ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНА ТЕХНІКА

https://doi.org/10.31649/1997-9266-2020-150-3-43-50

УДК 004.056.57

П. Р. Черненко[1]
М. М. Орлова[1]

ВРАЗЛИВОСТІ СИСТЕМИ БЕЗПЕКИ В ДОДАТКАХ ОС ANDROID

[1]Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Впродовж останніх років підприємства все частіше розробляють та використовують мобільні додатки для збільшення ефективності своїх бізнес-процесів. Співробітники, клієнти та постачальники в результаті отримують підвищення продуктивності робочих процесів за рахунок обміну інформацією в режимі реального часу, мобільності та кращої функціональності.

Незважаючи на переваги мобільних додатків, їх використання може призвести до потенційних серйозних збоїв у системі безпеки. Подібно до застарілих корпоративних рішень, мобільні додатки можуть містити вразливості, що піддаються атакам.

Вразливості та ризики, пов'язані з конфіденційністю, які присутні в додатках для ОС Android, що встановлені на мільйонах пристроїв, можуть використовуватися зловмисниками для отримання несанкціонованого доступу до інформаційних ресурсів організації або даних користувача. Більшість мобільних додатків для ОС Android ініціюють з'єднання з мережею, іншими додатками або сторонніми сервісами, що робить необачного користувача більш вразливим до атаки зловмисників. Тому забезпечення захисту, мобільне шифрування та ретельна перевірка додатків на вразливості необхідна на стадії розробки додатку.

В роботі продемонстровано деякі стандартні засоби для проведення статичного аналізу додатків для ОС Android без запуску на пристрої користувача. Позаяк соціальні мережі в наш час є найзначущим медіа-місцем у світі і найпоширенішим каналом для передачі даних, відео та аудіо, за допомогою вищезгаданих методів статичного аналізу, перевірено вісім додатків популярних соціальних мереж, якими на сьогоднішній день користуються мільйони користувачів, та продемонстровано типи вразливостей, які виявлено в цих додатках. Також в роботі проаналізовано загрози з найбільшим потенційним впливом на бізнес-середовище та сформульовано рекомендації щодо зменшення ризиків їх виникнення.

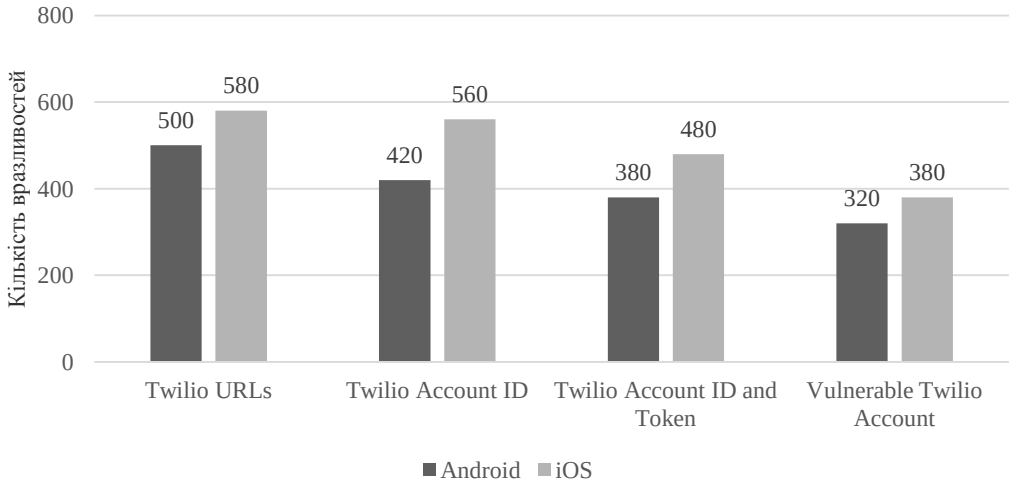
Ключові слова: ОС Android, APK, AndroBugs, Ostorlab, сканування вразливостей, соціальні мережі, конфіденційна інформація.

