

УДК 621.396.2:004.0565

Куцак С.В.¹, Корольков Р.Ю.¹

¹ старш. викл. ЗНТУ

ОЦІНКА ЗАХИЩЕНОСТІ СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ

Стрімкий розвиток телекомунікаційних технологій та поява нових стандартів цифрового стільникового зв'язку значно розширили спектр послуг, які надаються мобільними мережами, починаючи з передачі голосової інформації і закінчуючи високошвидкісною пакетною передачею даних. Останні, використовуючи сучасні мобільні термінали (абонентські станції) і спеціальне програмне забезпечення, дають можливість користувачам повноцінно застосовувати їх для різного роду діяльності: ведення бізнесу (он-лайн покупки, банківські платежі), навчання, відео-конференції, ділові переговори тощо. При цьому важливо також зазначити, що надання нових послуг потребує впровадження нових механізмів та засобів захисту інформації.

В даній роботі проводиться аналіз захищеності найбільш поширених стандартів мобільного зв'язку, якими є GSM, UMTS та CDMA.

Аналіз вимог [1, 2] щодо забезпечення безпеки інформації дозволив визначити основні складові сучасної системи захисту мережі зв'язку: коректна тарифікація послуг, що надаються; конфіденційність персональних даних; конфіденційність потоку навантаження; моніторинг дій користувачів і функціонування мережі; захист ресурсів мережі; управління системою захисту.

В стандарті GSM можна виділити наступні механізми захисту:

- шифрування даних в радіоканалі: використовується криптосистема з відкритим ключем, що реалізується алгоритмом шифрування A8;
- автентифікація користувача: використовується модуль ідентифікації абонента (SIM-карта), персональні PIN- і PUK-код та алгоритм автентифікації абонента A3;
- перепризначення TMSI: міжнародний ідентифікатор абонента мобільного зв'язку (International Mobile Subscriber Identity – IMSI) для поточної роботи замінюється тимчасовим ідентифікатором TMSI (Temporary Mobile Subscriber Identity), який присвоюється мобільному терміналу при його першій реєстрації у конкретному регіоні, що визначається ідентифікатором LAI (Location Area Identity), і анулюється при виході апарату за межі цього регіону;
- ідентифікація обладнання: використовується IMEI (International Mobile Equipment Identity – міжнародний ідентифікатор мобільного обладнання) – серійний номер мобільного пристрою, який встановлюється заводом-виробником та є унікальним для кожного мобільного телефону.

Для підвищення захищеності зв'язку в GSM також застосовуються: скремблери, криптофони, інвертори спектру, генератори шуму тощо.

Архітектура системи безпеки UMTS охоплює чотири компоненти:

1. Access domain security (Безпека доступу до домену).
2. Network domain security (Доменна безпека мережі).
3. User domain security (Доменна безпека користувача).
4. Application domain security (Доменна безпека додатків).

У відповідності зі специфікаціями 3GPP, можливості, що забезпечують безпеку для UMTS повинні захищати інформацію, ресурси та сервіси, вироблені або замінені, у всій мережі, від неправильного використання.

Основний механізм безпеки в UMTS базується на моделі безпеки GSM. Безпека включає в себе:

1. Поділ модуля абонента від терміналу.
2. Автентифікація.
3. Шифрування.
4. Конфіденційність ідентифікації абонента.
5. Перевірка терміналу.
6. Загрози безпеки в мережах 3G.

Криптографічні протоколи стандарту CDMA ґрунтуються на 64-бітному ключі автентифікації (A-key) і серійному номері мобільного терміналу – Electronic Serial Number (ESN). CDMA використовує стандартизований алгоритм шифрування CAVE (Cellular Authentication and Voice Encryption) для генерації 128 бітного підключа SSD (Shared Secret Data). Для автентифікації абонента в CDMA мережі використовується допоміжний ключ

SSD_A генерований CAVE алгоритмом з A-key, ESN і RANDSSD (випадкове двійкове число). A-key може бути перепрошитий кількома способами: на заводі, дилером у точках продажу, абонентом через інтерфейс терміналу, а також за допомогою OTASP (Over the Air Service Provisioning – ефірна служба ініціалізації). OTASP забезпечує легкий спосіб зміни A-key мобільного терміналу на випадок появи в мережі двійника мобільного терміналу. Секретність A-key є найважливішою компонентою безпеки CDMA системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Величко В.В. Передача данных в сетях мобильной связи третьего поколения / В.В. Величко. – М.: Горячая линия – Телеком, 2005. – 332 с.
2. Жуков С. Хакинг мобильных телефонов / Сергей Жуков. – М.: Бук-пресс, 2006. – 224 с.