

БЕЗКОНТАКТНА АТАКА ЗА ДОПОМОГОЮ ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ ДЛЯ МАНІПУЛЮВАННЯ СЕНСОРНИМ ЕКРАНОМ

Н. О. Кривчук^{1, a}, В. М. Степаненко¹

¹ Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
НН Фізико-технічний інститут

Анотація

У роботі розглянуто основні види та принципи дії ємнісних сенсорних екранів та проаналізовано вплив на них зовнішнього електромагнітного випромінювання. Досліджена безконтактна атака на ємнісні сенсорні екрани та проведено ряд експериментів, що підтверджують можливість імітувати сенсорні події (натискання, проведення та мультитодик). Запропоновано відповідні апаратні і програмні вдосконалення для протидії таким атакам та мінімізації ризику несанкціонованого доступу до пристроїв з сенсорними екранами.

Ключові слова: ємність, проведення, натискання, точки дотику, електроди, антена, смартфон

Вступ

Сенсорні екрани дозволили користувачам взаємодіяти з комп'ютерними пристроями, використовуючи тільки пальці і стали популярною альтернативою мишам і клавіатурам. Зокрема, ємнісні сенсорні екрани забезпечують можливість мультитодіку, тривалий термін служби та економічну ефективність, отже, широко використовуються на пристроях, таких як смартфони, планшети та годинники. Саме здатність вимірювати невеликі електричні поля і робить ємнісні сенсорні екрани чутливими до впливу електромагнітних випромінювань (ЕМВ)[1] [2]. Головною ідеєю є втручання в процес вимірювання ємності в сенсорних екранах, використовуючи електромагнітні сигнали, які направляються на приймальний електрод в сенсорному екрані. Як результат електро-рушійна сила з'являється в контурі, який бере участь у виявленні сенсорної точки. Саме так ми можемо ввести підроблені точки (натискання та проведення) на сенсорний екран.

1. Будова та принцип дії ємнісних сенсорних екранів

Найпростіша конструкція ємнісного сенсорного екрана передбачає нанесення з одного боку прозорого провідного шару, наприклад (ІОТ) оксиду індію та олова. На цей шар у чотирьох кутах екрана подається невелика напруга, яка утворює однорідне електричне поле. Коли до іншого боку скла торкається людський палець, контролер пристрою може визначити координати дотику за зміною ємності, яку визначає на підставі зміни напруги в кутах панелі.

На Рис. 1 показана типова архітектура ємнісних сенсорних екранів[3], яка включає сенсорний датчик,

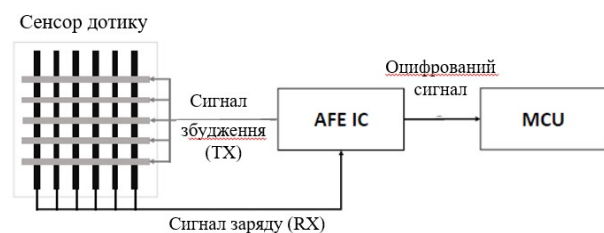


Рис. 1. Типова схема побудови ємнісного сенсорного екрана

аналогову фронтендову інтегральну схему (AFE IC) і мікроконтролер (MCU). Сенсорний датчик складається з сітки передавальних (TX) і приймальних (RX) електродів з прозорих провідних матеріалів, наприклад, індію-олово-оксиду (ІТО). AFE IC посиляє сигнали збудження на електроди TX і вимірює сигнал заряду від електродів RX. Сигнал заряду опіфровується і відправляється в MCU, який обробляє сигнал і виявляє сенсорні події (натискання, проведення і т.д.).

На базі цієї архітектури існують 2 ефективні методи, які роблять можливим мультитодик:

- Метод взаємного ємнісного виявлення, який відноситься до того, як вимірюється різниця ємності в одній точці;
- Метод рухомого сканування, який використовується в поєднанні з взаємним ємнісним виявленням для знаходження точок дотику.