Вступ

Останнім часом доставка програмного забезпечення кінцевому користувачу зазнала фундаментальних змін завдяки простоті завантаження, встановлення та використання додатків зі спеціалізованих платформ розповсюдження мобільних додатків. Високий попит користувачів на додатки для Android призвів до збільшення темпів виробництва, за яких додатки розробляються і випускаються на ринок без додаткових перевірок та сертифікацій. Незважаючи на те, що це сприяє створенню рівних умов для невеликих організацій та відомих компаній з розробки програмного забезпечення, масове зростання виробництва нових додатків може поставити під загрозу безпеку користувачів. Розгортання нової технології може мати негативні наслідки, викликаючи потенційну загрозу безпеки IT-ресурсів, даних і користувачів організації. Вкрай важливо, щоб IT-експерти та користувачі організації були повністю обізнані про ризики та розробляли плани щодо їх уникнення [1].

Час від часу повідомляється про витік активних даних користувачів великих компаній з розробки програмного забезпечення. Наприклад, компанія із забезпечення безпеки мобільних додатків Appthority Enterprise перевірила 1100 додатків, що використовують прикладний програмний інте-

рфейс, розроблений Twilio. Twilio — це платформа для розробників, яка призначена для інтеграції різних методів комунікації та використання існуючих навичок веб-розробки, коду, серверів, бази даних для швидкого та надійного вирішення проблем зв'язку. На рисунку показані вразливості в додатках, у яких виявлені жорстко запрограмовані розробниками журнали, де виводяться облікові дані користувачів та їх паролів [2].



Додатки, в яких жорстко запрограмовано вивід облікових даних в журнал

Доступ за допомогою таких облікових даних дає зловмиснику можливість запустити операцію стеження в масштабі, зазвичай доступному тільки уряду або операторам зв'язку. Масштаб, вимірюваний загальною кількістю встановлень додатків, швидше за все, торкнеться сотень мільйонів зламаних мобільних пристроїв користувачів, чиї дзвінки та текстові повідомлення будуть доступні зловмисникам.

Зміна тенденції привела до того, що мобільні пристрої стали незамінними компонентами повсякденного життя та невід'ємною частиною корпоративного процесу завдяки нинішньому розвитку передових технологій обробки даних, можливостей комунікацій та властивості ОС Android розміщувати багатоцільові сторонні додатки. Хоча мобільні додатки забезпечують гнучкість бізнесу, вони також створюють проблеми безпеки. Загрози безпеки мобільних додатків стали більш розповсюдженими після появи фактів існування додатків, які постраждали від шкідливих програм в Google Play [3].

Мета дослідження — виявити та проаналізувати проблеми безпеки в додатках для Android смартфонів, оскільки Android смартфони зберігають різноманітні дані, такі як мультимедіа, дані датчиків, журнали зв'язку та дані, що створюються та використовуються додатками, а користувач Android пристрою, в свою чергу, використовує його в багатьох місцях протягом дня та дозволяє підключення до різних мереж, які в більшості випадків не є захищеними. Встановлені Android додатки часто містять комбінацію цінних особистих та бізнес-даних. Це пояснюється тим, що той самий пристрій може використовуватися як для роботи, так і для розваг. Виявлення потенційних вразливостей безпеки в Android додатках, що часто використовуються, допоможе зрозуміти ризик, пов'язаний з мобільними додатками в рамках корпоративного використання. Для цього в роботі проаналізовано додатки популярних соціальних мереж та виявленні загрози безпеці.

Методи

Для аналізу додатків на наявність вразливостей без його запуску використовується метод статичного аналізу, який виконується на декомпільованому вихідному коді та супутніх файлах APK (Android application package) [4]. Цей метод є найретельнішим за використання фреймворків AndroBugs та Ostrolab та економічно ефективним з можливістю виявлення критичних та некритичних загроз в додатках з магазину Google Play. Статичний аналіз з використанням вище згаданих фреймворків використовуються для сканування файлів APK, визначення можливих вразливостей та звітності про будь-які виявлені вразливості.

