Лабораторная работа № 1-1 Troubleshooting

Любой VoIP вызов состоит из 2-х основных составляющих: *обмена сигнальной информацией* и *передачи между пользователями media потоков* с голосом и/или видео.

На первом этапе, в процессе *обмена сигнальной информацией*, клиенты напрямую либо посредством сервера договариваются между собой о параметрах устанавливаемого вызова. Если связь устанавливается с помощью сервера, на основе сигнальной информации сервер авторизует клиента, устанавливает кто и кому звонит, проводит маршрутизацию и коммутацию. Благодаря данным сигнального протокола клиенты и сервер согласуют метод шифрования, используемые media кодеки, обмениваются ip адресами и номерами портов, где ожидается приём media и тд. Происходит это по таким протоколам как SIP, XMPP и прочим.

Непосредственно «разговор», то есть обмен между клиентами голосовыми данными, как правило происходит по протоколу RTP. Данные внутри передаются в том виде, о котором договорились клиенты и сервер на «сигнальном» этапе. Обмен голосом возможен как напрямую между клиентами, так и через сервер — посредник. Во втором случае сервер может помочь клиентам с прохождением NAT и в выборе кодеков.

Часть 1.

Проверка работы кодеков

Теория

Под телефонными (VoIP) **кодеками** понимаются различные математические модели используемые для цифрового кодирования и компрессирования (сжатия) аудио информации. Многие из современных кодеков используют особенности восприятия человеческим мозгом неполной информации: алгоритмы голосового сжатия пользуются этими особенностями, вследствие чего не полностью услышанная информация полностью интерпретируется головным мозгом. Основным смыслом таких кодеков является сохранение баланса между эффективностью передачи данных и их качеством.

Изначально, термин кодек происходил от сочетания слов КОДирование/ДЕКодирование, то есть устройств, которые преобразовывали аналог в цифровую форму. В современном мире телекоммуникаций, слово кодек скорее берет начало от сочетания КОмпрессия/ДЕКомпрессия.

Кодек	Скорость передачи, Кб/сек.	Лицензирование
G.711	64 Кб/сек.	Нет
G.726	16, 24, 32 или 40 Кб/ сек.	Нет
G.729A	8 Кб/ сек.	Да
GSM	13 Кб/ сек.	Нет
iLBC	13.3 Кб/ сек. (30 мс фрейма); 15.2 Кб/ сек. (20 мс фрейма)	Нет
Speex	Диапазон от 2.15 до 22.4 Кб/ сек.	Нет
G.722	64 Кб/сек.	Нет

Цель

Исследовать работу кодеков

Задачи

1. Запустить wireshark.Настроить два phoner

2. Проверить что вызов устанавливается.

3. Снять дампы wireshark. Через анализатор определить кодек по которому было установлено соединение. (через тело пакета либо через handshake – call flow)

4. На одном из фонеров изменить порядок кодеков с помощью стрелок. Позвонить.

5. Снять дамп. Посмотреть какой кодек выбран.

6. Позвонить в обратную сторону. Снять дамп. Посмотреть какой кодек выбран.

7. Отключить кодеки, оставить только разные на разных терминалах. Позвонить. Снять дампы.

Контрольные вопросы

Ответить на контрольные вопросы письменно, обосновывая ответ скриншотами:

1. Какой терминал задает выбор кодека?
2. По какому принципу выбирается кодек?
3. Что происходит если на двух терминалах нет общих кодеков?

Часть 2

Проверка работы TCP/UDP

1. Запустить wireshark.Настроить два phoner
2. Проверить что вызов устанавливается.
3. Снять дампы wireshark. Через анализатор (через тело пакета) определить транспортный протокол по которому было установлено соединение.
4. На двух фонерах выбрать разный транспорт — TCP/UDP. UDP/TLS, TCP/TLS и произвести вызовы используя автответчик. Снять дампы через wireshark.

Контрольные вопросы

Ответить на контрольные вопросы письменно, обосновывая ответ скриншотами:

1. В чем разница TCP, UDP. TLS (устно, на защите)
2. Что происходит когда на разных телефонах активирован разные транспортные протоколы. Какие протоколы выбираются при звонках с разных терминалов?

Часть 3

Проверка sRTP/zRTP

Итак, что же собой представляет шифрованный VoIP вызов? Дальше речь пойдёт о SIP протоколе как наиболее популярном.
Как мы уже выяснили, звонок состоит из сигнальной и media частей, каждая из которых может быть зашифрована отдельно с применением специальных методов-протоколов. Для шифрования сигнальной информации применяется

SIP\TLS, для шифрования «голоса» ZRTP и SRTP протоколы.

SIP\TLS — грубо говоря, аналог HTTPS для обычного SIP. Протокол позволяет клиенту убедиться, что он общается с нужным сервером при условии, что клиент доверяет предоставленному сервером сертификату.

sRTP и zRTP — это два разных способа шифровать RTP потоки. Принципиальное отличие между ними в том, что обмен ключами для SRTP происходит в сигнализации (на первой сигнальной стадии установки вызова). А для ZRTP непосредственно в начале обмена RTP пакетами (во второй, «медийной» части) по специальному протоколу, основанному на методе криптографии Диффи — Хеллмана.

