МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК 004.056.5:510.22(043.3)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система захисту конфіденційних даних в мобільних пристроях

Виконавець: Д.В. Моісеєнко
Керівник: к.т.н., доцент С.Є. Карловский
Нормоконтролер: к.т.н., доцент С.Є. Карловский

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«__» _____ 20__ р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Моісеєнка Дмитра Вікторовича

1. Тема: *Система захисту конфіденційних даних в мобільних пристроях* затверджена наказом в.о. ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: проаналізувати існуючі системи та методики захисту системи в мобільних пристроях; на основі аналізу провести вторгенння та по висновках проведеного вторгнення вдосконалити систему захисту.
4. Зміст пояснювальної записки: аналіз існуючих систем та методів захисту інформації в мобільних пристроях; моделювання вторгнення в систему захисту та вдосконалення системи від майбутніх вторгнень

КАЛЕНДАРНИЙ ПЛАН
виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	19.04.2021	*Виконано*
2.	Аналіз літературних джерел	10.05.2021	*Виконано*
3.	Обґрунтування вибору рішення	12.05.2021	*Виконано*
4.	Збір інформації	13.05.2021	*Виконано*
5.	Дослідження сучасних систем і методик захисту в системах мобільних пристроях	15.05.2021-20.05.2021	*Виконано*
6.	Моделювання вторгнення в систему мобільних пристроїв, висновок по вторгненню	21.05.2021-26.05.2021	*Виконано*
7.	Вдосконалення систем захисту в мобільних пристроях, проведення аналізу на вторгення.	29.05.2021-05.06.2021	*Виконано*
8.	Перевірка на коректність оформлення дипломної роботи.	06.06.2021	*Виконано*
9.	Перевірка на антиплагіат	07.06.2021	*Виконано*
10.	Оформлення і друк пояснювальної записки	08.06.2021	*Виконано*
11.	Оформлення презентації	09.06.2021	*Виконано*
12.	Отримання рецензій від рецензента	10.06.2021	*Виконано*

Здобувач вищої освіти Д.В..Моісеєнко

(підпис, дата)

Керівник дипломної роботи С.Є. Карловський

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 71 с., рис., 16 джерел, 1 додаток.

Метою роботи– є вдосконалення системи захисту конфіденційної інформації в мобільних пристроях.

В роботі вирішено задачу захисту конфіденційної інформації в системах мобільних пристроях. Вдосконалення захищеності системи та рекомендації по її укріпленню.

В роботі проведенно тестування системи захисту та модулювання зламу системи. Проаналізовано вразливості системи і на основі цього проведено вдосконалення системи захисту.

Вдосконалення системи захистів в мобільних пристроях є актуальним на данний час так як кожна людина має мобільні пристрої, що є невід'ємною частиною життя.

Можливі напрямки розвитку цієї роботи пов'язані із розширенням системи Android та її подальшим збільшенням популярності на ринку. Тим самим з вдосконаленням системи вдосконалюються системи зламу її. Тестування проводилось з метою подальшого захисту інформації в мобільних пристроях.

Ключові слова: конфіденційна інформація, система захисту, мобільні пристрої, захист інформації.

ЗМІСТ

ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

BYOD – Bring Our Own Device

RKP – Real time Kernel Protection

SDP – Sensitive Data Protection

SE – Security Enhancements

DUHK – Device Unique Hardware Key

DRK – Device Root Key

SAK – Samsung Authorization Key

AES – Advanced Encryption Standard

OTA – Over The Air

EMM – Enterprise Mobility Management

MDM – Mobile Device Management

ВСТУП

Актуальність. На сьогодні проблема захисту інформації з обмеженим доступом у мобільних телефонах стає дедалі актуальнішою, тому, що мобільний телефон є майже у кожного. Дана технологія є повноцінним обчислювальним пристроєм, що підтримує більшу частину функціоналу традиційних електронно-обчислювальної машини (ЕОМ) за значно менших розмірів, що дозволяє обробляти інформацію віддалено й оперативно, скоротивши на цьому час і зусилля, витрати часу на переміщення до комп'ютера, тому що мобільний пристрій знаходитися практично завжди при собі. Враховуючи той факт, що збережена інформація може містити в собі інформацію різного рівня (типу) конфіденційності, то втрата її може нести значні збитки.

Об'єктами захисту є інформація, що міститься та обробляється на мобільному телефоні, права власника цієї інформації та власника мобільного пристрою, права користувача має бути захищені.

Доступ до інформації, яка зберігається, обробляється і передається в мобільному пристрої, здійснюється лише згідно з дозволу власника інформації чи уповноваженою ним особою.

Без дозволу власника доступ до інформації, яка зберігається, здійснюється лише у випадках, передбачених чинним законодавством

Метою є вдосконалення системи захисту конфіденційної інформації вмобільних пристроях.

Об'єкт дослідження захист від злому системи та проникнення шпигунськихабо вірусних програм для захисту від викрадення конфіденційних даних

Предмет дослідження: Система Enterprise mobility management. Проведення аналізу найпопулярніших систем Samsung KNOX, Google Protect, IOS. Аналіз вразливостей систем та можливості підвищеня захисту.

Практична цінність: Протестовано в наявній системі захист від вторгнень. Змодульовано вторгнення в систему для запропонування вдосконалення захищеності знаючи слабкі місця систем

Android — це портативна (мережева) операційна система для комунікаторів, планшетних комп'ютерів, електронних книжок, цифрових програвачів, наручних годинників, нетбуків і смартбуків, заснована на ядрі Linux. Це порівняно «молода» операційна система, використовувана на широкому спектрі мобільних пристроїв.

Завдяки своєї багатофункціональності, мобільні пристрої з операційною системою Android, можна віднести до ЕОМ, тому їм також притаманні слабкі місця з точки зору безпеки інформації, такі як [1, 2, 3]:

1. Можливість витоку інформації технічними каналами.
2. Можливість візуального зчитування інформації з дисплея пристрою.
3. Наявність вбудованої пам'яті на пристрої, або ж додаткової (флеш накопичувача).
4. Можлива наявність вразливостей в програмному та апаратному забезпеченні.

Особливостями ж самих мобільних пристроїв, що визначають для них загрози безпеки інформації, є:

1. Нестаціонарність (можливість непомітного винесення і повернення пристрою в контрольовану зону).
2. Компактні розміри.
3. Наявність дротових і бездротових інтерфейсів, за допомогою яких можна підключитися до даного пристрою.
4. Можливість використання пристрою як модем для підключення до мереж зв'язку загального користувача.
5. Можливість використання в якості знімного носія інформації (альтернатива флеш-накопичувача)

Однією з таких систем є платформа KNOX(«нокс»), розроблена компанією Samsung. Вона забезпечує високий рівень захисту для одних з найпоширеніших пристроїв для будь-яких організацій. Ця платформа є програмно-апаратним комплексом, який забезпечує апаратні засоби захисту, керування політиками та відповідність нормативним вимогам які входять за рамки стандартних функцій, звичайних для сучасного ринку пристроїв. Таким чином данні питання актуальні і потребують ретельного дослідження. безпечності даних однієї з них, а саме Samsung KNOX.

В даній роботі необхідно провести аналіз існуючих систем, дослідити основні загрози для смартфонів, захист від них за допомогою Samsung Knox, платформи, яка є реальним засобом для задовільнення сучасних потреб бізнеса.

РОЗДІЛ 1 АКТУАЛЬНІСТЬ МОБІЛЬНИХ ТЕХНОЛОГІЙ

В сучасному світі майже кожна людина має хоча б один «розумний» пристрій такий як смартфон, планшет чи ноутбук. Ними користуються кожен день, вони завжди знаходяться поряд з нами. Левова частка інформації яку ми отримуємо, ми отримуємо саме за допомогою таких пристроїв. В більшості випадках на смартфонах зберігається якщо не вся, то дуже велика кількість персональної, а іноді навіть і конфіденційної інформації. І якщо ця інформація належить лише власнику цього пристрою, то відповідальність за її збереження покладається лише на нього, але якщо цей пристрій використовується і для взаємодії з корпоративною інформацією, то питання інформаційної безпеки виходить на перший план. Інколи можливість застосування персональних пристроїв в робочих питаннях буває досить складною, або взагалі неможливою через встановлені політики безпеки в організаціях. Тому на початку XXI сторіччя було запропоновано використання нової IT-політики, яку назвали Bring Your Own Device (BYOD), або «візьми свій власний пристрій». Але найбільшої популярності ця концепція досягла лише в 2010-х роках за підтримки таких компаній як Intel, Citrix Systems та Unisys. [1]

1.1 Обґрунтування необхідності використання MDM систем

Першою реалізацією цієї політики стали Mobile Device Management(MDM) системи, які включали набір сервісів та технологій, які забезпечували контроль та захист мобільних пристроїв, які використовує організація та її співробітники. Керування мобільними пристроями переслідує дві задачі: забезпечення безпеки корпоративної інформації на пристроях, які знаходяться поза мережевої інфраструктури, а також контроль за станом самих пристроїв.

Одними з найпоширеніших проблем, з якими пересікаються більшість компаній є:

- втрата або крадіжка мобільного пристрою;
- атаки на пристрої, які вже утилізуються;
- вірусні атаки;
- фішингові атаки;
- автоматичне завантаження недозволених додатків;
- атаки через небезпечні мережі;

Вплив таких погроз може впливати на такі активи як особисті данні, інтелектуальна власність підприємства, фінансові активи, справність та доступність пристроїв та сервісів.

Сама думка про те, що доступ до конфіденційної інформації може бути не в корпоративній мережі викликає дуже багато сумнівів щодо доцільності використання подібних систем у фахівців з IT-безпеки. Тому перш за все, перед початком впровадження системи необхідно зважити всі переваги та ризики для бізнесу і вже потім приймати подальші рішення.

Принести власний пристрій (BYOD) є поширеною концепцією у більшості підприємств, наприклад 84% опитаних компанією IDC в США заявили, що вони дозволяють хоча б певний ступінь використання персональних пристроїв на робочому місці. Використання персональних пристроїв на робочому місці - це тенденція, яка торкається більшості IT-підрозділів. Хоча BYOD допомагає підприємствам скоротити витрати і може покращити задоволеність працівників, це також може бути проблемою безпеки.

За даними IDC, у підприємств з великим процентом використання BYOD виникли частіші проблеми з безпекою. Серед організацій с переважно більшим розгортанням BYOD, інциденти з мобільною безпекою були на 10-12% частішими. Серед фірм, що обмежують або забороняють BYOD, рівень відповідей на питання безпеки був нижчим за середній на 7%. Розмита межа робочих / особистих технології поширюється за межі пристроїв на додатки та

хмарні послуги. Користувачі зазвичай залучають до роботи особисті або бажані мобільні додатки, хмарне сховище, програми SaaS та інші технології, які, на їх думку, роблять їх більш продуктивними. Відповідно до опитування менеджерів IT Mobile Mobile IDC за 2017 рік (спонсор Google) більше 70% підприємств США та Європи допускають певну тіньову IT у своїх організаціях. Ці фірми розуміють, що все дозволений, але пильний підхід до некорпоративних хмарних та програмних технологій, які використовують працівники, може сприяти підвищенню продуктивності та підвищити задоволеність користувачів.

Еволюцією MDM систем стали Enterprise Mobility Management(EMM) системи, які включали окрім MDM також і Mobile Identity Management, Mobile Application Management, Mobile Content Mamgemet системи. Дана робота присвячена аналізу існуючих систем, їх можливостей, переваг та недоліків, виявленю можливих погроз при застосуванні EMM систем.[1]

1.2 Основні завдання та характеристики EMM систем

В першу чергу система EMM зосереджена на корпоративному керуванні, безпеці, керуванні та контролю мобільних розрахунків. Вона охоплює усі процеси і політики на всіх мобільних пристроях, які являються частиною або основними елементами бізнес-процесів. Сфера діяльності в основному направлена на безпеку, інтеграцію додатків та керуванні, а також на фінансові наслідки таких рішень.

Наприклад корпоративна політика повинна гарантувати те, що додаток буде інтегровано і він може бути використаним на мобільному пристрої, в одночас повинні забезпечуватися необхідні механизми безпечного доступу. Крім того організація повинна контролювати і керувати усіма процесами, пов’язаними з бізнесом та фінансовими расходами, пов’язаними з

використанням таких рішень пристроям які можуть належати організації або співробітнику.

Тож можна дати визначення EMM системі як набору людей, процессів і технологій, зосереджених на керуванні мобільними пристроями, бездротовими мережами та іншими сервісами мобільних обчислень в контексті бізнесу.

Для досягненя розділення особистої та корпоративної інформації були розроблені певні методи:

1) управління мобільними додатками (MAM). Управління пристроями на рівні додатків. Наприклад, налаштування їх доступу до інформації (як з бізнес-мережі, так і з інших додатків на пристрої);

2) управління мобільною ідентифікацією (MIM) Функціонал, що обмежує використання мобільного пристрою. Наприклад, призначення ролей користувачів;

3) управління мобільним контентом (MCM) Повний контроль на рівні корпоративного контенту. Може включати в себе обмеження копіювання і вставки, доступу до репозиторіїв бізнес-контенту. Майже завжди є частиною EMM системи;

4) управління мобільним пристроєм(MDM).

Система, що працює на рівні мобільного пристрою та забезпечує повний доступ до всіх його можливостей.

Не дивлячись на те, що усі методи розділення особистої та бізнес інформації мають одну й туж саму мету, а саме захист корпоративних додатків та інформації, підходи можуть розрізнюватись.[3,5]

На пристрої обов’язково створюється додатковий простір для збереження корпоративної інформації. Схематичне зображення наведено на рис.1.1[1].

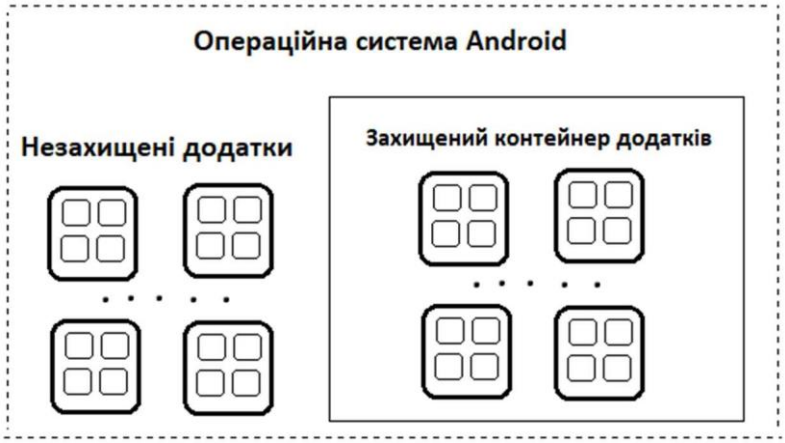

Рисунок 1.1 — Розділення даних

Це дозволяє досягти розподілення контенту на персональному девайсі користувача, що забезпечує безпеку. Реалізація цієї функції може бути різною та на пряму впливати на рівень захищеності від атак. Вона дозволяє забезпечувати різні механізми безпеки такі як:

1) завантаження оновлень контенту напряму до захищеного кнтейнера;
2) обмеження доступу до даних в контейнері в залежності від часу або місце розташування пристрою;
3) дистанційне видалення даних в контейнері.

1.2 Переваги та недоліки EMM систем

До переваг EMM систем можна віднести те, що організацією може контролюватися використання співробітниками їх пристроїв в робочій мережі.

Підвищується ефективність комунікацій співробітників організації, покращується якість забезпечення корпоративної безпеки через те, що адміністраторам безпеки не потрібно окремо налаштовувати кожен пристрій, а політики встановлюються массово на підключені пристрої. Окрім цього, з’являється ожливість доставки електронної пошти. Синхронізації календаря та контактів на смартфонах, плншетах та інших персональних пристроях. Для

досягнення захищеності застосовується захист каналу за допомогою віртуальної приватної мережі і служб віддалених робочів столів.