Демонструючи ефективність різних систем сканування вразливостей та звітуючи про результати перевірки їх наявності в мобільних додатках та засоби тестування, організації можуть використовувати ті самі процедури для виявлення та визначення придатності додатків для використання

на корпоративних мобільних пристроях. Також вимоги безпеки організації можуть бути дотримані для визначення середовища розгортання та використання мобільних технологій. В роботі висвітлюються деякі висновки, які необхідно враховувати перед схваленням додатків для публікації в Google Play.

Соціальні мережі в наш час є найзначущішим медіа-простором у світі і найпоширенішим каналом для передачі даних, тому для аналізу взято 8 різних додатків соціальних мереж. Звітність та оцінка ризиків, отримані в рамках сканування, демонструють цікаві результати. У табл. 1 наведено мобільні додатки, завантажені з Google Play, які досліджувалися в цій роботі.

Таблиця 1

Android додатки, що використовувались в дослідженні

Назва	Назва пакету	Версія	Дата публікації	Розмір (Мб)
Facebook	com.facebook.katana	268.1.0.54.121	30.04.2020	54,1
Instagram	com.instagram.android	140.0.0.30.126	05.05.2020	28,8
LinkedIn	com.linkedin.android	4.1.444	30.04.2020	54,1
Messenger	com.facebook.orca	263.0.0.18.125	05.05.2020	42,0
Skype	com.skype.raider	8.59.0.77	20.04.2020	35,6
Telegram	org.telegram.messenger	6.1.1	01.05.2020	32,8
Viber	com.viber.voip	12.8.0.19	18.04.2020	50,7
WhatsApp	com.whatsapp	2.20.147	05.05.2020	37,1

Порівняні та проаналізовані результати двох систем сканування додатків для отримання загального уявлення про ризики та вразливості, пов’язані з використанням провідних додатків соціальних мереж в рамках бізнес-процесу: AndroBugs Terminal Framework та OstorLab Cloud Framework.

AndroBugs — це сканер вразливостей додатків для Android, який забезпечує розширену оцінку безпеки додатків для Android та розкриває потенційні критичні проблеми, пов’язані з користувацькими додатками. AndroBugs перевіряє кожен компонент в додатку, щоб встановити недоліки безпеки та виявити логіку, яка може бути використана хакерами [5]. Проблеми безпеки проявляються в середовищі Android через такі фактори:

– Google не має досконалих методів, що забезпечують перевірку для оцінки безпеки додатків;

– в Google Play є багато вже опублікованих вразливих додатків [3].

– занадто багато додатків використовують вразливі API.

AndroBugs може допомогти покращити безпеку Android, але компанії повинні приділяти безпеці мобільних пристроїв таку саму увагу, що приділяється веб-безпец,і спираючись на звіти досліджень безпеки Android пристроїв.

Ostorlab Cloud Platform — це програма сканер, розташована у хмарному середовищі, призначена для перевірки додатків Android та iOS. Ця програма дає детальний звіт сканування безпеки протягом декількох хвилин.

Результати сканування

Усі файли APK були завантажені з Google Play за допомогою веб-завантажувача Evozi, так як напряму додаток з Google Play можливо тільки встановити на пристрій. Для сканування за допомогою Ostorlab необхідно завантажити файли APK у веб-інтерфейс https://www.ostorlab.co/, а для аналізу додатків за допомогою AndroBugs потрібно скористатись фреймворком з офіційного репозиторію на GitHub https://github.com/AndroBugs/AndroBugs_Framework, який працює як на Windows, так і на Linux.

Вразливості, знайдені використовуваними фреймворками, класифікуються в порядку пріоритетності та потенційного впливу на кінцевого користувача. Наступні вразливості виявлені після аналізу восьми мобільних додатків. У табл. 2 подані результати AndroBugs. Вразливості з інформаційною категорією, яка вказує на те, що в конкретному статичному аналізі не виявлено жодних проблем, не включені у цю таблицю.

