УДК 004.056.53

О.В. Сєвєрінов[1], В.М. Федорченко[2], В.І. Перепадя[3]

[1] *Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків*
[2] *Харківський національний економічний університет імені С. Кузнеця, Харків*
[3] *Харківський національний університет радіоелектроніки, Харків*

АНАЛІЗ ЗАГРОЗ ПЕРСОНАЛЬНИМ ДАНИМ В МОБІЛЬНОМУ ПРИСТРОЇ ПІД ЧАС ВИКОРИСТАННЯ РІЗНОМАНІТНИХ ДОДАТКІВ

Стаття присвячена аналізу сучасних загроз персональним даним в мобільних пристроях. Основна увага приділяється питанню захищеності інформації, яка зберігається та функціонує в Android-пристроях.

Ключові слова: *інформаційна безпека, захист мобільних пристроїв, загрози персональним даним, мобільні додатки, витік інформації, вразливості Android-платформ, вірус.*

Вступ

Розвиток інформаційних технологій призвів до того, що сучасний мобільний пристрій – смартфон/планшет чи інший «гаджет» найчастіше використовується в якості мобільного офісу, центру розваг та інструменту для споживання Інтернет-контенту. Сам пристрій може надати досить багато інформації про свого власника, адже в його пам'яті зберігаються: контакти колег, друзів та близьких з їхніми персональними даними; журнал дзвінків; корпоративна переписка; параметри точок доступу Wi-Fi, які розміщені в межах мешкання власника; додатки соціальних мереж (частіше зі збереженими паролями); банківські реквізити чи мобільний SMS-банкінг, фотографії, відеозаписи, нотатки та ін..

Така концепція ділових та персональних даних призводить до того, що абстрактна вартість інформації перевищує ціну самого пристрою. Саме тому задача захисту мобільного пристрою як від кіберзагроз так і від втрати/виходу з ладу являється критично важливою.

Мета статті – виявити та провести аналіз сучасних загроз персональним даним в мобільних Android-пристроях, що в подальшому дозволить запропонувати способи їх усунення.

Ризики,пов'язані з використанням мобільних пристроїв

З точки зору програмного забезпечення (ПЗ), яке встановлене на пристроях, існуючі загрози можна розділити на дві групи [1]:

шкідливе ПЗ (віруси, трояни) – зазвичай призначене для розкрадання персональних даних, отримання контролю над пристроєм або виведення його з ладу;

вразливості в прошивці або додатку, які, як правило, призводять до можливості обходу автентифікації, спотворення процесів обробки інформації на пристрої.

Європейська Агенція з мережевої та інформаційної безпеки наводить таку класифікацію ризиків безпеки для смартфонів і інших мобільних пристроїв [2]:

1. Витік даних в результаті втрати або викрадення.

Безперешкодний доступ до смартфону може виявитися золотою жилою для будь-якого зловмисника, який отримав доступ до приватної інформації. Якщо втрачений пристрій був не заблокований за допомогою PIN-коду або пароля, то у нового власника телефону буде доступ до всіх даних, в тому числі:

– електронної пошти, включаючи будь-які паролі або інформацію про обліковий запис, яка збережена на пристрої;

– облікових даних в соціальних мережах, таких як Facebook, Google +, Twitter або ВКонтакті;

– паролів, збережених в браузері;

– інформації про кредитну картку і паролі, збережені в таких додатках як Amazon і Google Wallet;

– адрес електронної пошти і номерів телефонів контактів;

– шляхів до захищених мереж Wi-Fi, які збережені на смартфоні;

– фотографій та відеофайлів, збережених на пристрої.

2. Ненавмисне розкриття даних.

Розробники часто надають більше функцій, ніж може відстежити користувач. Наприклад, користувач навіть не здогадується про те, що пристрій передає відомості про місцеположення щоразу, коли він відправляє фотографію, використовуючи додаток засобів соціального спілкування. Такі ризики можливі якщо:

– користувач відправляє фотографію з включеними даними місцеположення;

– хтось відмічає («тегує») користувача на фотографії без його відома;

– користувач «зареєструвався» в ресторані або кафе, використавши додаток розташування.

3. Вживані пристрої.

Згідно з дослідженнями Європейської Агенції з мережевої та інформаційної безпеки, якщо користувач не видалив інформацію зі свого старого мобільного пристрою належним чином, наступний власник може легко отримати доступ до історії викликів, контактів, електронних листів.

4. Фішингові атаки.

