РАЗРАБОТКА БЕСПРОВОДНЫХ СЕТЕЙ ФИНАНСОВЫХ ЦИФРОВЫХ СЕРВИСОВ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Беспалова Н.В.,
Финансовый университет при Правительстве Российской Федерации, Москва, Россия
NVBespalova@fa.ru
Осипов А.В., Плешакова Е.С., Гатауллин С.Т.
МИРЭА – Российский технологический университет, Москва, Россия
osipov_av@mirea.ru, pleshakova@mirea.ru, gataullin@mirea.ru

Аннотация. Финансовый сектор состоит из компаний и учреждений, предоставляющих финансовые услуги коммерческим организациям, охватывая широкий спектр отраслей, финансовые учреждения подвергаются кибератакам. Для защиты от кибератак безопасность становится все более актуальной среди финансовых учреждений. В связи с этим необходимо проводить исследования для создания более эффективных и всеобъемлющих методов безопасности для защиты от расширяющегося разнообразия сетевых атак. Уязвимости протокола SIP являются часто встречающимися киберпреступных действий, которые приводят к значительным потерям в финансовом секторе. Присущи проблемы с безопасностью. В статье анализируются механизмы обеспечения безопасности SIP-сетей. Авторами приводится анализ уязвимостей SIP-протокола. На основе анализа даны рекомендации по обеспечению безопасности SIP-сетей.

Ключевые слова: SIP протокол, уязвимости SIP протокола, RTP протокол, механизмы обеспечения безопасности, процедуры обеспечения безопасности, TLS, SRTP, iptables.

Введение

Технологии искусственного интеллекта и математические методы широко используются для решения прикладных задач для приоритетных отраслей цифровой экономики. Так, в следующих работах предлагаются передовые нейросетевые и математические методы обеспечения кибербезопасности [1-3]. Сегодня IP-телефония, или Voice over IP (VoIP), позволяет объединить раздельные сети передачи голоса и данных, что помогает снизить затраты. IP-телефония стала весьма популярной и находит широкое применение в большинстве финансовых организаций. IP-телефонии присущи такие угрозы как DoS-атаки, вредоносное ПО и преднамеренное вторжение. Протокол SIP устанавливает сеансы и передачи данных. Сеансы описывают процесс определения и завершения интернет-сессий пользователей [4].

1. Функционирование протокола SIP

SIP протокол определяет способ благодаря которому клиентская программа инициирует установление соединения. SIP протокол применяют для голосовых вызовов для «точка-точка», многосторонних сеансов. В отличии от RTP, Sip не зависит от транспорта мультимедиа. SIP также можно применять для обмена мгновенными сообщениями. Инфраструктура SIP состоит из пользовательского агента, сервера регистрации, сервера определения местоположения и прокси-сервера. Чтобы установить связь между пользовательскими агентами, используется набор сообщений. Набор сообщений состоит из INVITE и REFER. Маршрутизация происходит через SIP-прокси-серверы, размещённые в сети. Реализация SDP происходит в теле сообщения для предоставления информации о сеансе. Например, к нему можно отнести тип носителя, транспортный протокол, IP-адреса и номера портов конечных точек. Архитектура протокола SIP в модели «клиент-сервер» иллюстрируется на рисунке 1.

Рис. 1. Архитектура протокола SIP – «клиент-сервер»

Первый этап во время SIP-сессии отправляется запрос, в котором указывается IP-адрес. Следующий этап состоит в выборе порта и протокола. Это необходимо для подключения к требуемому устройству. В случае, когда информации о прокси-сервере нет применяются URI-данные. URI-данные включают в себя адрес пользователя, данные о порте и данные о протоколе. В случае, наличия IP-адреса устанавливает соединение с сервером. При передаче пакет с аудио информацией сервер задействует порты в диапазоне 10000 – 20000. Если информации о порте нет используется 5060 порт. Данный порт применяется в случае отправки незашифрованных сообщений SIP. Отправка осуществляется в вызове VoIP с передачей голоса по LTE (VoLTE) [5].

