



# برنامه نویسی امن

## گوشی‌های هوشمند همراه

نویسندگان:

دکتر محمد حسام تدین (عضو هیات علمی مرکز تحقیقات مخابرات ایران)  
مهندس سیما سینایی (پژوهشگر همکار در مرکز تحقیقات مخابرات ایران)  
مهندس فرید دریابار (پژوهشگر همکار در مرکز تحقیقات مخابرات ایران)



انتشارات آوای قلم

سرشناسه	: تدین، محمدحسام، ۱۳۵۳ -
عنوان و نام پدیدآور	: برنامه‌نویسی امن گوشی‌های هوشمند همراه/نویسندگان محمدحسام تدین، سیما سینایی، فرید دریابار.
مشخصات نشر	: تهران: آوای قلم، ۱۳۹۷. مشخصات ظاهری: ۲۳۰ ص: مصور، جدول.
شابک	: ۹۷۸-۶۰۰-۷۵۴۲-۹۶-۵
موضوع	: تلفن همراه -- برنامه‌نویسی
موضوع	: Programming -- Cell phones
موضوع	: تلفن همراه -- برنامه‌های کامپیوتری
موضوع	: Cell phones -- Computer programs
شناسه افزوده	: سینایی، سیما، ۱۳۶۵ - شناسه افزوده: دریابار، فرید، ۱۳۶۳ -
رده بندی کنگره	: TK ۶۵۸۰ ۱۳۹۷ ۱۳۶۴ ت۸/ت
رده بندی دیویی	: ۰۰۵/۲۶۸
شماره کتابشناسی ملی	: ۵۳۲۱۸۲۹

نام کتاب:

### برنامه‌نویسی امن گوشی‌های هوشمند همراه

نویسندگان:	محمد حسام تدین - سیما سینایی	تاریخ نشر:	۱۳۹۷
ناشر:	انتشارات آوای قلم	نوبت چاپ:	اول
طراحی روی جلد:	انتشارات آوای قلم	شمارگان:	۱۵۰ جلد
		قیمت:	۲۸۰۰۰۰ ریال
		شابک:	۹۷۸-۶۰۰-۷۵۴۲-۹۶-۵

این کتاب با همکاری و حمایت پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) به چاپ رسیده است.

آدرس: تهران - میدان انقلاب - خیابان کارگر شمالی - ابتدای خیابان نصرت - کوچه باغ نو - کوچه

داوود آبادی شرقی - پلاک ۴ - زنگ دوم

شماره تماس: ۶۶۵۹۱۵۰۴ تلفکس: ۶۶۵۹۱۵۰۵

فروشگاه اینترنتی کتاب: [www.khaniranshop.com](http://www.khaniranshop.com)

هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر و نویسنده ممنوع و شرعاً حرام است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گیرند.

