Лабораторная работа 1

Освоение функциональных возможностей программ для анализа сетевого трафика

1. Цель работы

Приобретение навыков по использованию основных программных инструментов анализа сетевого трафика.

2. Применяемое оборудование, ПО и данные

1) Персональный компьютер с ОС Windows, ОС Linux или ОС MacOS
2) ПО Wireshark
3) Подготовленный дамп SIP_CALL_RTP_G711.pcap

3. Порядок выполнения работы

3.1. Установить ПО Wireshark с официального сайта (https://www.wireshark.org/#download)

3.2. Открыть файл SIP_CALL_RTP_G711.pcap.

3.3. Ознакомиться с интерфейсом программы, всеми вкладками и основными рабочими областями.

3.4. Использовать фильтры:

- по адресу источника;
- по адресу получателя;
- по обоим адресам;
- по порту источника;
- по порту получателя;
- по обоим портам;
- по протоколам (UDP, TCP, RTP, SIP).

3.5. Построить графики потока (флоу-графы).

3.6. Построить графики входа/выхода (IO-графы).

3.7. Проанализировать джиттер.

4. Последовательность обработки результатов

Представить результаты работы, в следующем формате.

Вставить соответствующий скриншот

Рис. <*Номер рисунка*> — Название

Указать инструмент, использованный для получения.

5. Сделать выводы

Особенности процедуры анализа сетевого трафика:

- в чем заключается процедура;
- какие данные используются для анализа;
- в каком виде представляются результаты анализа.

Структура и функции программных инструментов анализа сетевого трафика:

- какую структуру имеют инструменты анализа сетевого трафика;
- какие функции выполняют инструменты анализа сетевого трафика;
- для каждой функции привести название и описать в чем заключается.

Лабораторная работа 2

Изучение технологии VoIP, принципов работы и основных протоколов

1. Цель работы

Приобретение навыков по использованию основных программных инструментов анализа сетевого трафика VoIP.

2. Применяемое оборудование, ПО и данные

1) Персональный компьютер с ОС Windows, ОС Linux или ОС MacOS
2) ПО Wireshark
3) Записанный дамп SIP_CALL_RTP_G711.pcap

3. Порядок выполнения работы

3.1. Открыть в Wireshark файл SIP_CALL_RTP_G711.pcap.

3.2. Проанализируйте все звонки данного дампа. Telephony → SIP Flows (Телефония → Потоки SIP).

3.3. Для всего RTP-потока проанализируйте важнейшие параметры: потери, задержки, вариация задержки. Telephony → RTP → RTP Streams → Analyse (Телефония → RTP → Потоки RTP → Анализировать).

3.4 Рассмотреть основные поля SIP-сообщения INVITE, которое отправляется для установления VoIP-вызова, т.е. является исходной точкой для анализа.

Обычно SIP INVITE включает от 4 до 6 полей с информацией, которая используется оконечными SIP-устройствами (телефонами, шлюзами) и операторами связи. Понимание содержимого INVITE и следующих за ним сообщений часто помогает определить источник проблемы. Кроме того, знание полей INVITE помогает при подключении SIP-операторов к 3CX или объединении 3CX с другими SIP АТС.

В сообщении INVITE пользователи (или SIP-устройства) определяются по URI. Обычно SIP URI – это номер телефона пользователя + адрес SIP сервера. SIP URI очень похож на e-mail адрес и записывается как sip:x@y:Port.

Request-Line-URI — поле содержит получателя вызова. В нем содержится та же информация, что и в поле To, но без отображаемого имени пользователя (Display Name).

Via — каждый SIP-сервер (прокси), через который проходит запрос INVITE, добавляет вверху списка Via свой IP-адрес и порт, на который было получено сообщение. Затем сообщение передается дальше по пути следования. Когда конечный получатель отвечает на запрос INVITE, все транзитные узлы «просматривают» заголовок Via и возвращают сообщение отправителю по тому же маршруту. При этом транзитный SIP-прокси удаляет свои данные из заголовка.

From — заголовок указывает на инициатора запроса с точки зрения SIP-сервера. Заголовок формируется таким же образом, как e-mail адрес (user@domain, где user — добавочный номер пользователя 3CX, a domain — локальный IP-адрес или SIP-домен сервера 3CX). Как и заголовок To, заголовок From содержит URI и, опционально, отображаемое имя пользователя Display Name. По заголовку From можно понять, как именно следует обрабатывать этот SIP-запрос.

