УДК 621.34

Володимир Володимирович ТУЛУПОВ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Олександр Сергійович ТКАЧЕНКО,
студент 3 курсу факультету № 6
Харківського національного університету внутрішніх справ

БЕЗПЕКА СУЧАСНИХ МЕРЕЖ РУХОМОГО ЗВ'ЯЗКУ СТАНДАРТУ LTE

У розвинених країнах світу продовжується перехід до інформаційної сервісно-технологічної економіки. Метою створення стандарту LTE є збільшення можливостей високошвидкісних систем мобільного зв'язку, зменшення вартості передачі даних, можливість надання широкого спектру недорогих послуг.

Мобільний зв'язок четвертого покоління передбачає використання цілого спектру технологій, які раніше розвивалися паралельно. Всі вони внесли свій внесок у специфікацію LTE реалізованої в двох основних варіантах технологій: з дуплексним частотним поділом LTE-FDD (Frequency Division Duplex) і часовим поділом LTE-TDD (Time Division Duplex) [1].

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 та самостійними. 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 наступні 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.

Є також проблеми і з самим стандартом. По-перше, дуже гостро стоїть завдання взаємодії з не LTE мережами. Якщо трафік між користувальницьким обладнанням і базовою станцією шифрується (це вимога стандарту) і загроза порушення конфіденційності стає неактуальною, то взаємодія базової станції з радіоконтролером мережі 3G по умовчанню ніяк не захищене а, отже, це пролом для можливих атак з боку зловмисників. По-друге, відсутність обов'язкової аутентифікації між ядром мережі і базовою станцією. Цю опцію оператор зв'язку для зниження своїх витрат щодо розгортання мережі LTE може і не задіяти зовсім. Не можна забувати і про обмеження LTE. Наприклад, збільшення швидкості підключення зазвичай обертається зменшенням радіусу дії базової станції, який в середньому для 4G становить близько 5 км і залежить від використовуваного частотного діапазону. Тому базових станцій в мережі стає більше, і вони розташовуються ближче одна до одної [1].

Ще одна особливість LTE в тому, що ця технологія орієнтована на підключення інтелектуальних пристроїв, з поширенням яких число потенційно небезпечних сервісів буде тільки зростати, що дозволить зловмисникам отримати доступ до конфіденційної інформації провайдера і побудувати нові витончені схеми інформаційних злочинів.

Всі функції захисту в LTE об'єднані стандартом і передбачають захист на декількох рівнях: на рівні доступу до мережі, на рівнях мережевого і користувальницького доменів, на рівні додатків та на рівні відображення і конфігурацій [2].

Кожен з цих рівнів передбачає аутентифікацію і авторизацію всіх пристроїв, чого немає в Інтернеті. Технологія LTE передбачає використання не тільки IP-адреси, але і системи розповсюдження ключів шифрування для всіх пристроїв, підключених до мережі з можливістю переходу зі 128 до 256-бітові ключі і введення нових алгоритмів, зберігаючи зворотну сумісність.

Крім алгоритмів шифрування і забезпечення комплексної безпеки в мережах 4G використовуються додаткові алгоритми, які навіть за умови того, що один з них буде зламаний, решта забезпечать безпеку мережі LTE. Крім того, в LTE зберігаються і методи аутентифікації користувачів по прив'язці до SIM карти, як в традиційному мобільному зв'язку. Користувач може заблокувати доступ до телефону з PIN-кодом.

Таким чином, виходячи з вищенаведеного, головною особливістю з точки зору захисту абонента розглянутого стандарту четвертого покоління рухомого зв'язку LTE, процес обслуговування приховується тимчасовими ідентифікаторами у відмінності з попередніми поколіннями зв'язку.

Список бібліографічних посилань

1. Ткаченко О. С., Тулупов В. В. Безпечне використання сучасного стандарту LTE у мережах рухомого зв'язку // Science, society, education: topical issues and development prospects. Abstracts of the 1st International scientific and practical conference. SPC "Sci-conf.com.ua". Kharkiv, Ukraine. 2019. Pp. 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: 09.03.2020).
2. Наконечний В. С. Захист інформаційних ресурсів у мережах нового покоління LTE. *Сучасний захист інформації.* 2016. № 4. С.10–15. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1242/1177 (дата звернення: 09.03.2020).

Одержано 30.04.2020