ПЕРЕХВАТ, ОТСЛЕЖИВАНИЕ И МОДИФИКАЦИЯ СЕТЕВОГО ТРАФИКА В УСТРОЙСТВАХ НА БАЗЕ ОС ANDROID

Желенок Д.А.

Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники
г. Минск, Республика Беларусь

Савенко А.Г. – старший преподаватель, м.т.н.

Аннотация. Данная работа описывает основные аспекты, связанные с настройкой окружения для анализа сетевого трафика, а также предоставляет описание для набора средств, позволяющих автоматизировать конфигурирование.

Нередко специалистам по информационной безопасности и реверс-инженерам необходимо анализировать сетевой трафик, создаваемый как операционной системой, так и отдельными приложениями. Анализ трафика в устройствах на базе операционной системе Android требует особую конфигурацию окружения. Обычно настройка сводится к 3 действиям: добавлению SSL сертификата в системное хранилище, настройке проксирования трафика через хост устройство и снятию привязки сертификата с приложения для которого планируется проводить мониторинг. Каждый из пунктов подробнее разобран ниже. Также описаны разработанные программы автоматизирующие основную часть работы.

Большинство приложений использует протокол HTTPS для взаимодействия по сети. HTTPS проверяет подключения, используя SSL сертификаты [1]. Это усложняет задачи, связанные с отслеживанием сетевых запросов. Чтобы это обойти, необходимо добавить в системное хранилище сертификат от приложения, через которое планируется вести перехват трафика. У Android также есть хранилище для пользовательских сертификатов, но поскольку не все приложения его используют, самым надёжным способом является добавление напрямую в систему. В разных версиях Android это делается разными путями. Чтобы упростить задачу было разработано приложение adb-install-certificate, которое производит преобразование сертификата в формат, понимаемый Android, определяет через adb [2] версию операционной системы и добавляет новый сертификат в системное хранилище. Для Android с версией 10 и выше, добавление можно делать только временное, после перезагрузки устройства необходимо устанавливать сертификат заново.

После установки сертификата необходимо настроить проксирование трафика, чтобы он шёл через приложение, которое сможет его перехватить, отобразить и переслать дальше. Для этого хост-устройство и Android-устройство должны находиться в одной сети. В настройках системы в качестве прокси выставляется адрес хоста и затем на хосте запускается приложение для перехвата трафика. Если всё настроено верно, то приложение будет отображать сетевую активность, которая происходит в данный момент. Для упрощения этого шага была разработана программа adb-proxy-wrapper которая проверяет что Android устройство имеет доступ к хосту, устанавливает через adb в качестве системного прокси свой IP-адрес и запускает переданную программу для перехвата. После его завершения происходит автоматический сброс прокси, чтобы устройство могло нормально функционировать. Также предоставлена программа mitm-workflow которая делает всё то же самое, но автоматически запускает mitmproxy. Mitmproxy – это набор утилит, предоставляющий прокси для перехвата трафика идущего через протоколы HTTP/1, HTTP/2 и WebSockets [3].

Некоторые приложения применяют привязку SSL-сертификата. Все запросы проверяются не с использованием системного хранилища сертификатов, а с использованием определённого, заданного на этапе разработки [4]. Это усложняет перехват трафика и требует выполнения отвязки сертификата. Поскольку доступа к коду приложения обычно нет, необходимо подменить его во время

выполнения. Для этого воспользуемся технологией Frida, которая позволяет перехватывать поток выполнения программы и вызывать другой код, описанный на языке программирования javascript [5]. В рамках этой работы была разработана программа frida-unpinning которая автоматически запускает Frida и использует распространённые способы отвязки сертификата для указанного приложения. После его запуска, целевое приложение будет использовать системное хранилище, что позволит отслеживать трафик.

Список использованных источников:

1. HTTPS mdn web docs [Электронный ресурс]. - Режим доступа: https://developer.mozilla.org/en-US/docs/Glossary/https - Дата доступа: 05.04.2022.

2. Android Debug Bridge (adb) [Электронный ресурс]. - Режим доступа: https://developer.android.com/studio/command-line/adb - Дата доступа: 05.04.2022.

3. Mitmproxy [Электронный ресурс] — Режим доступа: https://docs.mitmproxy.org/stable/ - Дата доступа: 05.04.2022.

4. SSL Certificate Pinning [Электронный ресурс] — Режим доступа: https://developer.android.com/training/articles/security-ssl#Pinning — Дата доступа: 05.04.2022.

5. Frida Dynamic Instrumentation Toolkit [Электронный ресурс] – Режим доступа: https://frida.re/docs/home/ - Дата доступа: 05.04.2022