До недоліків перш за все потрібно віднести вартість впровадження таких систем. По-друге це фрагментованість пристроїв та їх програмного забезпечення. В більшості випадків це, якщо не унеможливлює, то дуже ускладнює керування, налаштування та своєчасне оновлення програмного забезпечення на всіх пристроях. Для нормального функціонування системи в цілому потрібно мати в штаті кволіфікованих адміністраторів. Деякі співробітники можуть негативно ставитись до щільного контролю збоку організації, тому можуть виникнути складнощі. Політика безпеки в компанії може взагалі унеможливлювати використання персональних пристроїв, що робить недоцільним впровадження EMM системи.

1.4 Порівняння найпопулярніших систем

На сьогодняшний день на ринку існує дотатньо багато EMM систем [11]. Лідером на ринку вважається AirWatch by VMware. Інтерфейс програми наведено на рисунку 1.2 .

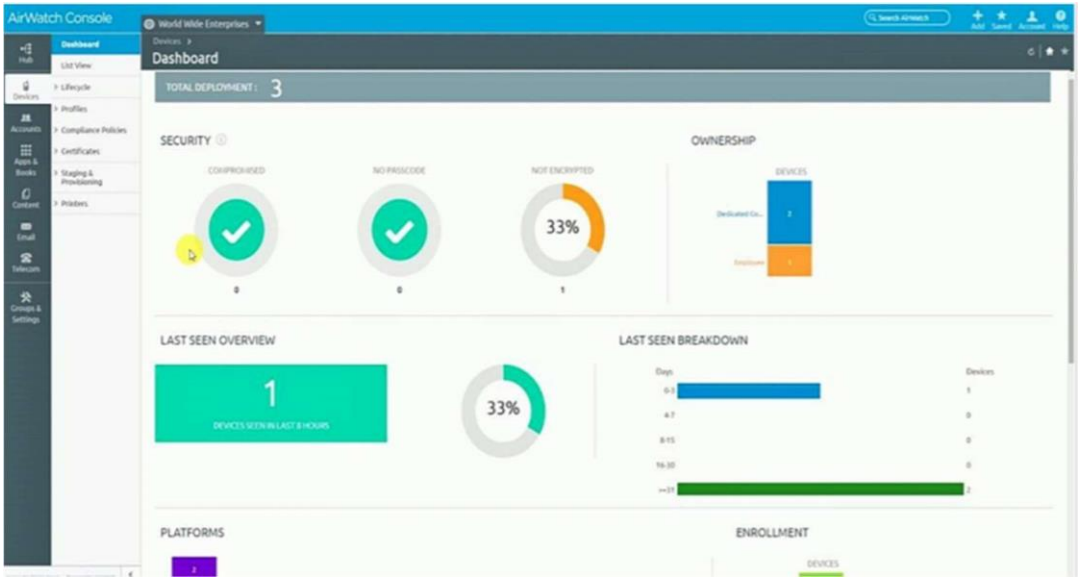

Рисунок 1.2 – Інтерфейс програми VMware AirWatch

Ця продукція користується попитом в таких галузях як енергетика, роздрібна торгівля, перевезння та інші. Підтримуються всі актуальни операційні системи такі як Android, IOS, Windows, MacOS. Може використовуватися для налаштувань пристроїв з Android Enterprise або Samsung Knox. AirWatch складається з чорирьох підсистем:

1) mobile device management. Можливість швидкої ініціалізації пристроїв для корпоративного використання, застосовувати політики безпеки та захищати корпоративні данні за умови доступу з мобільних систем, віддалено блокувати та видаляти данні з пам'яти пристрою;

2) mobile application management. Можливість керування та встановлення або видалення окремих додатків на рівні співробітників, персональних або робочих станцій підприємства;

3) mobile email management. Можливість забезпечення захищеності корпоративної пошти;

4) mobile content management. Можливість захищеного доступу до робочих даних.

Intune Enterprise Mobility+Security від Microsoft. Інтерфейс програми наведено на рисунку 1.3

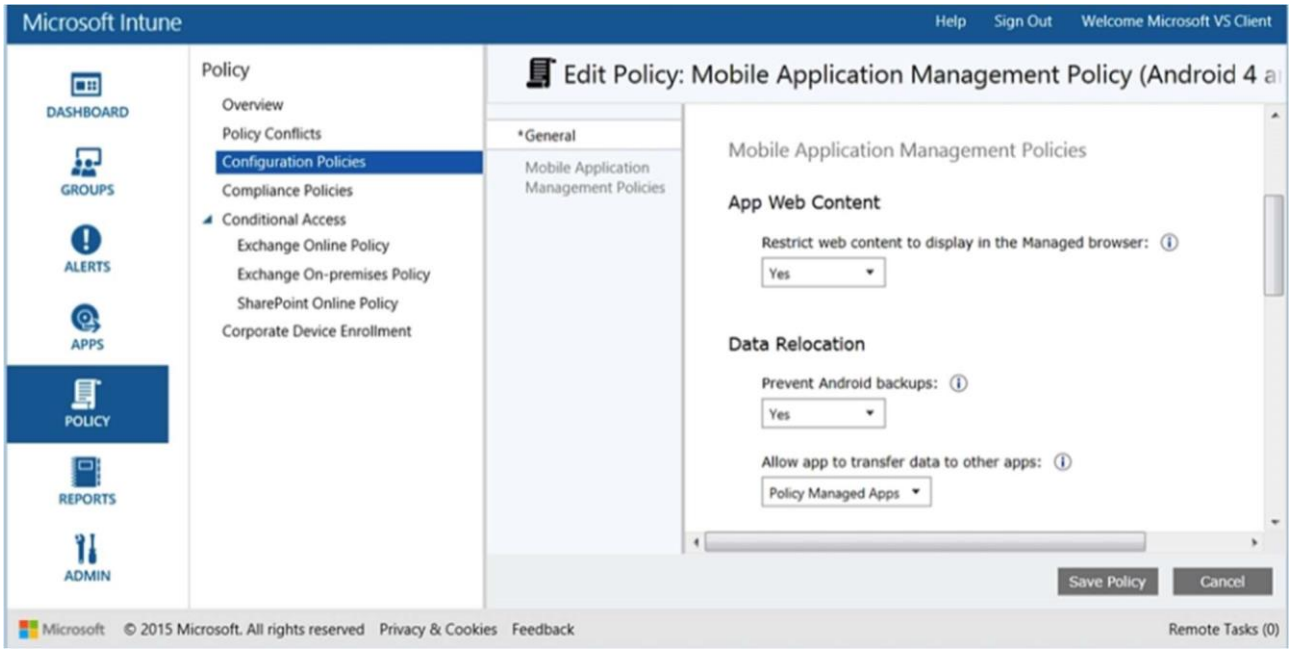

Рисунок 1.3 – Інтерейс програми Microsoft Intune

Intune поєднує в собі різні рішення Microsoft Azure щодо безпеки та управління ідентичністю для оновленої роботи порталу, хоча він все ще містить застарілі функції адміністратора. Він дозволяє вам визначити стратегію управління мобільним пристроєм, яка відповідає потребам вашої організації та застосовувати гнучкі керування мобільними пристроями та додатками, що дозволяє вашим працівникам працювати з вибраними ними пристроями та програмами, захищаючи інформацію вашої компанії[12, 15].

Intune призначений для підтримки вашої різноманітної мобільної екосистеми, що дозволяє безпечно керувати пристроями iOS, Android, Windows та macOS з одного, єдиного мобільного рішення. Це також допомагає захистити дані компанії з реєстрацією на пристроях або без них, створивши політику захисту додатків, а також досягти ефективності IT у хмарі, тому вам не доведеться підтримувати локальні сервери. Рішення пропонується в цінових планах, починаючи з плану Intune від 6 доларів США / місяць на місяць.

Cisco Meraki MDM рішення забезпечує уніфіковане управління мобільними пристроями, Mac, ПК та всією мережею з централізованої інформаційної панелі. Інтерфейс програми наведено на рисунку 1.4.

Він дає вам можливість застосовувати політику безпеки пристрою, розгортати програмне забезпечення та додатки, а також виконувати віддалене, живе усунення несправностей на тисячах керованих пристроїв. Уніфікована платформа управління кількома пристроями забезпечує централізоване управління, діагностику та моніторинг OTA для мобільних пристроїв, якими керує ваша організація, включаючи iPad, Android, Macs та ПК.

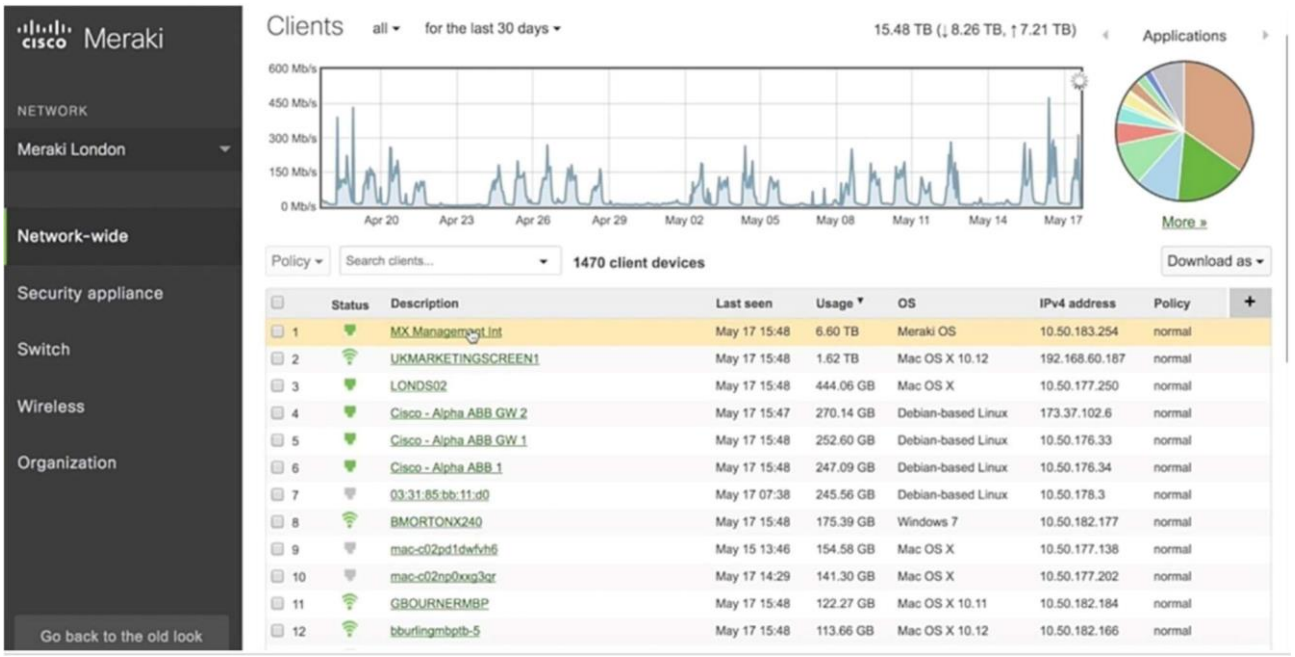

Рисунок 1.4 – Інтерфейс програми Cisco Meraki

Його системний менеджер контролює кожен з пристроїв вашої організації, показуючи корисні показники, такі як інформація про апаратне забезпечення та програмне забезпечення клієнта та недавнє місцезнаходження. Пропонуючи надійне виконання політики безпеки на мобільних пристроях, якими керує ваша організація, він може захищати пристрої та їх дані, контролювати їх використання за допомогою чіткої політики пароля та обмежувати доступ до магазину додатків, ігор та вмісту.Ціноутворення повністю ґрунтується на потребах вашої організації. Цінові ціни на MDM Cisco Meraki пропонуються на основі котирувань.

BlackBerry Enterprise Mobility Suite - це повне рішення EMM, створене для захисту даних вашого бізнесу та підвищення продуктивності робочої сили. Інтерфейс програми наведено на рисунку 1.5. Незалежно від того, в приміщенні чи в хмарі, або в поєднанні обох, це дозволяє вашій організації захищати та керувати всіма інтелектуальними кінцевими точками на вашому підприємстві за допомогою гнучких варіантів розгортання, тривалості мобільності та

технічної підтримки. Ви зможете мобілізувати свої критичні робочі процеси та бізнес-процеси та додатки, включаючи Microsoft Office 365.

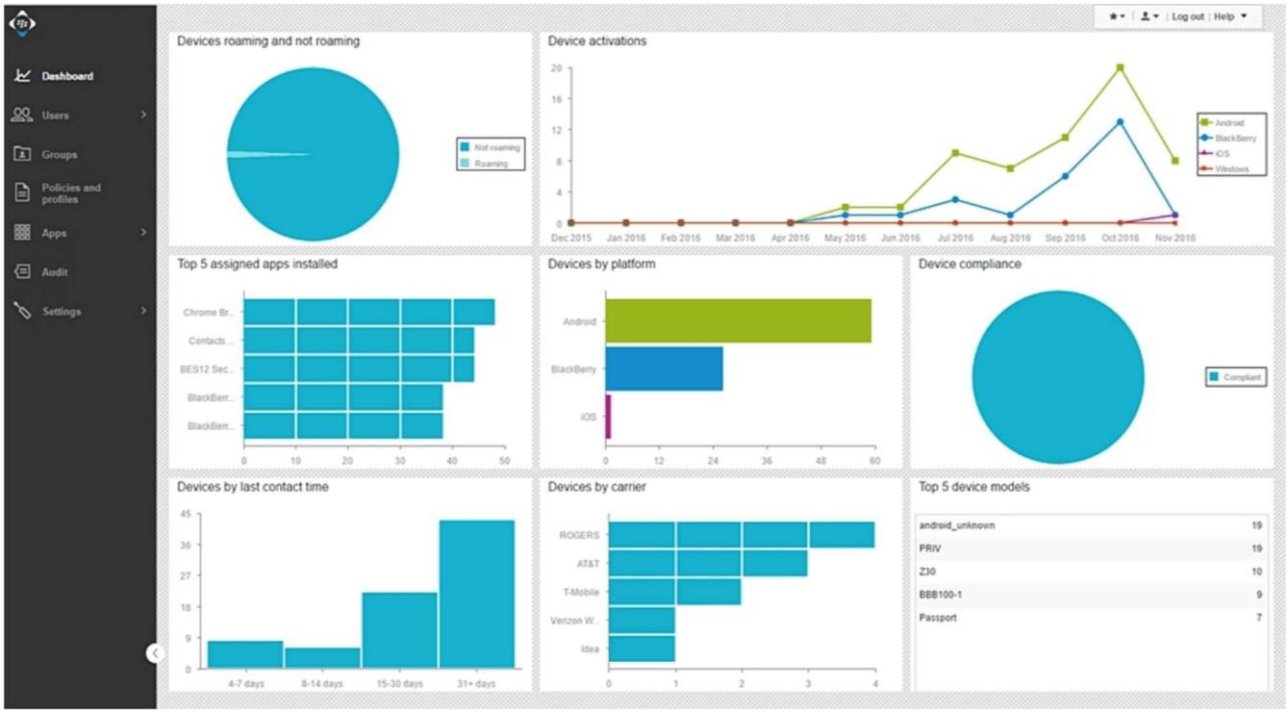

Рисунок 1.5 – Інтерфейс програми BlackberryEnterprise Mobility Suite

Enterprise Mobility Suite постачається з додатками для продуктивності та співпраці та підтримує постійно змінюваний набір сторонніх програм та спеціальних програм. Функція управління мобільним вмістом дозволяє отримувати доступ до ваших бізнес-файлів з SharePoint, OneDrive, Box та багато іншого, все з натурними можливостями редагування документів. Ви можете захистити файли навіть за межами брандмауера, спростити доступ та права, використовувати єдиний вхід та повну федерацію хмарних служб, а також двофакторну автентифікацію на основі токенів. Люкс поставляється у п'яти виданнях із спеціальними цінами на основі використання. MobileIron Platform це продукт компанії MobileIron, який є найбільш швидко розвивається у світі [12]. Інтерфейс програми наведено на рисунку 1.6.