1.1. Метод взаємного ємнісного виявлення

Датчики мають конденсатор на кожному перетині кожного рядка і кожного стовпця. Наприклад, мав би 12 на 16 мав би 192 незалежних конденсатора. Коли сигнал збудження поступає на електрод TX,

^anazarii.krivchuk@gmail.com

електрод генерує електричне поле, яке створює потік електричного заряду до повітряних електродів RX, що, по суті, утворює взаємну ємність C_M між електродами RX і TX на кожному перехресті, як показано на Рис. 2 [4]. Коли палець торкається екрану, він поглинає частину електричного поля і змінює взаємну ємність до $C_M - \Delta C_M$, де ΔC_M заряд, який поглинув палець (не забуваємо, що тіло людини хороший провідник). При цьому різниця зміни ємності сигналу заряду, виміряна електродом RX і виявляється точкою дотику на перетині RX і TX. Тобто і є місцем нашого дотику.

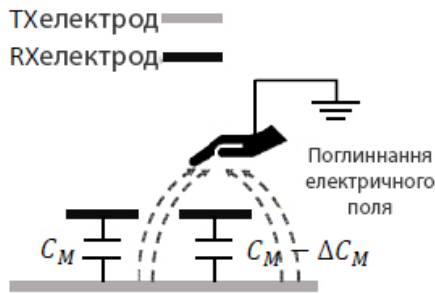


Рис. 2. Метод взаємного ємнісного виявлення

Сигнал збудження, як правило, є меандром з частотою від 100 кГц до 500 кГц. Взаємне ємнісне виявлення перевершує інші методи, такі як метод власної ємності, оскільки вона може ефективно знаходити точку дотику, використовуючи пари TX-RX електродів.

1.2. Метод рухомого сканування

Метод рухомого сканування[5],[6] призначений для визначення точок дотику на екрані, захоплюючи всі електроди TX по черзі, як показано на Рис. 3 Оскільки тільки один TX збуджений в потрібний час, сенсорний екран може визначити розташування дотику, за допомогою рядків і стовпців активних TX-RX пар. Також завдяки особливості конструкції, підтримується мультитач. Метод включає в себе кілька основних параметрів:

- N – кількість електродів TX ;
- T_p – час, необхідний для сканування всіх електродів TX;
- T_{p1} – час, необхідний для сканування одного електрода TX.

2. Модель загроз

Мета нападника - маніпулювати пристроєм жертви, вводючи підроблені дотики на сенсорний екран безконтактним способом. Робимо наступні припущення щодо нападу:

- **Пристрій жертви:** Пристрій жертви оснащений ємнісним сенсорним екраном, наприклад смартфон або планшет. Пристрій незмінний перед атакою і розміщується екраном вниз на поверхню (наприклад, стіл) під час атаки;

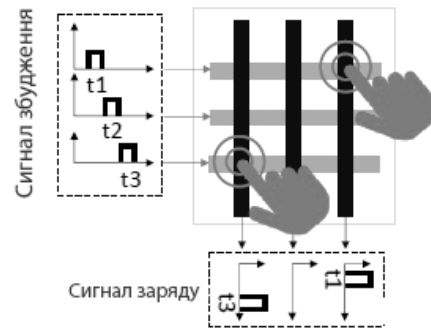


Рис. 3. Метод рухомого сканування

- **Обізнаність нападника:** Противник може знати модель пристрою жертви і придбати пристрій тієї ж моделі для попереднього вивчення. Крім того, противник може отримати номер телефону жертви за допомогою соціальної інженерії або інших методів;
- **Можливості нападника:** Зловмисник може атакувати пристрій, тільки маніпулюючи сенсорним екраном за допомогою електромагнітних сигналів. Однак противник не може фізично торкатися пристрою жертви або просити користувача виконувати будь-які дії;
- **Налаштування атаки:** Нападак може приховати обладнання для атаки під столом, де пристрій жертви можуть бути прикріплені до поверхні (наприклад, під столом у кімнаті для переговорів або зарядною станцією). Нападак також може дистанційно керувати обладнанням.