Таблиця 2

Результати сканування AndroBugs

Категорія	Вразливість	Facebook	Instagram	LinkedIn	Messenger	Skype	Telegram	Viber	WhatsApp
Critical	<Implicit_Intent> Implicit Service	✓	✓	✓	✓	✓	✓	✓	✓
Critical	<#CVE-2013-6272#> AndroidManifest Exported Lost Prefix	✓	—	—	✓	—	—	—	—
Critical	AndroidManifest ContentProvider Exported	✓	✓	—	✓	—	✓	✓	✓
Critical	<SSL_Security> SSL Implementation (Verifying Host Name in Custom Classes)	✓	✓	—	✓	—	—	—	—
Critical	<SSL_Security> SSL Connection	✓	✓	✓	✓	✓	✓	✓	✓
Critical	<SSL_Security> SSL Certificate Verification	✓	✓	—	✓	✓	—	✓	✓
Critical	<Command> Runtime Command	—	✓	—	—	—	—	✓	✓
Critical	<KeyStore><Hacker> KeyStore Protection	—	✓	—	✓	—	—	—	—
Critical	App Sandbox Permission	—	—	—	—	—	—	—	—
Critical	<WebView><Remote Code Execution><#CVE-2013-4710#> WebView RCE Vulnerability	—	✓	—	—	✓	✓	✓	✓
Critical	<#BID 64208, CVE-2013-6271#> Fragment Vulnerability	—	—	—	—	✓	—	—	✓
Critical	AndroidManifest "intent-filter" Settings	—	—	✓	—	—	—	✓	—
Critical	<Hacker> Base64 String Encryption	—	—	—	—	—	—	—	✓
Warning	External Storage Accessing	✓	✓	✓	✓	✓	✓	✓	✓
Warning	AndroidManifest Exported Components	✓	✓	✓	✓	✓	✓	✓	✓
Warning	<Sensitive_Information> Getting ANDROID_ID	✓	✓	—	✓	✓	—	✓	✓
Warning	<Sensitive_Information> Getting IMEI and Device ID	—	✓	—	—	✓	✓	✓	—
Warning	<WebView> WebView Local File Access Attacks	✓	✓	✓	✓	✓	✓	✓	—
Warning	<WebView> WebView Potential XSS Attacks	—	✓	✓	—	—	✓	✓	✓
Warning	Dynamic Code Loading	—	—	—	—	✓	✓	—	✓
Warning	AndroidManifest Normal ProtectionLevel of Permission	—	—	—	—	—	—	—	✓
Warning	Codes for Sending SMS	—	—	—	—	—	—	—	✓
Notice	<Command> Executing "root" or System Privilege	✓	✓	–	✓	✓	✓	✓	✓
Notice	File Unsafe Delete	✓	✓	✓	✓	✓	✓	✓	✓
Notice	<Debug><Hacker> Codes for Android Debug Mode	✓	✓	—	✓	✓	—	✓	✓
Notice	<Hacker> APK Installing Source	✓	✓	—	✓	✓	✓	—	✓
Notice	AndroidManifest Exported Components 2	✓	✓	✓	✓	✓	✓	✓	✓
Notice	<Database><#CVE-2011-3901#> Android SQLite Databases Vulnerability	—	✓	✓	✓	✓	—	✓	✓
Notice	<Signature><Hacker> Getting Signature Code	—	✓	✓	✓	✓	✓	✓	✓
Notice	Native Library Loading	—	—	—	—	✓	✓	✓	✓
Notice	<Hacker> Code Setting Preventing Screenshot Capturing	—	—	—	—	—	✓	—	✓
Notice	AndroidManifest Adb Backup	—	—	—	—	—	—	✓	✓
Notice	<KeyStore><Hacker> KeyStore File Location	—	—	—	—	—	—	✓	—

В табл. 3 продемонстровано вразливості, які виявлені після аналізу восьми мобільних додатків за допомогою фреймворку Ostrolab. Вразливості з категорією, яка несе інформативний та попереджувальний характер, не включені у цю таблицю.

