۹۶

پیشگفتار

امروزه موبایل به یکی از وسایل ضروری زندگی تبدیل شده‌است. این ابزار کوچک و نسبتا ارزان می‌تواند در مصارفی غیر از تماس تلفنی و ارسال پیامک مورد استفاده قرار بگیرد و بسیاری از عملیات را بدون داشتن محدودیت‌های لپ‌تاپ یا سایر کامپیوترهای رومیزی به انجام برساند. با رشد شگرف بازار گوشی‌های هوشمند، امکان استفاده از آن‌ها در فعالیت‌های مجرمانه نیز به طور مستمر در حال افزایش است. امروزه گوشی‌های هوشمند و دستگاه‌های تبلت حاوی سخت‌افزارهای توکار نظیر دوربین، شتاب‌سنج، سیستم موقعیت‌یاب جهانی[1]، واسط‌های بی‌سیم نظیر Wi-Fi، Bluetooth، NFC[2] و غیره می‌باشند. هر کدام از از این سخت‌افزارها می‌توانند در فعالیت‌های مجرمانه مورد دسترسی یا استفاده قرار گیرند. از این رو امنیت تلفن‌های همراه بیش از پیش مورد توجه قرار گرفته است. دستگاه‌های تلفن همراه نظیر گوشی‌های هوشمند و تبلت‌ها نیاز به پشتیبانی از اهداف امنیتی مانند محرمانگی، جامعیت و در دسترس‌پذیری دارند. برای رسیدن به این اهداف، دستگاه‌های موبایل بایستی در برابر بسیاری از تهدیدات امن شوند. دستگاه‌های موبایل مانند هر فن‌آوری جدید که امکانات و قابلیت‌های جدیدی را ارائه می‌کند، با چالش‌های امنیتی متعددی رو برو هستند. سازمان‌های مختلفی برای مقابله با تهدیدات موجود در این حوزه مطالعه می‌کنند و استانداردهایی را جهت امن کردن حوزه‌ی موبایل ارائه داده‌اند. در ادامه به بررسی بیشتر استانداردهای ارایه شده در این زمینه خواهیم پرداخت.

---

[1] Global Positioning System (GPS)

[2] Near Field Communications (NFC)

لیست استانداردهای امنیتی حوزه تلفن همراه

نام استاندارد	شماره استاندارد
User’s Guide to Telework and Bring Your Own Device (BYOD) Security, Rev. 1, (2016) راهنمای کاربران در دورکاری و امنیت بکارگیری دستگاه‌های شخصی (BYOD)	114-800 SP
Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,Rev. 2, (2016) راهنمای امنیت دورکاری، دسترسی از راه دور و بکارگیری دستگاه‌های شخصی (BYOD) در سازمان	SP 800_46
Securing Electronic Health Records on Mobile Devices, (2015) امن‌سازی پرونده‌های سلامت الکترونیک بر روی دستگاه‌های تلفن همراه	SP 1800-1
Vetting the Security of Mobile Applications, (2015) بررسی امنیت برنامه های کاربردی تلفن همراه	SP 800-163
Guidelines on Mobile Device Forensics, Rev. 1, (2014) دستورالعمل‌هایی برای جرم‌یابی دستگاه تلفن همراه	SP 800-101
Guidelines for Managing the Security of Mobile Devices in the Enterprise, Rev. 1, (2013) دستورالعمل‌هایی برای مدیریت امنیت دستگاه‌های تلفن همراه در فراسازمان	SP 800-124
Guidelines on Hardware-Rooted Security in Mobile Devices, (2012) دستورالعمل‌هایی درباره امنیت مبتنی‌بر سخت‌افزار در دستگاه‌های تلفن همراه	SP 800-164
Mobile Device Security: Cloud and Hybrid Builds, (2015) امنیت دستگاه‌های تلفن همراه: ساختار ابری و ترکیبی	SP 1800-4
Cell Phone Forensic Tools: An Overview and Analysis Update, (2007) ابزارهای جرم یابی تلفن همراه: بررسی اجمالی و تحلیل به روزرسانی	NISTIR 7387
Measuring the Usability and Security of Permuted Passwords on Mobile Platforms, (2016) اندازه‌گیری قابلیت استفاده و امنیت رمزهای عبور تغییریافته برروی پلت فرم‌های تلفن همراه	NISTR 8040