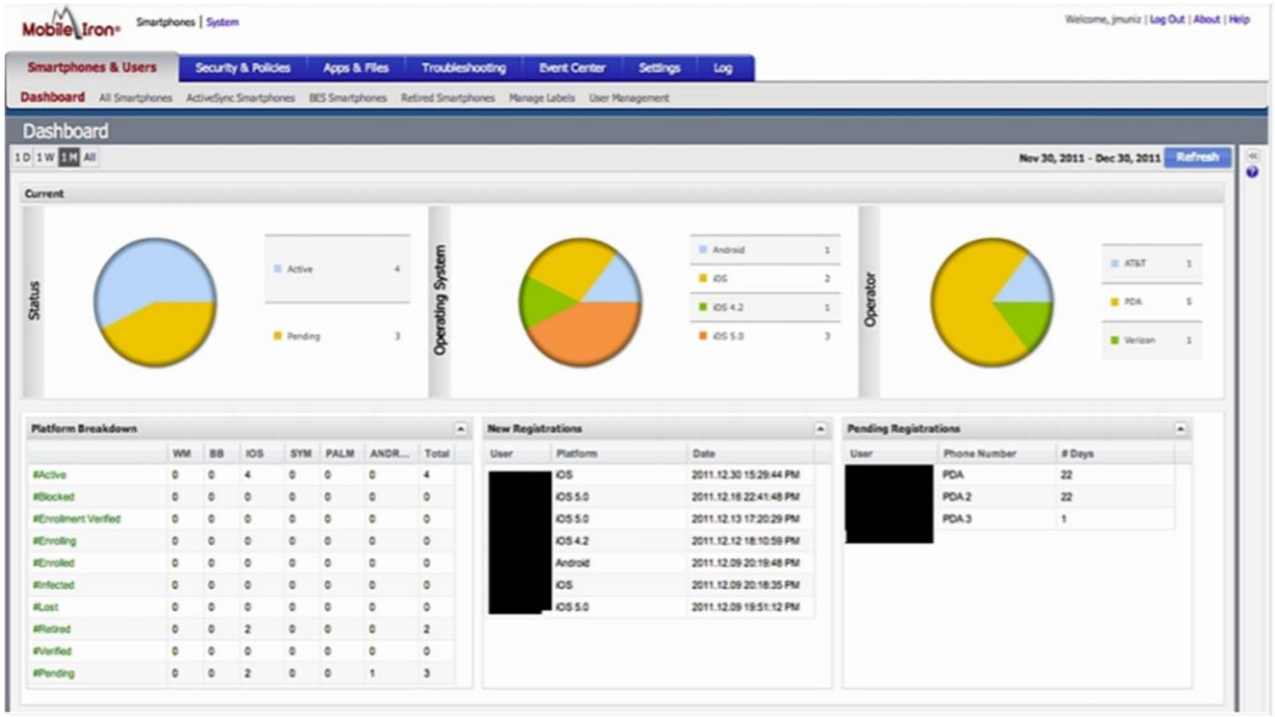

Рисунок 1.6 – Інтерфейс програми MobileIron Platform

Він об’єднує класичний набір засобів безпеки та EMM функціоналу, таких як MDM, MAM, MCM. Також підтримує багато популярних операційних систем, що дозволяє швидко впровадити цю систему до існуючої бізнес інфраструктури. Технологічно складається з двох серверів: MobileIron VSP та MobileIron Sentry. Перший відповідає за керування системою, облік пристроїв та поширення політики безпеки на кожен пристрій. Інший контролює підключення пристроїв, веде облік усіх спроб підключення, контролює доступ до поштового серверу. Обидва сервери можуть бути встановлені як віртуальна машина або як окремий дистрибутив. [9]

Платформа MaaS360Cloud від IBM дозволяє керувати операційними системами – Android, IOS, Windows та MacOS. Інтерфейс програми наведено на рисунку 1.7.

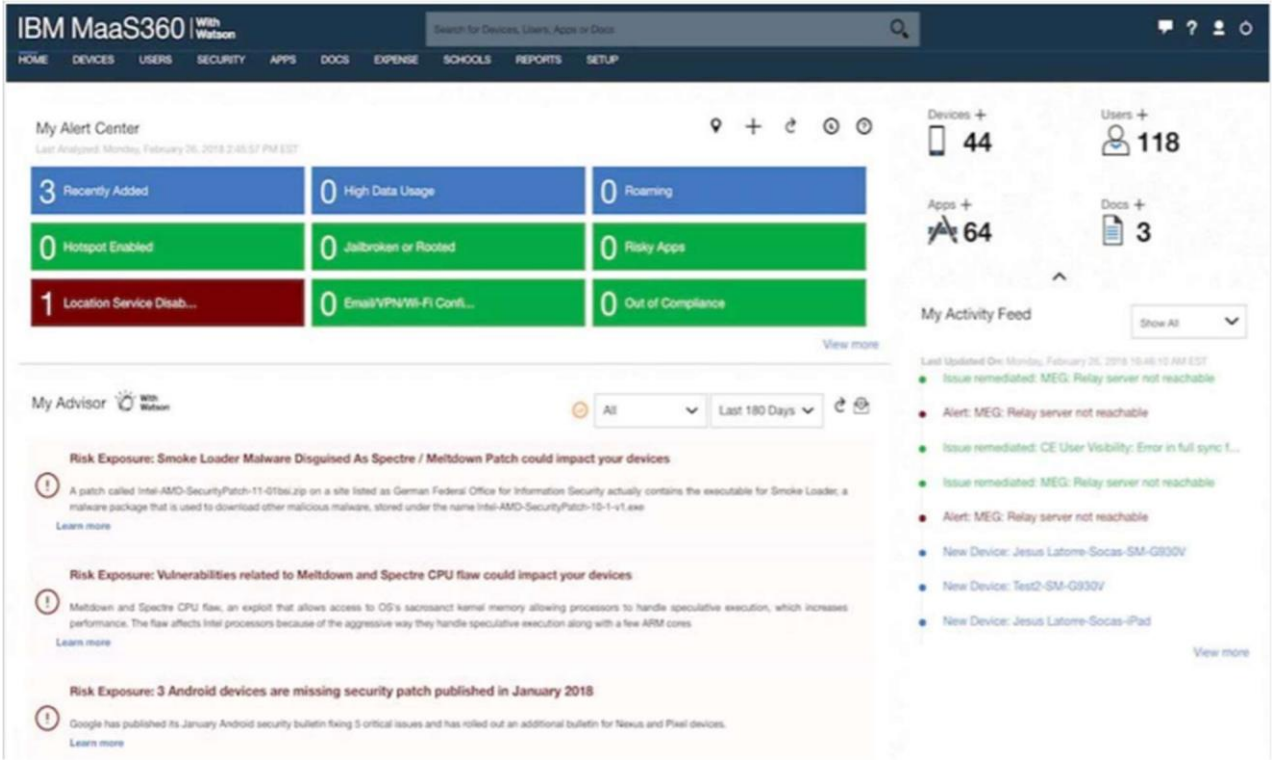

Рисунок 1.7 – Інтерфейс програми IBM MaaS360Cloud

MaaS360Cloud дозволяє керувати документами, поширювати додатки. Існує можливість захисту від різних вірусних атак та компрометації пристрою наприклад втрати або крадіжки. Створення VPN каналу для захисту інтернет з’єднань. Також сумісний з такою технологією як Android Enterprise та Samsung KNOX. Також плюсом даного продукту є його інтеграція з іншим продуктом компанії – штучним інтелектом IBM Watson [10].

Samsung KNOX for Enterprise є розробкою компанії Samsung та доступною тільки на пристроях цієї фірми виробника [2]. Інтерфейс програми наведено на рисунку 1.7.

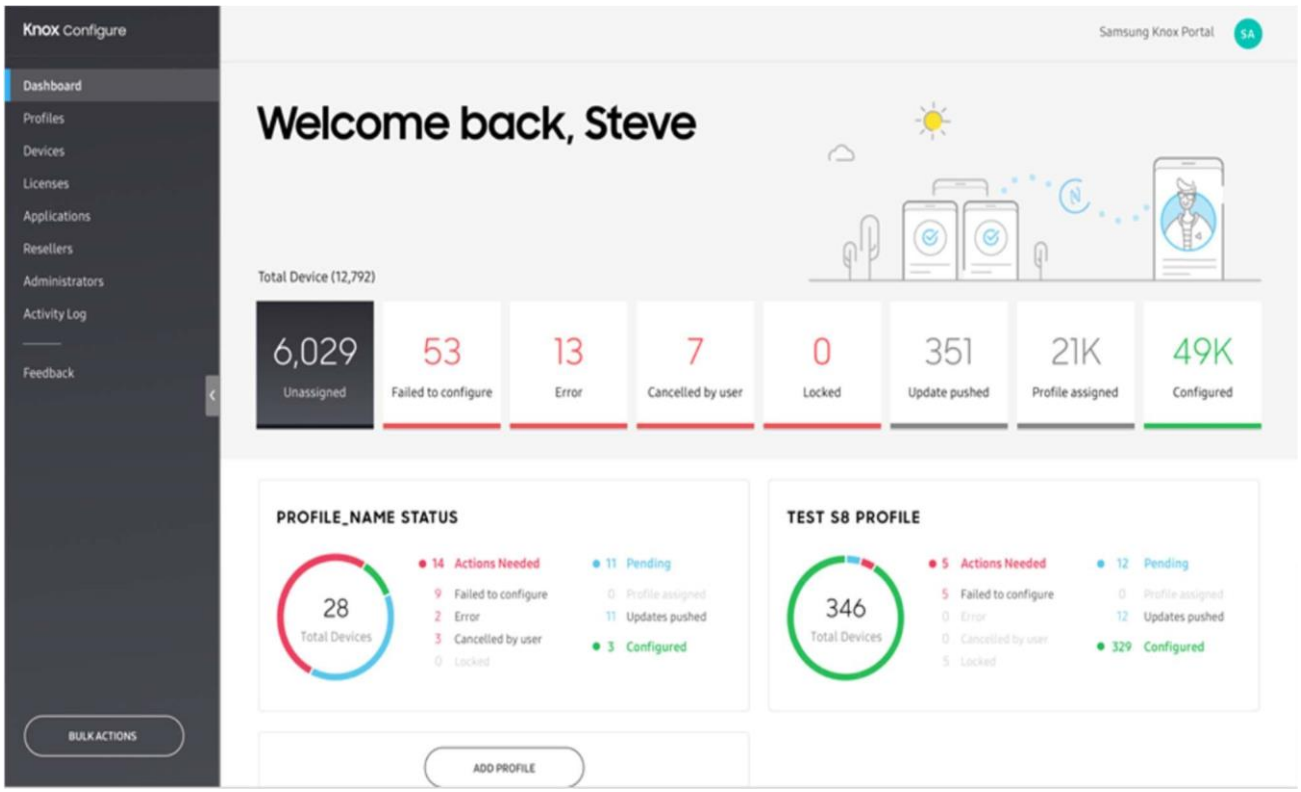

Рисунок 1.7 – Інтерфейс програми Samsung KNOX

Це можна віднести до найголовнішого недоліку цієї системи, однак це забезпечує наявність функцій, які не доступні для інших програмних продуктів.

1.5Висновок до розділу 1

Головними перевагами цієї системи є глибока інтеграція з «залізом» та програмним забезпеченням пристроїв, забезпечення гарантованого захисту корпоративних даних, наявності окремих VPN каналів для кожного додатка в, так званому захищеному контейнері, окремому захищеному середовищу для бізнес додатків, корпоративної інформації, тощо.

Наявність контролю за станом пристрою, можливість повного керування адміністраторами даними на окремому пристрої. Однією з можливостей, яка виділяє цю систему від інших є можливість реєстрації пристрою в системі,

налаштування на ньому усіх політик безпеки, встановлення необхідного програмного забезпечення ще до відкриття заводського пакування та першого запуску пристрою. Що значно облегшує та пришвидшує імплементацію цього продукту[2].

РОЗДІЛ 2 ОСНОВНІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОС ANDROID

Використання цих систем не може вберегти пристрій від втрати, або крадіжки, але вони позволяють мінімізувати ризики, які можливі при даних випадках.

Однією з основних можливостей є віддалене керування, видалення усіх даних. Можливе навіть блокування доступу до робочої зони, якщо зловмисник знає пароль доступу. Щодо досліджень утилізованих пристроїв, в системі в обов’язково застосовується шифрування усіх важливих даних.

Для захисту від встановлення небезпечного програмного забезпечення застосовуються механізми налаштувань прав на пристрої. Наприклад адміністраторами можливе блокування встановлення будь-яких програм, окрім програм з офіційного магазину додатків, який керується організацією. Крім того, деякі системи постійно моніторять стан системи і виявляють будь-яке вторгнення, що забезпечує гарантію якості та надійності системи в цілому. Що стосується захисту під час мережевого обміну інформацією, то основним засобом є VPN.

Окремі системи також можуть використовувати автентифікацію при доступі до корпоративної мережі та звісно використовується шифрування усього трафіку.

Присутня можливість створювати для кожного додатка окремий VPN канал, що також створює додаткову захищеність за умови використання загальнодоступних, або ненадійних мереж. Це також створює додаткові переваги для сервера, тому що не потрібно постійно підтримувати канал для усіх додатків.

2.1 Безпека ОС Android

Android – це надійна операційна система, яка встановлена на дуже велику кількість пристроїв, починаючи від мобільних телефонів і закінчуючи головними пристроями в автомобілі. Вона базується на таких основах, як відокремлення системних процесів, архітектурі довіреної ОС, а також вона використовує потужний аналізатор загроз який використовує машинне навчання та хмарні обчислення для визначення загроз за допомогою великої бази знань компанії Google[10].

Багато підприємств скоро розширять кількість мобільних пристроїв, які будуть використовуватися в корпоративній сфері за допомогою сучасних підходів та концепцій як MDM або BYOD.

Але, незважаючи на те, що мобільність підприємств зростає, безпека даних залишається головною перешкодою на шляху впровадження нових технологій використання мобільних пристроїв.

Зараз одними з найпоширеніших загроз для мобільних пристроїв є:

1. використання для доступу до глобальної мережі через незахищені точки доступу Wi-Fi, в яких можлива атака MITM(людина посередині);
2. можливість крадіжки або втрати пристрою, яка дозволить зловмиснику отримати повний фізичний доступ до пристрою;
3. шкідливе програмне забезпечення, яке може бути встановлено не навмисно самим користувачем і яке буде тихо збирати усю потрібну зловмиснику інформацію та навіть робити фото, відео та аудіо фіксацію усього, що трапляється навколо пристрою.

Однак остання загроза є найменш вірогідною через сам принцип побудови системи Android, де кожен додаток виконується відокремлено від інших та отримати доступ до даних іншої програми без отримання прав root неможливо.

Розробники операційної системи Android включили безпеку ще на етапі її проектування. Це гарно відображається в дворівневій моделі безпеки, що

використовується додатками Android. Android, по своїй суті, покладається на одну з функцій безпеки, що надаються ядром Linux, а саме запуск кожної програми як окремого процесу з власним набором структур даних і з запобіганням втручання інших процесів у його виконання.

На рівні застосунка, для отримання системних дозволів, Android використовує більш дрібні дозволи для надання можливості взаємодії зсистемними ресурсами або іншими додатками. Майже для кожного дозволу потрібно явне підтвердження користувача. За замовчуванням жодна програма не має дозволу для виконання будь-яких операцій, які можуть негативно вплинути на інші програми, дані користувача або систему. Приклади таких операцій включають надсилання SMS-повідомлень, отримання інформації о контактах та доступ до Інтернету. Відтворення музичних файлів або перегляд зображень не підпадають під такі операції, і, таким чином, додаток не потребує явно вимагати дозволу на це. Дозволи на рівні додатків надають засіб для отримання доступу до вмісту з обмеженим доступом та API.

