звукова система приєднані двостороннім зв'язком, тому контролер може як відправляти команди, так і отримувати дані.

Клієнти різних операційних систем і платформ мають зв'язок тільки до контролера, і не під'єднані безпосередньо до датчиків і пристроїв. Саме це і дозволяє забезпечити абстрактність і гнучкість системи.

Література:

1. 9 DIY Smart Home Automation Projects for a Shoestring Budget https://www.makeuseoF. com/tag/budget-smart-home-projects/.
2. OpenHAB Distribution https://github.com/openhab/openhab-distro.

ВРАЗЛИВОСТІ МЕРЕЖ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Гарист А. В.

начальник відділу

Українського науково-дослідного інституту спеціальної техніки

та судових експертиз Служби безпеки України

м. Київ, Україна

Незважаючи на появу мереж нового покоління 4G, які використовують іншу систему сигналізації Diameter, проблеми безпеки протоколу SS7 будуть залишатися актуальними ще довгий час, так як оператори зв'язку все ще повинні забезпечувати підтримку стандартів 2G та 3G, а також взаємодію між мережами різних поколінь. Більш того, дослідження доводять, що протокол Diameter схильний тим же загрозам, що і SS7.

Адресація вузлів в мобільному зв'язку при взаємодії між операторами відбувається не за IP-адресами, а за адресами Global Title, формат яких нагадує телефонні номери. Адреси Global Title в обов'язковому порядку повинні входити в діапазон телефонних номерів, закріпленими за оператором зв'язку, а якщо на національному рівні діапазони розбиваються по регіонах, то і адреси Global Title вузлів мережі повинні відповідати регіональним діапазонам.

Для взаємодії вузлів ядра мобільного оператора використовується протокол MAP – Mobile Application Part. Протокол MAP націлений на реалізацію функцій, які властиві саме мережі мобільного зв'язку, такі як аутентифікація і реєстрація мобільного апарату в мережі, локалізація абонента для здійснення вхідного виклику, підтримка безрозривного

мовного каналу зв'язку при пересуванні абонента. Кожній операції відповідають певні повідомлення протоколу MAP зі своїм набором параметрів.

Для мобільних комунікацій використовуються телефонні номери, які називаються MSISDN – Mobile Subscriber Integrated Services Digital Network Number. Цей номер присвоюється абоненту при укладанні договору з мобільним оператором. Але в надрах мережі зв'язку абоненти адресуються за ідентифікатором – IMSI (International Mobile Subscriber Identity), який прив'язується до конкретної SIM-карти. Переважна більшість операцій вимагають адресації абонента саме по IMSI, отже, для проведення більшості атак, спрямованих на конкретного абонента, зловмиснику в першу чергу потрібно дізнатися цей ідентифікатор.

Потрібно також зазначити, що в протоколах SS7 не закладені можливість аутентифікації вузлів, фільтрації повідомлень за списками доступу, динамічна маршрутизація нових вузлів мережі.

Для здійснення атаки на протокол SS7 зловмисник підключається до сигнальної мережі SS7 і відправляє службову команду Send Routing Info в мережевий канал, вказуючи номер телефону абонента, який атакується в якості параметра. Домашня абонентська мережа відправляє у відповідь наступну технічну інформацію: IMSI і адресу MSC, по якій надаються послуги підписнику.

Після цього зловмисник змінює адреси білінгової системи в профілі підписника на свої власні адреси псевдобілінгової системи. Як відомо, ніяку перевірку така процедура не проходить. Далі атакуючий вводить оновлений профіль в базу даних VLR через повідомлення «Insert Subscriber Data».

Коли абонент, якого атакують здійснює вихідний дзвінок, його комутатор звертається до системи зловмисника замість фактичної білінгової системи. Система зловмисника відправляє комутатору команду, що дозволяє перенаправити виклик третій стороні, яка контролюється зловмисником.

В сторонньому місці встановлюється конференц-зв'язок між трьома підписниками, два з них є реальними (абонент А і абонент В), а третій вводиться зловмисником незаконно і здатний прослуховувати і записувати розмову.

Відповідним чином зловмисник має можливість отримати і SMS повідомлення, вказавши свій MSC/VLR. Таким чином можна зібрати одноразові SMS-паролі для двухетапної авторизації в різних сервісах. SMS вимагає від MSC/VLR підтвердження його доставки, і якщо його не відправляти, а замість цього перереєструвати абоненту на «справжній» MSC, то через кілька хвилин буде зроблена ще одна спроба доставки повідомлення і воно надійде адресату. Тобто одне і те ж SMS буде відправлено два рази: спочатку зловмиснику, а потім адресату.

Перехоплення повідомлень та прослуховування телефонної розмови можна виконувати за допомогою IMSI-перехоплювачів. Вони налаштовуються таким чином, щоб мобільний телефон жертви вважав, що це єдине доступне з'єднання, так як віддають перевагу тій стільниковій вишці, чий сигнал найбільш сильний для того, щоб максимізувати якість сигналу і мінімізувати власне енергоспоживання.

Крім того, в мережах GSM (2G) тільки мобільний телефон повинен проходити процедуру аутентифікації, від стільникової вишки цього не потрібно, тому його легко ввести в оману, в тому числі щоб відключити на ньому шифрування даних.

Деякі мобільні телефони навіть в режимі LTE виконують команди без попередньої аутентифікації, хоча стандарт LTE до цього зобов'язує. Крім того, оскільки LTE-інтерфейс розроблявся як модернізація UMTS-інтерфейсу, який є модернізованим GSM-інтерфейсом, то його структура не бездоганна. Крім того, незважаючи на широке поширення мереж 3G і 4G, мережі 2G як і раніше забезпечують резервний доступ, якщо 3G і 4G стають недоступними.

Атаки можливі із-за недоліків, які вбудовані в сам стандарт LTE. Сама серйозна слабкість – це форма шифрування, яка не захищає цілісність даних. Відсутність аутентифікації даних дозволяє зловмисникам непомітно маніпулювати IP-адресами в зашифрованому пакеті.

Висновки.

На сьогоднішній день вдалося скоротити ризики витоку інформації про мережу і абонента із впровадженням системи SMS Home Routing, яка здійснює фільтрацію повідомлень. Наразі із цим мережі мобільного зв'зку використовують системи фільтрації і блокування сигнального трафіку.

Тільки комплексний підхід до рішення проблем безпеки, який включає регулярний аналіз захищеності, підтримання параметрів мережі в актуальному стані, постійний моніторинг сигнального трафіку і своєчасне виявлення нелегітимної активності, може забезпечити високий рівень захисту від злочинців.

Література:

1. Positive Technologies, Уязвимости сетей мобильной связи на основе SS7, [Електронний ресурс]. – Режим доступу: http://www.ptsecurity.ru/download/PT_SS7_security_2014_rus.pdf

2. Tobias Engel (2008), Location Mobile Phones using SS7-25. Chaos Communication Congress, [Електронний ресурс]. – Режим доступу:http://media.ccc.de/v/25c3-2997-en-locating_mobile_phones_using_ss7