ДОСЛІДЖЕННЯ МЕТОДІВ БЛОКУВАННЯ ТЕЛЕФОНУ ТА ЇХ ЗЛАМОСТІЙКІСТЬ

Куценко О.В.
Науковий керівник – к.т.н., доцент. Ликов Ю.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. КРіСТЗІ, тел. (057) 702-14-30
e-mail: oleksandra.kutsenko@nure.ua

This work is devoted to modern developments in the field of information security. The main focus is on methods for locking smartphones namely fingerprint scanning. The problem of information security is one of the most important problems of our time. Especially when people save almost all information on their mobile phones to date.

З появою NFC і прив'язкою пластикових карт до смартфону його захист став дуже актуальним питанням. Сучасний телефон легко захистити від несанкціонованого використання за допомогою блокування різними методами. Такими методами є:

пароль та PIN-код;
графічний ключ;
сканер відбитка пальця;
сканер розпізнання обличчя;
сканер райдужної оболонки;
блокування "Smart Look".

Метою роботи є знайти вразливі місця сучасних методів блокування телефону, а саме дактилоскопічного сканера.

Дактилоскопічні сканери (thumbscanners, dactyloscopic scanners) - активно прогресуючий клас сканерів, заснований на зчитуванні відбитків пальців з відповідним кожному індивідууму папілярних візерунків з метою його автоматичної ідентифікації та прийняття певного рішення. Це зручний і швидкий спосіб розблокування. Якість в даному випадку означає швидкість, з якою сканер зможе розпізнати ваш палець і розблокувати смартфон. Що стосується безпеки, то це, мабуть, один з найбільш надійних методів тому що обійти захист дактилоскопічного сканера не так легко. На даний момент сканер відбитка пальця має найвищий захист. [1] Можна зустріти дактилоскопічні модулі таких типів:

• Оптичний
• Напівпровідниковий
• Ультразвуковий

Виробники використовують злегка різні один від одного за швидкістю і точністю алгоритми ідентифікації ключових характеристик відбитка. Зазвичай ці алгоритми «шукають» місце, де закінчуються бугорки і лінії або де бугорок розділяється на два. Ці та інші відмінні риси називаються шаблоном відбитка або детальним протоколом введення

відбитка. Якщо у відсканованому відбитку збігаються кілька таких особливостей, то відбиток буде зарахований як схожий. Замість того, щоб порівнювати кожен раз цілий відбиток, порівняння особливостей шаблону зменшує кількість необхідної для ідентифікації відбитка обчислювальної потужності, допомагає уникнути помилок при змазуванні відбитка і також дозволяє сканувати поміщений не по центру палець або взагалі лише частина відбитку. Злом датчика відбитків мають на увазі імітацію пальця, за допомогою якого можна розблокувати смартфон. Наскільки докладної і якісної повинна бути імітація, з якого матеріалу виконана - залежить від технології, на якій побудований датчик конкретної моделі смартфона. Так, ультразвукові датчики марно намагатися обійти за допомогою відбитка, роздрукованого з високою роздільною здатністю на спеціальній токопровідному папері, але стандартні ємнісні сканери таким чином перехитрити можна. [2]

Один з таких методів використали співробітники Університету штату Мічиган. Використовуючи спеціальні струмопровідні чорнила виробництва компанії AgIC, вони роздрукували на звичайному струменевому принтері різні зразки відбитків. За допомогою надрукованих "пальців" дослідникам вдалося без проблем розблокувати відразу два популярних смартфона - Samsung Galaxy S6 і Huawei Honor 7. Розблокування відбувається без будь-яких помилок – папірець з нанесеним на нього рисунком смартфони сприймають як звичайний палець. Єдиною умовою, за словами вчених, є точна відповідність роздруківки реальному розміру пальця.[3]

В роботі досліджено взламостійкість різних дактилоскопічних сканерів. Було виявлено що біометрична ідентифікація не є абсолютно надійною. Особливо на великих обсягах даних (тобто, при великій кількості користувачів), адже датчику треба буде порівнювати з великою кількістю відбитків і ймовірність того, що система ідентифікації дасть збій збільшується. Щоб захистити смартфон, не потрібно використовувати прості графічні ключі (шаблони фігур) для блокування екрану. Треба уникати посилань на імена, дати і загальні слова при використанні ПІН-коду і паролів. Вимикати всі функції, які дозволяють дати доступ до смартфону третій стороні. І найкраще – використовувати подвійний захист і мінімізувати кількість невдалих спроб розблокування.

Список використаних джерел

1. https://megabook.ru/article/%D0%94%D0%B
2. http://android.mobile-review.com/articles/discussion/41448/
3. https://rg.ru/2016/03/09/najden-prostoj-sposob-vzlomat-liuboj-smart-fon.html