Протокол SIP имеет клиент-серверную модель. В связи с этим можно обозначить основные функциональные элементы. К ним относятся абонентский терминал, прокси-сервер, сервера переадресации и сервера определения местоположения пользователей. Первый функциональный элемент из которого состоит протокол SIP это абонентский терминал. Функционирует как устройство для управления установлением и завершением звонков. Реализация возможна в двух вариантах аппаратно (SIP-телефон) и программно. Второй функциональный элемент прокси-сервер. Устройство, которое принимает и обрабатывает запросы от терминалов, выполняя соответствующие этим запросам действия. Следующий функциональный элемент из которого состоит протокол SIP прокси-сервер, состоящий из клиентской и серверной частей. Данный элемент принимает вызовы, инициировать запросы и возвращать ответы. Сервер переадресации. Устройство, хранящее записи о текущем местоположении всех имеющихся в сети терминалах и прокси-серверах. Сервер переадресации не предназначен для управления вызовами и генерации запросов. Следующий функциональный элемент из которого состоит протокол SIP сервер определения местоположения пользователей. Включает адресную информацию. Данный элемент служит для обеспечения персональной мобильности пользователей. В свою очередь уровень транзакций можно разделить на две части. Первая часть – клиентская, вторая часть серверная [6–7]. Схема работы транзакции представлена на рисунке 2.

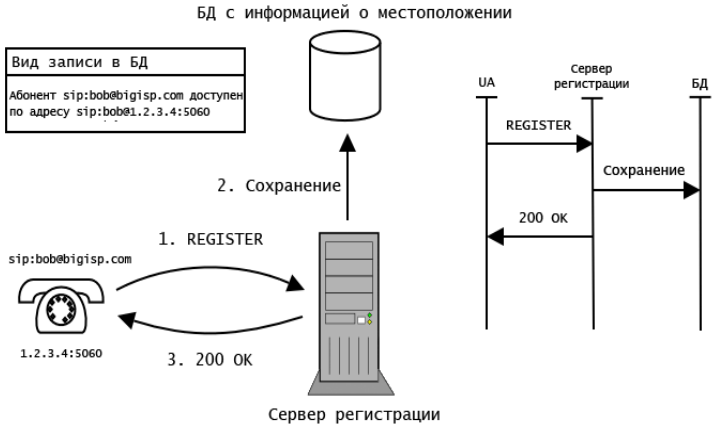

Рис. 2. Работа транзакции

Рассмотрим алгоритмы сжатия Alaw и Ulaw.

Алгоритм Alaw (A-закон) — это метод сжатия звуковых данных, в котором присутствует потеря информации:

$$F(x) = sgn(x)\begin{cases} \frac{A|x|}{1+\ln(A)} \\ \frac{1+\ln(A|x|)}{1+\ln(A)} \end{cases}, \ |x| < \frac{1}{A}, \frac{1}{A} \leq |x| \leq 1 \quad (1)$$

где A — параметр сжатия (A = 87,7).

Алгоритм Ulaw (μ-закон):

$$F(x) = sng(x)\frac{\ln(1+\mu|X|)}{\ln(1+\mu)}, \quad -1 \leq x \leq 1 \quad (2)$$

где μ = 255 (8 бит).

2. Изучение уязвимостей протокола SIP

Протокол SIP функционирует в интернете. Данная среда является сложной и динамичной. SIP-сообщения сталкиваются с разнообразными угрозами безопасности и подвержены атакам. В данной

работе мы рассмотрим уязвимости протокола, что послужит основой для формирования рекомендаций, которые позволят устранить уязвимости. Для демонстрации потенциальных уязвимостей мы проведем ряд атак на протокол. Для этих целей будем применять Svwar и Svmap [8-9]. На протокол SIP совершается несколько типовых атак. Существующие атаки на интерфейс типа DoS и DDoS представляют серьезную проблему. Так, например, в VoIP состоит из компонент, обрабатывающих сигналы, к ним относятся мультимедийные шлюзы, IP-телефоны, IP-АТС и VoIP-брандмауэры.

2.1. Атаки DoS

Вид DoS-атак, работающий на уязвимостях протокола SIP. Происходит повышенная нагрузка на атакуемый SIP-сервер. Атака реализуется путем отправки на него потока сообщений с ложными данными. Результатом такого вида атак будет срыв работы голосовых сервисов. Данный тип атак происходит из-за фальсификации полезной нагрузки сообщения. В протоколе SIP анализаторы SIP-сообщений, работающие с входящими данными, которые могут быть некорректными, то основное требование это гибкость протокола и защита от атак. Например, для реализации атаки вызывается переполнение буфера потоком некорректной информации, таким образов выявляются уязвимости в системе.

