АНАЛІЗ ЕФЕКТИВНОСТІ АКУСТИЧНОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ СЕНСОРИ КОМП'ЮТЕРНОЇ МИШІ

Мартинчук О.О., Брайко В.С.

Кафедра Інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: oleksandr.martynchuk@nure.ua
vladyslav.braiko@nure.ua

Abstract

This paper presents an analysis of the effectiveness of the acoustic leak channel through computer mouse sensors, i.e. Mic-E-Mouse, a new side-channel attack that uses high-performance optical mouse sensors to covertly eavesdrop on users. The attack exploits the capabilities of advanced optical sensors, especially those with high resolution and polling rates. It detects the subtle transverse surface vibrations caused by the user's confidential speech, effectively turning the mouse into a rudimentary microphone. The collected raw motion data is significantly degraded due to non-uniform sampling and quantization. To overcome these limitations, interpolation, ad hoc Wiener filtering, and a neural network for speech reconstruction are used. This pipeline achieves significant results, including a signal-to-noise ratio improvement of up to +19 dB and a 40% increase in speech transmission index compared to raw data, demonstrating that auditory tracking using conventional peripherals is now technically feasible, efficient, and productive.

Сучасні високопродуктивні оптичні сенсори, що використовуються в комп'ютерних мишах, особливо ігрових, становлять неочевидну вразливість. Ці пристрої, розроблені для надзвичайної точності та високої частоти опитування (до 4KHz і вище), можуть виявляти мікроскопічні переміщення робочої поверхні. Дослідження можливостей такого каналу витоку інформації, тобто миші як мікрофону Mic-E-Mouse вперше демонструє, що ці сенсори можна експлуатувати як побічний канал для акустичного підслуховування. Цей метод заснований на аналогії «миша-мікрофон», де сенсор, що фіксує переміщення в дюймах на точку (DPI D), може виявляти рухи розміром до $\frac{1}{D}$ дюйма, включаючи поперечні вібрації (перпендикулярні поверхні), спричинені звуковими хвилями мови користувача. На рис. 1 представлено зростаючу чутливість мишей, яка виводить сенсори PAW3395 та PAW3399 в зону особливої вразливості.

Графік на рис. 1, ілюструє, як зростання DPI та частоти опитування робить сучасні сенсори, такі як PAW3395/PAW3399, сприйнятливими до акустичних атак.

Атака Mic-E-Mouse реалізується шляхом збору високочастотних даних про рух миші $(\Delta x, \Delta y, \Delta t)$ через скомпрометоване або легальне програмне забезпечення на комп'ютері жертви. Зібраний сигнал є вкрай низькоякісним, страждаючи від сильного квантування, нерівномірної вибірки та нелінійної частотної характеристики.

Для подолання цих перешкод розроблено програмний конвеєр Mic-E-Mouse. Загальна схема атаки представлена на рис. 2, яка включає збір даних про вібрації, їх передачу та подальшу обробку.

Схема, що представлена на рис. 2, демонструє етапи атаки: від захоплення вібрацій в безпечному середовищі до збору даних та відновлення аудіосигналу через обробку сигналу та машинне навчання.