3. Проектування атаки

Наша мета полягає в тому, щоб вводити керовані сенсорні події, такі як дотики та проведення, у цільову область сенсорного екрана та використовувати їх для маніпулювання пристроєм. Для досягнення цієї мети нам необхідно вирішити наступні технічні проблеми:

- 1) **Ефективність введення підроблених точок дотику:** Ми знаємо, що введення за допомогою ЕМВ можливе, проте підроблені точки дотику вводяться за допомогою непередбачуваних сигналів. Для цього завдання ми вивчаємо три основні фактори, які впливають на ефективність введення сенсорної точки, тобто *передавальну антену, частоту сигналу та відстань атаки*. Наша мета - знайти оптимальні варіанти та значення цих факторів, які в поєднанні можуть досягти максимальної інтенсивності ін'єкції сенсорної точки економічно ефективним способом;
- 2) **Створення контрольованих сенсорних подій:** Підроблені точки дотику можуть поширюватися тільки випадковим чином на екрані. Щоб досягти керованих сенсорних подій, таких як натискання та проведення, нам потрібно сконцентрувати підроблені сенсорні точки в цільову область екрана та налаштувати їх положення за бажанням. Щоб вирішити цю проблему, ми вивчаємо методи, щоб випадково розподілені точки дотику

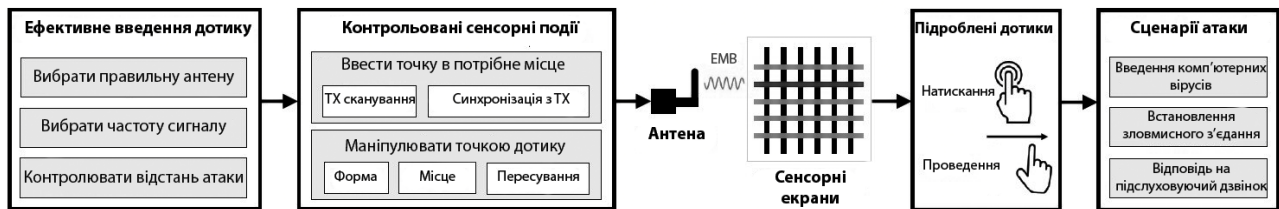


Рис. 4. Проектування атаки

ку неодноразово з'являлися в звуженій області сенсорного екрана. Регулюючи *час передачі, період передачі та положення антени*, ми можемо контролювати положення введених точок дотику.

Проектування атаки показане на Рис. 4. На першому етапі ми готуємо сигнал ЕМВ для ефективного введення точок дотику, вибираючи правильну антену, підбираючи частоту сигналу, контролюючи відстань атаки. На другому етапі ми розробляємо сигнал ЕМВ для керованих сенсорних подій, досліджуючи сенсорний екран, синхронізацію та регулюючи ключові параметри сигналу. Після цих етапів створений сигнал ЕМВ випромінюється антеною для атаки на сенсорний екран смартфона. Наша атака може викликати два типи основних сенсорних подій, натискання та проведення, які можуть бути використані для побудови більш складної сенсорної поведінки для різних сценаріїв атаки.

4. Експериментальна установка

У цій частині ми використовуємо установку, як показано на Рис.5, і встановлюємо тривалість передачі на 3 Тр₁, період передачі буде таким же, як період сканування Тр (120 Гц), а частота сигналу ЕМВ - 46 МГц. Відстань за замовчуванням між антенами і екраном становить 5 мм. Цільовий смартфон (Nexus 5X) підключається до ноутбука для запису сенсорної ін'єкції.

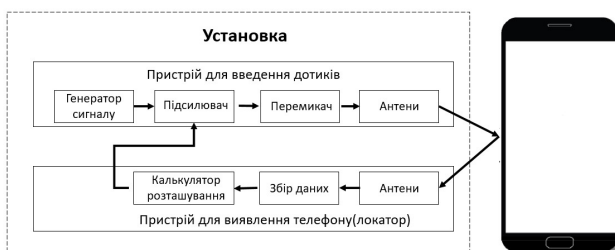


Рис. 5. Схема еспериментальної усагновки

Збір даних: Щоб кількісно оцінити результати атаки, нам потрібно отримати дані про сенсорні події, наприклад, час та місце введення точок. Ми можемо отримати дані або з програми Android, або за допомогою Android Debug Bridge (ADB), інструменту командного рядка, який може з'єднуватися з пристроями Android.

