УДК 004

А. В. Юхименко, студент, О. В. Чебанюк, професор, д.т.н.
НТУУ «КПІ імені Ігоря Сікорського», Україна

МЕТОДИКА ПОПЕРЕДЖЕННЯ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ ГІРОСКОП У МОБІЛЬНИХ ПРИСТРОЯХ НА ОС ANDROID

A. V. Yukhymenko, student, O. V. Chebanyuk, Dr., Prof.

THE METHODOLOGY OF SPOKEN INFORMATION LEAKAGE PREVENTION THROUGH GYROSCOPE IN ANDROID MOBILE DEVICES

Сучасні мобільні пристрої надають широкі можливості для обробки та обміну інформацією. Водночас високий рівень апаратних можливостей, програмних засобів та бездротових технологій значно розширює можливості зловмисників для несанкціонованого отримання інформації.

Поняття мобільного пристрою об’єднує переносні пристрої (handheld devices), що можуть мати доступ до мережі і здатні виконувати: збирання, обробку, накопичення, зберігання та передавання інформації [2][3]. Поняття включає: мобільні телефони (у т.ч. смартфони), планшети, смарт-годинники, електронні книги та ін.

За даними ресурсу [1], станом на липень 2021 у світі понад 5.27 млрд. унікальних користувачів мобільних телефонів — приблизно 67% населення світу. Кількість користувачів мережі інтернет — 4.8 млрд. людей, з них 92.1% виходять в інтернет з мобільних пристроїв.

Наразі переважна більшість мобільних пристроїв у світі працюють під керуванням двох ОС: Android та IOS (понад 98%) [2]. Будь-яка вразливість у коді цих ОС може перетворити мобільний пристрій на закладний і є проблемою глобального масштабу.

У даній роботі розглядається актуальна загроза витоку мовної інформації у мобільних пристроях на ОС Android та пропонується методика виявлення потенційно небезпечних додатків.

У матеріалах праці [3] розглядалася можливість отримання мовної інформації з даних гіроскопу мобільного пристрою, що забезпечується особливостями конструкції датчика.

У складі MEMS датчика гіроскопу, що втановлюється у мобільні пристрої є легкий вантаж, що може переміщатись під дією зовнішніх сил. У тому числі коливатись у полі акустичних хвиль. При наявності акустичних коливань, дані на виході датчика модулюються за амплітудою, завдяки чому його можна використовувати в якості мікрофона.

Результати роботи [3] свідчать також про успішне розпізнавання мовної інформації, яку було отримано з даних гіроскопа мобільного пристрою, з використанням нейронної мережі.

В ОС Android існує механізм керування дозволами. Він визначає, до яких функцій пристрою може отримати доступ додаток. На сайті компанії Google представлено список функцій [4], для використання яких додаток повинен отримати дозвіл. Серед них використання даних гіроскопа не потребує дозволу. Враховуючи можливість одержання мовної інформації з даних гіроскопа та відсутність вимоги надання спеціального дозволу для його використання, існує загроза витоку мовної інформації на пристроях з ОС Android.

Положення методики, що пропонується в даній роботі, дозволять визначати потенційно небезпечні додатки — ті, що можуть реалізувати розглянуту загрозу витоку мовної інформації з використанням гіроскопу мобільного пристрою.

Методика передбачає виконання наступних дій:

Проаналізувати список активних процесів в ОС мобільного пристрою. Серед, додатків, виконуваних в даний момент, необхідно скласти множину тих, що використовують дані гіроскопа. Відсортувати сформовану множину додатків за швидкістю зчитування даних (sampling rate) у порядку спадання, та розділити на підмножини відповідно до порогового коефіцієнту.

Позначити додадок як безпечний, чи потенційно небезпечний залежно від того, до якої підмножини він включений.

Під пороговим значенням мається на увазі найбільша частота зчитування даних гіроскопа, при якій відновлення мовної інформації неможливе або значно ускладнене.

Положення методики можуть бути втілені в окремому додатку для пристроїв на ОС Андроїд. Це надасть можливість користувачам проводити сканування активності зчитування даних гіроскопа активними додатками та запобігати реалізації загрози шляхом зміни дозволу для додатку чи завершення процесу.

Високий рівень технологій сучасних мобільних пристроїв, їх значне поширення та доступ до мережі значно розширює можливості зловмисників для несанкціонованого отримання інформації.

Можливість використання гіроскопу у якості мікрофона становить загрозу витоку мовної інформаії у мобільних пристроях.

Реалізація запропонованої методики у додатку дозволить користувачам мобільних пристроїв визначати потенційно небезпечні додатки та попередити реалізацію представленої загрози витоку.

Література:

1. DIGITAL AROUND THE WORLD [Електронний ресурс] – Режим доступу до ресурсу: https://datareportal.com/global-digital-overview.

2. Poetker B. The Mobile Operating Systems That Matter Right Now (+Effects on Development) [Електронний ресурс] / Bridget Poetker. – 2021. – Режим доступу до ресурсу: https://www.g2.com/articles/mobile-operating-systems?__cf_chl_captcha_tk__=pmd_AqqGJl98nhYsip05OK6.D5_xG6vl.C7LDF8jODuDnzg-1634778643-0-gqNtZGzNAzujcnBszQdl.

3. Michalevsky Y. Gyrophone: Recognizing Speech from Gyroscope Signals [Електронний ресурс] / Y. Michalevsky, D. Boneh, G. Nakibly – Режим доступу до ресурсу: https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-michalevsky.pdf.

4. Як змінити дозволи для додатків на телефоні Android [Електронний ресурс] – Режим доступу до ресурсу: https://support.google.com/android/answer/9431959?hl=uk.