Mobile, PIV, and Authentication, (2014) تلفن همراه، اعتبارسنجی هویت شخصی و احراز هویت	NISTR 7981
Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation, (2006) شناسایی مبتنی‌بر اثرانگشت و دستگاه‌های دستی (قابل حمل) تلفن همراه: مرور اجمالی و پیاده سازی	NISTIR 7290
Smart Cards and Mobile Device Authentication: An Overview and Implementation, July (2005) احرازهویت دستگاه‌های تلفن همراه و کارت‌های هوشمند: مرور اجمالی و پیاده سازی	NISTIR 7206
Mobile Application Vetting Services for Public Safety, (2016) سرویس‌های بررسی برنامه‌های کاربردی تلفن همراه برای امنیت عمومی	NISTIR 8136
Usability and Security Considerations for Public Safety Mobile Authentication, (2015) ملاحظات کاربردی و امنیتی برای امنیت عمومی احرازهویت دستگاه‌های تلفن همراه	NISTIR 8080
Proximity Beacons and Mobile Device Authentication: An Overview and Implementation, (2005) احرازهویت دستگاه تلفن همراه: مرور اجمالی و پیاده سازی	NISTIR 7200
Guidelines for Manage the Security of Mobile Devices, (2013) راهنمایی برای مدیریت امنیت دستگاه‌های تلفن همراه	ITL BULLETIN

در ادامه شرح مختصری درباره استانداردهای فوق ارایه شده است:

- **SP 800-114: User's Guide to Telework and Bring Your Own Device (BYOD) Security**

این سند راهنمایی‌هایی را جهت امن‌سازی شبکه و دستگاه‌های الکترونیکی شخصی نظیر رایانه، لپ‌تاپ و تلفن همراه در فرآیند دورکاری ارایه می‌کند و به طور خاص بر روی امنیت دورکاری شامل دسترسی از راه دور به منابع غیر عمومی سازمان‌ها تمرکز دارد. این راهنمایی‌ها دربرگیرنده توصیه‌های عمومی برای تامین امنیت دستگاه‌های تلفن همراه مورد استفاده در دورکاری می‌باشند. همچنین توصیه‌هایی برای حفاظت از اطلاعات ذخیره شده بر روی رایانه‌های دورکاری و رسانه‌های قابل حمل فراهم می‌کند.

- **SP 800-46: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security**

هدف این سند، کمک به سازمان‌ها در کاهش ریسک‌های مرتبط با فن‌آوری‌های سازمان در دورکاری از جمله دسترسی از راه دور سرویس‌دهنده‌ها، دستگاه‌های مورد استفاده در دورکاری (مانند BYOD) و ارتباط راه دور می‌باشد. این مستند بر روی اهمیت تامین امنیت اطلاعات حساس ذخیره شده بر روی دستگاه‌های دورکاری و انتقال آن‌ها از طریق دسترسی از راه دور در سراسر شبکه‌های خارجی تمرکز دارد. سازمان‌ها بایستی از امنیت تمامی تجهیزات دورکاری نظیر کامپیوترهای شخصی، تلفن‌های هوشمند و تبلت‌ها اطمینان حاصل نمایند.

- **SP 1800-1: Securing Electronic Health Records (HER) on Mobile Devices**

استفاده از دستگاه‌های تلفن همراه در مراقبت‌های سلامتی گاهی اوقات از مرز حریم خصوصی و حفاظت‌های امنیتی آن دستگاه عبور می‌کند. سرقت اطلاعات شخصی اغلب دارای اثرات منفی مالی است اما سرقت اطلاعات پزشکی، به عمق حریم خصوصی افراد نفوذ می‌کند. در حال حاضر سرقت هویت پزشکی در هر سال میلیاردها دلار هزینه در بر دارد و تغییر اطلاعات پزشکی می‌تواند سلامتی افراد را از طریق تشخیص اشتباه، تاخیر درمان یا تجویز نادرست به خطر بیاندازد. این سند نشان می‌دهد که چگونه فناوری‌های موجود می‌توانند نیازهای سازمان را جهت حافظت بهتر از اطلاعات درون سیستم‌های EHR برطرف سازند. به طورخاص بیان می‌شود که چگونه مهندسان امنیت و متخصصان فناوری اطلاعات با استفاده از ابزارها و فناوری‌های دردسترس تجاری و منبع باز سازگار با استانداردهای امنیت سایبری می‌توانند به سازمان‌های بهداشت و درمان در استفاده از دستگاه‌های تلفن همراه جهت به اشتراک‌گذاری امن پرونده‌های سلامت بیمار کمک نمایند.