Стандарт SIP RFC 3261 предусматривает, что если отображаемое имя Display Name не передается, IP-телефон или VoIP-шлюз (UAC) должны использовать Display Name «Anonymous», например, From: «Anonymous» <sip:10000@10.172.0.2>.

To — этот заголовок указывает на получателя запроса. Это может быть как конечный получатель вызова, так и промежуточное звено. Обычно в заголовке содержится SIP URI, однако возможны и другие схемы. Однако SIP URI должен поддерживатся во всех имплементациях протокола SIP, независимо от производителя оборудования. Заголовок To

также может содержать отображаемое имя Display Name, например, To: «Имя Фамилия» <sip:101@10.172.0.2>).

Обычно поле To содержит SIP URI, указывающий на первый (следующий) SIP-прокси, который будет обрабатывать запрос. Это не обязательно должен быть конечный получатель запроса.

Contact — заголовок содержит SIP URI, по которому можно связаться с отправителем запроса INVITE. Это обязательный заголовок, который должен содержать только один SIP URI. Он является частью двусторонней коммуникации, соответствующей первоначальному запросу SIP INVITE. Весьма важно, чтобы заголовок Contact содержал корректную информацию (включая IP-адрес), по которому отправитель запроса ожидает ответа. URI Contact используется и в дальнейших коммуникациях, уже после установления сеанса связи.

Call-ID — уникальный идентификатор сеанса связи или всех регистраций отдельного клиента. Его значение задаётся стороной, инициирующей вызов. Содержит буквенно-числовое значение, символ-разделитель (@) и имя рабочей станции, которая присвоила это значение (например, 123abc@site.domen.ru). Следует указать, что если с одной мультимедийной конференцией связано несколько соединений, то каждое из них будет иметь собственный Call-ID.

CSeq — уникальный идентификатор запроса, связанного с одним соединением. Используется для корреляции запросов и ответов. Содержит числовое значение (от 1 до 232) и текстовое указание типа запроса (например, 2 INVITE).

Record-route используется прокси-сервером, если он желает, чтобы все последующие запросы проходили через него. В таком случае прокси-сервер вписывает в заголовок свой адрес.

Content-Type указывает формат, в котором описан сеанс связи (например, SDP). Само же описание сеанса содержится в теле сообщения.

Content-Length указывает длину тела сообщения.

Allow — поле содержит список параметров (SIP-методов), разделённых запятой. Они описывают, какие возможности протокола SIP поддерживает данный отправитель (устройство). Полный список методов: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, PRACK, REFER, REGISTER, SUBSCRIBE, UPDATE.

4. Порядок обработки результатов

Представить результаты работы, в следующем формате.

Вставить соответствующий скриншот

Рис. <*Номер рисунка*> — Название

Указать инструмент, примененный для получения.

5. Сделать выводы

- Указать, какие протоколы использованы в конкретном VoIP-соединении.
- Указать и записать адреса конченых точек звонка.
- Указать и записать параметры SIP-протокола.
- Записать параметры джиттера.

Лабораторная работа 3

Ознакомление с принципами функционирования и основными протоколами VoLTE

1. Цель работы

Ознакомится с ключевыми аспектами настройки оборудования eUTRAN, EPS, IMS, а также проанализировать сетевой трафик сети LTE.

2 Применяемое оборудование, ПО и данные

1) Персональный компьютер с ОС Windows, ОС Linux или ОС MacOS
2) ПО Wireshark, ПО PuTTY (для Windows), любой терминал (для Linux и MacOS)
3) Записанные дампы

3. Порядок выполнения работы

3.1. Ознакомиться с конфигурационными файлами различных элементов конфигурации LTE-сети и IMS-сети.

3.2. По очереди открыть различные дампы

3.3. ok_voice_call.pcapng

Здесь можно прослушать голос

3.4. 3009 2ue ok.pcapng

Сравнить UE capabilities

3.5. Открыть файлы ho1.pcapng и ho2.pcapng и проанализировать процедуру хэндовера.

4. Порядок обработки результатов

Представить результаты работы, в следующем формате.

Вставить соответствующий скриншот

Рис. <*Номер рисунка*> — Название

Указать инструмент, использованный для получения.

5. Сделать выводы