Показники: Ми оцінюємо продуктивність системи з двох точок зору: схожість з реальними людськи-

ми дотиками та здатність до атаки. Введені точки дотику і реальні точки дотику людини можуть вирізнятися в основному в двох аспектах: форма і концентрація точок дотику, які можна кількісно оцінити за наступними показниками:

- 1) *Діапазон*, що є різницею між максимальною та мінімальною координатами X/Y введених точок. У ньому описується форма введених точок;
- 2) *Стандартне відхилення координат X/Y*, яке описує концентрацію введених точок.

Показники для оцінки можливостей атаки включають швидкість введення, затримку атаки та швидкість успіху:

- 1) *Швидкість введення*, який є кількістю введених точок за одиницю часу;
- 2) *Затримка атаки*, який є часом, необхідний для введення першої успішної сенсорної події з моменту початку атаки;
- 3) *Швидкість успіху*, що є часткою атак, які успішно вводять потрібну сенсорну подію.

5. Результати атаки

Результати будуть розглядатися для кожного виду сенсорних подій: натискання, проведення та мульти-дотику.

5.1. Натискання

Ми встановлюємо період передачі на Тр і повторюємо експерименти 100 разів з тривалістю кожного експерименту 3 секунди. Оскільки Тр змінюється з плином часу, ми вимірюємо його постійно і коригуємо період передачі. Після запису даних ін'єкційних точок ми обчислюємо діапазон координат X і Y, стандартне відхилення координат, швидкість введення. Показники введених точок наведені на Рис.6 (PDF - функція щільності ймовірності).

- **Діапазон:** Середнє значення діапазону ($Range_x$) по осі X і діапазону ($Range_y$) по осі Y становить 36,3 пікселів і 175,8 пікселів відповідно;
- **Стандартне відхилення координат X/Y:** Середнє значення стандартного відхилення по осям std_x і std_y - 5,4 пікселів і 44,0 пікселів відповідно;
- **Швидкість введення:** Середнє значення швидкості введення становить 45,38 точок/с. Максимальна швидкість дотику людини становить близько 7 точок/с, така швидкість може задовольнити вимоги нападника;
- **Затримка атаки:** Становить менше 0,5 секунди. Що є дуже гарним показником.

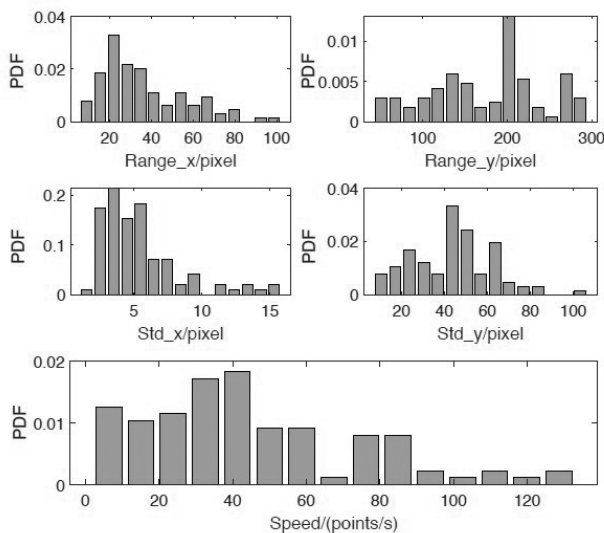


Рис. 6. Продуктивність введених дотиків у 100 випробуваннях, включаючи діапазон координат X та Y (зверху), відхилення координат (посередині) та швидкість введення (знизу)

5.2. Проведення

Ми оцінюємо затримку атаки та швидкість успіху введених проведень, встановивши період передачі T до 7,7 мс і неодноразово намагаючись провести пальцем вгору. Успішними вважалися спроби, в яких немає непотрібних наразі дотиків або проведень пальцем вниз, до настання першого успішного проведення пальцем вгору по Nexus 5X. Детальні показники можна побачити на Рис.7.