Таблиця 3

Результати сканування Ostrolab

Категорія	Вразливість	Facebook	Instagram	LinkedIn	Messenger	Skype	Telegram	Viber	WhatsApp
Hardening	Application code not obfuscated	—	—	—	—	—	✓	—	✓
Potentially	Insecure Random Seed	—	✓	—	—	—	—	—	✓
Potentially	Intent Spoofing	—	✓	—	—	✓	✓	—	✓
Potentially	Services declared without permissions	✓	—	✓	✓	✓	✓	✓	✓
Potentially	Untrusted External Storage File Access	—	✓	—	—	✓	—	—	—
Potentially	Clear text HTTP request	—	—	—	—	—	✓	—	—
Potentially	Backup mode enabled	—	—	—	—	—	—	✓	—
Important	Exported activites, services and broadcast receivers list	✓	✓	✓	✓	✓	—	✓	✓
Medium	ELF binaries do not enforce secure binary properties	✓	✓	—	—	✓	—	✓	✓
Medium	Insecure Network Configuration Settings	✓	✓	✓	✓	✓	✓	✓	✓
Low	Insecure Network Configuration Settings	—	✓	—	—	—	—	—	✓

Оцінка вразливостей та ризиків

На основі висновків, отриманих за допомогою вищезазначених інструментів, проаналізовано вісім різних додатків соціальних мереж, які зазвичай використовуються на смартфонах Android. Результат вказує на різні рівні ризиків, які існують в Android пристроях, наражаючи користувача на небезпеку витоку як індивідуальних, так і організаційних даних при взаємодії зі встановленими додатками з Google Play. Отже, це означає, що цілеспрямований аналіз є необхідним для конкретних додатків.

Загрози, які несуть вразливі додатки для вразливих додатків:

– витік особистих даних через мережу, наприклад, даних електронної пошти, IMEI, GPS, MAC;

– незашифрований зв’язок через мережу;

– витік файлів, доступних для читання або запису;

– погана авторизація та автентифікація;

– зловмисне програмне забезпечення для крадіжки інформації;

– інші відомі вразливості.

Витік конфіденційних даних. Витік конфіденційних даних може статися, коли програма зберігає інформацію про користувачів неналежним чином. Мобільні програми повинні уникати зайвого зберігання даних на пристрої. Згідно з OWASP «Незахищене зберігання даних відбувається в тому випадку, коли команди розробників припускають, що користувачі не матимуть доступу до файлової системи пристроїв і налаштовують збереження конфіденційних фрагментів інформації у сховищах даних пристроїв. Файлові системи пристроїв часто легкодоступні, і користувач повинен очікувати, що зловмисник перевірятиме сховища даних. Розблокування пристрою або отримання прав суперкористувача, як правило, обходить будь-який захист шифруванням, а в деяких випадках, коли дані не захищені належним чином, перегляд даних додатку можливий за допомогою спеціалізованих інструментів після підключення пристрою до комп’ютера.» [6].

Шість додатків можуть бути чутливі до вразливості бази даних Android SQLite (CVE-2011-3901). Тим більше, що всі додатки використовують незахищений спосіб видалення файлів. Використовуючи file.delete(), будь-який зловмисник, особливо на пристроях з правами суперкористувача, може відновити все, що було видалено. Крім того, майже всі використовують або мають виклики API до мережі. Важливим є забезпечення правильної обробки конфіденційної інформації. Варто також зазначити, що майже всі додатки мають доступ до інформації про ANDROID_ID, IMEI та deviceID.

Незашифрований зв’язок. Найважливішою особливістю архітектури клієнт-сервер є обмін інформацією. Коли відбувається обмін інформацією, дані можуть передаватися через мережу опера-

тора або Інтернет. Під час розробки програми, якщо не бути обережним під час обміну даними між клієнтом та сервером, є ймовірність, що дані можуть бути скомпрометовані під час передачі. Найкращий спосіб захисту даних під час обміну — це їх шифрування. Воно допомагає запобігти розкриванню перехоплених даних, особливо у випадку імен користувачів, паролів та даних банківських карток. За даними OWASP, мобільні додатки часто не захищають мережевий трафік [7]. Вони можуть використовувати SSL/TLS (Secure Sockets Layer, Transport Layer Security) під час аутентифікації, але не при інших запитах, піддаючи дані та ідентифікатори сеансу ризику бути перехопленими. Також наявність безпеки передачі не означає, що вона реалізована враховуючи весь свій потенціал. Виявити основні недоліки легко. Потрібно спостерігати за мережевим трафіком пристрою. Специфічніші недоліки вимагають перевірки архітектури та конфігурації додатків.