## چکیده

با توجه به روند رو به رشد استفاده از برنامه‌ها در گوشی‌های هوشمند و درصد بالای آسیب‌پذیری‌های ناشی از رعایت نکردن برنامه‌نویسی امن نسبت به آسیب‌پذیری‌های گوشی‌های هوشمند همراه، امروزه امنیت برنامه‌ها از بزرگ‌ترین چالش‌های امنیتی این حوزه محسوب می‌شود. راهکارهای معمول ارائه‌شده برای پیشگیری از این آسیب‌پذیری‌ها، انجام ارزیابی‌های امنیتی حین چرخه حیات توسعه نرم‌افزار شامل استخراج نیازمندی‌ها، طراحی، پیاده‌سازی، آزمون، انتشار و پشتیبانی، پس از تولید محصول است. توسعه‌دهندگان برنامه‌های گوشی‌های هوشمند، با رعایت اصول برنامه‌نویسی امن، نقش مهمی در تامین امنیت کاربران و حفظ حریم خصوصی آن‌ها دارند. بنابراین، شناخت وظایف و مسئولیت‌های توسعه‌دهندگان و تدوین الزامات امنیتی برای کاهش احتمال وقوع مخاطره در این حوزه اهمیت ویژه‌ای دارد. در این کتاب، با تمرکز بر مخاطره‌های موجود در برنامه‌های گوشی‌های هوشمند، راه‌های مقابله و جلوگیری از تهدیدها و آسیب‌پذیری‌های امنیتی در مجموعه‌ای از رهنمودها و الزامات ارائه می‌شود تا توسعه‌دهندگان برنامه‌ها متناسب با هر مرحله از چرخه حیات توسعه نرم‌افزار به این الزامات عمل کنند. الزامات و رهنمودهای ارائه شده مستقل از سیستم عامل و برنامه نویسی برنامه‌های سامانه‌های هوشمند ارائه شده است و هر برنامه‌نویسی قادر است به خوبی و آسانی موارد مطرح شده را مورد استفاده قرار دهد. به علاوه شرکت‌های فعال در حوزه برنامه نویسی گوشی‌های هوشمند می‌توانند با تهیه چک لیست از موارد الزامات گفته شده در این کتاب نسبت به تهیه برنامه‌های مختلف، مبتنی بر اصول صحیح امنیتی اقدام کنند. همچنین شرکت‌های مشتری برنامه‌ها جهت اطمینان خاطر خود، می‌توانند در قراردادهای کاری خود با توسعه‌دهندگان برنامه‌ها، توصیه‌های امنیتی این کتاب را در تولید و توسعه برنامه‌ها از آنها مطالبه نمایند.

امیدواریم توانسته باشیم با این تلاش، سهم کوچکی در امن سازی فضای استفاده از گوشی‌های هوشمند در کشور عزیزمان ایران را به‌جای آورده باشیم.

## تشکر و قدردانی

از آقای دکتر رضا سپهی و کارشناسان همکار خانم مهسا امیدوار، آقای اشکان پارسی، آقای امین چهاردولی، آقای مهدی وجدی، آقای مجید صالحی، آقای آرش رامز، خانم مرجان بحرالعلوم و خانم شیوا ابراهیمی برای آرایه نظریات سازنده‌شان در تهیه این کتاب تشکر و قدردانی می‌شود. از مرکز تحقیقات مخابرات ایران، مرکز ماهر سازمان فناوری اطلاعات ایران، آقای هادی سجادی، آقای بیگلریان، آقای تسلیمی، خانم عباس زاده و تمام یاوران ما در انجام این کار برای تمام حمایت‌ها تشکر می‌گردد.

