ЕЛЕМЕНТ БЕЗПЕКИ NEAR FIELD COMMUNICATION

Вацлавик Олег, Маркевич Богдан

Львівський державний університет безпеки життєдіяльності, Львів, Україна

Summary. The security element on the SIM card can be directly connected to the NFC interface, even when the voltage is fed by the phone rather than the NFC interface instead. This allows the security element to work together with the NFC interface in card emulation mode, even when the battery of the phone is practically discharged.

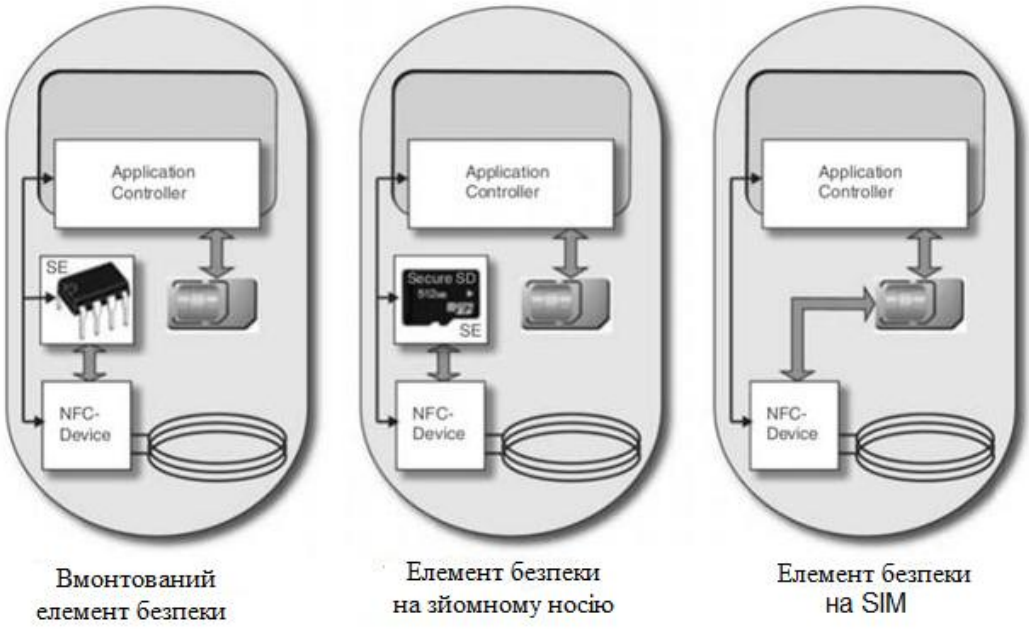
Keywords: security element, Near Field Communication, hardware module, operating system.

Деякі функції, які залежать NFC, наприклад, додатки для проведення платежу, або покупки електронних квитків вимагають, щоб дані які зберігаються в пам'яті були захищені, так як зловмисник потенційно може маніпулювати даними або читати їх з пам'яті. Дані, доступ до яких може отримати зловмисник, можуть бути дуже критичні - наприклад, відомості про банківську карту, отримавшидоступ до яких, зловмисник може створювати клони карт.

Тому ці критичні додатки повинні працювати в захищеному середовищі, бажано на окремому чіпі, а не в основному процесорі телефону. Елемент безпеки (ЕБ) являє собою комбінацію апаратних і програмних засобів, які забезпечують механізми захисту для підтримки безпечного середовища для зберігання і виконання.

ЕБ повинен мати операційну систему, в якій додатки встановлюються і використовуються (як правило, додатки встановлюються у вигляді JAVA-аплетів). Приклад таких ОС: MULTOS (Multi Application Card Operating System) або Java Card OS .

Існує кілька варіантів апаратних модулів, які можуть слугувати як елемент безпеки в смартфонах (Малюнок 1) :



Малюнок 1 - Варіанти апаратних модулів, що використовуються в якості ЕБ

Вбудований апаратний ЕБ може бути безпосередньо вбудований в телефон. Тому він не може бути видалений або переведений в інший девайс. Це рішення має деякі недоліки: права доступу до вбудованого ЕБ повністю контролюються виробником телефону і якщо вони строгі, то ЕБ не може навіть дозволити встановити користувальницькі додатки.

UICC (Universal Integrated circuit card) ЕБ міститься на SIM / USIM-карті мобільного телефону і може обслуговувати кілька додатків, випущених різними постачальниками додатків.

Знімний носій (наприклад, SD-карта) складається з пам'яті, вбудованої смарт-елемента карти і смарт-карти контролера. Він забезпечує такий же високий рівень безпеки, як смарт-карта і сумісний з більшістю основних стандартів для смарт-карт. Його переваги в тому, що він легко змінюється в діапазоні від телефону до телефону - на відміну від UICC, який пов'язаний з певним номером мобільного телефону.

Елемент безпеки містить операційну систему, яка дозволяє запускати кілька додатків у віртуальній машині поверх рідної ОС смартфона. Типова ОС використовується в ЕБ – JavaCard OS. Вона має фреймворк під назвою Java Card Runtime Environment (JCRE), який підтримує програми, реалізовані в обмеженої версії мови Java (підмножина конструкцій оригінального мови Java і бібліотечних функцій). Використання віртуальної машини дозволяє відокремити критично важливі дані, від всіх інших. Однак і тут є свої підводні камені.

Операційна система елемента безпеки може запускати обмежена кількість додатків і тримати в пам'яті обмежена кількість даних. Залишається питання, що буде з важливими даними, що містяться в пам'яті елемента безпеки, якщо необхідно буде зберегти нові дані, але місця в пам'яті для збереження не буде. Крім того, не виключена помилка розробника, який може не вказати, що його програма має запускатися з використанням елементу безпеки. Сам же елемент безпеки, не може розпізнавати додатки, які передають дані що підлягають захисту.

Література

1. Minihold R. Near Field Communication (NFC) Technology and Measurements. White Paper. – http:// eetimes.com/electrical-engineers/education-training/ tech-papers/secure/rohde-and-schwarz/4213132?isSurveySuccess=True
2. Fisher J. NFC in cell phones: the new paradigm for an interactive world. – IEEE Communications Magazine, 2009, v.46, №6, p.22.
3. Smart Posters: how to use NFC tags and readers to create interactive experiences that benefit both consumers and businesses. – April 2011, www.nfcforum.org/resources/white_papers/NFC_Smart_ Posters_White_Paper.pdf
4. Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications. – http:// www.nfc-forum.org/resources/white_papers/nfc_ forum_marketing_white_paper.pdf