Усі додатки містять URL-адреси, які не використовують SSL. Посилаючись на результат AndroBugs, Viber має найбільшу кількість URL-адрес (12), далі — WhatsApp (9), Telegram (5), Instagram (4), LinkedIn (4), Skype (1), Messenger (1) та Facebook (1). Крім того, лише додатки LinkedIn та Telegram перевіряють валідність сертифікату SSL, що не дозволяє використання непідписаних сертифікатів, сертифікатів за терміном дії, що закінчився, або з невідповідним Common Name (CN).

Виявлення інформації, що може бути зчитана. Уникнення жорстко запрограмованих даних, таких як паролів та даних банківських карток, є високопріоритетною вимогою для будь-якого розробника, оскільки більшість додатків, можуть видати ці дані при процедурі reverse engineering. Хакер може отримати доступ до цієї конфіденційної інформації, що сприятиме подальшому доступу до ресурсів компанії. В додатках не виявлено дозволи режимів «MODE_WORLD_READABLE» або «MODE_WORLD_WRITEABLE» для різноманітних сервісів.

Погана авторизація та автентифікація. Автентифікація та авторизація стосуються привілеїв користувача, потрібних для використання програми. У додатку з функціональними можливостями, які перевищують загальнодоступні функції, може бути потрібний дозвіл на доступ до безкоштовних функцій. Автентифікація стосується ідентифікації користувача в додатку. Авторизація вказує на те, що користувач має право робити в додатку. Коли процес авторизації та автентифікації не може захистити додаток, привілейовані функції стають загрозою, що робить додаток вразливим до атак. Авторизація та автентифікація повинні описуватися точно під час розробки програми, щоб гарантувати, що сторонні користувачі не зможуть отримати доступ до конфіденційної інформації. Цього можна досягти, забезпечивши захищені функції обробки сеансу та входу.

Відомі вразливості. В табл. 4 подані відомі вразливості, знайдені в проаналізованих додатках.

Таблиця 4

Відомі вразливості, знайдені в додатках

Ідентифікатор	Додаток	Опис	Платформа
CVE-2013-6271	Facebook, Messenger	Дозволяє зловмиснику зняти блокування пристрою та обійти обмеження [8]	Android 4.4
CVE-2011-3901	Instagram, LinkedIn, Messenger, Skype, Viber, WhatsApp	Вразливість SQLite, що призводить до розкриття інформації [9]	Android 4.0
CVE-2013-4710	Skype, Telegram, Viber, WhatsApp, Instagram	Дозволяє JavaScript керувати хост-додатком [10]	Android 4.2

Крадіжка інформації шкідливими програмами. Мобільні пристрої, зокрема пристрої з ОС Android, надають декілька способів завантаження та встановлення додатків, наприклад, з офіційного магазину Google Play, з інших сторонніх платформ або з сайтів завантаження APK. На сьогодні більшість поширюваних шкідливих програм для смартфонів використовують сторонні платформи розповсюдження додатків, в основному, з метою крадіжки даних з пристрою [11].

ZitMo — один з найпоширеніших шкідливих кодів для мобільних пристроїв, створений в 2010 році для Symbian OS та призначений для пересилання SMS-повідомлень. ZitMo для Android націлений на перехоплення SMS, що використовуються для двофакторної аутентифікації у разі здійснення банківських операції на смартфоні [12], [13].

Існують також шкідливі програми, які націлені на крадіжку інформації з аккаунтів Facebook. Якщо інформація аккаунту не може бути зібрана, вони запускають підроблений користувальницький інтерфейс входу в Facebook для крадіжки облікових даних користувача. Як тільки шкідлива програма підключається до реальної сторінки Facebook, вона повністю контролює профіль користувача [14].