- **Швидкість успіху:** Щоб обчислити швидкість успіху, ми вимірюємо кількість помилкових подій перед першим успішним проведенням вгору, наприклад, дотиками та проведеннями пальцем вниз. Кількість помилкових подій становить 30 з 80 разів, що призводить до успіху в 62,5% (50/80);
- **Затримка атаки:** В середньому потрібно 1,6 секунди, щоб ввести успішне проведення пальцем вгору.

5.3. Мультидотик

Жести мултидотику стали популярною операцією введення, вони можуть бути або кількома одночасними натисканнями, або кількома проведеннями в різних місцях екрана. Найнадійнішим способом реалізації введення з декількома дотиками є одночасне введення нажат'я або проведень у різні лінії RX. Щоб ввести мултидотик до сенсорного екрана, ми використовуємо антени. Перемикач вмикання/вимикання вибере кілька антен у правильних місцях для випромінювання сигналу ЕМВ, при цьому кожна обрана антена буде пов'язана з відповідними лініями RX. Таким чином, злоумисник може успішно вводити дотики по цільових лініях RX одночасно і домогтися багатотактного введення. Ми перевіряємо можливість введення трьох точок дотику за допомогою трьох антен, а результати продуктивно-

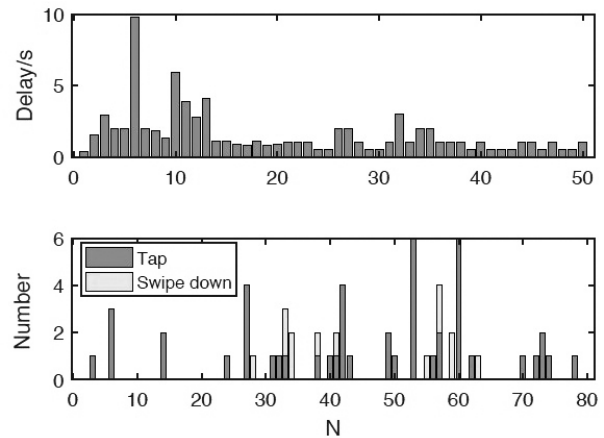


Рис. 7. Продуктивність введення проведень вгору в 80 випробуваннях, включаючи затримку часу до введення успішного проведення пальцем вгору (зверху) та кількість неавтономних сенсорних подій, наприклад, дотиків або проведень (знизу)

сті введення мултидоту аналогічні можливостям і властивостям атаки за допомогою однієї антени (аналогічно Розділу 5.2)

6. Потенційні контрзаходи

Деякі смартфони можуть бути менш вразливі до атаки, що може бути пов'язано з кращим електромагнітним екрануванням або ефективною перевіркою. Тому, щоб покращити безпеку даного дипу девайсів можна спробувати ті чи інші контрзаходи:

- **Покращення якості екрану:** Виробники можуть покращити сенсорний екран, щоб захистити його від загрози атаки. По-перше, додавання електромагнітного екранування ефективно для блокування ЕМВ. По-друге, підвищення напруги сигналу збудження може збільшити відношення сигнал/шум, що зменшить вплив ЕМВ. По-третє, можна використати метод рухомого сканування, який заснований на більш складній формі сигналу збудження і може бути використаний для фільтрації введеного струму ЕМВ. Хоча ці контрзаходи можуть зменшити вплив ЕМВ на сенсорний екран, вони вимагають змін апаратного забезпечення сенсорного екрана або призводять до більш високого споживання енергії. Таким чином, ці контрзаходи не підходять для існуючих сенсорних екранів;
- **Алгоритм виявлення:** Виробник може вдосконалити алгоритм виявлення сенсорного екрана. Наприклад, атаку можна виявити за допомогою інтервалу між натисканням і підйомом пальця. Щоб дослідити ефективність цього методу, ми обчислюємо інтервал дотику нападника та 30 добровольців. Ми випадковим чином вибираємо 2000 зразків від нападника і добровольців і аналізуємо розподіл інтервалу за допомогою коробкового графіку від Matlab. Як показано на Рис.8, верхня межа нападника є нижчою, ніж нижня межа з добровольцями. Ми можемо встановити поріг, наприклад, пунктирна лінія на

