ПРОБЛЕМЫ БЕЗОПАСНОСТИ SIP-ТЕЛЕФОНИИ

Полудворянин С. М., Нестеренков С. Н.
Кафедра программного обеспечения информационных технологий, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: siarheipoludvaranin@gmail.com, nsn@bsuir.by

В последние годы протокол SIP получил широкое распространение. Среди основные преимуществ SIP-телефонии перед традиционной телефонией выделяют снижение затрат, масштабируемость, гибкость и надежность. Однако миграция на SIP-телефонию создает новые проблемы для организаций, которые не существовали при использовании телефонной сети общего пользования. В частности, необходима задуматься о безопасности SIP-телефонии.

Введение

Время аналоговой телефонии (PSTN) подходит к концу. Привычные телефонные линии переводят на современную гибкую технологию – SIP-телефонии (Session Initiation Protocol). SIP является протоколом управления прикладного уровня для создания, изменения и завершения сеансов связи с одним или большим количеством участников. В понятие сеанса входят мультимедиа конференции, обучение на расстоянии, Internet-телефония и подобные приложения[1]. В ближайшем будущем неизбежен полный переход аналоговых телефонных линий на IP-телефонию, а корпоративных АТС на протокол SIP. Согласно аналитическому отчету компании IHS количество SIP-транков в мире за первое полугодие 2017 года выросло 26% по сравнению с прошлым годом и достигло 30 миллионов штук[2]. Однако вместе с распространением технологии мы все чаще слышим сообщения о взломах и кибер-атаках на телефонные сервисы. В этой статье мы рассмотрим несколько угроз, возникающих при использовании протокола SIP, и способы эти угрозы реализовать.

I. Неавторизированный доступ к данным

Открытые текстовые протоколы предоставляют всю информацию любому, кто способен перехватывать сетевой трафик. Анализирую полученные данные можно получить доступ для конфиденциальной информации. Возьмем к примеру процесс аутентификации. В сип-протоколе пароли кодируются с помощью алгоритма MD5[1], который уже давно считается небезопасным. Множество телекоммуникационного оборудования, а также программные решения, поставляются с известными паролями по умолчанию. Если эти пароли остаются без изменений, злоумышленники могут легко получить их. Полученные данные аутентификации могут быть использованы для подмены легальной регистрации SIP-аккаунта на серверах VoIP провайдера (Registration hijacking). Полученный SIP-аккаунт может быть использован для совершения огромного количества звонков на специальные дорогие номера, а также рассылки аудио спама. Суммы, которые придется заплатить владельцу скомпрометированного аккаунта, могут быть весьма и весьма значительными. В некоторых случаях аутентификация может осуществляться на основе известной пары IP-адреса и порта. В случае если у клиента-жертвы нет выделенного IP-адреса, злоумышленник, находящийся с ним в одной локальной сети, получает возможность осуществлять звонки за счет жертвы. Такая ситуация может возникнуть, если провайдер осуществляет доступ к сети Интернет через NAT (от англ. Network Address Translation — «преобразование сетевых адресов»), за которым помимо законного абонента сервиса IP-телефонии могут находиться другие пользователи. В качестве примера можно привести бизнес-центр, где большое количество фирм проходят через NAT местного провайдера.

II. Перехват и целостность данных

Для прослушивания аналоговой телефонной линии злоумышленнику потребуется получить физический доступ к линии или коммуникационному оборудованию. В IP-телефонии возможность просушивания разговоров резко увеличилась благодаря большому количеству сетевых узлов между субъектами разговора. Скомпрометировав хотя бы одну сетевую ноду, атакующий получит доступ к медиа-трафику. На данный момент с сети Интернет предостаточно бесплатного программного обеспечения для преобразования VoIP-трафика в аудиофайлы и их прослушивания.Полученную таким образом информацию очевидно можно использовать с целью шантажа или шпионажа или применить в социальной инженерии. Для SIP-протокола характерно отсутствие взаимной аутентификации в большинстве случаев обмена сообщениями между сервером и клиентом. Без взаимной аутентификации злоумышленник, осуществляющий атаку типа «человек посередине»[3], может подменять исходящие/входящие пакеты клиента-жертвы, нарушая целостность передаваемой информации. Получив возможность для подме-

ны данных, злоумышленник может перенаправлять звонки клиента на произвольный номер, в том числе на несуществующий (приводя к DoS). Перехватывая INVITE-пакеты, злоумышленник подменяет ответ пакетом с кодом 301 Moved Permanently, перенаправляя звонок. Злоумышленник, зная или подбирая некоторые атрибуты звонка, способен разрывать активные сессии, отправляя заранее сформулированные вредоносные пакеты, содержащие запрос на завершение соединения(SIP BYE-request)[4].

