Тема 15. Захист інформації в стільниковій мережі

Атака типу man-in-the-middle (MITM), що буквально означає «людина посередині» – це тип кібер-атаки, при якому зловмисники перехоплюють розмову або передачу даних шляхом підслуховування, або прикидаючись його легальним учасником. Жертві здаватиметься, що відбувається стандартний обмін інформацією, але, вставивши себе в «середину» схеми забезпечення розмови чи передачі, зловмисник може непомітно перехопити інформацію.

Метою MITM-атаки є отримання конфіденційних даних, таких як дані банківського рахунку, номери банківських карток або облікові дані для входу, які можуть бути використані для скоєння подальших злочинів, таких як крадіжка особистих даних або незаконні перекази коштів. Оскільки MITM-атаки здійснюються в режимі реального часу, вони часто залишаються непоміченими, поки не стає занадто пізно.

Успішна MITM-атака включає дві конкретні фази: перехоплення і дешифрація.

Перехоплення передбачає, що зловмисник втручається в процес передачі даних з/в мережу жертви, перехоплюючи їх за допомогою «підставної» мережі, перш ніж дані будуть реально відправлені адресату або надійдуть до мережі жертви. Фаза перехоплення - це, по суті, те, як зловмисник вводить себе як "людину посередині". Зловмисники часто роблять за допомогою створення в громадському місці підробної точки доступу Wi-Fi, для підключення до якої не потрібний пароль. Якщо жертва підключається до такої «підставної» точки доступу, то зловмисник отримує доступ до будь-якого онлайн-обміну даними, який вона виконує.

Як тільки зловмисник успішно вклиниться між жертвою та іншою бажаною стороною обміну інформації, він зможе використати різні методи для продовження атаки:

- IP-спуфінг (підміна IP-адрес): Кожен пристрій, підключений до Wi-Fi, має свою адресу Інтернет-протоколу (IP), який відіграє центральну

роль у тому, як взаємодіють комп'ютери та пристрої в мережі. Спуфінг (підміна) IP-адрес передбачає, що зловмисник змінює IP-пакети, щоб видати себе за комп'ютерну систему жертви. Коли жертва намагається отримати доступ до URL-адреси, підключеної до цієї системи, вона неусвідомлено відправляється на сайт зловмисника.

- ARP-спуфінг: Під час заміни протоколу дозволу адрес (ARP) зловмисник використовує фальсифіковані повідомлення ARP, щоб зв'язати свою MAC-адресу з легальною IP-адресою жертви. Підключивши свою MAC-адресу до IP-адреси жертви, зловмисник отримує доступ до будь-яких даних, відправлених на її IP-адресу.
- DNS-спуфінг: Підміна сервера доменних імен (DNS), також відома як «отруєння» DNS-кешу, передбачає, що зловмисник змінює IP-адресу DNS-сервера, щоб мати можливість перенаправляти веб-трафік жертви з передбачуваного реального веб-сайту на шахрайський веб-сайт, який дуже схожий на оригінальний. У цьому випадку жертва впевнена, що вона підключається до оригінального веб-сайту, і якщо жертва авторизується за допомогою свого облікового запису, то зловмисники зможуть отримати доступ до персональних, реєстраційних даних та іншої конфіденційної інформації.

MITM-атака не зупиняється лише фазі перехоплення. Після того, як зловмисник отримає доступ до зашифрованих даних жертви, вони повинні бути розшифровані, щоб зловмисник міг їх прочитати та використовувати у своїх шкідливих цілях. Для розшифровки даних жертви може бути використаний ряд методів без попередження користувача або появи в програмі жертви будь-якого попередження:

- Підміна HTTPS (HTTPS-спуфінг): Підміна HTTPS - це метод обману вашого браузера, в результаті якого браузер «вважає», що веб-сайт, що завантажується, безпечний і автентичний, хоча це не так. Коли жертва намагається підключитися до захищеного сайту, до її браузера надсилається підроблений сертифікат, який натомість приводить

жертву на шкідливий веб-сайт зловмисника. Це дає зловмиснику доступ до будь-яких даних, якими жертва ділиться на цьому сайті.

– Перехоплення SSL (SSL Hijacking): Щоразу, коли ви підключаєтеся до незахищеного веб-сайту, адреса якого в полі для URL-адреси починається з «HTTP», ваш сервер автоматично перенаправляє вас на захищену версію HTTPS цього сайту. При перехопленні SSL зловмисник використовує свій власний комп'ютер і сервер для перехоплення цього перенаправлення, що дозволяє йому переривати будь-яку інформацію, передану між комп'ютером користувача та сервером. Це дозволяє кібер-злочинцеві отримати доступ до будь-якої конфіденційної інформації, яку користувач використовує під час свого підключення до цього веб-сайту.
– SSL Stripping: SSL stripping передбачає, що зловмисник перериває з'єднання між користувачем та веб-сайтом. Це робиться шляхом зниження рівня захищеного HTTPS-з'єднання користувача до небезпечної HTTP-версії веб-сайту. У цьому випадку користувача підключають до незахищеного сайту, тоді як зловмисник підтримує з'єднання із захищеним сайтом, роблячи дії користувача видимими для зловмисника навіть у незашифрованому вигляді.

Нижче наведено низку можливих заходів, які допоможуть підвищити безпеку мобільних додатків, захистивши їх від сторонніх впливів, покращивши продуктивність.

– Увага на життєвий цикл програми! Він поділяє процес розробки на кілька стадій, на кожній з яких автоматично виконується аудит безпеки, що дозволить виявити вразливість ще на етапі створення програми;
– Зупиняйте розробку під час виявлення серйозних загроз. Важливо миттєво реагувати на появу подібних недоліків і відразу ж працювати над їх усуненням;

– Забезпечте додаток сумісністю з актуальними стандартами безпеки – OWASP Top-10 та SANS 25. Вони надають інформацію про всі можливі вразливості та небезпеки у сфері мобільних пристроїв;
– Проводьте пентести (тестування на проникнення). Вони дозволять ідентифікувати можливі проблеми шляхом імітації атак хакерів. Бажано виконувати ці дії після кожного оновлення.