Рис. 8, щоб визначити, чи належить точка дотику користувачеві або зловмиснику. Крім того, розподіл ємності має певний шаблон, коли сенсорний екран знаходиться під нашою атакою, а не використовується людиною. Виходячи з цих фактів, виробник міг виявити аномальні точки дотику, заблокувати їх і попередити користувача.

- **Перевірка особистості:** Дозволи на застосування можуть обмежуватися, а перевірка особистості повинна проводитися при виконанні дій високого ризику. Наприклад, проведення перевірки особистості перед підключенням до пристрою Bluetooth або невідомого Wi-Fi. Перевірка особистості може бути здійснена шляхом повторного пошуку користувача для перевірки його відбитка пальця, обличчя або надання його PIN-коду або пароля.

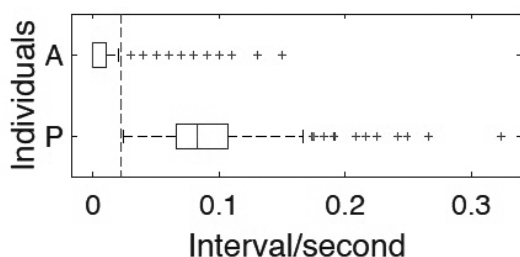


Рис. 8. Сенсорний інтервал 30 добровольців (P) та нападника (A). Сенсорні події від людини і нападника можна відокремити, встановивши поріг, представлений пунктирною лінією

Висновки

В результаті аналізу конструкції і принципу дії ємнісних сенсорних екранів встановлено їх вразливість до зовнішнього електромагнітного випромінювання. Таким чином, виникає можливість створити небез-

печну безконтактну атаку на сучасні смартфони, планшети і т.д., що використовують ємнісні сенсорні екрани. Проведений аналіз показав, що ми можемо формувати та скеровувати електромагнітні сигнали ближнього поля і, тим самим, імітувати сенсорні події в цільові області на сенсорному екрані без необхідності фізичного дотику або доступу до пристрою жертви. Як результат, зловмисник може непомітно отримати несанкціонований доступ до смартфона жертви та маніпулювати ним. Для мінімізації ризику таких безконтактних атак, запропоновано ряд програмних та апаратних контрзаходів, а саме: покращення якості екрану за допомогою додаткового електромагнітного екранування, запровадження вдосконаленого алгоритму виявлення дотиків та введення перевірки особистості (FaceID, сканування відбитку пальця) перед важливою дією на пристрої.

Перелік використаних джерел

1. Staff Embedded. Understanding electromagnetic interference sources in touchscreens. // Embedded. — 2011. — no. 1. — P. 1.
2. E. Keiser B. Principles of electromagnetic compatibility. — 3 ed. — 1987. — P. 15–102 c. — Access mode: <https://www.biblio.com/book/principles-electromagnetic-compatibility-3rd-edition-b/d/1454175192>.
3. Kwon O., An J., Hong S. Capacitive touch systems with styli for touch sensors sources in touchscreens // IEEE Sensors Journal. — 2018. — no. 2. — P. 4832–4846.
4. Lee J., Cole M. T., Chi Sun Lai J. An analysis of electrode patterns in capacitive touch screen panels // Display technology. — 2014. — no. 4. — P. 362–366.
5. Hotelling S., Strickon J., Huppi B. Multipoint touchscreen // US Patent 7,663,607. — 2010. — no. 3. — P. 8–30.
6. Hotelling S., Krah C.H., Huppi B. Multipoint touch surface controller // US Patent 8,279,180. — 2012. — no. 1. — P. 9–20.