➢ SP 800-163: Vetting the Security of Mobile Applications

اخیرا سازمان‌ها برای تسهیل فرآیندهای کسب‌وکار خود اقدام به توسعه برنامه‌های کاربردی تلفن همراه کرده‌اند. استفاده از این برنامه‌های کاربردی با وجود مزایای آن‌ها، مسائل امنیتی بالقوه‌ای را هم بوجود آورده است. سازمان‌ها بایستی برای کاهش خطرات ناشی از آسیب‌پذیری‌های برنامه‌های کاربردی الزامات امنیتی خود را توسعه دهند. فرآیند ارزیابی امنیت بایستی برای حصول اطمینان از رعایت این الزامات توسط برنامه‌های کاربردی اجرا شود. این فرآیند، فرآیند بررسی برنامه‌های کاربردی[۳] نام دارد و شامل دنباله‌ای از فعالیت‌ها برای تعیین میزان تطابق برنامه‌های کاربردی با نیازمندی‌های امنیتی سازمان می‌باشد. این فرآیند شامل دو بخش است: تست برنامه، پذیرش یا عدم پذیرش برنامه. این سند نیازمندی‌های عمومی برای ایجاد برنامه‌های کاربردی امن را نیز توصیف می‌کند. این سند همچنین فرآیند تست برنامه و پذیرش یا عدم پذیرش آن، مسائل و توصیه‌های مرتبط با امنیت برنامه‌ها در طول مرحله تست، داده‌های حساس، مسائل مربوط به کد منبع، ابزارهای خودکار برای تست، آسیب‌پذیری‌های سیستم‌عامل اندروید و IOS و غیره را بیان می‌کند.

➢ SP 800-101: Guidelines on Mobile Device Forensics

این راهنما اطلاعات اولیه درباره ابزارهای جرم‌یابی تلفن همراه و نگهداری، کسب اطلاعات، ارزیابی، تجزیه و تحلیل و گزارش شواهد دیجیتالی موجود بر روی دستگاه‌های تلفن همراه را فراهم می‌کند. این اطلاعات مربوط به اجرای قانون، پاسخ به حادثه و سایر تحقیقات می‌باشد. به طور عمده این سند بر روی مشخصات دستگاه‌های تلفن همراه از جمله ویژگی‌های تلفن همراه، گوشی‌های هوشمند و تبلت‌ها با قابلیت صوت سلولی[۴] تمرکز دارد.

---

[3] Applications vetting process

[۴] Cellular voice

- **SP 800-124: Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013**

هدف از انتشار این سند کمک به سازمان‌ها در مدیریت و تامین امنیت دستگاه‌های تلفن همراه نظیر تلفن‌های هوشمند و تبلت‌ها به صورت مرکزی می‌باشد (لپ‌تاپ‌ها خارج از حوزه‌ی این راهنما می‌باشند). این سند توصیه‌هایی را برای انتخاب، پیاده‌سازی و استفاده از تکنولوژی‌های مدیریت متمرکز فراهم آورده و نگرانی‌های امنیتی ذاتی در استفاده از دستگاه‌های تلفن همراه را توضیح می‌دهد و پیشنهاداتی را برای تامین امنیت دستگاه‌های تلفن همراه در طی چرخه حیات آن‌ها ارایه می‌دهد.

- **SP 800-164: Guidelines on Hardware-Rooted Security in Mobile Devices, October 2012**

دستورالعمل‌های ارایه شده در این سند جهت فراهم کردن یک مبنای مشترک از فناوری‌های امنیتی در نظر گرفته می‌شود که می‌توانند در طیف وسیعی از دستگاه‌های تلفن همراه به منظور تامین امنیت دستگاه‌های تلفن همراه متعلق به سازمان و همچنین دستگاه‌های ورودی به داخل یک سازمان، از جمله دستگاه‌های شخصی مورداستفاده در محیط سازمان، پیاده سازی شوند. این راهنما بر روی ارایه سه قابلیت امنیتی صحت دستگاه، ایزوله‌سازی و مخازن محافظت شده از طریق استفاده از اصول اعتماد مبتنی بر سخت‌افزار تمرکز می‌کند.