Кожна програма Android (або її компонент) працює в окремому віртуальному середовищі Dalvik або ART. Віртуальна машина (VM) - пісочниця. Однак не потрібно вважати, що це саме ця пісочниця забезпечує безпеку. Віртуальну машину оптимізовано для ефективної роботи на пристроях, з невеликим обсягом пам’яті. Перевірки дозволів Android не здійснюються всередині віртуальної машини, а, скоріше, всередині кода ядра Linux і застосовуються під час виконання.

Доступ до засобів низького рівня Linux надається через ідентифікатор користувача та групи прав, інші додаткові менш вразливі для системи функції безпеки отримуються через дозволи Маніфесту.

Пісочниці ядра Linux розрізняють програми та не дозволяють їм отримати доступ до даних або інформації користувачів інших програм або здійснення таких операцій, як доступ до Інтернету, здійснення телефонних дзвінків або отримання SMS-повідомлень. Якщо програмі необхідно виконати

вищезазначені операції (наприклад, доступ до Інтернету), отримати інформацію користувача (наприклад, контакти) або спілкуватися з іншими програмами (наприклад, спілкуватися з програмою електронної пошти), потрібно спеціально запросити ці дозволи. Ці дозволи декларуються у файлі конфігурації (Manifest.xml). Коли програма встановлена, Android пропонує користувачеві або дозволити, або відхилити дозволи (див. Рисунок 2.1).

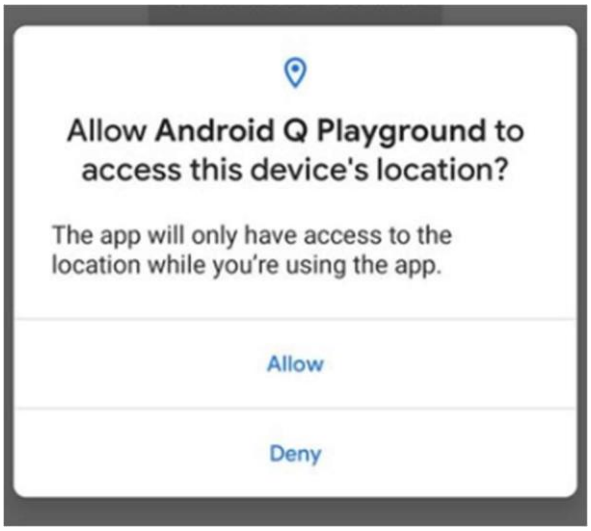

Рисунок 2.1 — Діалогове вікно для надання дозволу

Користувач не може вибрати певні дозволи – тобто дозволити доступ до Інтернету та відхилити доступ до SMS. Програма запитує набір дозволів, і користувачі або схвалюють, або відхиляють їх усі. Коли користувач затвердив ці дозволи, Android (через ядро Linux) надасть доступ до запитуваних операцій або дозволить взаємодіяти з різними додатки / компонентами. Слід зауважити, що з версії Android 6.0 була впроваджена можливість користувачу коригувати дозволи навіть після того, як він їх підтвердив.

Дозволи на Android також відображаються кінцевому користувачеві під час завантаження програм з "офіційного" магазину додатків Android – Google Play (див. Рисунок 2.2).

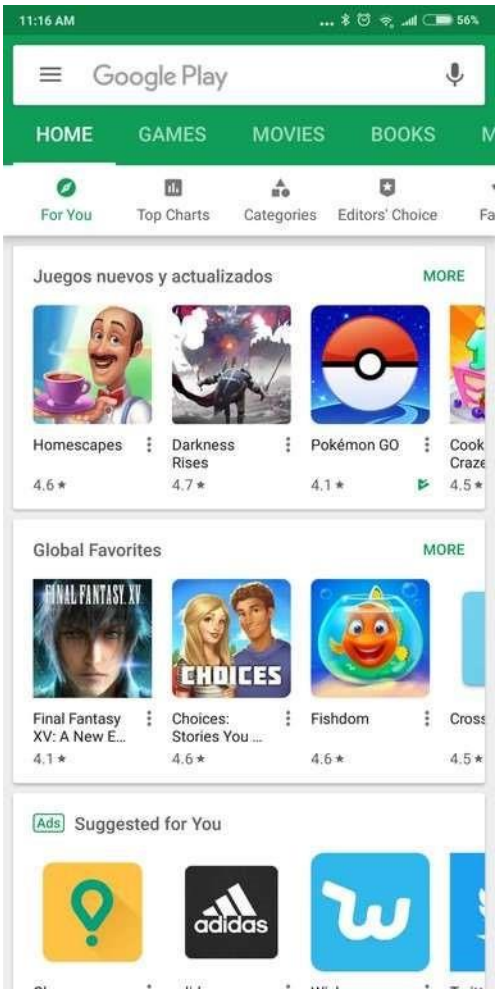

Рисунок 2.2 — Магазин додатків Google Play

Однак, це може бути не завжди так, оскільки дозволяє встановлювати застосунки з будь якого джерела. Якщо користувач просто завантажує .apk файли, система попереджає про можливу небезпеку, але користувач може всеодно встановити дане програмне забезпечення.

2.2 Додаткові засоби безпеки

Незважаючи на те, що пристрої під керуванням операційної системи Android мають потужні основи безпеки, цілий ряд хмарних сервісів підтримує пристрої Android для подальшого покращення та забезпечення загальної

безпеки платформи. Google Mobile Services (GMS) - це пакет програм, що ліцензуються Google сторонніми виробниками програмного забезпечення та партнерів Android, що дозволяє легко контролювати попередню інсталяцію таких програм, як Gmail, Hangouts, Карти, Фотографії, YouTube, Google Play Store та інші основні додатки Google. Менш очевидним для користувачів Android є основні можливості безпеки, які поставляються із GMS. Будь-який пристрій, що має ліцензію на GMS, також має функції сканування програмного забезпечення на основі пристроє та хмарно заснованих засобів для безпеки, а саме базовий набір послуг та функцій, який називається Google Play Protect. Вони варіюються від сканування на пристрої для використання потенційно небезпечних додатків (PHA) та експлуатування додатків, до програми Find My Device (раніше «Диспетчер пристроїв Android») для пошуку втрачених чи вкрадених пристроїв та виявлення наявності прав рут[16].

2.3 Система захисту Samsung KNOX

Забезпечення захищеності системи в цілому забезпечується використанням програмно-апаратних засобів та виконанням перевірок стану пристрою з моменту включення і до моменту вимкнення.

Апаратна безпека - Довірена середа відокремлює критично важливий для безпеки код від решти операційної системи. Таке стратегічне поділ гарантує, що тільки довірені процеси, які ізольовані і захищені від атак і експлойтів, можуть виконувати важливі операції, такі як шифрування і дешифрування даних. Довірені середовища виконують перевірки цілісності перед виконанням будьякого програмного забезпечення. Ці перевірки виявляють зловмисні спроби змінити довірену середу і програмне забезпечення, яке працює на пристрої.

Апаратна підтримка - довірене середовище підтримується апаратними засобами, якщо апаратний захист ізолює середу від решти працюючої системи.

Ця ізоляція гарантує, що уразливості в основний операційній системі прямо не впливають на безпеку довіреного середовища. Середовище також пов'язує перевірки цілісності програмного забезпечення, що працює в довіреному середовищі, з криптографічними сигнатурами, що зберігаються в апаратному забезпеченні пристрою. Перевірки цілісності з апаратною підтримкою не дозволяють зловмисникові використовувати вразливості програмного забезпечення для обходу засобів захисту і завантаження незатвердженого програмного забезпечення в довірену середу[11].

Платформа KNOX використовує апаратне довірене середовище, а конкретні компоненти залежать від апаратного забезпечення пристрою. Наприклад процесори ARM надають Trusted Execution Environment(TEE), які використовують такі компоненти, як TrustZone, ARM Hypervisor Mode и Embedded Secure Elements. Функції KNOX, які використовують довірене середовище, включають Захист ядра в реальному часі (RKP), Довірене завантаження(Trusted Boot), Атестацію «здоров'я» пристрою (Device Health Attestation), Керування сертифікатами, Захист важливих даних(SDP) та Мережеву аналітику платформи(NPA).

Ізоляція додатків використовується для запобігання навмисного або випадкового доступу шахрайських додатків до несанкціонованих даних. Платформа Knox надає кілька форм ізоляції додатків для створення захищеного простору, контейнера додатків на пристроях Samsung. Кожен варіант заснований на одній і тій ж технології ізоляції ядра під назвою Security Enhancements for Android (SE для Android.) SE для Android - це інтеграція SELinux і Android, розширена для охоплення компонентів Android і парадигм проектування.

Android Enterprise на пристроях Samsung забезпечує ізоляцію додатків за допомогою робочих профілів, які забезпечують базову ізоляцію корпоративних додатків від особистих додатків. При використанні Android Enterprise на пристроях Samsung Knox надає такі функції, як захист ядра в реальному часу

(RKP), безпечні корпоративні додатки і зберігання сертифікатів та ключів на апаратному рівні, що робить Android Enterprise ще краще на пристроях Samsung.

Knox Workspace ґрунтується на Android Enterprise, надаючи додаткові поліпшення безпеки та управління. Зокрема, Knox Workspace виграє від перевірок цілісності з апаратною підтримкою. Ці перевірки виявляють будь-яке втручання в пристрій або його засобів захисту і блокують робочу область.

Knox також підтримує Захист конфіденційних даних(SDP), шифрування даних під час роботи пристрою і дешифрування тільки після того, як користувач пристрою автентифікується, щоб розблокувати робочу область Knox. Крім того, Knox Workspace надає більше управління пристроєм, наприклад, примусова двухфакторна аутентифікація для Knox Workspace, використання облікових даних Active Directory підприємства для аутентифікації і керований імпорт і експорт корпоративних даних в Knox Workspace.

Служба управління SE для Android (SEAMS) дозволяє ізолювати один додаток або невеликий набір довірених додатків, щоб заблокувати додатки в одному контейнері. Контейнери додатків, створені за допомогою SEAMS, забезпечують ті ж переваги, що і Knox Workspace. Однак на відміну від перших двох варіантів, контейнери SEAMS не мають спеціального графічного інтерфейсу. Додатки в контейнері SEAMS відображаються разом з іншими додатками на пристрої, але вони відзначені значком щита, який показує, що вони ізольовані і захищені від додатків, які не використовують загальний контейнер. Користувач може створювати стільки контейнерів SEAMS, скільки захоче на льоту.

За допомогою Knox Workspace підприємства можуть розгортати додаткові політики безпеки і управління для забезпечення виконання вимог, наприклад тих, які необхідні для роботи в строго регульованих галузях, таких як фінанси, охорона здоров'я і уряд[2].

Підприємства можуть захищати особисту та корпоративну інформацію, використовуючи наступні функції:

1) автентифікація користувача - пристрої Samsung Knox підтримують не тільки автентифікацію за паролем, PIN коду і шаблоном, а й новітні біометричні аутентифікації: відбитки пальців, райдужна оболонка ока особи, інтелектуальне сканування. Доступні параметри як для аутентифікації на екрані блокування пристрою, так і для окремої аутентифікації в Knox Workspace. За допомогою платформи Knox можливо забезпечити примусову двохфакторну аутентифікацію для облікових даних Knox Workspace або Enterprise AD, щоб забезпечити більш надійний захист даних;

2) шифрування даних пристрою - пристрої Samsung Knox забезпечують шифрування даних через SDP який пов'язан з апаратно підтримуваним Root of Trust та аутентифікацією користувача. Це шифрування забезпечує розшифровку даних тільки на пристрої, на якому вони зберігаються, і тільки власником пристрою. DualDAR шифрування пропонує два варіанти шифрування для досягнення ще більш високого рівня надійності;

3) шифрування мережевих даних - пристрої Samsung Knox пропонують найширший вибір VPN можливостей, надаючи можливість налаштовувати окремий VPN для робочого простору Knox, а також для окремих додатків, щоб ще більше посилити ізоляцію даних. Knox також пропонує постійний доступ до VPN, VPN на вимогу, обхід локального VPN, HTTP-проксі через VPN, множинні активні тунелі, строгий контроль витоку даних і ланцюжки або каскадування VPN;

4) відстеження, блокування та видалення пристроїв - пристрої Samsung Knox дозволяють відслідковувати, геозону і автоматично блокувати пристрої на основі подій і політик безпеки. Наприклад, пристрій, який покидає вказаний географічний периметр, заблоковано, стерто усю інформацію або відновлено до заводських налаштувань за замовчуванням.

2.4 Безпека платформи Samsung Knox

Root of Trust

На приклад кожен пристрій в системі одночасно інфіковано шкідливим програмним забезпеченням яке може переглядати конфіденційну інформацію. Атаки та експлойти продовжують удосконалюватися, намагаючись попередити різноманітні міри безпеки для мобільних пристроїв.

Для вирішення цієї проблеми було запропоновано використання стеку Root of Trust, який мінімізує вразливості, виявляє вторгнення та блокує конфіденційну інформацію у разі виявлення погроз.

Він відповідає на такі питання безпеки, як:

1) як дізнатись, чи була завантажена скомпрометована операційна система?
2) чи можемо ми вірити, що наші сертифікати надійно зберігаються?
3) чи модифікував експлойт ядро або інші компоненти системи?[2]

Досягнення надійного середовища досягається чотирма засобами:

1) встановлення апаратного Root of Trust, на який спираються інші компоненти;
2) створення довіри під час завантаження системи за допомогою таких функцій, як Trusted Boot;
3) підтримує довіру під час використання пристрою завдяки захисту ядра в реальному часі;
4) доведення своєї надійності за допомогою Атестації працездатності пристрою.

Root of Trust створюється завдяки наступним крокам:

1) генерується унікальний ключ для даного пристрою(DUHK) за допомогою апаратного генератора випадкових чисел;
2) далі DUHK генерує і шифрує кореневий ключ пристрою(DRK) та ключ підтвердження Samsung(SAK). DRK і SAK включають код аутентифікації,

який дозволяє перевірити IMEI і серійний номер пристроїв. Це дозволяє користувачам отримати підтвердження того, що вони користуються саме с тим пристроєм, з яким повинні;

3) використання DUHK доступно тільки для операційної системи TrustZone, яка використовує його для створювання наступних унікальних для кожного довіреного додатка ключів. DRK і SAK являються закритими ключами, які дозволяють довіреним додаткам підтверджують свою справність. Ці додатки глибоко інтегруються з апаратним забезпеченням для досягнення більшої безпеки;

4) після запуска пристрою, Samsung використовує ключ безпечного завантаження(SSBK) для перевірки усього програмного забезпечення;

5) програмне забезпечення перевіряє кожну функцію платформи Knox, перед її запуском. Так як кожна перевірка складає ланцюг перевірок, яка починається з самої першої перевірки на апаратному Root of Trust, неважливо в який ланці була атака, система це виявить[1].

Для миттєвого блокування та недопущення запуску інших захищених частин системи, в платформі використовується так званий гарантійний запобіжник. Це одноразовий програмний запобіжник, який вказує на те, що пристрій ніколи не був в несанкціонованому стані. Якщо один з компонентів перевірки виявляє використання нелегітимних компонентів або якщо відключені деякі компоненти системи наприклад SELinux, система активує запобіжник.

Коли запобіжник активовано виконуються наступні міри безпеки:

1) не проходить перевірка працездатності пристрою;

2) видаляються усі ключі які використовуються для шифрування даних;

3) система Knox більше не працює на даному апаратному забезпечені, запобігаючи надання доступу до захищених даних, додатків всередині захищеного контейнера[2].

Trusted Boot

Trusted Boot – це функція, яка ідентифікує і розпізнає несанкціоновані та застаріли завантажувачі до того, як вони можуть скомпрометувати пристрій[1]. Якщо відбувається завантаження неавторизованих компонентів, підприємство може довіряти лише тому, що тільки перевірені та поточні компоненти можуть бути завантажені після перевірки авторизованості
завантажувачів.

