даних серверної частини. В середньому атаки, які посилають більше ніж 100 запитів в секунду можуть вимкнути сайти середніх розмірів.

Все сказане дозволяє зробити висновок, що різні види атак можуть залишити різні цифрові сліди, а отже буде легше зрозуміти, де їх шукати.

Список використаних джерел

1. Світличний В. А. Дослідження атак на відмову в обслуговуванні інформаційно-телекомунікаційних систем // Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. Одеса : ОДУВС, 2018. С. 88-89.

2. DDoS-атака: что это, как работает и виды атак // VPS.ua : сайт. 27.08.2018. URL: https://vps.ua/blog/ddos-attacks-and-their-types/ (дата звернення: 19.11.2020).

Одержано 21.11.2020

УДК 621.34

Скарбенчук Ірина Віталіївна
студентка 4 курсу факультету № 6
Харківського національного університету внутрішніх справ
Тулупов Володимир Володимирович
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-4794-743X

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ МЕРЕЖАХ РУХОМОГО ЗВ'ЯЗКУ

В основі забезпечення захисту інформації в мережах рухомого зв'язку лежать законодавчі та нормативно-правові норми, морально-етичні звичаї суспільства, організаційні та апаратно-програмні засоби та способи функціонального забезпечення інформаційної безпеки цифрових систем, каналів, мереж зв'язку.

Необхідно зауважити, що забезпечення надійного захисту інформації в мережах рухомого зв'язку перш за все, залежить від наявності певних чинників, які безпосередньо забезпечують та впливають на ступінь захищеності інформації в мережі, а саме:

– врахування особливостей відповідної технології зв’язку в процесі розробки необхідної моделі комплексного захисту інформації згідно способів та властивостей передавання/приймання фізичного сигналу, самого фізичного середовища – каналу, мережі, апаратно-програмних засобів цифрових систем зв’язку;

– наявність математичної моделі сигналу або каналу, в якій закладено параметри якісного і кількісного рівнів взаємозв’язку вхідного і вихідного сигналу.

У розвинених країнах світу продовжується перехід до інформаційної сервісно-технологічної економіки. Враховуючи особливості кожного стандарту необхідно використовувати притаманні лише йому технології, методи та засоби захисту інформації.

Найпоширенішим стандартом стільникового зв’язку в Україні є стандарт зв'язку четвертого покоління LTE (Long Term Evolution), який вважається перспективним. За даними, наприклад компанії HUAWEI, LTE забезпечує швидкість до 326,4 Мбіт/с від базової станції до користувача і до 172,8 Мбіт/с у зворотному напрямку.

З точки зору безпеки таких LTE мереж враховуючи різні технології ускладнює пошук її вразливостей. В мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) за протоколом IP.

З фізичної точки зору в мережах LTE використовуються великі смуги частот, високорівнева модуляція сигналу, технологія MIMO (Multiple Input Multiple Output) яка дозволяє збільшити смугу пропускання каналу, при якому для передачі даних використовуються дві і більше антени і така ж кількість антен для прийому. Разом вони забезпечують адекватну завадостійкість, високі швидкості передачі даних і ємність мережі. Важливою особливістю мережі 4G є те, що з її архітектури зникло поняття контролера радіомережі (RNC), який в 3G виконував основну функцію з управління комунікаційними ресурсами. Тому базові станції в LTE стали більш інтелектуальними і самостійними - вони отримали можливість маршрутизувати трафік, що дозволило організовувати

з'єднання між абонентами безпосередньо, минаючи ядро мережі. Щоб звести до мінімуму атаки на конфіденційну інформацію, базова станція повинна забезпечити виконання таких важливих операцій, як кодування та розшифрування користувачів даних, а також зберігання ключів.

Стандарт LTE виділяє п'ять основних груп безпеки це, насамперед:

– архітектура безпеки мережі повинна забезпечити користувачів надійним доступом до сервісів і захист від атак на інтерфейси;

– мережевий рівень повинен дозволяти вузлам мережі безпечно обмінюватися як даними користувачів, так і керуючими даними і забезпечувати захист від атак на провідні лінії;

– користувальницький рівень повинен забезпечувати безпечний доступ до мобільного пристрою;

– рівень додатків повинен гарантувати безпечний обмін повідомленнями;

– видимість і можливість зміни налаштувань безпеки повинна дозволяти користувачеві дізнаватися, чи забезпечується безпека і включати різні режими для її забезпечення.

Щодо методів захисту, необхідно зауважити, що багатьма країнами та операторами стільникового зв’язку активно використовується шифрування (RSA), яке в подальшому вимагає коди автентифікації абонента. З точки зору безпеки таких LTE мереж враховуючи різні технології ускладнює пошук її вразливостей. В мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) за протоколом IP.

З фізичної точки зору в мережах LTE використовуються великі смуги частот, високорівнева модуляція сигналу, технологія MIMO (Multiple Input Multiple Output) яка дозволяє збільшити смугу пропускання каналу, при якому для передачі даних використовуються дві і більше антени і така ж кількість антен для прийому. Разом вони забезпечують адекватну завадостійкість, високі швидкості передачі даних і ємність мережі.

Важливою особливістю мережі 4G є те, що з її архітектури зникло поняття контролера радіомережі (RNC), який в 3G виконував основну функцію з

управління комунікаційними ресурсами. Тому базові станції в LTE стали більш інтелектуальними і самостійними - вони отримали можливість маршрутизувати трафік, що дозволило організовувати з'єднання між абонентами безпосередньо, минаючи ядро мережі.

Щоб звести до мінімуму атаки на конфіденційну інформацію, базова станція повинна забезпечити виконання таких важливих операцій, як кодування та розшифрування користувачів даних, а також зберігання ключів.

Стандарт LTE виділяє п'ять основних груп безпеки це, насамперед:

– архітектура безпеки мережі повинна забезпечити користувачів надійним доступом до сервісів і захист від атак на інтерфейси;

– мережевий рівень повинен дозволяти вузлам мережі безпечно обмінюватися як даними користувачів, так і керуючими даними і забезпечувати захист від атак на провідні лінії;

– користувальницький рівень повинен забезпечувати безпечний доступ до мобільного пристрою;

– рівень додатків повинен гарантувати безпечний обмін повідомленнями;

– видимість і можливість зміни налаштувань безпеки повинна дозволяти користувачеві дізнаватися, чи забезпечується безпека і включати різні режими для її забезпечення.

Список використаних джерел

1. Ткаченко О. С., Тулупов В. В. Безпечне використання сучасного стандарту LTE у мережах рухомого зв’язку // The 1st International scientific and practical conference «Science, society, education: topical issues and development prospects» (December 16-17, 2019) SPC «Sci-conf.com.ua». Kharkiv : 2019. С. 276-280. URL: https://sci-conf.com.ua/wp-content/uploads/2020/01/science-society-education_topical-issues-and-development-prospects_16-17.12.2019.pdf (дата звернення: 12.11.2020).

Одержано 20.11.2020