- **SP 1800-4: Mobile Device Security: Cloud and Hybrid Builds, November 2015**

دستگاه‌های تلفن همراه، امکان دسترسی به اطلاعات توسط کارمندان را در هر زمان و هر مکانی به‌وجود آورده‌اند. دسترسی به اینترنت از طریق ارتباطات Wi-Fi و cellular امکان‌پذیر است. با رشد تکنولوژی تلفن همراه، تمایل کارمندان به استفاده از تلفن همراه برای دسترسی به اطلاعات، سرویس‌ها و سایر منابع سازمان برای انجام فعالیت‌های کاری افزایش یافته است. متاسفانه کنترل‌های امنیتی همگام و مناسب با

خطرات امنیتی دستگاه‌های تلفن همراه نیستند. ذخیره داده‌های حساس بر روی دستگاه‌های تلفن همراه که از امنیت کمی برخوردار هستند می‌تواند موجب حمله و دسترسی غیر مجاز به این اطلاعات گردد. راهنمای ارایه شده چگونگی تامین امنیت داده‌های ذخیره شده بر روی تلفن همراه کارمندان توسط تکنولوژی‌های موجود را نشان می‌دهد.

- **NISTIR 7387: Cell Phone Forensic Tools: An Overview and Analysis, March 2007**

هدف این گزارش اطلاع‌رسانی درباره‌ی قابلیت‌های نرم‌افزارهای جرم‌یابی است. این گزارش یک مرور کلی بر ابزارهای کنونی و طراحی شده برای کسب، بازرسی و گزارش داده‌های کشف شده بر روی دستگاه‌های قابل حمل ارایه می‌نماید و اطلاعاتی درباره قابلیت‌ها و محدودیت‌های آن‌ها بیان می‌کند. این نشریه به عنوان یک دستورالعمل گام به گام به منظور انجام عملیات جرم‌یابی نیست. هدف آن معرفی تکنولوژی‌های متنوع موجود و حوزه‌های مورد توجه به خوانندگان می‌باشد.

- **NISTR 8040 :Measuring the Usability and Security of Permuted Passwords on Mobile Platforms, April 2016**

این سند یک روش اندازه‌گیری برای تعیین اثرات ناشی از بهینه‌سازی قابلیت استفاده از ثبت[5] رمزعبور، به طور خاص برای محیط‌های ورودی محدود به عنوان مثال تلفن‌های همراه لمسی، بر روی امنیت پیشنهاد می‌دهد. این مستند روشی برای بهینه‌سازی ورود رمزهای عبور تصادفی بر روی دستگاه تلفن همراه با استفاده از جایگشت ارایه می‌دهد. این گزارش دو هدف را به دنبال دارد: ۱) بررسی حالت فعلی قابلیت استفاده و معیارهای امنیتی مناسب برای رمزعبورها، ۲) بحث پیرامون تجارب استفاده از این معیارها در دنیای واقعی.

---

[5] Entry

- **NISTR 7981: Mobile, PIV, and Authentication, March 2014**

هدف این سند بررسی و تحلیل گزینه‌های مختلف موجود جهت احراز هویت الکترونیکی می‌باشد که از هر دو بخش سرمایه‌گذاری در زیرساخت PIV[۶] و قابلیت‌های امنیتی منحصر به فرد دستگاه‌های تلفن همراه مانند گوشی‌های هوشمند و تبلت‌ها بهره می‌برد.

- **NISTIR 7290: Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation, March 2006**

این گزارش مکانیسم‌های احراز هویت مبتنی بر اثر انگشت شامل واحدهای حسگری را توصیف می‌کند که با دستگاه از طریق واسط‌های استاندارد پشتیبانی شده توسط اکثر دستگاه‌های دستی[۷] ارتباط برقرار می‌کند. این گزارش به بررسی اجمالی دو نوع مختلف احراز هویت کاربر می‌پردازد و جزییات طراحی و پیاده‌سازی راه‌حل‌ها را بیان می‌کند.

- **NISTIR 7206: Smart Cards and Mobile Device Authentication: An Overview and Implementation, July 2005**

امروزه استفاده از تلفن همراه در محیط‌های کاری افزایش یافته است. با وجود فراهم کردن مزایای بهره‌وری توسط این دستگاه‌ها، خطراتی مثل دسترسی از راه دور به اطلاعات، امنیت سازمان را به خطر می‌اندازد. فراهم کردن مکانیسم احرازهویت کاربران اولین خط دفاع در برابر استفاده غیرمجاز از دستگاه‌های بدون مراقب، گم شده و یا دزدیده شده می‌باشد. این گزارش دونوع کارت هوشمند جدید که از واسط‌های استاندارد پشتیبانی شده توسط دستگاه‌های تلفن همراه استفاده می‌کنند را توصیف می‌کند. این راه حل به هدف

---

[6] Personal Identity Verification

[۷] handheld

کمک به سازمان‌ها در افزودن کارت‌های هوشمند به دستگاه‌های تلفن همراه به منظور احراز هویت و سایر اعمال امنیتی ارائه شده است.