Фішинг (Phishing) – шахрайська форма збору даних, при якій атакуючий намагається обдурити користувача з метою розкрадання персональних даних, відправляючи їм підроблені повідомлення, які на перший погляд здаються справжніми. Phishing може проявлятися в різноманітних формах:

– підроблені додатки, призначені для імітації справжніх, популярних додатків, таких як, «Angry Birds»;

– електронні листи, які нібито приходять з перевірених джерел, таких як банки та інші фінансові установи;

– SMS-повідомлення, що імітують законних відправників, наприклад мобільного оператора.

Одним з найпоширеніших видів атак став також фішинг з використанням URL- адрес, схожих на адреси веб-сайтів податкових служб, подарункових ваучерів, преміальних програм і облікових записів в соціальних мережах [3].

5. Атаки на основі шпигунських програм.

Якщо мобільний пристрій заражений шпигунським програмним забезпеченням (spyware), то його шкідливий код може відправити особисті дані користувача на віддалений сервер без його відома. Найчастіше інформація, яка викрадається програмами-шпигунами, включає в себе всі натискання клавіш, починаючи з моменту зараження; імена, номери телефонів і адреси електронної пошти контактів; інформацію про кредитну картку.

6. Network spoofing або перехоплення даних.

Тип атаки, що маскує зловмисника, програму або адрес шляхом фальсифікації даних з метою несанкціонованого доступу до інформаційної системи [4].

За допомогою цієї атаки зловмисники полюють на тих, хто використовує загальнодоступні, відкриті мережі Wi-Fi. Якщо користувач не застосовує VPN (або відвідує сайти, які вимагають вводити пароль, але не використовують SSL), то існує ймовірність викрадення паролів до незашифрованих веб-сайтів та паролів до пошти, які передаються через незашифроване з'єднання на веб-сайт.

Віруси для платформи Android

На даний час у світі не існує повністю безпечної системи, і Android не є виключенням. Новину про виявлення першої шкідливої програми для системи Android в 2010 році [5] користувачі сприйняли як спосіб викачки грошей антивірусними компаніями. З часом кількість загроз для Android продовжувала збільшуватися. Не зважаючи на це, значний відсоток користувачів Android досить скептично відноситься до проблеми розповсюдження електронних вірусів.

Перше місце серед шкідливих програм для операційної системи (ОС) Android займають SMS-троянці (сімейство Android.SmsSend). Їх головною метою являється відправка високотарифних повідомлень на спеціальні короткі номери. Доля зібраних таким чином коштів збагачує зловмисників. Подібні програми відрізняються одна від одної лише незначними змінами в інтерфейсі та номерами, на які відправляються повідомлення. Зазвичай їх поширюють під виглядом розповсюджених додатків та ігор, використовуючи відповідні іконки.

Наступними йдуть більш серйозні троянські програми. До таких відносяться: Android.DreamExploid, Android.Gongfu, Android.Wukong, Android.Geinimi, Android.Spy тощо. Ці програми, залежно від сімейства, займаються збором конфіденційної інформації користувача, додаванням закладок в браузер, виконанням команд, які дають зловмисники, відправкою SMS-повідомлень, а також визначенням додатків і т.п.

Особливу увагу слід приділити комерційним програмам-шпигунам. Залежно від класу, ціни та виробника, вони перехоплюють вхідні та вихідні SMS-повідомлення і дзвінки, роблять аудіозапис середовища, відстежують координати, збирають статистичні дані браузера (закладки, історію відвідувань) і т.п. Переважна кількість таких програм становить небезпеку, адже після їх установки на пристрій не створюється значок, і визначити їх можна в системному меню зі списком додатків за непрямими ознаками.

Окремо вслід звернути увагу на рекламні продукти, які використовують розробники ігор та програм для заробітку. Після натискання на рекламне повідомлення, яке з'являється на екрані, користувач потрапляє на сайт товару або послуги, а розробник, таким чином, отримує певну грошову винагороду. Зазвичай дані рекламні модулі не становлять загрози для користувачів, однак серед них зустрічаються і більш шкідливі. Наприклад, якщо рекламне повідомлення з'явиться не всередині додатку, а в статусному рядку пристрою, то його приймають за системне. Такі дії вигідні зловмисникам тим, що вони можуть використовувати для реклами фрази «Потрібне термінове оновлення системи» (велика ймовірність, що замість оновлення користувач отримає троянця).

Велика кількість модулів поводить себе досить активно, збираючи персональні дані користувачів

(номер телефону, IMEI, використовуваного оператора і т.д.), додаючи закладки в браузер та ярлики на робочий стіл. Програми, в яких використовуються такі модулі, ідентифікуються як рекламні засоби або Adware (наприклад, Adware.Startapp, Adware.Airpush, Adware.Leadbolt та ін.).