Підприємства можуть перевіряти цілісність пристрою на вимогу за допомогою Knox Attestation, яка зчитує зібрані дані вимірювань Trusted Boot, а також налаштування SE для Android, щоб сформувати основу для вердикту стану пристрою.

Стан завантажувача записується в безпечну пам'ять TrustZone під час завантаження пристрою. Під час виконання програми, що працюють в захищеній TrustZone, можуть використовувати ці значення для прийняття рішень, критичних для безпеки, наприклад:

1) використовування криптографічних ключів з Knox Keystore;
2) увімкнення контейнеру додатків Knox Workspace.

Якщо виявлено несанкціоновані або застарілі версії компонентів системи, встановлюється запобіжник. Після установки запобіжника конфіденційні робочі програми та дані в робочому просторі Knox постійно шифруються і стають недоступними, оскільки цілісність пристрою більше не гарантується і не перевіряється. Власник пристрою все ще може завантажити пристрій і запустити особисті додатки. Така гнучкість забезпечує хороший баланс між споживчими функціями, такими як виклики зі смартфона і особисті додатки, і вимогою захисту корпоративних даних.

До прийняття Trusted Boot для роботи з Secure Boot, пристрої Samsung використовували Secure Boot для запобігання завантаження неавторизованих завантажувачів і операційних систем під час запуску. Безпечне завантаження здійснюється кожним завантажувачем, перевіряючим підпис наступного

завантажувача в послідовності, використовуючи ланцюжок сертифікатів з апаратним коренем. Якщо перевірка не вдалася на будь-якому етапі, процес завантаження завершується.

Захист ядра в реальному часі

Захист ядра є основою безпеки пристрою і захисту корпоративних даних. Коли зловмисники виявляють уразливості в програмному забезпеченні, вони часто нарощують привілеї і ставлять під загрозу ядро ОС.

Скомпрометоване ядро може сприяти витоку конфіденційних даних і навіть дозволити віддалений моніторинг і управління вразливим пристроєм. Інші більш поширені засоби захисту, такі як Trusted Boot або сховища ключів з апаратною підтримкою, не мають великого значення, якщо саме ядро контролюється під час виконання. Після того, як пристрій завантажиться і розшифрує конфіденційний контент, компрометація ядра може привести до витоку даних, які безпосередньо впливають на цілісність даних підприємства.

В рамках пропозицій щодо забезпечення безпеки платформи Knox RKP використовує монітор безпеки в ізольованому середовищі виконання. Залежно від моделі пристрою, виділений гипервизор або захищений апаратний світ, який забезпечувався б технологією ARM TrustZone, забезпечують ізольоване середовище виконання. Схематичне зображення системи наведено на рисунку 3.1 [1].

Механізм захисту ядра не може існувати повністю тільки в ядрі, оскільки зловмисник може обійти його, якщо в самому ядрі є вада. Ядро є найнижчим рівнем детального контролю над ОС і, як таке, зазвичай не може ефективно контролюватися з будь-якого нижчого рівня в системі.

RKP унікально використовує монітор безпеки в ізольованому середовищі виконання. Запуск в ізольованому середовищі виконання зазвичай ставить під загрозу здатність механізму безпеки переглядати ядро і відстежувати дії під час виконання. Проте, RKP процвітає завдяки використанню запатентованих методів для управління пам'яттю пристрою, а також перехоплює і перевіряє

критичні дії ядра, перш ніж дозволити їх виконання. Таким чином, RKP може запобігти скомпрометований ядро від обходу інших засобів захисту. Це запобігання значно зменшує серйозність атак на ядро і обмежує ефективність експлойтів, які зазвичай наносять шкоду мобільного пристрою.

Оскільки RKP завжди активний і не вимагає контролю управління, захист ядра можлива тільки в тому випадку, якщо вона відповідає суворим вимогам зручності використання і продуктивності. Захист RKP активується «з коробки», не впливаючи на продуктивність клієнтів [15].

PKM періодично контролює ядро, щоб визначити, чи були законні код і дані ядра змінені зловмисно. PKM також контролює ключ SE для структур даних Android в пам'яті ядра ОС, щоб запобігти пошкодженню шкідливих атак і потенційне відключення SE для Android. PKM захищає код ядра Linux і сторінки даних від шкідливих атак і допомагає запобігти атакам, що намагаються відключити SE для Android.

Під час збору прошивки пристрою хеш SHA1 кожного коду ядра і сторінка даних тільки для читання обчислюється і збирається в файл вимірювань. Ці вимірювання підписані Samsung для забезпечення цілісності та достовірності даних до їх включення в прошивку. Коли TIMA ініціалізується, PKM отримує вимірювання сторінки ядра і перевіряє підпис, щоб довести цілісність і автентичність відбитку, перш ніж зберігати вимірювання в безпечному середовищі[2]. Під час роботи пристрою TIMA періодично перераховує вимірювання працюючого ядра і порівнює їх з підписаними вимірами, що зберігаються на пристрої. При виявленні будь-якої невідповідності порушення реєструється як в системних журналах, так і для користувача.

Коли PKM працює, він зчитує адреси фізичної пам'яті, які використовуються SE для Android, щоб визначити:

1) SE для Android включений;
2) SE для Android знаходиться в примусовому режимі.

Якщо від шкідливого коду вдається відключити SE для Android або переключити його в дозволяє режим, РКМ виявляє зміна стану і повідомляє про порушення, щоб швидко допомогти адміністратору в діагностиці проблем.

Атестація працездатності пристрою

Мобільний пристрій може бути зламано, якщо неавторизовані агенти отримають права доступу суперкористувача до потужних системних файлів, які керують роботою пристрою і доступом до даних. Ця втрата контролю можлива, якщо користувач пристрою створює свої пристрої для отримання повного контролю над мікропрограмою, файлами, призначеним для користувача інтерфейсом і програмами у пристрої. На жаль, шкідливі програми можуть використовувати цю вразливість для крадіжки паролів, злому посвідчень, доступу до секретної інформації, установки додатків і зміни прошивки.

Підприємства з програмами «Принеси свій власний пристрій» особливо схильні до ризику, так як співробітники можуть потенційно використовувати пристрої Android на робочому місці. Ризики варіюються від невиявленого розкриття конфіденційних корпоративних активів до більш масштабних і більш підступних атак на інші корпоративні ресурси та інфраструктуру. Суб'єкт господарювання повинен мати надійний спосіб виявлення, якщо пристрій скомпрометовано, перш ніж дозволити користувачам пристрою розгорнути його на робочому місці.

Шкідливе ПО може потенційно перехоплювати і підробляти результати перевірки працездатності пристрою, що робить зламані пристрій безпечним. Платформа Knox використовує надійну апаратну середу для надійного виявлення і повідомлення про скомпрометовані пристрої. Оскільки кореневий ключ пристрою (DRK) унікальний для кожного пристрою, він може пов'язувати дані з пристроєм за допомогою криптографічних підписів. Ключ атестації Samsung (SAK) підписує дані атестації, щоб довести, що вони отримані з безпечного світу TrustZone на пристрої Samsung Knox.

Атестація Knox працює в тандемі з Trusted Boot і періодичними вимірами ядра, щоб забезпечити цілісність пристроїв під час розгортання, завантаження і експлуатації.

Як працює Knox Атестація:

1) перевірка пристрою ініціюється або IT-адміністратором підприємства, що використовує консоль EMM або веб-скриптом, який виконує регулярну перевірку;

2) веб-сервер, який ініціював перевірку, запитує одноразовий номер від сервера атестації Samsung. Одноразовий номер - це просто довільне число, яке використовується в криптографічного зв'язку для унікальної ідентифікації кожного результату атестації.

3) веб-сервер дає команду пристрою почати перевірку, передаючи одноразовий номер в якості ідентифікатора перевірки.

4) агент Knox Attestation на пристрої працює в розділі Secure World в ARM TrustZone, створюючи великий двійковий об'єкт, то є великий двійковий об'єкт. Цей BLOB-об'єкт являє собою знімок поточного стану пристрою. Він містить дані про те, чи було пристрій коли-небудь рутовано, або якщо пристрій має завантажувач або файл прошивки, який не був встановлений на заводі або був частиною офіційного оновлення.

5) сервер атестації Samsung перевіряє підпис даних на BLOB-об'єкт, щоб переконатися, що вони отримані з надійного джерела Samsung, аналізує дані BLOB-об'єктів і видає вердикт, який вказує, зламано чи пристрій.

6) Повідомити вердикт користувачеві пристрою;

7) Негайно заборонити пристрою доступ до корпоративних систем;

8)Видалити всі корпоративні додатки або ресурси, вже наявні на Пристрою [1].

2.5 Висновок до розділу 2

Отже, розглянуті варіанти захисту інформаціїна смартфонах з платформою Android, можназробити висновок — дана операційна системамає як власні, внутрішні засоби захисту, так самоможе й підтримувати додаткові засоби захисту,розробленими іншими розробниками.Вбудовані внутрішні засоби захисту є доситьзручним інструментам захисту даних на мобільних телефонах.

Враховуючи тип блокування,виділяють різні види безпеки. Вони досить ефективні, але від зовнішніх атак, тобто якщо хтосьпрагне зайти на мобільний телефон та подивитись якісь певні дані, то зловмисник зустрічаєперешкоду, у вигляді: паролю, малюнка, розпізнавання обличчя чи PIN. Але від внутрішніхатак, вірусів дані засоби безпорадні. Водночас,як додаткове програмне забезпечення, може забезпечити, як безпеку від внутрішніх, так і відзовнішніх атак. сканування відбитків пальців.

РОЗДІЛ 3. СИСТЕМИ ЗАХИСТУ

3.1 Захист конфіденційних даних

Захист даних в стані спокою (DAR) на мобільних пристроях є серйозною проблемою. Незважаючи на те, що галузевим стандартом є шифрування всіх даних на пристрої, ці дані розшифровуються і стають доступними після успішного завантаження пристрою. Цей процес доступу означає, що, як тільки пристрій втрачено або вкрадено, витончена атака може витягувати дані, поки пристрій все ще працює, навіть якщо пристрій заблоковано. Компанія Samsung розробила технологію захисту конфіденційних даних (SDP) для вирішення цієї конкретної проблеми(рис.3.2) [1].

SDP відповідає вимогам профілю захисту основних мобільних пристроїв (MDFPP), визначених Національним партнерством із забезпечення інформаційної безпеки (NIAP) для DAR, що означає, що SDP схвалений для використання урядом США і збройними силами.

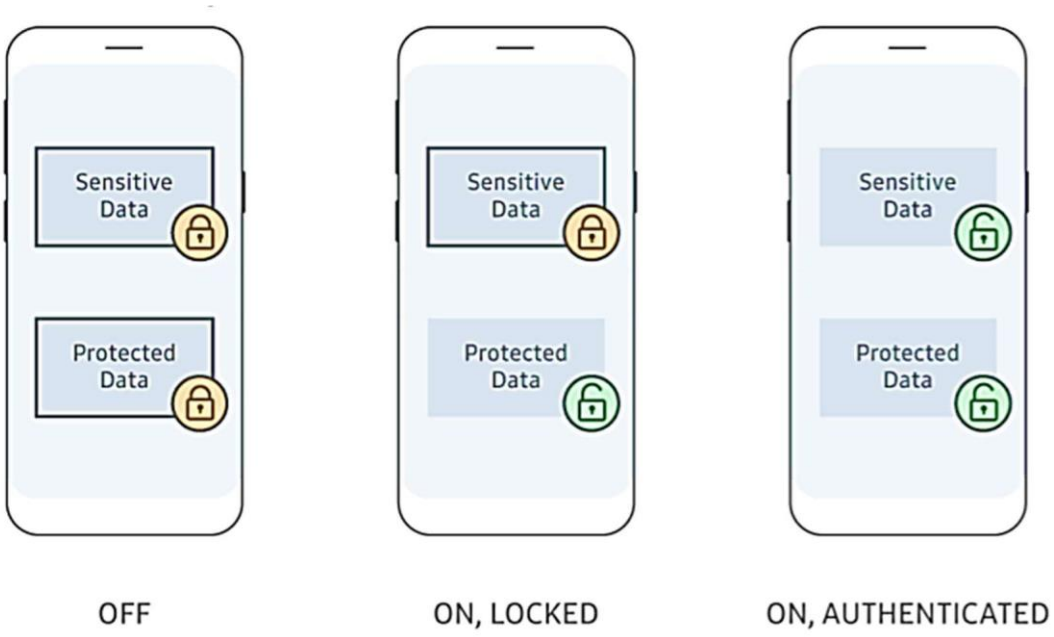

Рисунок 3.1 — Два рівня захисту конфіденційних даних

KPE захищає призначені для користувача дані на пристрої за допомогою шифрування Data-at-Rest. Дані залишаються зашифрованими на диску, і можуть бути розшифровані тільки при включенні пристрою. Відновлення ключів розшифровки даних пов'язано з:

1) апаратним забезпеченням пристрою, тобто дані можуть бути відновлені тільки на одному пристрої;
2) вимірювання цілісності пристрою під час завантаження;
3) облікові дані користувача залежать від конфігурації

Крім того, передбачений механізм для необов'язковою маркування даних як конфіденційних, які згодом не можуть бути розшифровані, поки пристрій знаходиться в заблокованому стані. Ось два режими захисту, які KPE надає для Data-at-Rest:

Захищено: всі файли, що зберігаються на пристрої, за замовчуванням вважаються захищеними. Захищені дані зберігаються в файлової системи пристрою у вигляді зашифрованих даних і дешифруються тільки тоді, коли додаток звертається до даних. Цей механізм забезпечує захист даних в стані спокою, коли пристрій вимкнений. Навіть якщо Ви знаходитесь в стані блокування, додатки можуть отримувати доступ до захищених даних. Конфіденційно: Файли також можуть бути позначені як конфіденційні з використанням механізму захисту конфіденційних даних (SDP). SDP використовує схему управління ключами, яка гарантує, що конфіденційні файли можуть бути розшифровані тільки в розблокованому стані, видаляючи ключі з ОЗУ, коли пристрій заблоковано. Однак SDP також забезпечує можливість запису і шифрування нових файлів в заблокованому стані з використанням криптографії з відкритим ключем.

Пристрої Samsung Galaxy, що підтримують Knox 3.3 і вище, можуть підтримувати шифрування файлів на основі Android (FBE) для Data-at-Rest. Шифрування даних здійснюється на пристрої з використанням:

1) механізм шифрування EXT4 FBE;

2) апаратний криптомодуль FIPS (AES256-XTS)

3) При бажанні зовнішня SD-карта може використовуватися з:

- складена файлова система eCryptfs;
- FIPS-сумісним криптомодулем ядра (AES256-CBC).

Ключі FBE виводяться з використанням введення пароля, який є або жорстко заданим паролем за замовчуванням, або паролем користувача пристрою, використовуваним для розблокування пристрою.

Перебуваючи в розблокованому стані, SDP працює наступним чином:

- шифрує конфіденційні дані, використовуючи ключ шифрування файлу (FEK). Ці ключі шифруються за допомогою SDPK.sym (секретний ключ захисту
- даних, симетричний), який шифрується за допомогою SdpMasterKey. зберігає SdpMasterKey в пам'яті тільки при розблокованому пристрої, щоб дозволити дешифрування SDPK.sym і SDPK.pri (private).
- зашифровує ключ SdpMasterKey, використовуючи ключ, який захищений тимчасовими ключами, отриманими з пароля користувача пристрою, так і ланцюжком ключів до ключу кореневого шифрування (REK) з використанням сховища ключів.
- очищає SdpMasterKey при його переході в їхній заблокований статус і повторно отримує його, коли користувач розблокує пристрій або робочу область.

Перебуваючи в заблокованому стані, SDP обробляє записи додатків конфіденційних даних по-різному:

- відхиляє спроби додатки відкрити файли з конфіденційними даними, оскільки KPE більше не має ключів, необхідних для отримання конфіденційних даних з пам'яті, і не може їх повторно витягувати, поки користувач не розблокує пристрій або робочий простір.

