Секція 1

ДОСЛІДЖЕННЯ ПІДСИСТЕМ ЗАХИСТУ ОС ANDROID

Шипунов М. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Цуранов М. В.

Актуальність. На сьогоднішній день смартфони надійно закріпилися у повсякденному житті багатьох людей. Найпоширенішими сценаріями використання мобільних пристроїв є: переглядання пошти, обмін миттєвими повідомленнями або відеозйомка. Наразі існують різні мобільні операційні системи. Прикладом таких систем є: IOS, KaiOS, BlackBerry OS, Android. За даними сайту statcounter станом на квітень 2023, IOS займає 30,61% пристроїв, а Android – 68,61% [1]. З цього можна зробити висновки, що найпопулярнішою мобільною ОС є Android.

Наразі мобільні пристрої мають велику кількість датчиків, наприклад: мікрофон, динамік, камера, акселерометр, барометр, датчик освітлюваності, термометр, Wi-Fi модуль, сканер відбитку пальця. Це все перетворює смартфон в універсальний пристрій, який стає незамінним помічником у повсякденному житті. Однак всі ці можливості можуть бути використані не тільки власником, а й зловмисником.

Метою роботи є дослідження методів захисту, вбудованих в операційну систему Android.

Основні положення. Головною проблемою пристроїв на операційній системі Android є швидкість отримання виправлень безпеки. Ця проблема виникла через архітектурні особливості самої ОС, що призводить до сповільнення процесу створення оновлень системи. За даними офіційного інструмента для розробки додатків «Android Studio» станом на 01.06.23, версія операційної системи під назвою Tiramisu, яка вийшла у серпні 2022 року, встановлена лише на 5,2% пристроїв. В свою чергу найпоширенішою залишається версія Oreo, яка вийшла у серпні 2017 року [2]. З цього можна зробити висновки, що більшість користувачів не мають актуальної версії операційної системи. Наразі безпеку мобільних пристроїв можна поділити на 3 рівні: ядро, система Android та прикладний рівень. Розглянемо їх детальніше.

На рівні ядра реалізовані базові системи захисту: розмежування доступу, SeLinux та IPC. Система розмежування доступу у системі Android перейшла від базового ядра Linux. Також у ядрі ОС реалізована підсистема SeLinux. Дана технологія є частиною Linux Security Module (LSM), та розпізнає різні об’єкти ядра і конфіденційні дії, що виконуються над ними. Ще однією системою у складі ядра системи є IPC. Дана технологія контролює обмін даними між різними процесами в ОС [3].

Рівень ОС постійно модифікується та отримує нові методи підвищення рівня захищеності з кожною версією системи. Розглянемо найважливіші зміни

в ОС: обов'язкове попередження користувача під час додавання нового сертифікату до системи, журнал дій для всіх додатків у системі, шифрування повного диску, технологія Treble, яка розділила Android на 2 складові: рівень ОС та рівень вендору. Завдяки цьому, розробники могли оновлювати драйвери та версію системи незалежно один від одного. Це дозволило прискорити створення швидких оновлень безпеки. З появою версії Android 11, до системи було додано можливість видати одноразове дозволення додатку на використання модулю системи.

Прикладний рівень захисту є найменш захищеним. Незважаючи на наявність великої кількості стороннього ПЗ для захисту мобільних пристроїв, залишається проблема каналу отримання додатків. Це зумовлено наявністю можливості встановлювати додатки з невідомих джерел та слабкої модерації фірмового магазину від Google.

Починаючи з 2015 року, Google випускає щомісячні «патчі безпеки Android» з метою екстреного виправлення проблем безпеки у ОС. Дані патчі виправляють проблемі на всіх трьох розглянутих рівнях безпеки.

Висновки. Проаналізувавши найпопулярніші мобільні операційні системи було виявлено, що найпоширенішою є система Android. Головною причиною популярності даної ОС є її відкритість. Але одночасно це є її найбільшим недоліком, так як система розроблюється без прив'язки до апаратної платформи. Це призводить до того, що кожний виробник пристроїв вимушений самостійно адаптувати систему до кожного з своїх пристроїв. Нажаль, під час адаптації безпека не є пріорітетною.

Проаналізувавши 3 рівні безпеки операційної системи Android було виявлено, що найбільш вразливим є рівень програмного забезпечення. Це зумовлено тим, що він є найменш контрольованим. Наявність вбудовані системи «Play захист» не покращує ситуацію, так як вона носить лише рекомендаційний характер, тому більшість користувачів ігнорують повідомлення про можливу небезпеку.

Список літератури

1. Mobile Operating System Market Share Worldwide. *Statcounter*. URL – https://gs.statcounter.com/os-market-share/mobile (дата звернення: 30.05.2023);
2. Android Studio. *Android*. URL – https://developer.android.com/studio (дата звернення: 31.05.2023);
3. Linux з підвищеною безпекою в Android. *Android*. URL: https://source.android.com/docs/security/features/selinux?hl (дата звернення: 01.06.2023).

Відомості про авторів

Шипунов Микита Юрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.shypunov@student.csn.khai.edu
Цуранов Михайло Віталійович, старший викладач кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ (ХНУВС), ukrear2006@gmail.com