Вразливості операційної системи Android і програмного забезпечення, яке в ній функціонує

Всі програми в архітектурі Android не мають доступу до закритих даних інших додатків, шляхом обмеження прав доступу. Головною проблемою, з якою можуть зіткнутися користувачі, являється можливість надання прав root іншим програмам чи скриптам. Ці вразливості (наприклад, CVE-2009-1185, CVE-2011-1823) стають у нагоді розробникам шкідливих програм. За допомогою експлойтів (програмних модулів і скриптів) з метою отримання прав рівня root, вони безперешкодно встановлюють інші програми без дозволу користувача (модифікації Android.DreamExploid і Android.Gongfu). Існують і такі шкідливі програми, які спонукають користувача виконати необхідні дії і надати шкідливій програмі необхідні повноваження шляхом його обману без використання жодних експлойтів.

Ключовим елементом безпеки Android являється система дозволів (Permission System). При встановленні додатку користувачу представляється перелік всіх доступних програмі функцій. Після цього вони можуть виконувати закладені в них функції без відома користувача. Демонстрація всіх існуючих можливостей програм перед встановленням, начебто, повинна допомагати в забезпеченні належного рівня безпеки, проте, не всі користувачі звертають детальну увагу на перелік функцій. Окрім того, існує велика ймовірність, що якась певна функція в подальшому буде використана в інтересах зловмисників. Існують також додатки, які не потребують жодних дозволів для своєї виконання своїх завдань, що, в свою чергу, створює хибне відчуття повної безпеки.

Загрозу також представляють неофіційні або сторонні прошивки. Перш за все, шкідливі програми вбудовуються в такі прошивки з моменту створення. Далі, коли додаток підписується цифровим підписом образу системи, він отримує права, аналогічні правам самої системи. Відповідно до Android Open Source Project (AOSP) підпис для образу являється приватним, тому така ситуація можлива наприклад в разі крадіжки підпису. Схожий метод зараження використовувався, зокрема, програмою Android.SmsHider, яка без відома користувачів, встановлювала троянський apk файл.

Як стандартні системні програми, так і додатки від виробників Android-пристроїв, теж вразливі. Недоліки браузера WebKit дозволяють шкідливим програмам виконати JavaScript-код і надають доступ до захищених даних браузера.

Дані користувачів можуть бути скомпрометовані у випадку, якщо при роботі з ними розробники прикладного ПЗ не забезпечують достатнього рівня безпеки. Атаці піддаються реєстраційні дані, які зберігаються в незахищеному вигляді – паролі від банківських карт та інші конфіденційні дані. Якщо під час роботи додатку ця ж інформація передається в мережі в незашифрованому вигляді, то вони теж потенційно вразливі до компрометації з боку зловмисників. Подібним прецедентом була ситуація з програмою Skype, у цьому випадку в незашифрованому вигляді зберігалася інформація профілю, контакти, історію листування та інші персональні дані користувачів.

Відкритість системи Android

Відкритість системи Android полягає в декількох поняттях [5]. По-перше, код ОС Android доступний і може використовуватися, модифікуватися і покращуватися розробниками відповідно до їх ідей та потреб. З одного боку, це плюс для розробників пристроїв та виробників, з іншого – це дає змогу зловмисникам знаходити вразливості та помилки. По-друге, можна встановити додатки як з офіційного каталогу додатків Google Play, так і з будь-якого іншого доступного сайту. По-третє, розробка додатків є практично розповсюдженою та доступною справою, оскільки для розміщення своїх продуктів в офіційному каталозі необхідно заплатити всього $25, а поширення програм поза його межами взагалі безкоштовне. По-четверте, програми, що розміщуються в Google Play до недавнього часу не піддавалися попередній перевірці або тестуванню з боку Google. Нещодавно з'явилася система Bouncer, яка перевіряє додатки, розміщені в каталозі Play, на наявність небезпечних функцій; облікові записи розробників також піддаються перевірці.

Фрагментація платформи

Досить велика кількість розробників мобільних пристроїв використовує систему Android, через це перед споживачами відкривається широкий вибір пристроїв з різноманітним функціоналом. З іншого боку розробка додатків с великим охопленням пристроїв – надзвичайно складна і трудомістка задача для кожного Android-розробника.