- шифрує будь-які нові конфіденційні дані додатки, використовуючи обидва: пара асиметричних ключів ECDH для конфіденційних даних (SDPK.pri / pub)
- пара ключів ECDH для кожного файлу [DataK.pri / pub], згенерувала від імені додатку захищає приватну частину пари ключів ECDH (SPDK.pri) за допомогою SdpMasterKey, того ж ключа шифрування ключа, який використовується для шифрування секретних даних FEK кожного файлу.
- очищає ключ SdpMasterKey при переході в заблокований статус. Knox Chamber є спеціалізованим каталогом в файлової системі контейнера Нокса. Всі збережені файли в каталозі Knox Chamber автоматично позначаються як конфіденційні і обробляються механізмом SDP [3].

Перевагами Knox SDP є:

1) відповідність MDFPP - Knox SDP сертифікований як відповідний MDFPP. Без Knox SDP базова система Android НЕ сертифікується як задовольняє вимогам MDFPP, що вимагає форми SDP. Відповідність MDFPP є вимогою для багатьох державних установ і компаній, з якими вони працюють. Samsung має більше MDFPP-сертифікованих продуктів, ніж будь-який інший постачальник мобільних рішень.

2) детальний контроль - можливо використовувати Knox SDP для захисту не тільки всього пристрою, контейнера або окремих файлів, а й обраних стовпців бази даних.

3) пароль для кожної програми - можливо додатково налаштувати Knox SDP для дешифрування конфіденційних даних конкретного додатка тільки після того, як користувач додатка введе пароль для конкретного додатка. В цьому випадку аутентифікація розблокування пристрою або контейнера сама по собі не розшифровує дані програми. Пароль додатка також необхідний для більш високого рівня безпеки.

4) захист додатків - Knox SDP включений за замовчуванням для захисту електронної пошти Samsung, а також камери Knox[2].

3.2 Контейнер застосувань

Knox Workspace - це контейнер застосувань, який надає підприємствам рішення для безпечної ізоляції особистих і робочих даних на одному пристрої. Захищена кращої в своєму класі апаратної безпекою, Knox Workspace надає ІТадміністраторам детальні політики управління.

Knox Workspace використовує багато функцій безпеки платформи Knox. наприклад:

1) користувачі пристрої не можуть створювати або використовувати робочу область Knox, якщо пристрій скомпрометовано через неавторизованих загрузчиков або несанкціонованих модифікацій.

2) дані Knox Workspace пристрої захищені від цих типів експлойтів ядра, які можуть поставити під загрозу інші мобільні платформи одним або декількома з наступних способів:

3) шкідливий процес в особистому просторі, який використовує відображення даних ядра.

4) привілеї процесів, запущених в особистому просторі, ростуть, щоб забезпечити доступ до даних в робочій області.

Завдяки ізоляції робочих і особистих даних користувач пристрою має доступ до двох окремих просторів. Для підвищення продуктивності в певних ситуаціях часто потрібно обмін даними з одного простору в інше. Наприклад, при використанні програми телефону в особистому просторі може знадобитися виклик робочого контакту, збереженого в безпечному робочому місці. Завдяки Knox Workspace IT-адміністратор має деталізовані політики управління для управління імпортом і експортом даних в і з Knox Workspace. Ці дані можуть включати додатки, файли, дані буфера обміну, журнали викликів, контакти, події календаря, закладки, повідомлення, ярлики і SMS.

З метою забезпечення відповідальності та підвищення продуктивності ІТадміністратор не може застосовувати ефективні політики на мобільному

пристрої як для особистих, так і для робітників даних. Knox Workspace надає ІТадміністратору можливість конфігурувати і контролювати критичні функції тільки для контейнера. IT-адміністратор може включити або відключити наступне виключно для контейнера: блютуз, NFC, доступ через USB, зовнішнє сховище.

IT-адміністратор підприємства повинен гарантувати, що тільки уповноважені люди мають доступ до робочих даними всередині контейнера. Knox Workspace підтримує розширені механізми аутентифікації для задоволення всіх потреб підприємства.

IT-адміністратор може застосовувати і налаштовувати:

1) складний пароль або графічний пароль;
2) двухфакторну аутентифікацію;
3) перевірка автентичності Active Directory.

Крім того, IT-адміністратор може заблокувати контейнер для обмеження доступу. Це обмеження необхідно, коли пристрій не відповідає вимогам, втрачено або вкрадено[3].

3.3 Мережева безпека Samsung Knox

Стандартний Android поставляється з базовими можливостями VPN, які підходять для більшості споживачів. Але багатьом підприємствам потрібна вища безпеку і більш гнучкі засоби керування VPN для великих розгортання. Інфраструктура Knox VPN включає в себе найбільш просунутий корпоративний набір функцій, який гарантує, що VPN-з'єднання ефективні, надійні, безпечні і відповідають галузевим нормам і рекомендаціям. Платформа VPN Knox Platform дозволяє інтегрувати сторонні VPN-клієнти на додаток до вбудованого VPN-клієнта[2].

Платформа Knox VPN підтримує всі поширені типи VPN, протоколи та параметри конфігурації. При розгортанні VPN-рішень корпоративні ІТадміністратори повинні забезпечити безперебійну роботу VPN-з’єднань, не витрачати ресурси сервера, обмежувати витрати на ліцензування VPN-рішень і застосовувати суворі політики безпеки, що запобігають витік даних.

Платформа Knox надає наступні відмінні риси та переваги VPN:

1) гнучкість у використанні VPN-тунелю для всього пристрою, тільки для Knox Workspace або тільки для однієї програми.

2) унікальна можливість використовувати один VPN-тунель для трафіку як всередині, так і за межами робочого простору Knox, не вимагаючи окремих VPN-клієнтів і ліцензій.

3) перевага економії витрат при використанні VPN-тунелів на вимогу, тільки коли додатки в профілі VPN працюють.

4) зручність обходу VPN-тунелів, коли пристрій знаходиться в локальній корпоративній мережі.

5) строгий охоплення кутових випадків для запобігання витоку даних поза VPN-тунелів навіть під час завантаження пристрою.

6) можливість підключення декількох тунелів одночасно.

7) додаткову безпеку ланцюжка VPN (також відомої як каскадні або вкладені VPN) для більшої анонімності, наприклад, в класифікованих розгортання [1].

Наступні функції Knox VPN також доступні, але залежать від клієнта VPN:

1) QoS або відстеження трафіку і формування. Інфраструктура Knox VPN може інформувати VPN-клієнта, коли будь-які встановлені додатки генерують будь-якої трафік.

2) автоматичне перепідключення VPN-тунелів при відключенні з боку сервера. Роз'єднання на стороні сервера важче виявити і обробити, ніж роз'єднання на стороні пристрою, які зазвичай пов'язані з виявляються умовами,

такими як втрата з'єднання або наявність нових мережевих з'єднань, таких як нове з'єднання Wi-Fi.

3) вбудований клієнт Android VPN (також званий StrongSwan) доступний на всіх пристроях Samsung, а також інтегрований в платформу VPN платформи Knox, забезпечуючи додаткові властивості, доступні на платформі Knox. Вбудований VPN-клієнт, навіть без інфраструктури Knox VPN, відрізняється від того, що пропонує Android, надаючи нижче описаны функції VPN:

1) компоненти криптографії, сертифіковані FIPS 140-2;

2) сертифікація CPA на рівні Foundation, заснована на успішній оцінці Common Criteria щодо профілю захисту для VPN-клієнтів IPsec v1.4;

3) характеристики безпеки IPSec VPN-клієнта версії 2.5, встановлені NCSC.

Застосовуються такі алгоритми обміну ключами в Інтернеті (IKE і IKEv2):

1) IPsec IETF RFCs - IKEv1

2) IKEv1 - основний і агресивний режими обміну IKE з попередніми загальним ключем, сертифікатами, гібридної аутентификацией RSA і EAP-MD5

3) IKEv2 з PSK і аутентифікації на основі сертифікатів

4) KEv2 - попередній загальний ключ, сертифікати, методи аутентифікації EAP-MD5 EAP-MSCHAPv2 і мобільні розширення

5) Triple DES (56/168-бітний), AES (128/256-бітний) з MD5 або SHA

6) IKEv1 Suite B, підтримувана аутентифікації на основі сигнатур PSK і ECDS

7) IKEv2 Suite B, підтримувана сигнатурами ECDSA

3.4 Можливості Samsung Knox для адміністрування пристрою

Через платформу Knox підприємства можуть:

1) заборонити відкат прошивки - ця опція запобігає зловмисну чи випадкову установку дійсних, але застарілих версій прошивки на пристрої підприємства. На пристроях Samsung Knox запобіжник Rollback Prevention кодує мінімально прийнятну версію затвердженого Samsung програмного забезпечення. При певних оновленнях наступний набір запобіжників згорає, щоб вказати, що нове оновлення тепер є мінімальною версією, дозволеної для завантаження. Ви не можете відключити цю базову вбудовану функцію безпеки;

2) відключити автоматичне оновлення прошивки - IT-адміністратори можуть заборонити користувачам переходити в свої настройки Android, щоб включити або відключити автоматичне оновлення прошивки;

3) вимкнути всі оновлення OTA - IT-адміністратори можуть заборонити користувачам переходити до своїх налаштувань Android, щоб включити або відключити оновлення програмного забезпечення в цілому. Це обмеження включає в себе оновлення мікропрограм, виправлень безпеки, виправлень помилок і додатків;

4) вимкнути поновлення, підключені через USB - IT-адміністратори можуть заборонити користувачам завантажуватися в режимі завантаження і встановлювати оновлення програмного забезпечення вручну. Це обмеження включає в себе оновлення за допомогою інструментів оновлення Odin, Kies і Smart Switch[1, 3].

Дистанційне блокування адміністратора пристрою дозволяє IT-адміністратору віддалено блокувати пристрій, наприклад, коли воно не відповідає вимогам. Як тільки пристрій заблоковано, його може розблокувати тільки ITадміністратор, але не користувач пристрою. Ця функціональність вирішує дві проблеми:

1) запобігає несанкціонований доступ користувачів до пристрою, якщо воно втрачено або вкрадено;

2) забороняє користувачам з дійсними обліковими даними використовувати пристрій, наприклад, якщо облікові дані вкрадені або користувачеві більше не дозволено використовувати пристрій.

При стоковому Android, IT-адміністратор може заблокувати пристрій, тільки якщо він зараз розблокован. Якщо пристрій вже заблоковано, адміністратор не може заблокувати його, щоб запобігти майбутнім несанкціонованим входам.

Більшість постачальників не пропонують складних варіантів управління SD-картою. Як правило, підприємства повинні вибрати один з двох варіантів: дозволити повний доступ для читання і запису до SD-карті або повністю заблокувати її [2].

Платформа Knox вирішує цю проблему галузі, надаючи підприємствам незалежний контроль над доступом для читання і запису. Knox може:

1) дозволити доступ на читання, але заблокувати доступ на запис;
2) дозволити доступ для запису, але заблокувати доступ для читання.

Цей рівень контролю означає, що ви можете забезпечити односторонній доступ до конфіденційних даних для ефективного задоволення ваших вимог безпеки.

Щоб пом'якшити атаки, що здійснюються через з'єднання Bluetooth, Knox надає наступні елементи управління:

1) повністю відключіть Bluetooth - вимкніть фонові перевірки Bluetooth і Bluetooth;

2) блокувати певні типи профілів Bluetooth. Обмежте типи пристроїв Bluetooth, які користувач може підключити до пристрою, наприклад:

3) дозволити Bluetooth-навушники

4) блокувати передачу файлів через Bluetooth, що може привести до витоку особистих даних

Knox може обмежувати або дозволяти різні типи USB-пристроїв, зокрема, класи USB-пристроїв, певні через usb.org. Ця функція включає доступ до наступних класів пристроїв USB:

1) аудіо, відео, аудіо / відео;
2) масове зберігання;
3) безпека контенту;
4) інтелектуальна картка;
5) принтер;
6) концентратор, Type-C, бездротовий контролер;
7) пристрій інтерфейсу людини (HID);
8) комунікації, CDC Control, CDC Data

Наприклад, можливо заблокувати всі USB-пристрої, крім зчитувачів смарт-карт.

Організації, яким необхідно усувати серйозні порушення безпеки, використовують журнали аудиту для криміналістичного аналізу дій, що призводять до фактичних і потенційних порушень. У регульованих галузях ці контрольні журнали є обов'язковою вимогою для виконання аудиту безпеки.

Завдяки платформі Knox IT-адміністратор підприємства може використовувати консоль EMM для включення ведення журналу аудиту на всіх корпоративних пристроях. IT-адміністратори можуть час від часу активно витягати журнали аудиту, щоб виявляти і захищати від шкідливих програм або вірусів в самий найближчий час. У разі можливого вторгнення IT-адміністратори можуть аналізувати зареєстровані події на предмет несанкціонованих дій.

Audit Log платформи Knox надає вичерпну інформацію про події пристрою, включаючи:

1) контейнерний діяльність Knox Workspace;
2) політики паролів, встановлені для пристроїв і контейнерів;
3) установка і видалити програму;

4) помилка сертифіката і генерація ключа;

5) створення та видалення облікового запису;

6) спроби обміну файлами через Wi-Fi

Щоб краще керувати сховищем пристроїв, IT-адміністратори можуть контролювати розмір журналу аудиту.

Переваги для підприємства включають в себе:

1) раннє виявлення і захист від шкідливих програм і вірусів;

2) розширення можливостей IT-адміністраторів за допомогою потужних даних для усунення неполадок;

3) дотримання обов'язкових вимог в регульованих галузях;

4) відповідність вимогам профілю захисту мобільних пристроїв (MDFPP) 2.0 для збору подій.

3.5 Сертифікація Samsung Knox

Платформа Knox успішно виконала суворі вимоги безпеки, встановлені урядами і великими підприємствами по всьому світу, надаючи організаціям надійне рішення для мобільної безпеки. Сертифікати, отримані платформою Knox, дозволяють розгортати її мобільні пристрої в таких високочутливих галузях, як військові.

Платформа Knox сертифікована на відповідність вимогам безпеки наступних країн: Україна, США, Великобританія, Нідерланди, Франція, Іспанія, Німеччина, Китай, Південна Корея, РФ, Казахстан та інші[1, 2].

Безпека мережі для пристроїв Apple

Системи iOS та iPadOS оснащено вбудованими технологіями мережевого захисту для авторизації користувачів і захисту їхніх даних під час передавання.

3.6 Система мережевої безпеки iOS та iPadOS

Система мережевої безпеки iOS та iPadOS підтримує:

- вбудовані протоколи Cisco IPsec, IKEv2, L2TP;
- SSL VPN через програми App Store;
- Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) і DTLS;
- SSL/TLS з сертифікатами X.509;
- WPA/WPA2/WPA3 Enterprise з 802.1X;
- автентифікацію на основі сертифікату;
- автентифікацію через спільний секрет і Kerberos.

Шифрування FaceTime та iMessage

Операційні системи iOS, iPadOS і macOS створюють унікальні ідентифікатори для кожного користувача FaceTime і iMessage, які допомагають гарантувати, що вся комунікація буде зашифрована, скерована належним чином і досягне потрібного абонента.

VPN і IPsec

Багато корпоративних середовищ використовують певні типи віртуальних приватних мереж (VPN). Ці сервіси VPN зазвичай потребують мінімум налаштувань і конфігурації для роботи з пристроями Apple, які можуть бути інтегровані в багато типово використовуваних технологій VPN.

iOS, iPadOS і macOS підтримують протоколи й методи автентифікації IPsec. Перегляньте розділ Вступ до VPN на пристроях Apple.

