УДК 621.396.2
Кащук О. - ст. гр. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ ТРЕТЬОГО ПОКОЛІННЯ

Науковийкерівник: к.т.н., доцент Фриз М.Є.

Kashchuk O.
Ternopil Ivan Pul'uj National Technical University

ANALYSIS INFORMATION PROTECTION SYSTEMS THIRD GENERATION MOBILE COMMUNICATION

Supervisor: M.Fryz

Ключовіслова: ДАНІ, МЕРЕЖІ, БЕЗПЕКА.
Keywords: DATA, NETWORK, SECURITY.

На сьогодні існує досить багато різних систем зв'язку, які суттєво допомагають в роботі та повсякденному житті. Чільне місце серед них займають системи мобільного зв'язку. І зпоявою цих систем значно збільшився обмін та потік різноманітної інформації. Однак у системах мобільного зв'язку передавання інформації між мобільною й базовою станціями відбувається радіоканалом, що накладає досить жорсткі вимоги на забезпечення їхньої інформаційної безпеки, що реалізується на основі відповідних криптографічних алгоритмів. Оскільки інформація дуже важлива, а кількість людей бажаючих заволодіти нею досить велика, то її слід захищати. Тому стандарти системи мобільного зв'язку передбачають різноманітні механізми захисту інтересів законних користувачів і мережі від несанкціонованного доступу та незаконного використання інформації.

Мережі третього покоління 3G працюють на частотах дециметрового діапазону (близько 2 ГГц), швидкість передавання даних становить понад 2 Мбіт/с. Такі мережі надають можливість організувати відеозв'язок, дивитись на мобільному телефоні фільми й телепрограмми та ін. В світі існує два стандарти 3G: UMTS (чи W-CDMA) та CDMA-2000. UMTS більш розповсюджений в основному в Європі, CDMA2000 – в Азії та США.

Термін 3G використовується для опису сервісів мобільного зв'язку стандартів наступного покоління, які забезпечуються більш високу якість звуку, а також високошвидкісний інтернет-звязок та мультимедійні сервіси. Мобільні мережі третього покоління (3G) відрізняються від мереж другого покоління (2G), таких як наприклад цифровий стандарт мобільного звязку GSM, зв'язок перехідного покоління (2.5G) GRPS набагато більшою швидкістю передавання даних, а також більш широким набором і високою якістю послуг, що надаються.

Протоколи, що забезпечують безпеку передавання інформації в CDMA-IS-41 мережах, є одними з кращих в індустрії. Крім того сам CDMA стандарт за своєю

побудовою робить перехоплення сигналу і його розшифрування дуже складним і дорогим завданням доступним, фактично, тільки державним спецслужбам. Криптографічні протоколи стандарту CDMA грунтуються на 64-бітному аутентифікаційному ключі (A-key) і серійному номері мобільного телефону - ElectronicSerialNumber (ESN).

Для аутентифікації абонента в CDMA мережі використовується допоміжний ключ SSD_A генерований CAVE алгоритмом з A-key, ESN і RANDSSD. Мережа генерує і розсилає відкрито по ефіру випадкове число RAND *, мобільні пристрої, що реєструються в мережі, використовують його як вхідні дані для CAVE алгоритму, що генерує 18-бітний аутентифікаційний цифровий підпис (AUTH_SIGNATURE), і посилає його на базову станцію. Цей цифровий підпис звіряється в центрі комутації (далі згадується як MSC - MobileservicesSwitchingCenter) з підписом генерується самим MSC для перевірки легітимності абонента. Число RAND * може бути як одним і тим же для всіх користувачів, так і генеруватися щоразу нове (використання конкретного методу визначається оператором).

Перший випадок забезпечує дуже швидку аутентифікацію. І мобільний телефон і мережа ведуть 6-бітові лічильники викликів, що забезпечу ємможливість детектування працюючих двійників: для цього достатньо лише контролювати відповідність значень лічильників на телефоні та на MSC. Секретний ключ A-key є перепрограмувальний, в разі його зміни інформація на мобільному телефоні і в HLR / AC повинна бути синхронізована. A-key може бути перепрошитий кількома способами: на заводі, дилером у точках продажу, абонентом через інтерфейс телефону, а також за допомогою OTASP (overtheairserviceprovisionig). OTASP передавання використовує 512 бітний алгоритм узгодження ключів Diffie-Hellman'a, що гарантує достатню безпеку. OTASP забезпечує легкий спосіб зміни A-key мобільного телефону на випадок появи в мережі двійника мобільного телефону. Зміна A-key автоматично спричинить за собою відключення послуг двійнику мобільного телефону і повторне включення послуг легітимному абоненту. Таким чином, як можна було помітити, секретність A-key є найважливішою компонентою безпеки CDMA системи.

Таким чином було проаналізовано основні функції, та протоколи що забезпечують шифрування для захисту інформації в мобільних мережах третього покоління.Результати аналізу дозволять обгрунтовано використовувати мобільні мережі третього покоління при розробці відповідних інформаційних мереж, які їх використовують.

Список використанихджерел

1. Берлин А.Н. «Курс Сотовые системы связи Лекция №3 Многостанционный доступ с кодовым разделением и сети CDMA» -: Видавництво Вильямс 2011 р., 376 с., ISBN n/a