III. Ограничение доступности

Для сервисов IP-телефонии кране важно быть всегда доступными для клиентов и предоставлять хорошее качество связи.Именно поэтому они так подвержены атакам типа «отказ в обслуживании» (Denial of Service, DoS). Атака DoS может быстро снизить уровень QoS до неприемлемого уровня. Эта атака нацелена на превышение предельной нагрузки на систему большим количеством коротких звонков или информационного мусора. Если для атаки создается сеть из большого количества «зомби-компьютеров», то такую атаку называют DDoS-атакой (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). DoS-атаки могут иметь различные формы и мотивацию. Наиболее простой способ атаки на SIP сервер это инициация большого количества сессий с различными идентификаторами с целью исчерпания оперативной памяти сервера. Различные типы SIP-запросов (REGISTER, INVITE или OPTIONS) могут быть использованы для такого вида атаки[5]. Другой сценарий, который может использовать злоумышленник, изображен на Рис. 1. В этом случае злоумышленник пытается «вести себя» как законный пользователь. Скорее всего, злоумышленник будет пытаться реализовать различные сценарии с отправкой множества INVITE запросов. Это приводит к отказу в обслуживании сервера SIP провайдера или АТС жертвы. Без постоянного отслеживания признаков подобных атак и применения пассивных средств защиты, это приводит к тому, что серверы IP-телефонии не справляются с возросшей нагрузкой и не в состоянии обслуживать подключенных абонентов. DDoS атака может применяться и на медиа-сервера. Она осуществляется путем отправки большого количества RTP-пакетов. Если цель не способна обработать такое количество пакетов, то качество связи ухудшается, либо сервер перестает работать. Посколько большинство реализаций RTP базируется на UDP, такой трафик легко генерировать. Выход из строя одного медиа-сервера может нарушить работу передачи голосового трафика всей сети.

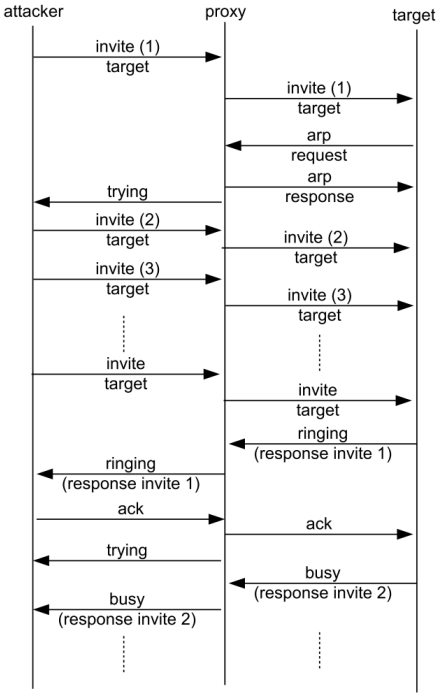

Рис. 1 – DDoS INVITE-запросами

IV. Заключение

В этой статье мы рассмотрели основные проблемы безопасности IP-телефонии и виды угроз, с которыми можно встретиться. Клиенты и провайдеры SIP-телефонии должны серьезно относится к требованиям безопасности и конфиденциальности своих голосовых звонков. Кроме того, они должны учитывать последствию в случае взлома.

1. Гольдштейн, Б. С. IP-Телефония / Б. С. Гольдштейн, А. В. Пинчук, А. Л. Суховицкий. – СПб.: БХВ, 2014. – 336 с.
2. SIP Trunks to Top 53 Million in 2021 [Electronic resource] / D. Myers – IHS Markit, 2017. – Mode of access: https://technology.ihs.com/596390/sip-trunks-to-top-53-million-in-2021. – Date of access: 14.08.2018.
3. Нестеренков, С. Н. Защита информации в приложениях масштаба предприятия / С. Н. Нестеренков, Б. В. Никульшин // Технические средства защиты информации : тез. докл. VIII Белорус.-рос. науч.-техн. конф., Браслав, 24-28 мая 2010 г. / Белорус. гос. ун-т информатики и радиоэлектроники ; редкол.: Л. М. Лыньков [и др.]. – Минск, 2010. – С. 60–61.
4. Lohiya, K. End to End Encryption Architecture for Voice over Internet Protocol /K. Lohiya, N. Shekokar, S. R. Devane //International Journal of Computer Applications – 2012. – Vol. 41. – P. 31–34.
5. Wang, Y. A Practical Method for SIP-DoS Attack Effect Evaluation /Y. Wang, Y. Yang //Journal of Information & Computational Science – 2012. – Vol. 9. – P. 333–345.