SSL/TLS

Підтримку криптографічного протоколу SSL 3 і симетричного ключа шифрування RC4 припинено в iOS 10 і macOS 10.12. Клієнти або сервери TLS, упроваджені за допомогою API SecureTransport, типово не мають увімкненого ключа шифрування RC4, і не можуть під’єднатися, якщо RC4 — єдиний

доступний ключ шифрування. Для додаткового захисту служби та програми, які вимагають RC4, слід оновити, щоб ввімкнути симетричні ключі шифрування.

Додаткові засоби захисту

TLS 1.2 підтримує і AES 128, і SHA-2.iOS і iPadOS підтримують SSL 3 і Transport Layer Security (TLS 1.2, і TLS 1.3). Safari, Календар, Пошта й інші інтернет-програми використовують ці протоколи для запуску зашифрованих каналів комунікації між iOS, iPadOS, macOS і корпоративними сервісами.

Також можна налаштувати мінімальну й максимальну версію TLS набору даних вашої мережі 802.1X з EAP-TLS, EAP-TTLS, PEAP, і EAP-FAST. Наприклад, можна задати:

Однакову версію TLS для обох.

1) Менше значення для TLSMinimumVersion і більше значення для TLSMaxmimumVersion, що потім буде узгоджено з сервером RADIUS.

2) Жодного значення, що дозволить пристроєві, який подає запит до 802.1X, узгодити версію TLS з сервером RADIUS.

3) iOS, iPadOS і macOS вимагають гілковий сертифікат сервера, підписаний за допомогою сімейства алгоритмів підпису SHA-2, і використовують або ключ RSA (довжиною щонайменше 2048 бітів), або ключ ECC (довжиною щонайменше 256 бітів).

4) В iOS 11, iPadOS 13.1 і macOS 10.13 та новіших додано підтримку TLS 1.2 в автентифікації 802.1X.

Сервери автентифікації, які підтримують TLS 1.2, можуть потребувати оновлення для сумісності:

- Cisco: ISE 2.3.0
- FreeRADIUS: оновлення до версії 2.2.10 і 3.0.16.
- Aruba ClearPass: оновлення до версії 6.6.x.
- ArubaOS: оновлення до версії 6.5.3.4.
- Microsoft: Windows Server 2012 - сервер політики мережі.
- Microsoft: Windows Server 2016 - сервер політики мережі.

WPA2/WPA3

Усі платформи Apple підтримують стандартні для галузі методи автентифікації та протоколи шифрування Wi-Fi. Так забезпечується автентифікований доступ і конфіденційність за під’єднання до таких безпечних бездротових мереж:

- WPA2 Personal
- WPA2 Enterprise
- WPA2/WPA3 Transitional
- WPA3 Personal
- WPA3 Enterprise
- WPA3 Enterprise зі 192-розрядним захистом

Недоліки системи Ios та його вразливості

На новій версії операційній системі є вразливість яка дозволяє з резервної копії системи котру створює користувач взяти файл котрий не є захищеним зі змістом паролю для систем хмарного захисту даних то ми отримаємо доступність до наступних елементів :

- відключити Find my iPhone і блокування Activation Lock;
- включити двухфакторную аутентифікацію, якщо вона не була включена;
- змінити пароль від Apple ID / iCloud; з цим паролем отримати доступ до хмарним резервних копій, синхронізованим даними і паролів з хмарної зв'язки ключів iCloud Keychain, причому з усіх пристроїв, прив'язаних до цього облікового запису;
- скачати фотографії з iCloud Photo Library (згадали Celebgate);
- заблокувати або видалити дані з інших пристроїв, прив'язаних до даного Apple ID;

- скинути пароль на локальну резервну копію, підключити телефон до комп'ютера і витягти всі дані;
- витягти всі паролі з зв'язки ключів або переглянути їх на самому пристрої.

3.7 Висновок до системи мережевої безпеки iOS та iPadOS:

Система IOS має ключі шифрування котрі тяжкі для взлому системи, де система при вірному використанні ключів шифрування та ввімкненій всій системи захисту, користувач має систему що надійно захистить всі його данні. Але вразливість системи котру звичайний користувач може зруйнувати зайшовши до резервної копії що була зроблена на комп’ютері.

Вивід з цього маємо, що система IOS добре захищена але при необхідності її захист можна обійти або зі сторони хакера зможе легко проникнути в середину.

3.8 Система захисту Google Play Protect

Google Play Protect включає набір API, які взаємодіють та обробляють інформацію між додатками на пристроях, за допомогою вбудованих функцій захисту пристроїв та хмарні служби безпеки. У 2017 році Google Play Protect автоматично відключив PHA з приблизно 1 мільйона пристроїв. Google рецензує всі додатки, перш ніж публікувати їх у магазині Google Play. Окрім перегляду програм, поданих у Google Play, його хмарні системи шукають додатки у загальнодоступних джерелах. Google Play Protect також розглядає програми, які знаходить поза Google Play для PHA. За даними Google, Google Play Protect заважав користувачам Android встановлювати PHA за межами

Google Play

Приблизно 1,6 мільярда разів у 2017 році. Google Play Protect охоплює всі засоби безпеки, які роками захищають безпеку пристроїв користувачів Android. Наприклад, служба Verify Apps у Google Play Protect сканує програми для PHA, перш ніж користувачі встановлять їх, незалежно від їх походження.

Verify Apps

Послуга Verify Apps виконує періодичну перевірку на всьому пристрої, яка інспектує додатки перед встановленням та виконує регулярні сканування всіх встановлених програм. Якщо PHA знайдено, сповіщення просить користувача видалити його. У випадках, коли PHA не надає можливих переваг користувачам, Google Play Protect може видалити PHA з уражених пристроїв та заблокувати майбутні встановлення[16].

AutoScan

AutoScan - це ще одна послуга, яка щодня перевіряє пристрої Android на предмет наявності PHA та інших ознак підробки. (Цей сервіс минулого року сканував майже 800 мільйонів пристроїв на день таких, як смартфони, планшети та телевізори з ОС Android.)

AutoScan працює разом з Verify Apps як частина багатошарового підходу сканування Google до програмного забезпечення та безпеки Android. Якщо AutoScan виявить PHA або інші індикатори ризику на пристрої, це може викликати додаткове локальне сканування програм для подальшого вивчення проблеми. Хоча архітектура безпеки пристрою / хмари, що базується на хмарі, забезпечує надійний захист, вона значною мірою працює поза зони видимості для кінцевих користувачів.

Google Play Protect був представлений у травні 2017 року, щоб розкрити цю функціональність та допомогти користувачам зрозуміти «стан здоров'я» своїх пристроїв. Google Play Protect забезпечує активні сповіщення користувачів Android про те, коли відбувається сканування на пристрої, стан безпеки кожного додатка, який переглядають або завантажують із магазину Google Play, та загальний стан додатків на пристрою.

Швидке поширення оновлень програмного забезпечення є проблемою в такій різноманітній екосистемі, як Android. Google розповсюджує критичні оновлення безпеки через GMS, коли ця служба працює незалежно від оператора або версії програмного забезпечення Android. Це може облегшити відправлення нового програмного забезпечення, як тільки виявляться нові загрози[16].

Project Treble

Крім критичних оновлень, часті оновлення ОС також забезпечують безпеку та продуктивність користувачів. З цією метою Google запустив Project Treble у 2017 році, щоб зробити його основні служби ОС більш модульними та однорідними, що дозволяє легше впроваджувати оновлення програмного забезпечення для операторів та виробників пристроїв. Treble змінює фреймворк для взаємодії компонентів операційної системи Android та компонентів постачальника пристроїв (чіпи від Qualcomm, MediaTek тощо).

Це вирішує проблему швидких оновлень шляхом впорядкування процесу, коли виробники девайсів працюють з виробниками чіпів для перевірки нових оновлень ОС Android. Treble створює стандарт інтерфейсу постачальника для компонентів нижчого рівня для взаємодії з ОС.

Виробники пристроїв та виробники чіпів більше не повинні переробляти низькорівневий код при кожному випуску, прискорюючи час оновлення. Це посилює безпеку, оскільки знімається потреба у пряму доступу до драйверів ядра, які керують відтворенням медіа, що забезпечує більш надійну «пісочницю» та ускладнює скомпроментуваня фреймворку для використання ядра. (Однак підприємства можуть також навмисно затримувати оновлення ОС на пристроях, які рекомендовано програмою Android Enterprise, щоб дозволити IT-командам тестувати та оновлювати додатки для роботи на останній версії Android.).

В телефонах на базі Android компанії Google Pixel є своя апаратна система захисту котра реалізована чіпом вбудований в плату телефона.

Titan M - це модуль безпеки «другого покоління» з низьким енергоспоживанням, розроблений і виготовлений Google. Він є частиною сімейства Titan. Даний процесор відповідає за кілька функцій. Зокрема, він зберігає дані лічильника відкату Android Verified Boot, забезпечує підтримку модуля Android Strongbox Keymaster, перешкоджає спробам розблокувати завантажувач і встановити більш старі версії ПЗ. Крім того, процесор має пряму електричну зв'язок з бічними клавішами смартфона, так що при спробах злому вони будуть заблоковані.

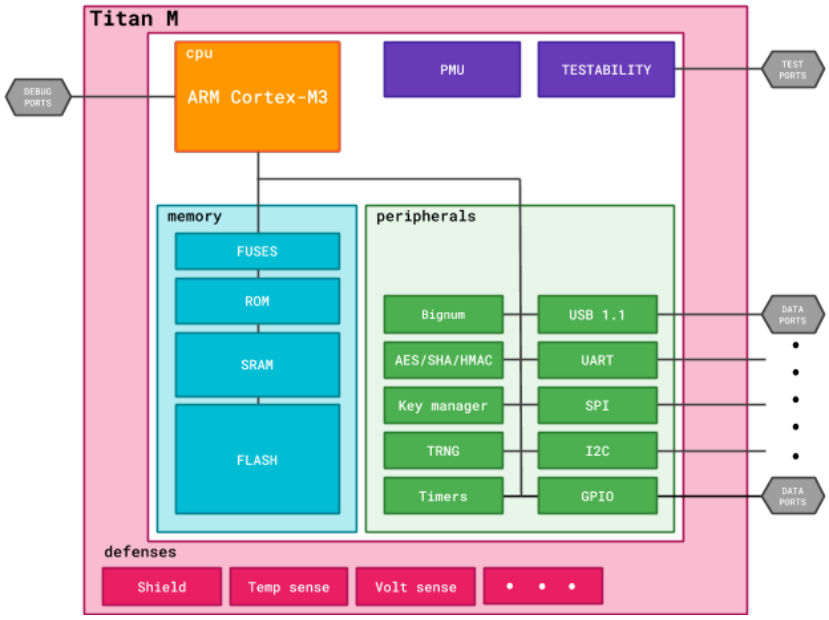

Рисунок 3.2 – конструкція процесору Titan M

В основі Titan M лежить процесорний ядро Cortex-M3. Крім того, є апаратне прискорення AES і SHA, а також програмований співпроцесор. Надалі Google має намір розширити можливості Titan M. Зокрема, компанія говорить про можливість використання процесора в системах двофакторної аутентифікації, управління медичними пристроями, в системах платежів P2P і так далі.

3.9 Висновок до захисту Google

Система захисту Google більше розрахована на хмарне середовище та сервіси котрі можуть контролювати систему телефона та сканують на можливість проникнення в систему, або атаки на неї. Знов ж таки вона має конкретні недоліки та легкі для користувача можливості обходу системи захисту на телефонах на базі Android котрі не є саме телефонами компанії Google.

Такими недоліками є:

- Отримання рут-доступу і використання експлойтів.
- Уразливість в конкретному додатку може привести до витоку даних
- Атака на довірену апаратне і програмне забезпечення може бути корисна в ланцюжку експлойтів.
- У деяких випадках Google Smart Lock дозволяє обійти блокування екрану без аутентифікації користувача.

3.10 Проведення тестування

3.11

Інженери Samsung в Knox реалізують системи захисту даних, які випереджають загрози, що виникають в реальному світі. Наприклад, починаючи з Galaxy Note20 і Galaxy S20 в смартфонах з'явилася захист від зовнішніх фізичних впливів. Окремий процесор, який використовується для зберігання біометрії, ваших даних, шифрування пам'яті, відтепер навчився розпізнавати не тільки зміна компонентів пристрою, що було нормою і до того. Цей процесор навчили визначати електромагнітний вплив, коливання температури, використання лазера - все ті методи, якими зловмисники можуть спробувати зчитати інформацію з пристрою.

У звичайному житті такий вплив на пристрій повністю виключено, це атаки, що проводяться в лабораторіях, і атакуючі мають високий рівень як знань, так і використовуваних технологій. Можна говорити, що найчастіше це та чи інша держава, оскільки обмежене число «приватників» може похвалитися доступом до подібних технологій злому.

Зазвичай атаки будуються на тому, що зловмисники зламують ядро Android, а вже потім модифікують код системи, отримують доступ до даних. У Knox система перевіряє всі компоненти, в реальному часі здійснюється захист ядра, виглядає це ось так.

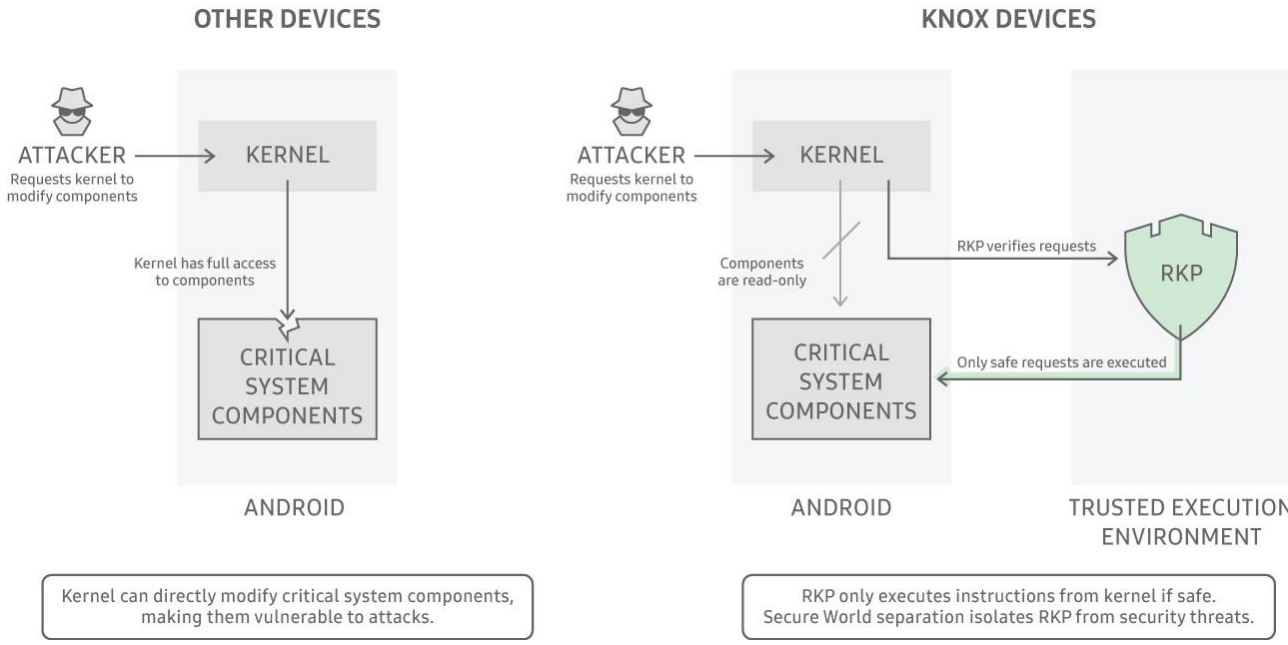

Рисунок 3.3 – система захисту в телефонах Samsung

Тобто перед тим, як дозволити вносити зміни в ядро системи, в Knox перевіряється, наскільки такий запит відповідає політиці безпеки. Але найголовніше, що при кожній спробі атакувати пристрою адміністратор отримує попередження і може бачити виникаючі загрози. Спроба злому завжди залишає сліди і не проходить непоміченою, що дозволяє почати пошуки нападників.

