УДК 004.056

О. П. Войтович
Б. Д. Панченко

КІБЕРАУДИТ В ОС ANDROID

Вінницький національний технічний університет

Анотація

Розглянуто проблеми, що призвели до необхідності використання засобу аудиту в операційній системі Android, основні показники, що відслідковуються при моніторингу пристрою та виконуваних додатків, та розглянуто реалізації схожих засобів.

Ключові слова: кібераудит, *Android, моніторинг додатків, моніторинг системи.*

Abstract

The problems that led to the need to use Android auditing application, the main characteristici that are used for device monitoring, and examples of modern implementations are considered.

Keywords: cyber auditing, *Android, monitoring device, monitoring applications.*

Вступ

З кожним днем в житті людей все більшу роль відіграють смартфони та інші портативні засоби. Найбільш поширеною на сьогоднішній день операційною системою для мобільних пристроїв є Android, що на даний момент становить близько 73% від всіх мобільних операційних систем [1]. Набувши такого широкого поширення нею користуються всі прошарки населення, включаючи дітей, робочих державних служб, та простих громадян, в зв'язку з чим збільшується кількість кібератак, через це доцільно розробити систему для моніторингу роботи пристрою та його додатків, оскільки вбудованими системними засобами можна отримати лише обмежену кількість інформації.

Метою роботи є удосконалення існуючих засобів для моніторингу стану системи та додатків операційної системи Android, що також дозволить вчасно виявляти кібератаки.

Результати дослідження

Важливим фактором, що ускладнює захист забезпечення належного рівня захисту в ОС Android є її відкритість і надзвичайна фрагментованість [2]. На ринку присутні сотні різноманітних моделей пристроїв, кожна з яких має свої програмні особливості, якими наділили їх виробники. Через різницю політики Google і компанії виробника часто страждають вже користувачі пристроїв.

Небезпечні додатки можуть попасти до пристрою самими різними способами, і для того, щоб уникнути зараження ШПЗ необхідно дотримуватись рекомендацій з безпеки [3].

Оскільки мобільні пристрої, в силу своєї поширеності, застосовуються в різних сферах діяльності, то запропоновано дві реалізації засобу, в залежності від потреб користувача, а саме: реалізацію для особистого користування, та для підприємств.

Перша реалізація засобу направлена на аудит власного пристрою, та має дві версії: версію для пристрою з рут-правами, та версію для пристрою без таких прав.

Версія з рут-правами має більші можливості моніторингу та направлена на максимально можливий збір даних з пристрою, оскільки дана версія має доступ до функцій, що відсутні на пристрої без рут-прав. Звичайна версія міститиме базовий набір можливостей моніторингу, доступний для відповідної версії операційної системи користувача. Обидві реалізації містять опцію вибору даних, що зберігатимуться на веб-ресурс, щоб користувач міг відкинути непотрібні йому дані.

Наступна реалізація засобу призначена для підприємств, що слідують концепції COPE (Corporate-Owned, Personally-Enabled) [4]. Концепція полягає в тому, що працівники використовують не власні, а видані організацією пристрої. Перевагами цієї концепції над іншими є те, що на відміну від BYOD (Bring Your Own Device), де працівники користуються

власними пристроями, організація зберігає доступ до робочих даних працівника навіть після того, як він покине роботу, а також організації можуть обмежити можливість встановлення програм та передвстановити власні. За статистикою, близько 17% підприємств забезпечує всіх працівників смартфонами, і близько 31% повністю покладаються на пристрої працівників, інші використовують гібридні підходи [4]. Основною перевагою BYOD вважається те, що вона зберігає гроші підприємства, але на практиці це виливається в заощадження на рівні близько 11% порівняно з COPE [4]. Реалізація засобу для корпорацій передбачає передвстановлення на робочі пристрої спеціальної версії програми, використання якої потребує рут-прав. За допомогою неї можна слідкувати за необхідними для працедавця критеріями, такими як, наприклад, активність користування програмами, що не входять до списку робочих, активність користування пристроєм в цілому чи окремими його компонентами. Залежно від того, чи надав працівник дозвіл на обробку персональних даних, відповідальній особі надається можливість слідкувати за поглибленою статистикою використання пристрою, або ж, якщо такого дозволу не було отримано, то відповідальна особа отримує сповіщення про надмірне використання або невикористання показників, що цікавлять роботодавця, таких як, наприклад, надмірне використання неслужбових програм. Працівнику, згідно закону про захист персональних даних, також надається доступ до особистого кабінету на веб-ресурсі, де він має змогу відслідковувати свою статистику власноруч.

Основними параметрами, що може відслідковувати засіб є: час використання додатків, витрати ресурсів додатків, список додатків з небезпечними дозволами, навантаження пристрою в конкретні моменти часу (на CPU, GPU, RAM), температурні показники пристрою в конкретні моменти часу, список останніх дзвінків пристрою (час дзвінка, дата дзвінка, тип дзвінка), список СМС повідомлень, список встановлених додатків.

Розроблюваний засіб також міститиме систему підтримки прийняття рішень (СППР). Існують різні види СППР, наприклад такі, що використовують нейронні мережі, ситуаційний аналіз, когнітивне моделювання та інші [5]. Розроблюваний засіб міститиме СППР, що сповіщатиме користувача чи роботодавця про інциденти на основі заданого порогового значення і також виявлятиме небезпечні СМС повідомлення на основі аналізу тексту.

Висновок

Отже, за допомогою засобу кібераудиту в операційній системі Android, в залежності від мети використання, вирішується ряд задач, таких, як виявлення надмірного використання ресурсів програмами, використання небезпечних дозволів, своєчасне виявлення атак та постійне відслідковування діяльності з метою ефективного виявленння небезпечних додатків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mobile Operating System Market Share Worldwide [Електронний ресурс]. –Режим доступу: URL: https://gs.statcounter.com/os-market-share/mobile/worldwide – Назва з екрану.

2. Войтович О. П., Гурський М. В. Система моніторингу та аудиту безпеки в ОС Android : дис. – ВНТУ, 2017.

3. Войтович О. П. и др. Засіб моніторингу для операційної системи Android //Вісник Хмельницького національного університету. Технічні науки. – 2017. – №. 3. – С. 236-241.

4. BYOD, CYOD, COPE, COBO – What do they really mean? [Електронний ресурс]. – Режим доступу: URL https://www.wired.com/brandlab/2018/06/byod-cyod-cope-cobo-really-mean/

5. Барановская Т.П., Канатов А.А., Иванова Е. А. Разработка системы принятия решений для оценки устойчивости предприятия // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета

Панченко Богдан Дмитрович — студент групи 1БС-16б, факультет інформаційних технологій, Вінницький національний технічний університет, Вінниця, e-mail : r7m260@gmail.com

Войтович Олеся Петрівна — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет

Bohdan Panchenko — student, Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: r7m260@gmail.com

Olesia Voitovych — PhD, Cand. of Tech. Sc., Assistant Professor of Information Security department, Vinnytsia National Technical University, Vinnytsia