2.2. DoS путем вмешательства в поток атака

Злоумышленник может оправлять пакеты и форматированные пакеты, применяя для этого специальные инструменты. Слабым местом является отправка клиентом повторного запроса, который называется REGISTER. Запрос состоит из информации, включающей учётные данные для регистрации на сервере. Клиент может передавать строку авторизации, причем в нескольких запросах, например REGISTER, INVITE или BYE. Для успешной атаки достаточно направить клиенту вредоносный SIP пакет, применяя для этого специальные инструменты, с ответом 401 Unauthorized, намеренно располагая клиента отправить учётные данные.

2.3. Перегрузка потоком данных

Самый часто используемый метод проведения DoS-атаки — отправка большого количества SIP-сообщений злоумышленником. Это делается для того, чтобы перегрузить систему обработки пользователя и вызвать сбой в её работе. Этот вид атак самый распространенный вид атак на протокол SIP.

2.4. Атака - Man inthe middle

Рассмотрим вид атаки человек посередине. Данный вид атаки реализуется путем установления соединения злоумышленника с жертвами для передачи сообщений. Таким образом создается видимость общения по безопасному каналу. Но при этом злоумышленник контролирует весь диалог. Успешная реализация MITM-атаки состоит из перехвата и дешифрация. Фаза перехвата состоит из вмешательства в процесс передачи данных. Данные перехватываются перед реальной отправкой адресату. Далее реализуется вторая фаза. После получения доступа к данным, необходимо данные расшифровать.

2.5. Срыв сессий

Данный вид атаки представляет собой атаку, при реализации которой злоумышленник стремится нарушить процесс аутентификации пользователя, а также вызвать задержки в передаче данных. Пример успешной реализации данного вида атаки состоит в следующем. Злоумышленник фальсифицирует сообщения о завершении и отправляет их на конечное устройство. Успешная реализация атаки состоит в завершение сеанса связи пользователя. Так же срыв сессии в SIP происходить посредством внедрения фальшивых сигнальных пакетов. Для противодействия этому виду атак следует применять аутентификация отправителя запроса BYE.

2.6. Атака на VoIP-аутентификацию

IP телефония содержат механизмы аутентификации. Они позволяют применить механизмы после предъявления пароля, разрешающего пользователю доступ к IP-телефону. Запрос REGISTER отправляется непосредственно на IP-PBX сервер в процессе соединения с сетью VoIP. Этот запрос необходим для регистрации с телефоном идентификатора пользователя. Запрос на регистрацию состоит из информации о пользователе, данных аутентификации. Данная информация полезна для реализации атаки. Для обеспечения безопасности следует установить многофакторную

аутентификацию для доступа к системам управления VoIP. Стоит острая необходимость применять обновляемые пароли. Не менее важно ограничивать доступ к VoIP-инфраструктуре только авторизованным пользователям (рисунок 3).

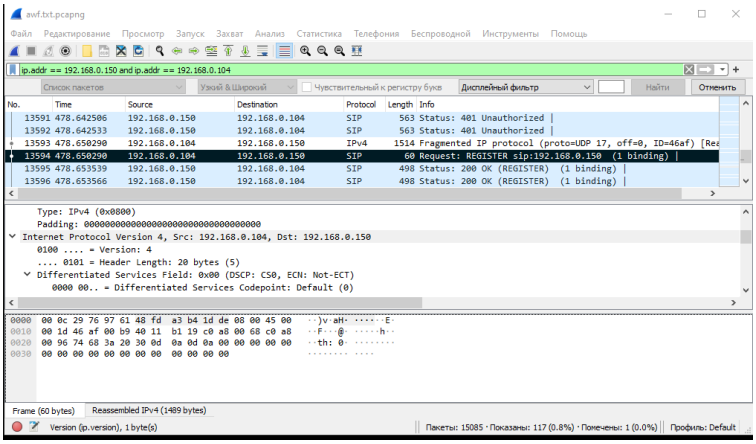

Рис. 3. Пакеты журналирования

Злоумышленники могут применять инструменты для взлома хэшей паролей предварительно составив словарь, и получив тем самым доступ к данным (рисунок 4).