Висновки

В результаті проведеного дослідження проаналізовано вразливості, які існують в широко використовуваних додатках соціальних мереж. Установи та організації часто стикаються із загрозами безпеки даних і конфіденційності, але визначити пріоритетність цих загроз в руслі загальних проблем безпеки та загроз, що постійно змінюються, складно.

Проаналізовано загрози з найбільшим потенційним впливом на бізнес-середовище та сформульовано рекомендації щодо зменшення ризиків їх виникнення. Вразливий додаток, що має доступ до корпоративних даних, є потенційним каналом для таких загроз і рідко відстежується під час взаємодії з обмеженим комерційним середовищем. Google Play, з великою кількістю додатків, в основному зберігає неспотворені мобільні додатки. Витік даних з додатків, незашифрований зв'язок та вразливості несанкціонованого доступу демонструють необхідність для установ та організацій розуміти та захищати від ширшого набору ризиків для конфіденційних даних.

Як AndroBugs, так і OstroLab показують, як прості помилки розробника можуть спричинити втрати значних обсягів даних в сотнях додатків, відкриваючи можливість для масового витоку даних та стеження за користувачами організації. Результати підкреслюють проблеми безпеки, які повинні бути розглянуті організаціями та користувачами додатків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] A. Coyne, "ANZ retires Grow, goMoney apps," 2018. [Online]. Available: https://www.itnews.com.au/news/anz-retires-grow-gomoney-apps-485437 .

[2] Eavesdropper: How a Mobile Developer Error is Exposing Millions of Conversations, Industry report, Appthority, 2017

[3] L. Stefanko, "Banking Trojans continue to surface on Google Play," 2018. [Online]. Available: https://www.welivesecurity.com/2018/10/24/banking-trojans-continue-surface-google-play/ .

[4] V. K. Velu, Mobile Application Penetration Testing, USA: Packt Publishing, 2016.

[5] S. Quirolgico, J. Voas, T. Karygiannis, C. Michael, and K. Scarfone, "Vetting the Security of Mobile Applications," NIST Special Publication 800-163, 2015. https://doi.org/10.6028/nist.Sp.800-163 .

[6] Mobile Top 10 2014-M2, OWASP, 2014. [Online]. Available: https://www.owasp.org/index.php/Mobile_Top_10_2014-M2 .

[7] Mobile Top 10 2014-M3, OWASP, 2014. [Online]. Available: https://www.owasp.org/index.php/Mobile_Top_10_2014-M3 .

[8] CVE-2013-6271, National Vulnerability Database Common Vulnerabilities and Exposures, 2013. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6271 .

[9] CVE-2011-3901, National Vulnerability Database Common Vulnerabilities and Exposures, 2011. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3901 .

[10] CVE-2013-4710, National Vulnerability Database Common Vulnerabilities and Exposures, 2013. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4710 .

[11] Mobile Malware Evolution, Kaspersky, 2016. [Online]. Available: https://securelist.com/files/2017/02/Mobile_report_2016.pdf .

[12] Security Guidance for Critical Areas of Mobile Computing, Cloud Security Alliance, 2012. [Online]. Available: https://cloudsecurityalliance.org/artifacts/security-guidance-for-critical-areas-of-mobile-computing/ .

[13] D. Maslennikov, ZeuS-in-the-Mobile for Android, 2011. [Online]. Available: https://securelist.com/zeus-in-the- mobile-for-android-10/29258/ .

[14] M. Zhang, and S. Aimoto, Android Malware Harvests Facebook Account Details, 2018. [Online]. Available: https://www.symantec.com/blogs/threat-intelligence/android-malware-harvests-facebook-details .

Рекомендована кафедрою програмного забезпечення ВНТУ

Стаття надійшла до редакції 15.04.2020

Черненко Павло Романович — аспірант кафедри системного програмування і спеціалізованих комп'ютерних систем, e-mail: p.chernenko-2021@kpi.ua ;

Орлова Марія Миколаївна — канд. техн. наук, доцент кафедри системного програмування і спеціалізованих комп'ютерних систем.

