

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ В СИСТЕМАХ БЕЗКОНТАКТНОЇ ПЕРЕДАЧІ ДАНИХ

Метик А.В., Северінов О.В.

Харківський національний університет радіоелектроніки, Харків, Україна

Технологія NFC стає популярною в сучасному світі та з кожним днем її застосування набирає обертів. На сьогоднішній день існує безліч напрямків, де застосовується NFC, наприклад безконтактна оплата в магазинах, оплата проїзду, контроль якості, контроль доступу та інше.

На даний час існує безліч загроз безпеці інформації при безконтактній передачі даних [1, 2]. Основні з них зчитування приватної інформації та доступ до майна. Проблемами використання NFC-систем є:

- застосування небезпечного протоколу UDP;
- відсутність шифрування транзакцій між хостом і клієнтом;
- відсутність легкої автентифікації хостів і користувачів;
- надання дозволів відповідно до звичайних правил доступу.

Метою доповіді є аналіз методів захисту інформації при безконтактній NFC-передачі даних. На основі проведеного аналізу були отримані основні вразливості системи NFC до атак, та методи захисту від даних атак на систему [3, 4]. Аналіз показав, що одним з найпростіших методів захисту від атак на систему NFC є маленька відстань між засобом зчитування та пристроєм або картою користувача. Але це ні в якій мірі не гарантує захисту даних.

Основним методом захисту NFC-передачі даних є створення захищеного каналу для NFC. Для створення загального секретного ключа між двома пристроями використовується стандартний протокол узгодження ключа Diffie-Hellmann з подальшим симетричним шифруванням 3DES або AES.

В якості додаткових методів захисту можуть використовуватись створення токенів при кожній передачі даних, а також використання специфічних протоколів формування ключів NFC.

Але на даний час методи захисту NFC-систем потребують подальшого вивчення та вдосконалення.

Список літератури

1. О.В. Северінов, В.М. Федорченко, В.І. Перепада. Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків. Системи озброєння і військова техніка, 4 (2016): 42-45.
2. О.В. Северінов, А.Г. Хренов, А.О. Поляков. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі. Системи обробки інформації, 9 (2015): 101-104.
3. Технология NFC в смартфонах и ее практическое использование [Электронный ресурс] - Режим доступа: <http://www.ixbt.com/mobile/nfc-2013.shtml>
4. What is NFC? Everything you need to know [Электронный ресурс]. - Режим доступа: <http://www.techradar.com>.