Коли виходить чергове оновлення операційної системи, розробники додають не лише нові функції, а й усувають раніше виявлені вразливості. Існують випадки, коли пристрій стає об'єктом хакерських атак через несвоєчасне оновлення ОС або, взагалі, відсутність оновлення програмного забезпечення. Причиною можуть бути як технічні, так і економічні фактори.

Соціальний фактор

Не дивлячись навіть на високий рівень захисту системи, людський фактор відіграє не останню роль в її безпеці. При здійсненні нападу на мобільну систему зловмисники зазвичай використовують компоненти соціальної інженерії [3–4]. Соціальний інжиніринг відноситься до психологічної маніпуляції людьми в інформаційній мережі. Наприклад, поширення шкідливих програм через рекламу в додатках за допомогою використання гучних фраз («Терміново оновити систему», «Версія браузера застаріла», «Встановіть оновлення Skype» і т.п.).

Аналогічна ситуація і з розповсюдженням шкідливих програм шляхом розсилки спама по SMS (бекдор Android.Crusewind). Іншим компонентом соціальної інженерії являється хибна безкоштовність програми («Нова версія Need for Speed», «Оновлення Dr Web безкоштовно!»), а також залучення тематики «для дорослих» («Гарячі дівчата, качай тут!», «Колекція фото супер красуні» і т.п.).

Захистом від цих загроз є уважність з боку самих користувачів. Зазвичай зловмисники підробляють популярні сайти, повторюючи їх оформлення, структуру, або створюють точну копію. Також можуть підробляються і додатки, і, з великою ймовірністю, неуважний користувач надасть зловмиснику доступ до своєї конфіденційної інформації.

Висновки

Проведений аналіз показав, що існує багато ризиків втрати персональних даних, пов'язаних з використанням мобільних пристроїв. Не дивлячись на велику кількість загроз та вразливостей мобільної платформи, у даний час ведеться робота щодо посилення безпеки Android. Результати проведеного аналізу можуть стати основою для розробки рекомендацій щодо заходів захисту персональних даних користувачів та зменшення масштабів неконтрольованого витоку інформації при використанні мобільних пристроїв.

Список літератури

1. Проблемы безопасности мобильных устройств, систем и приложений [Електронний ресурс]. – Режим доступу до ресурсу: http://itzashita.ru/mobilnyie-ustroystva/bezopasnost-mobilnyih-ustroystv-sistem-i-prilozheniy-chast-1.html.

2. Мобильная безопасность: все ,что нужно знать [Електронний ресурс]. – Режим доступу до ресурсу: http://freeprotection.ru/mobilnaya-bezopasnost-vsyo-chto-nuzhno-znat/.

3. Федорченко В.Н. Анализ угроз для мобильных устройств и способов их защиты / В.Н. Федорченко, И.В. Гензерский, Н.Ю. Шевякова // Системи обробки інформації. – 2011. – № 7. – С. 68-71.

4. Сєвєрінов О.В. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі / О.В. Сєвєрінов, А.Г. Хрєнов, А.О. Поляков // Системи обробки інформації. – 2015. – № 9. – С. 101-104.

5. Уязвимости платформы Android. Настоящее и будущее [Електронний ресурс]. – Режим доступу до ресурсу: https://habrahabr.ru/company/drweb/blog/142993/.

Надійшла до редколегії 10.11.2016

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський національний університет радіоелектроніки, Харків**.**

АНАЛИЗ УГРОЗ ПЕРСОНАЛЬНЫМ ДАННЫМ В МОБИЛЬНОМ УСТРОЙСТВЕ ВО ВРЕМЯ ИСПОЛЬЗОВАНИЯ РАЗЛИЧНЫХ ПРИЛОЖЕНИЙ

А.В. Северинов, В.Н. Федорченко, В.И. Перепадя

Статья посвящена анализу угроз персональным данным в мобильных устройствах. Основное внимание уделяется вопросу защищенности информации, которая хранится и функционирует в Android-устройствах.

Ключевые слова: *информационная безопасность, защита мобильных устройств, угрозы персональным данным, мобильные приложения, утечка информации, уязвимости Android-платформ, вирус.*

ANALYSIS OF PERSONAL DATA THREATS IN A MOBILE DEVICE WHILE USING A VARIETY OF APPLICATIONS

O.V. Sievierinov, V.N. Fedorchenko, V.I. Perepadya

This article analyzes the threats to personal data on mobile devices. The focus is on the issue of protection of information stored and functions in Android-devices.

Keywords: *information security, the protection of mobile devices, the threat of personal data, mobile applications, information leakage, vulnerability Android-platform, virus.*