Важно то, что для SRTP обязательным условием надёжности шифрования звонка является одновременное использование SIP\TLS + SRTP, иначе злоумышленнику не составит труда получить ключи (которые будут переданы по не шифрованному SIP) и прослушать разговор. В то время как для ZRTP это не важно, RTP поток будет надёжно зашифрован не зависимо от того, шифруется сигнализация или нет. Более того протокол умеет определять наличие «man in the middle» (в том числе серверов услуг!) между непосредственно говорящими клиентами. Это позволяет быть уверенным в том, что разговор невозможно прослушать, по крайней мере с точки зрения прослушивания сети/среды передачи данных.

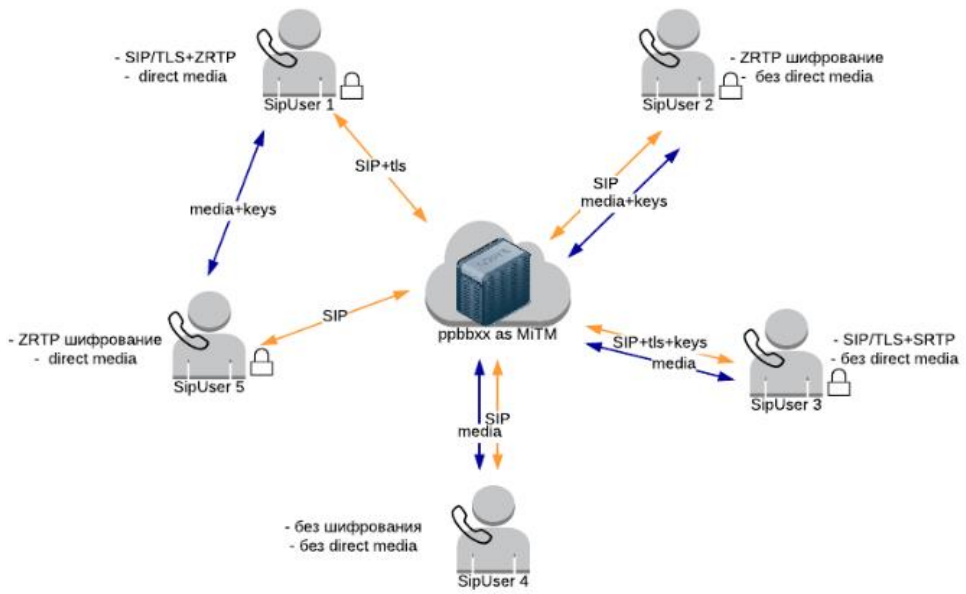

Схема подключ

ения SIP клиентов с различными настройками шифрования:

Оба пользователя используют SIP\TLS и SRTP. В этом случае обмен ключами для шифрования media происходят по защищенному сигнальному протоколу. Предполагается доверие к серверу, участвующему в установке связи. Посторонние не могут получить доступ ни к сигнальной информации, ни к голосовым данным. Недостаток в том, что пользователь не уведомлен на уровне протокола (клиента) и не убежден, что второй пользователь также использует шифрованное подключение к серверу.

1. Оба пользователя используют ZRTP, голос при этом проходит через сервер. В этом случае сервер определяется ZRTP протоколом как Trusted MitM (man in the middle). Обмен ключами происходит по алгоритму, основанному на методе Диффи — Хеллмана (что и гарантирует невозможность прослушки) по протоколу RTP. Если при этом используется защищенный SIP\TLS — посторонние так же не могут получить доступ ни к сигнальной информации, ни к «голосу». Как и в первом варианте предполагается доверие к коммутирующему серверу, но в отличии от него для надёжного шифрования голоса не требуется обязательное использование защищенного SIP\TLS. Также, в отличии от первого варианта, каждый пользователь видит, что разговор шифруется до сервера с обоих сторон, а также то, что оба подключены к одному и тому же (доверенному) серверу.

2. Оба пользователя используют ZRTP, но media устанавливается напрямую между клиентами. Так как обмен ключами проходит напрямую между клиентами, даже сервер, осуществивший коммутацию, не может прослушать разговор. В этом случае оба клиента отображают информацию о том, что установлен безопасный прямой сеанс связи. Убедиться в этом можно сверив SAS (короткие строки авторизации) — они будут одинаковыми. Если требуется скрыть от посторонних сигнальную информацию, следует использовать SIP\TLS. Это самый

безопасный вариант, но в этом случае сервер не сможет выполнять многие функции, которые в других ситуациях выполняются на нем, к примеру запись непосредственно разговора, перекодирование голоса для клиентов с разными настройками аудиокодеков и тд.

3. Один пользователь использует первый метод, описанный выше, а другой — второй. В этом случае так же требуется доверие к серверу. Сигнальная информация шифруется с помощью SIP\TLS. Для пользователя с ZRTP протокол сообщит, что шифрованное соединение установлено до сервера (End at MitM). Используется ли шифрование с другой стороны на уровне протокола узнать не удастся.

Цель работы

Изучить sRTP, zRTP

1. Запустить wireshark.Настроить два phoner

2. Проверить что вызов устанавливается.

3. Снять дампы wireshark. Через анализатор (через тело пакета) определить протокол шифрования по которому было установлено соединение.

4. На двух фонерах выбрать разные протоколы шифрования — sRTP/zRTP, zRTP/sRTP, SSL и произвести вызовы используя автответчик. Снять дампы через wireshark.

Контрольные вопросы

Ответить на контрольные вопросы письменно, обосновывая ответ скриншотами:

1. В чем разница sRTP, zRTP, TLS (устно, на защите)

2. Что происходит когда на разных телефонах активирован разные протоколы безопасности? Какие протоколы выбираются при звонках с разных терминалов?