Починаючи з версії Android 4.3, Samsung почав встановлювати на всі свої пристрої програму KNOX, яка призначається для захисту і збереження особистих даних користувачів android пристроїв Samsung. З одного боку - це дуже важливо, але з іншого - приносить масу незручностей користувачам, особливо які мають на свій Samsung root права. Якщо ви один з них, тоді напевно вам доводилося бачити таке повідомлення: «Додаток SuperSU спробувало отримати доступ до елементу система на вашому пристрої без дозволу. Ця

спроба заблокована. Для підвищення безпеки можна видалити додатки, завантажені з неавторизованих джерел»

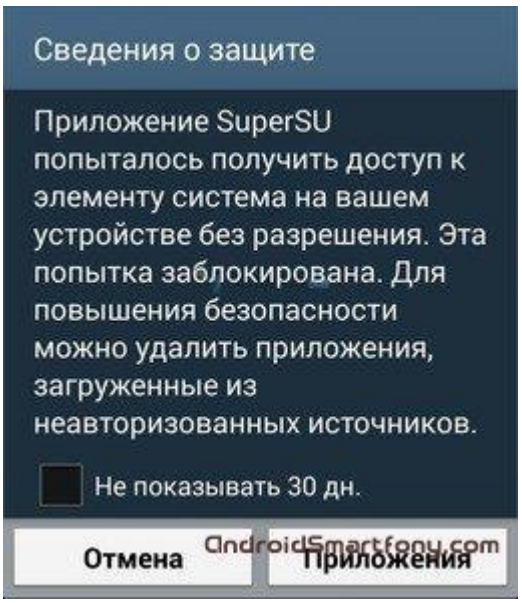

Рисунок 3.4 – попередження системи про блокування прав

Це означає, що Samsung KNOX блокує root права, і відповідно ви не можете їх повноцінно використовувати. Вихід один: відключити або видалити KNOX зі свого апарату. Зробити це можна кількома способами, описаними нижче.

Для проведення злому системи першочергово видаляємо системні додатки

Рисунок 3.4 – видалення системних додатків захисту

Далі через програму Odin проводимо встановлювання зламаної прошивки з root правами суперкористувача

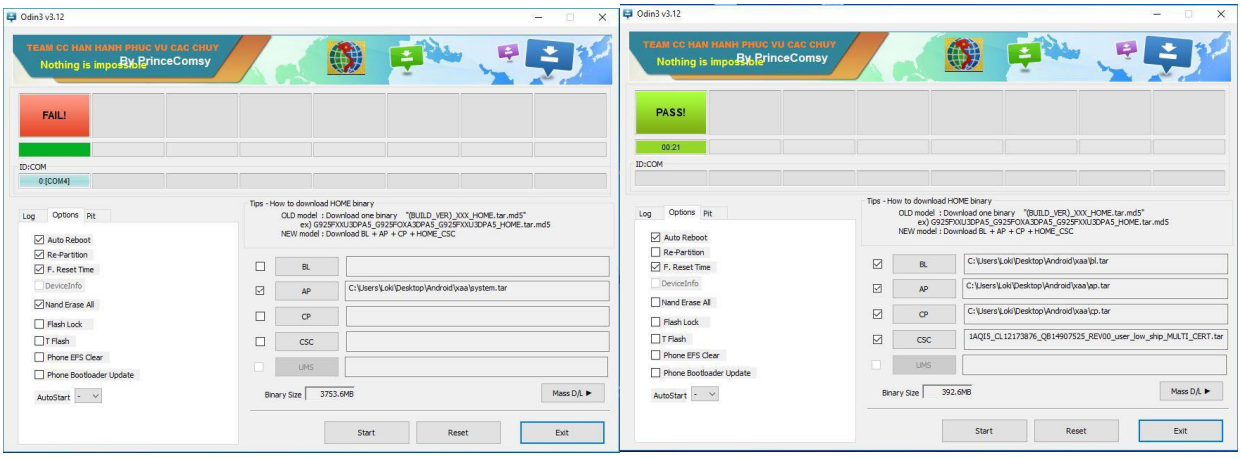

Рисунок 3.5 – злам системи програмою Odin

В якості підтвердження отримання прав та злому системи сама система підтверджує це спливаюче повідомлення

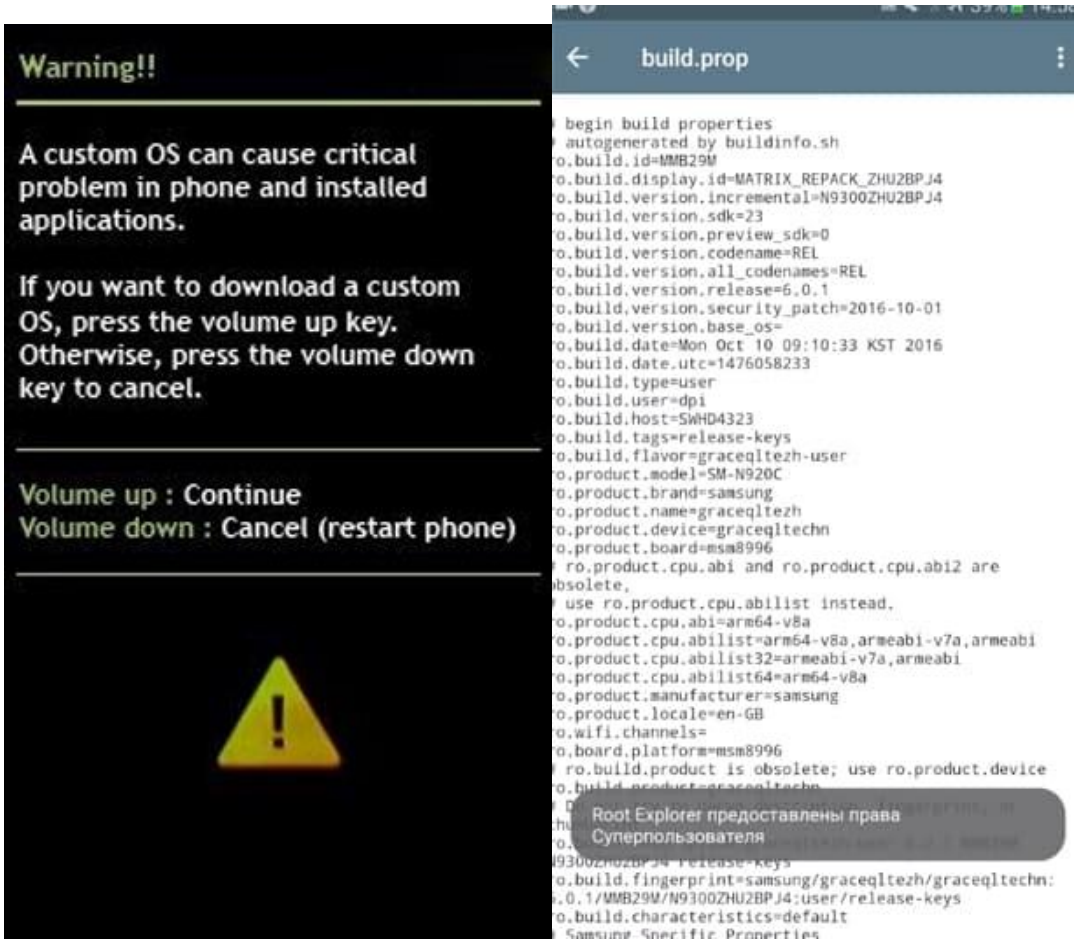

Рисунок 3.6 – підтвердження системи про отримання прав супер користувача.

3.11 Вдосконалення захисту

Вдосконалення системи відбувається завдяки мобільному антивірусу, процеси що перешкоджають зламу системи:

- Перевірка безпеки пристрою
- Сканування ОС телефону
- Встановлення захисту в інтернеті
- Резервне копіювання системи за потрібності її відновлення

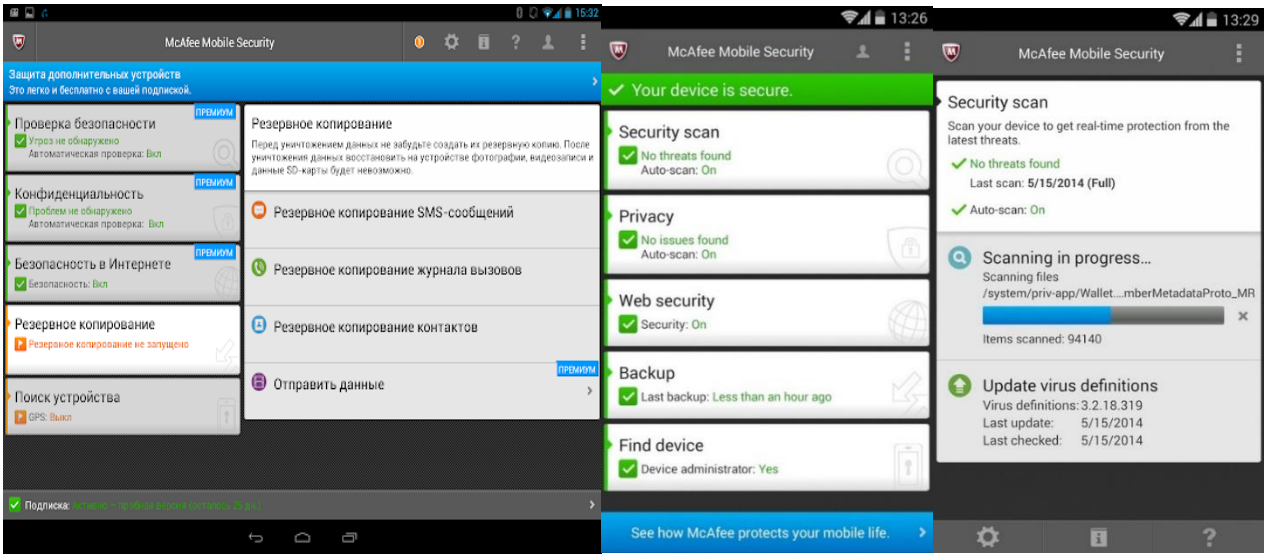

Рисунок 3.7 – захист системи завдяки антивірусу в мобільному додатку

3.12 Висновок до розділу 3

Система захисту в мобільних пристроях на сьогоднішній день становить важливу роль у забезпеченні захисту конфіденційної інформації. Провівши тестування та змоделювавши злам системи можемо побачити вразливість такої системи. Слабкі місця її знаходяться у дозволах для користувача котрий може навіть без додаткових програм видалити системні додатки що відповідають за забезпечення та проведення захисту.

Сама система маючи такі недоліки все одно вважається однією х найбільш безпечних систем на пристроях з операційною системою Android. Проведене вдосконалення системи Samsung Knox було вдосконаленою за рахунок мобільного антивірусу котрий вразливість зі сторони додатків що встановлюються на мобільний пристрій з передвстановлених маркетів програм. Так як сам антивірус перевіряє всі програми що були завантажені на пристрій, він має виявити в додатку модулі зламу або вторгнення в систему.

ВИСНОВКИ

Збільшення ринку мобільних пристроїв сприяє їх більш масовому використанню в корпоративному сегменті для оптимізації робочого процесу та економії коштів.

Використання EMM систем дозволяє отримати гарантії захищеності корпоративної інформації, що в умовах дуже великої поширеності персональних гаджетів, є важливим аспектом успішного бізнесу. Окрім захищеності, ці системи дозволяють автоматизувати деякі потреби бізнес процесів, наприклад автоматизоване налаштування пристроїв під конкретного співробітника, ще до того, як пристрій достануть перший раз з коробки.

Платформа Knox забезпечує IT-адміністраторам, адміністраторам безпеки можливість безпечного масового розгортання обладнання для мобільних пристроїв і швидкої інтеграції з існуючою бізнес-інфраструктурою і застосунками. Вона виконує багато перевірок для запобігання доступу до конфіденційних даних навіть за наявності компрометації системи. Надійність системи підтверджується наявністю сертифікатів відповідності в більш ніж 10 країнах світу.

До недоліків цього продукту можна віднести можливість використання цієї системи тільки на пристроях однієї компанії, закритість ісходного коду та неможливість відновлення працездатності системи після атак. Ще одним недоліком можна вважати доступ до деяких можливостей лише на платній основі.

Недоліками систем EMM в цілому є складність управління великою кількістю різноманітних пристроїв під керуванням різних операційних систем, відсутність стандартизованості між виробниками та розробниками EMM систем.

Однак, не зважаючи на всі ці недоліки, деякі компанії розробляють свої сервіси для своїх продуктів, і якщо при впроваджені політики BYOD буде використовуватись конкретний програмний продукт, розроблений спеціально для використання з певними пристроями, багато недоліків пов’язаних з фрагментованістю пристроїв будуть виключені.

В ході написання роботи було проведено аналіз систем захисту та методів забезпечення збереження конфіденційності даних. Було з модульовано злам системи таким чином було виявлено вразливості системи. На основі проведеного зламу системи було запропоновано вдосконалення завдяки мобільному антивірусу, що забезпечує сканування додатків на мобільному пристрої на наявність модулів злому та проникнення в систему.

.

ПЕРЕЛІК ПОСИЛАНЬ

1. Нечволод К.В. Аналіз безпеки даних в ЕММ системах / К.В. Нечволод, О.В. Сєвєрінов, А.В. Власов // Системи управління, навігації та зв'язку. – Полтава: ПНТУ. - 2019. – Вип. 3(55). – С. 131-134

2. Knox S. White paper: An overview of samsung knox //https://www.samsung. com/global/business/businessimages/resource/whitepaper/2019/06/Samsung KNOX whitepaper June-0. pdf. – 2019.

3. Kanonov U., Wool A. Secure containers in Android: the Samsung KNOX case study //Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices. – ACM, 2016. – С. 3-12.

4. Ning P. Samsung knox and enterprise mobile security //Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices. – ACM, 2014. – С. 1-1.

5. Madden J., Madden B. Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD. – Jack Madden, 2013. 176

6. Kravets A. G., Bui N. D., Al-Ashval M. Mobile security solution for enterprise network //Joint Conference on Knowledge-Based Software Engineering. – Springer, Cham, 2014. – С. 371-382.

7. Peraković D., Husnjak S., Cvitić I. Comparative analysis of enterprise mobility management systems in BYOD environment //The 2nd Reseach Conference In Technical Disciplines, RCITD. – 2014. – С. 82-85.

8. Redman P., Girard J., Wallin L. O. Magic quadrant for mobile device management software //Gartner G00211101, April. – 2011.

9. Ortbach K., Brockmann T., Stieglitz S. Drivers for the adoption of mobile device management in organizations. – 2014.

10. Android developer[Електроний ресурс]:[Веб-сайт]-Режим доступу: https://developer.android.com/about/dashboards Distribution dashboard

11. Android Enterprise Solutions Directory[Електроний ресурс]:[Веб-сайт]-Режим доступу: https://androidenterprisepartners.withgoogle.com/emm/ EMMs

12. VMWare AirWatch[Електроний ресурс]:[Веб-сайт]-Режим доступу: https://www.air-watch.com/

13. MobileIron[Електроний ресурс]:[Веб-сайт]-Режим доступу:https://www.mobileiron.com/

14. IBM MaaS360 with Watson[Електроний ресурс]:[Веб-сайт]-Режим доступу: https://www.ibm.com/security/mobile/maas360

15. Нечволод К.В. Аналіз безпеки даних на основі платформи Samsung Knox / К.В. Нечволод, О.В. Сєвєрінов // Комп'ютерні та інформаційні системи і технології. Третя міжнародна науково-технічна конференція. Збірник наукових праць. Х: ХНУРЕ, 2019.– С. 80-81.

16. Нечволод К.В. Аналіз захищеності системи Android для використання в корпоративному сегменті / К.В. Нечволод, О.В. Сєвєрінов // Комп'ютерні та інформаційні системи і технології. Global Cyber Security Forum. Збірник наукових праць. Х: ХНУРЕ, 2019.– С. 78-79.