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

P. R. Chernenko[1]
M. M. Orlova[1]

Security Vulnerabilities in Android OS Applications

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

During the past few years, commercial organizations and businesses are actively developing and using mobile applications to increase the efficiency of their business processes. As a result, employees, customers and suppliers get increased productivity in the work environment through real-time information exchange, mobility, and better functionality.

Despite the advantages of mobile apps, their usage can lead to potentially dangerous security issues. Like legacy enterprise solutions, mobile apps can contain vulnerabilities that can be attacked and lead to leaks of data.

Vulnerabilities and privacy risks that are present in Android apps that are installed on millions of devices can be used by hackers to gain unauthorized access to an organization's information resources or private user data. Most Android mobile apps initiate connections to the network, other apps, or third-party services, making a reckless user more vulnerable to malicious attacks. Therefore, security, mobile encryption, and thorough application vulnerability testing are required at the application development stage.

This work demonstrates some standard tools for performing static analysis of Android OS applications without running them on the user's device. Social networks are currently the most important media place in the world and the most widely used channel for data, video, and audio transmission. Therefore, the above-mentioned static analysis methods were used to test eight popular social network applications that are currently used by millions of users. The paper demonstrates the types of vulnerabilities that were found in these applications, also analyzes the threats with the most significant potential impact on the business environment and provides recommendations for reducing the risks of their occurrence.

Keywords: Android OS, APK, AndroBugs, Ostorlab, vulnerabilities scan, social networks, confidential information.

Chernenko Pavlo R. — Post-Graduate Student of the Chair of System Programming and Specialized Computer Systems, e-mail: p.chernenko-2021@kpi.ua ;

Orlova Maria M. — Cand. Sc. (Eng), Associate Professor of the Chair of System Programming and Specialized Computer Systems

П. Р. Черненко[1]
М. М. Орлова[1]

Уязвимости системы безопасности в приложениях ОС ANDROID

[1]Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»

В последние годы предприятия все чаще разрабатывают и используют мобильные приложения для повышения эффективности своих бизнес-процессов. Сотрудники, клиенты и поставщики в результате получают повышение производительности рабочих процессов за счет обмена информацией в режиме реального времени, мобильности и лучшей функциональности.

Несмотря на преимущества мобильных приложений, их использование может привести к потенциальным серьезным сбоям в системе безопасности. Подобно устаревшим корпоративным решениям, мобильные приложения могут содержать уязвимости, подвергающиеся атакам.

Уязвимости и риски, связанные с конфиденциальностью, которые присутствуют в приложениях для ОС Android, установленных на миллионах устройств, могут использоваться злоумышленниками для получения несанкционированного доступа к информационным ресурсам организации или данных пользователя. Большинство мобильных приложений для ОС Android инициируют соединение с сетью, другими приложениями или сторонними сервисами, что делает опрометчивого пользователя более уязвимым к атаке злоумышленников. Поэтому обеспечение защиты, мобильное шифрование и тщательная проверка приложений на уязвимости необходима на стадии разработки приложения.

В работе продемонстрированы некоторые стандартные средства для проведения статического анализа приложений для ОС Android без запуска на устройстве пользователя. Так как социальные сети в наше время являются наиболее значимым медиа-пространством в мире и наиболее широко используемым каналом для передачи данных, видео и аудио, с помощью вышеупомянутых методов статического анализа, проверено восемь приложений популярных социальных сетей, которыми на сегодняшний день пользуются миллионы пользователей, и продемонстрированы типы уязвимостей, выявленных в этих приложениях. Также в работе проанализированы угрозы с наибольшим потенциальным влиянием на бизнес-среду и сформулированы рекомендации по уменьшению рисков их возникновения.

Ключевые слова: ОС Android, APK, AndroBugs, Ostorlab, сканирование уязвимостей, социальные сети, конфиденциальная информация.

Черненко Павел Романович — аспирант кафедры системного программирования и специализированных компьютерных систем, e-mail: p.chernenko-2021@kpi.ua ;

Орлова Мария Николаевна — канд. техн. наук, доцент кафедры системного программирования и специализированных компьютерных систем