УДК 004.056.52

АНАЛІЗ ЗАГРОЗИ РОЗПІЗНАВАННЯ НАТИСКАНЬ КЛАВІШ ФІЗИЧНОЇ КЛАВІАТУРИ НА ОСНОВІ ДАНИХ З АКСЕЛЕРОМЕТРА СМАРТФОНУ

Звягіна І. Д.
email: iryna.zviahina@nure.ua
Науковий керівник – ст. викл. Ликова Г.О.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ
м. Харків, Україна

This study explores the threat of keystroke recognition attacks based on smartphone accelerometer data. An analysis of the experiment results is conducted to analyze the impact of different factors on the success rate of the attack. The findings provide insights into potential security risks and highlight the feasibility of exploiting motion sensors for unauthorized data interception.

Багато дослідників вивчало можливість використання датчиків, вбудованих у мобільні пристрої, для реалізації атак, спрямованих на несанкціоноване отримання конфіденційних даних жертви. Зокрема, у наявних публікаціях описано дослідження атак розпізнавання мови користувача, паролів, цифрових PIN-кодів та просто друкованого тексту[1-2].

Методи атак спрямованих на несанкціоноване зняття інформації за допомогою смартфону розташованому поруч з клавіатурою ПК умовно можемо розділити на наступні:

- на основі аналізу аудіо-сигналів[1];
- на основі вимірювання прискорення та кутової швидкості[2].

Короткий аналіз літератури за темою роботи показав, що хоча більшість досліджень, що вивчають загрозу розпізнавання тексту, який жертва вводить на фізичній клавіатурі, демонструють високу точність у лабораторних умовах, їх практична реалізація великою мірою залежить від великої кількості факторів.

Перспективними залишаються атаки на фізичні клавіатури, що базуються на даних про прискорення та кутову швидкість смартфона[2]. Це зумовлено тим, що виробники ґаджетів недостатньо уваги приділяють безпеці таких датчиків як акселерометр та гіроскоп. На відміну від мікрофона[1], доступ до яких вимагає прямої згоди від користувача, датчики руху можуть використовуватися будь-яким застосунком без попереднього дозволу. Це створює додатковий канал витоку інформації та надає зловмиснику можливість встановити шкідливе програмне забезпечення та непомітно збирати конфіденційні дані користувача. Також даний метод не потребує фізичного доступу до смартфону жертви.

Дана робота має на меті привернути увагу до проблеми недостатнього захисту датчиків руху у смартфонах та довести те, що їх вразливість може становити реальну загрозу безпеки для конфіденційних даних користу-

вачів.

З метою оцінки можливості реалізації вище згаданої атаки в реальних умовах, проаналізуємо результати експерименту, проведеного американськими науковцями з Університету Кібербезпеки Дарвіна Дісона[2].

У цьому досліді було задіяно 20 людей, що сидячи за столом друкували випадковий текст на фізичних клавіатурах, смартфони в той час були розташовані поруч із ними. Учасників не обмежували у виборі слів, швидкості чи стилі друку. Експеримент також проводився в зашумленому середовищі, де 40% учасників розмовляли під час друку.

Для збору даних використовувалися по черзі 1, 2, 4 і 8 телефонів, що зчитували дані з акселерометра, гіроскопа та мікрофона. Було проведено кілька дослідів у різних умовах для порівняння результатів відносно них[2].

В таблиці 1 представлено результати експерименту залежно від типу клавіатури, якою користується жертва. Можна спостерігати, що ноутбук і механічна клавіатура демонструють приблизно однаковий рівень точності розпізнавання, тоді як безпровідна клавіатура дає дещо гірші результати.

Таблиця 1 – Результати експерименту в залежності від типу клавіатури

Тип клавіатури	**Точність для 1 спроби**	**Точність для 5 спроб**
Клавіатура ноутбука	43,2%	70,2%
Механічна USB клавіатура	38,3%	69,9%
Безпровідна механічна клавіатура	33,4%	64,3%

Таблиця 2 показує результати експерименту в залежності від кімнати, в якій він проводився. На жаль автори наукової роботи не надають додаткових даних про те, чим саме відмінні два приміщення. Результати показують, що зміна кімнати має деякий вплив на точність розпізнавання слів, однак він не є суттєвим.

Таблиця 2 – Результати експерименту в залежності від кімнати

Кімната	**Точність символів**	**Точність слів**	**Точність слів, Топ-5**
Кімната А	32,3%	25,9%	32,9%
Кімната Б	27,8%	21,4%	28,3%

Таблиця 3 в свою чергу демонструє результати проведеного експерименту в залежності від матеріалу поверхні, на якій розташовується клавіатура та смартфон. Бачимо, що у випадку з дерев’яним столом, точність розпізнавання є суттєво більшою в порівнянні з металевою чи іншою

поверхнею.

Таблиця 3 – Результати експерименту в залежності від матеріалу стола

Стіл	**Точність символів**	**Точність слів**	**Точність слів, Топ-5**
Дерев'яний	32,2%	25,9%	32,9%
Суміш	15,9%	8,2%	15,3%
Металевий	13,2%	2,4%	5,9%

В Таблиці 4 можемо спостерігати результати експерименту в залежності від того, чи рухався телефон під час атаки. Бачимо, що ефективність розпізнавання доволі сильно залежить від цього фактору і підвищує шанси зловмисника більш ніж на 10% при статичному розташуванні ґаджета.

Таблиця 4 – Результати експерименту в залежності від рухів телефона

Розташування	**Точність символів**	**Точність слів**	**Точність слів, Топ-5**
Статично	32,6%	24,5%	31,6%
Систематичні зсуви	29,5%	20,6%	28,4%
Випадкові зсуви	22,8%	18,2%	25,3%

Отже, проаналізувавши результати експерименту, проведеного американськими науковцями з Університету Кібербезпеки Дарвіна Дісона, можна зробити висновок, що, попри вплив численних факторів на ефективність атак, спрямованих на несанкціоноване зняття інформації з клавіатури, загроза їх реалізації залишається актуальною навіть в умовах, максимально наближених до реальних.

Список використаних джерел:

1. R. Schlegel, K. Zhang, X.-y. Zhou, M. Intwala, A. Kapadia, andX. Wang, "Soundcomber: A stealthy and context-aware sound trojanfor smartphones" in NDSS, vol. 11, 2011, pp. 17–33.

2. Tyler Giallanza, Travis Siems, Elena Sharp, Erik Gabrielsen, Ian Johnson, Mitchell A. Thornton, and Eric C. Larson, "Keyboard Snooping from Mobile Phone Arrays with Mixed Convolutional and Recurrent Neural Networks" in Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 3, 2, 2019, Article 45, 22 pages