## سرفصل مطالب

صفحه	عنوان
۷	۱ مقدمه.....
۹	۱-۱ چرخه حیات.....
۱۰	۲-۱ مخاطرها.....
۱۱	۲ چرخه حیات توسعه برنامه امن.....
۱۳	۱-۲ چرخه حیات توسعه امن میکروسافت.....
۱۵	۲-۲ مدل چرخه حیات OWASP.....
۱۷	۳-۲ مدل چرخه حیات توسعه امن CISCO.....
۱۹	۴-۲ مدل پیشنهادی چرخه حیات توسعه امن برنامه.....
۲۱	۵-۲ الزامات مربوط به مراحل چرخه حیات توسعه امن برنامه.....
۲۵	۳ مقدمه‌ای بر ارزیابی مخاطره.....
۲۵	۱-۳ تهدیدها.....
۲۶	۱-۱-۳ روش STRIDE برای مدل‌سازی تهدید.....
۲۷	۲-۱-۳ زیست بوم گوشی هوشمند همراه برای مدل‌سازی تهدید.....
۲۹	۳-۱-۳ تهدید جعل اطلاعات.....
۳۱	۴-۱-۳ تهدید تحریف اطلاعات.....
۳۲	۵-۱-۳ تهدید انکار.....
۳۴	۶-۱-۳ تهدید افشای اطلاعات.....
۳۵	۷-۱-۳ تهدید ممانعت از ارائه خدمت.....
۳۷	۸-۱-۳ تهدید ارتقای مجوز دسترسی.....
۳۸	۲-۳ آسیب‌پذیری‌ها.....
۳۹	۱-۲-۳ آسیب‌پذیری‌های مرتبط با ضعف در احراز اصالت و اعطای مجوز.....
۴۳	۲-۲-۳ آسیب‌پذیری‌های مرتبط با حفاظت ناکافی در لایه انتقال.....
۴۷	۳-۲-۳ آسیب‌پذیری‌های مرتبط با نشت ناخواسته اطلاعات.....
۵۱	۴-۲-۳ آسیب‌پذیری‌های مرتبط با ذخیره نامن داده‌ها.....
۵۵	۵-۲-۳ آسیب‌پذیری‌های مرتبط با رمزنگاری شکننده.....
۵۷	۶-۲-۳ آسیب‌پذیری‌های مرتبط با تزریق در سمت سرویس‌گیرنده.....
	۷-۲-۳ آسیب‌پذیری‌های مرتبط با تصمیم‌گیری‌های امنیتی، براساس ورودی‌های نامعتبر.....
۶۱	
۶۶	۸-۲-۳ آسیب‌پذیری‌های مرتبط با مدیریت نادرست نشست.....

۶۹.....	آسیب‌پذیری‌های مرتبط با محافظت نکردن از کدهای دودویی	۹-۲-۳
۷۳.....	آسیب‌پذیری‌های مرتبط با کنترل ضعیف سمت سرور	۱۰-۲-۳
۷۶.....	دارایی‌ها	۳-۳
۷۸.....	دسته‌بندی برنامک‌ها	۴-۳
<b>۸۵.....</b>	<b>مخاطره‌های امنیتی</b>	<b>۴</b>
۸۵.....	مخاطره شماره یک: ضعف در احراز اصالت و اعطای مجوز	۱-۴
۹۸.....	مخاطره شماره دو: حفاظت ناکافی در لایه انتقال	۲-۴
۱۰۹.....	مخاطره شماره سه: نشت ناخواسته اطلاعات	۳-۴
۱۱۸.....	مخاطره شماره چهار: ذخیره ناامن داده‌ها	۴-۴
۱۲۶.....	مخاطره شماره پنج: رمزنگاری شکننده	۵-۴
۱۳۶.....	مخاطره شماره شش: تزریق در سمت سرویس‌گیرنده	۶-۴
۱۴۵.....	مخاطره شماره هفت: تصمیم‌گیری‌های امنیتی بر اساس ورودی‌های غیرقابل اعتماد	۷-۴
۱۵۲.....	مخاطره شماره هشت: مدیریت نادرست نشست	۸-۴
۱۵۹.....	مخاطره شماره نه: محافظت نکردن از کدهای دودویی	۹-۴
۱۷۱.....	مخاطره شماره ده: کنترل‌های ضعیف سمت سرور	۱۰-۴
<b>۱۸۱.....</b>	<b>پیوست‌ها</b>	
۱۸۱.....	پیوست الف: چرخه توسعه امن مایکروسافت	
۱۸۱.....	الف-۱ مدل بهینه‌سازی SDL مایکروسافت	
<b>۱۹۶.....</b>	<b>پیوست ب: چرخه حیات OWASP</b>	
۱۹۷.....	ب-۱ شروع	
۱۹۸.....	ب-۲ آموزش	
۱۹۹.....	ب-۳ الزامات	
۲۰۰.....	ب-۴ طراحی	
۲۰۱.....	ب-۵ توسعه	
۲۰۱.....	ب-۶ آزمون	
۲۰۴.....	پیوست ج: متدولوژی امتیازدهی مخاطره OWASP	
۲۱۵.....	واژه نامه و علائم اختصاری	
۲۲۵.....	منابع	