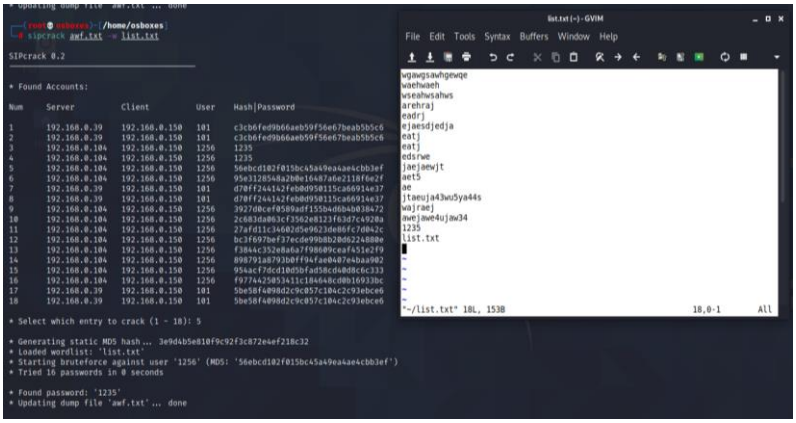

Рис. 4. Доступ к данным

В частности, совершать звонки другим абонентам, прослушивать и управлять легальными звонками.

3. Механизмы обеспечения безопасности

На основе представленных выше угроз можно определить основные принципы безопасности, которые нужно внедрить для защиты сетей, работающих на основе протокола SIP. К основным принципам безопасности относится защита данных и сохранение их конфиденциальности при передаче сообщений, предотвращение спуфинг-атак, организация безопасного обмена данными без риска утечки информации о пользователе и сохранения конфиденциальности участников сессии, обеспечение устойчивости к атакам, направленным на отказ в обслуживании. Наиболее эффективным способом защиты информации является комплексное шифрование. При этом мы можем гарантировать что сообщение не было изменено. Однако при работе с SIP-пакетами невозможно осуществить полное сквозное шифрование. Это связано с тем, что поля запроса: Request-URI, Route, Via, должны быть доступными для прокси-сервера, чтобы запросы могли быть корректно обработаны. Существует еще один подход, который заключается в использовании протокола SSL/TLS. При таком подходе процесс аутентификации с использованием TLS включает обмен сертификатами. Можно сделать вывод применение SSL/TLS имеет множество преимуществ. Практическое применение подтверждает его эффективность. В связи с тем, что SSL/TLS работает поверх протоколов TCP/IP его эффективно внедрять в среду VoIP. Также SSL/TLS работает ниже протоколов HTTP или FTP. Однако основным недостатком SSL/TLS можно считать его неработаспособность через протокол UDP.

4. Рекомендации для применения протокола SIP с использованием TLS

Прокси-серверам необходимо работать на базе протокола TLS с поддержкой одно- и двусторонней аутентификации. Пользователь должен иметь возможность устанавливать соединение с использованием TLS и TCP, а также получать сообщения с помощью этой комбинации протоколов. Прокси-серверы, серверы перенаправления и регистрации, должны обладать сертификатом, удостоверяющим их подлинность. Так же они должны содержать идентификационную информацию и соответствовать доменным именам. В соответствии с указанными выше условиями все компоненты сети SIP должны иметь функцию проверки сертификатов. Для этого существуют центры сертификации. Данные центры — это доверенные организации. В свою очередь они берут на себя функции сертификации. Центры распределяя сертификаты для узлов SIP-сетей.

5. Рекомендации для применения протокола SRTP с использованием SIP

Использование стандартных соединений SIP/RTP зачатую не является безопасным, поскольку потоки RTP и сообщения SIP могут быть перехвачены и прослушаны. В связи с этим рекомендуется использовать стандартный SIP/RTP только в локальных сетях (LAN). В прочих случаях необходимо использование протоколов с дополнительным режимом шифрования. Такие протоколы получили название SIPS, их функционал расширен технологией TLS (Transport Layer Security), обеспечивающей шифрование голоса в защищенные IP-пакеты и их передачу от отправителя к получателю после установки безопасного соединения.