- **NISTIR 8136: Mobile Application Vetting Services for Public Safety, June 2016**

هدف این سند بررسی سطح بالایی از سرویس‌های بررسی برنامه‌های کاربردی همراه با ویژگی‌های فراهم شده توسط این خدمات و نحوه‌ی ارتباط آن‌ها با نیازهای امنیتی عمومی است. این سند با هدف کمک به سازمان‌های امنیتی عمومی در انتخاب سرویس‌های بررسی برنامه‌های تلفن همراه جهت استفاده در تحلیل برنامه‌های کاربردی تلفن همراه در نظر گرفته شده است. لازم به ذکر است این سند برای ارزیابی کیفیت یا تاثیر این خدمات در نظر گرفته نشده است.

- **NISTIR 8080: Usability and Security Considerations for Public Safety Mobile Authentication, November 2015**

این گزارش موسسه NIST به بررسی فناوری‌های احرازهویت دستگاه‌های تلفن همراه می‌پردازد که می‌تواند در مواجه با محدودیت‌های به وجود آمده توسط تجهیزات حفاظت شخصی و سیستم‌های اطلاعاتی برای گروه‌های امداد و نجات استفاده شود. هدف کلی این کار تجزیه و تحلیل مناسب‌ترین و کاراترین راه‌حل‌های احراز هویت برای گروه‌های امداد و نجات در یک زمینه مشخص است. این تحقیق اولین تجربه در زمینه قابلیت استفاده از احرازهویت تلفن همراه برای امنیت عمومی است و نیاز به تحقیقات و تجزیه و تحلیل‌های بیشتر است. افزایش تجهیزات و برنامه‌های کاربردی تلفن همراه، تکنولوژی جدیدی را در اختیار گروه‌های امداد و نجات برای کمک در موقعیت‌های اورژانسی قرار داده است. اگرچه گروه‌های امداد و نجات در حوزه‌های مختلفی فعالیت دارند، این گزارش بر روی خدمات آتش‌نشانی، اورژانس پزشکی و اجرای قانون تاکید دارد.

- **NISTIR 7200: Proximity Beacons and Mobile Device Authentication: An Overview and Implementation, June 2005**

فعال‌سازی احراز هویت کاربران اولین گام دفاعی در برابر استفاده غیر مجاز از دستگاه‌های تلفن‌همراه، گم‌شده و یا دزدیده شده، است. انواع مختلفی از احراز هویت وجود دارد. دو فاکتور موقعیت و زمان می‌تواند به تمامی روش‌های احراز هویت اضافه گردد. این دو فاکتور به موقعیت و زمان قابل قبول برای احراز هویت اشاره دارند. مکانیزم ارایه شده در این گزارش به جنبه‌ی موقعیت در احراز هویت اشاره دارد. این گزارش یک راه خلاقانه برای مکانیزم احراز هویت براساس وجود سیگنال از یک فرستنده رادیویی بی‌سیم برای دسترسی را توصیف می‌کند.

- **ITL BULLETIN: Guidelines for Manage the Security of Mobile Devices, July 2013**

این راهنما به سازمان‌ها در مدیریت متمرکز امنیت دستگاه‌هایی نظیر تلفن همراه و تبلت‌ها کمک می‌کند. استاندارد SP 800-124 نیز برای بررسی این موضوع ارائه شده است. این سند مسائل امنیتی در زمینه استفاده از دستگاه‌های تلفن همراه را شرح می‌دهد و توصیه‌هایی برای انتخاب، پیاده‌سازی و استفاده از فناوری‌های مدیریت متمرکز جهت تامین امنیت دستگاه‌های تلفن همراه در طی چرخه‌ی حیات آن‌ها ارائه می‌دهد. اگرچه این نشریه در درجه اول امنیت دستگاه‌های سازمانی را پوشش می‌دهد، اما این اطلاعات می‌تواند برای دستگاه‌های شخصی نیز اعمال شود.