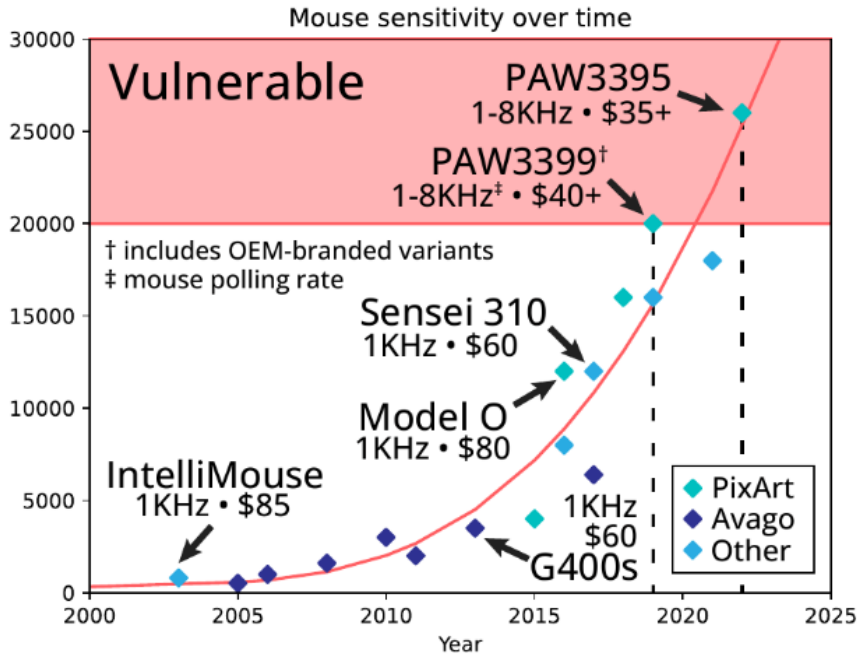

Рис. 1. Чутливість сенсорів миші з часом та зони вразливості

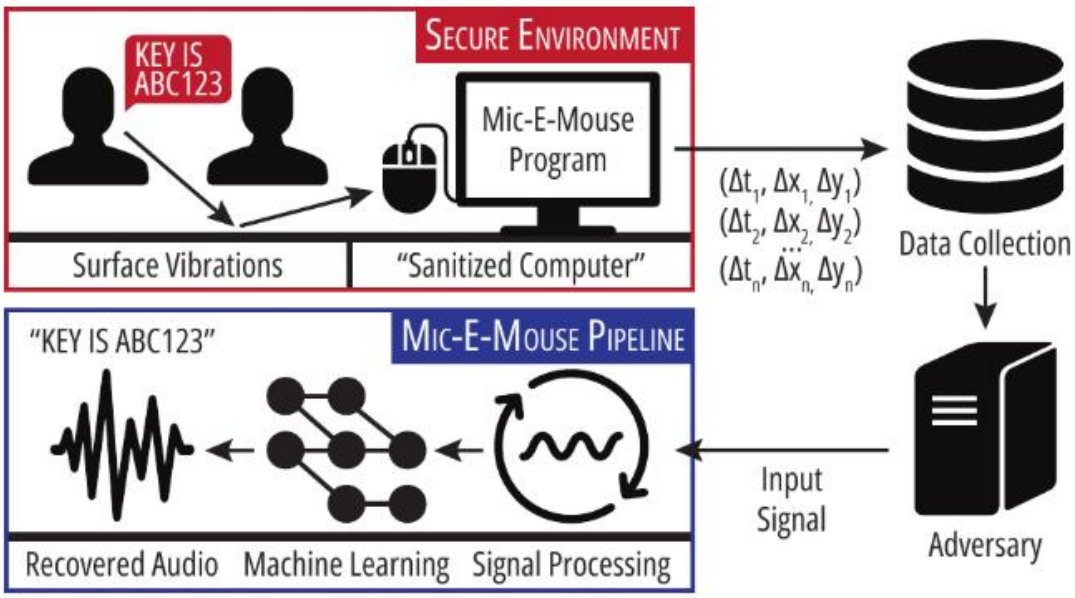

Рис. 2. Процес обробки сигналу Mic-E-Mouse

Процес обробки сигналу включає такі основні етапи:

– передискретизація: Використання sinc-інтерполяції для перетворення нерівномірної вибірки сирих даних на придатний для аудіообробки формат;

– зниження шуму: Застосування налаштованої фільтрації Вінера (Wiener filtering), тренованої на профілях шуму конкретного сенсора;

– реконструкція мови: Використання трансформерних нейронних мереж для кінцевого перетворення очищеного сигналу на розбірливу мову.

Ефективність цих етапів, що призводить до відновлення мови, проілюстровано на рис. 3.

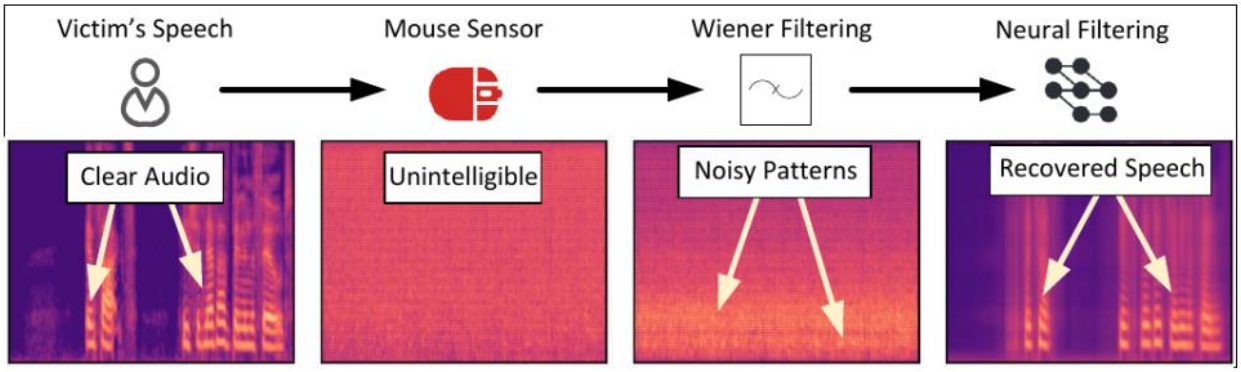

Рис. 3. Відновлення розбірливої мови

Результати досліджень Mic-E-Mouse доводять, що високопродуктивні оптичні сенсори є ефективним засобом прихованого аудіоспостереження. Було досягнуто значне покращення якості сигналу: збільшення SI-SNR на +19 дБ та точність розпізнавання мовлення від 42% до 61% на автоматизованих тестах. Дослідження продемонструвало показник помилок слів (WER) 16,79%. З урахуванням постійного вдосконалення сенсорних технологій та зниження їхньої вартості, зростає кількість вразливих пристроїв, що розширює потенційну поверхню атаки. Необхідна подальша увага до цієї уразливості з боку користувачів, компаній та урядових структур.

Література

1. Mic-E-Mouse Covert Eavesdropping through Computer Mice. Режим доступу: https://sites.google.com/view/mic-e-mouse.

2. Fakih M., Dharmaji R., Mahmoud Y. Bouzidi H. Faruque M. Dept. of Electrical Engineering and Computer Science, University of California, Irvine, CA, USA. Invisible Ears at Your Fingertips: Acoustic Eavesdropping via Mouse Sensors. Режим доступу: https://arxiv.org/pdf/2509.13581.

3. Invisible Ears at Your Fingertips: Acoustic Eavesdropping via Mouse Sensors. The Moonlight. Режим доступу: https://www.themoonlight.io/en/review/invisible-ears-at-your-fingertips-acoustic-eavesdropping-via-mouse-sensors.

4. Optical Mice Turned into Covert Eavesdropping Devices in 'Mic-E-Mouse' Attacks. Cyber Insider. Режим доступу: https://cyberinsider.com/optical-mice-turned-into-covert-eavesdropping-devices-in-mic-e-mouse-attacks/.

5. «Mic-E-Mouse» Attack Lets Hackers Steal Sensitive Data via Mouse Sensors. GB Hackers. Режим доступу: https://gbhackers.com/mic-e-mouse-attack-hackers-steal-sensitive-data/.