УДК 004.021

ПРОБЛЕМИ БЕЗПЕКИ ANDROID - ЗАСТОСУНКІВ

Шевчук Р.П.[1)], Вінарчук Ю.А.[2)], Шпак В.Б.[3)]
Тернопільський національний економічний університет
[1)]к.т.н., доцент, [2)]магістрант, [3)]викладач

I. Вступ

На даний час операційна система (ОС) Android займає понад 85% ринку мобільних ОС та є найбільш популярною системою для персональних мобільних пристроїв (ПМП) [1]. Кількість Android - застосунків завантажених в Google Play складає понад 2,8 млн [2], при цьому більшість з них при встановленні вимагають доступу до різноманітних даних та сервісів ПМП. Відповідно до результатів відкритого дослідження безпеки Android – застосунків, понад 21 % проаналізованих застосунків потенційно загрожують безпеці користувачів [3].

Основні проблеми у захисті Android – застосунків пов'язані із недоліками реалізації механізмів захисту. Більшість проблем цієї категорії можна уникнути ще на етапі проектування застосунків і розробки технічних завдань для програмістів.

II. Мета роботи

Метою роботи є аналіз проблем безпеки Android – застосунків та розробка рекомендації щодо їх запобігання.

III. Аналіз проблем безпеки Android – застосунків

ОС Android являє собою програмний стек для ПМП, який включає ОС, програмне забезпечення проміжного рівня, а також додаткові користувацькі застосунки. Дискреційна модель доступу реалізована в ОС Android, дозволяє кожному застосунку встановлювати права доступу до даних та сервісів ПМП. В якості матриці доступу для кожного Android – застосунку виступає системний файл manifest.xml.

До основних видів атак на Android – застосунки відносять:

- декомпіляція файлу застосунку;
- перехоплення даних;
- атаки через відлагоджувальні інструменти.

На основі аналізу атак було сформовано перелік основних проблем безпеки Android – застосунків та розроблено рекомендації щодо їх запобігання (таблиця 1).

Таблиця 1

Аналіз проблем безпеки Android – застосунків

Назва проблеми	Клас небезпеки	Рекомендації щодо запобігання
Використання незахищених локальних сховищ даних	Дуже висока	Використовувати захищенні сховища даних
Зберігання даних у коді	Висока	
Використання симетричних алгоритмів із зберіганням приватного ключа	Висока	Використовувати симетричні алгоритми із випадково генерованим ключем
Використання асиметричних алгоритмів із приватним ключем, відомим серверу	Залежить від ступеня захисту сервера	Унеможливити розшифрування сервером приватних ключів користувача
Використання власних алгоритмів шифрування та захисту даних	Середня	Використовувати відомі крипто алгоритми
Передача даних у відкритому вигляді	Середня	Шифрувати дані
Зберігання даних у відкритому вигляді в захищених сховищах	Середня	
Ігнорування факту роботи із рутованими або зараженими ПМП	Середня	При підтвердженні проблеми, завершувати роботу застосунку
Делегування функції застосунку веб-оглядачам	Середня	Не використовувати вмонтований веб-оглядач

Реверсна інженерія алгоритмів	Низька	Обфускація коду

Аналіз таблиці 1, підтверджує тезу, що більшість проблем безпеки Android – застосунків можна усунути ще на стадії розробки. Для цього необхідно дотримуватись практики безпечної розробки (SDLC - security development life cycle) [6] і приділяти належну увагу тестуванню механізмів захисту. Для зниження ризиків також рекомендується регулярно проводити аналіз захистів застосунків на всіх етапах життєвого циклу програмного забезпечення.

Висновок

У роботі проведено аналіз проблем безпеки Android – застосунків та розроблено рекомендації щодо їх запобігання.

Для зниження ризиків пов'язаних із безпекою Android – застосунків рекомендується дотримуватись практики безпечної розробки і приділяти належну увагу тестуванню механізмів захисту на всіх етапах життєвого циклу програмного забезпечення.

Список використаних джерел

1. Smartphone operating systems: global market [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.statista.com
2. Number of apps available in leading app stores [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.statista.com
3. WhiteHat Security Application Security Statistics Report. – 2017. – P. 60.
4. Howard M., Lipner S. The security development lifecycle: a process for developing demonstrably more secure software. Microsoft Press, 2006, 352 p.

УДК 004.432.4

ОСОБЛИВОСТІ ІДЕНТИФІКАЦІЇ ГОЛОСОВИХ КОМАНД ПЕРСОНАЛЬНиМИ МОБІЛЬНиМИ ПОМІЧНИКАМИ НА БАЗІ СЕРВІСУ GOOGLE VOICE

Шевчук Р.П. [1)], Ензельт А.О. [2)], Дериш І.Р. [3)]

Тернопільський національний економічний університет

[1)] к.т.н., доцент; [2,3)] магістрант

I. Вступ

Сьогодні досить поширеною є практика реалізації персональних мобільних помічників для мобільних пристроїв, які взаємодіють з користувачами в розмовній формі, використовуючи природні звороти мови та дозволяють в реальному масштабі часу надавати різноманітну інформацію. Як правило, більшість мобільних помічників використовують зовнішні сервіси та бази даних для обробки запитів та виконання певних завдань. При цьому в їх основі лежать ідеї персоналізації та передбачення, які дозволяють надавати користувачам інформацію тоді, коли вона їм потрібна.

Основними функціями мобільних помічників є [1-8]: 1) голосове управління; 2) голосовий ввід тексту; 3) голосовий пошук; 4) надання інформації відповідно до запитів користувача та контексту; 4) формування відповідей на поставленні запитання.

При розробці персональних мобільних помічників застосовують клієнтський і клієнт-серверний підходи. У ПЗ першого типу, наприклад у Speereo Software [1], алгоритм розпізнавання голосу реалізуються на самому пристрої. Перевагою таких помічників є незалежність від доступу до мережі Інтернет, однак продуктивність їх роботи залежить від потужності мобільного пристрою, тому вони використовуються рідко. При використанні клієнт-серверного підходу, голосовий сигнал зчитується мобільним пристроєм користувача і через Інтернет надсилається серверу на якому відбувається процес розпізнавання голосу. Для таких систем характерне навчання на основі зразків вже розпізнаних голосових вибірок. Прикладом таких мобільних помічників є Google Now [2], Siri [3], Vlingo [4], Maluuba [5], Sherpa [6], Amazon Alexa [7] та інші.

II. Мета роботи

Метою роботи є дослідження особливостей ідентифікації голосових команд персональними мобільними помічниками на базі сервісу Google Voice.