Например, в RTP есть функция аутентификации сообщений. Она применяется для защиты данных. В SRTP применяется аутентификационная метка, включающая в себя информацию из исходного сообщения, а также частичное содержимое пакетных заголовков, что позволяет осуществлять валидацию передаваемых данных и обеспечивать целостность информации. Основная задача использования аутентификационной метки предотвращение фальсификации данных и снижение риска искажения данных. Помимо этого, аутентификация сообщений позволяет осуществлять автоматическую блокировку атак повторного доступа.

6. Защита от отказа в обслуживании (DoS-атак)

Далее сформированы рекомендации для минимизации DDoS-атак на сервер. Важным инструментом является интеграция хост-защиты. Она располагается на границе домена управления. При DoS и DDos атаках на прокси-сервер, при которых происходит избыточный объем сообщений, происходит ресурсоисчерпание. Данный вид атаки нарушит передачу трафика. Обработка SIP-транзакций на прокси-сервере требует вычислительных ресурсов. В связи с этим можно сказать что прокси-сервер зависящие от состояния, более уязвимы.

7. Рекомендации по защите SIP-сетей

В ходе работы были сформулированы рекомендации, представленные на рисунке 5.

Рис. 5. Рекомендации по защите SIP-сетей

8. Заключение

Обнаруженные уязвимости SIP протокола демонстрируют, что механизмы защиты лишь частично удовлетворяют критериям информационной безопасности, предъявляемым к передаваемым данным, тем не менее их использование позволяет реально снизить риск нарушения целостности и конфиденциальности циркулирующей в сети информации. В ходе работы были был проведен анализ основной проблематики и сформулированы рекомендации по устранению типовых проблем в области безопасности сетей, работающих на основе протокола SIP. Было выявлено что некоторые способы обеспечения безопасности SIP в итоге опираются на защищённость устройств. Разработанные меры касаются не только безопасности определённого протокола, но и функционирования системы в целом. Оптимальным способом обезопасить сеть будет использование перечисленных нами ранее мер.

Уязвимости протокола SIP, как и других протоколов, влияют на конфиденциальность, целостность и доступность данных. Мы проанализировали данные уязвимости.

Хотя протокол SIP имеет свои слабые стороны, он предоставляет разнообразные методы для защиты передаваемых данных. Эти механизмы обеспечивают безопасность от определённых угроз, но их совместное использование повышает уровень защищённости сети от хакерских атак. Представленные ранее методы и меры по обеспечению безопасности подробно рассматриваются в третьей главе исследования, где также демонстрируются различные способы их реализации.

Литература

1. *Ivanyuk, V.* Forecasting of digital financial crimes in Russia based on machine learning methods. J ComputVirol Hack Tech (2023). https://doi.org/10.1007/s11416-023-00480-3.
2. *Boltachev, E.* Potential cyber threats of adversarial attacks on autonomous driving models. J ComputVirol Hack Tech (2023). https://doi.org/10.1007/s11416-023-00486-x.

3. *Efanov, D., Aleksandrov, P. & Mironov, I*. Comparison of the effectiveness of cepstral coefficients for Russian speech synthesis detection. J ComputVirol Hack Tech (2023). https://doi.org/10.1007/s11416-023-00491-0.
4. *Ahmadi, S.* (2024). A Comprehensive Study on Integration of Big Data and AI in Financial Industry and its Effect on Present and Future Opportunities. International Journal of Current Science Research and Review, 7(01), 66-74.
5. *Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M.* (2024). A comprehensive study of artificial intelligence and cybersecurity on Bitcoin, crypto currency and banking system. Annals of Data Science, 11(1), 103-135.
6. *Budianto, E. W. H., & Dewi, N. D. T.* (2023). Mapping Research Topics on Operational Risk in The Sharia and Conventional Financial Industry: VOSviewer Bibliometric Study and.
7. *Wanof, M. I.* (2023). Digital technology innovation in improving financial access for low-income communities. Technology and Society Perspectives (TACIT), 1(1), 26-34.
8. *Etim, G. S., Ada, J. A., Eyo, I. E., Ndem, S. E., & James, E. E.* (2023). Electronic banking and customers' access to banking services in rural settlements. RES MILITARIS, 13(3), 1161-1177.
9. *Weerawarna, R., Miah, S. J., & Shao, X.* (2023). Emerging advances of blockchain technology in finance: a content analysis. Personal and Ubiquitous Computing, 27(4), 1495-1508.