Риск отправки поддельных данных может быть реализован с помощью атак на сетевой приложение на сервере, а также с помощью манипуляции данных передаваемых мобильному приложению для последующей отправки.

АУДИТ БЕЗОПАСНОСТИ ТРАФИКА В СИСТЕМЕ IP-ТЕЛЕФОНИИ

Д.В. Куприянова, Д.Н. Одинец

Протоколы SIP и RTP, используемы для передачи медиа данных, были разработаны без учета необходимости защищать передаваемую информацию, в следствии чего возможны следующие виды атак и уязвимостей: фрод звонков, вирус, попавший в сеть IP-телефонии может начать рассылать спам ее абонентам, нарушение звонков – атакующий рассылает пакеты клиентам звонка, DoS – за счет отправки большого количества сообщений «Invite» и «Registrer» нарушается работу компонентов SIP, атакующий прослушивает весь трафик в IP-телефонии, подбор паролей, Man-In-The-Middle – атакующий проникает в звонок между пользователями, и может не только прослушивать, но и изменять сообщения между клиентами.

Для защиты передаваемы данных, предлагается использовать протокол TLS – протокол защиты транспортного уровня. Данный протокол использует асимметричное шифрования для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений. Также для защиты данных может быть использован IPsec – набор протоколов для обеспечения защиты данных, передаваемых по протоколу IP, обеспечивающих аутентификацию, проверку целостности и/или шифрование IP-пакетов. В отличие от IPSec, TLS протокол реализуется на транспортном уровне и не требует поддержки на промежуточных устройствах.

Для улучшения защиты может быть использован VPN. В случае невозможности использования VPN, необходимо использовать VLAN. Данные решения создают виртуальную сеть, что позволяет передавать данные в надежных сетях.

В данном случае лучшим выбором будет использование VPN который позволяет шифровать данные, так как в этом случае нет необходимости реализации шифрования на клиентах, отсутствует риск ошибок в реализации шифрования, VPN может быть обновлен для использования более современных методов шифрования без необходимости обновления кода клиента [1–3].

Список литературы

1. Security in a SIP network: Identifying network attacks [Электронный ресурс]. URL: https://searchunifiedcommunications.techtarget.com/feature/Security-in-a-SIP-network-Identifying-network-attacks (дата обращения: 05.04.2019).

2. How to Address WoIP Security Challenges [Электронный ресурс]. URL: http://www.centurylinkbrightideas.com/how-to-address-voip-security-challenges/ (дата обращения: 05.04.2019).

3. SIP Server Security with TLS: RPE [Электронный ресурс]. URL: https://www.researchgate.net/publication/235601569_SIP_Server_Security_with_TLS_Relative_Performance_Evaluation (дата обращения: 05.04.2019).

СПОСОБЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д.В. Куприянова, Д.Ю. Перцев

Анализ ситуации, проведенный BSA Global Software Survey [1], показывает, что рынок нелицензионного ПО уменьшается, однако по состоянию на 2018 г. составляет 37 % и оценивается более чем в 46 млрд. долларов. С учетом этого проблема защиты авторских прав по-прежнему является актуальной. К основным способам защиты ПО относится: лицензионный ключ, жесткая привязка к носителю информации, USB-ключ. Лицензионный ключ является самым простым способом защиты и предполагает генерацию ключа по некоторому шаблону с привязкой к имени пользователя или аппаратной конфигурации системы. Основным

недостатком подхода является относительная простота взлома, осуществляемая путем анализа дизассемблированного кода. Развитием указанного подхода является проверка ключа через Интернет. При этом, как правило, существует сервер, через который проверяется лицензия. Данный подход более сложен для взлома и, как правило, предполагает подмену сервера на собственный. Жесткая привязка к носителю информации и USB-ключ являются схожими по принципу действия. Данные подходы предполагают постоянный опрос устройства (флеш-устройство, компакт-диск и другие), при его обнаружении считывается ключ в программе и сравнивается с ключом, записанным на устройстве. После чего принимается решение, является ли копия программы лицензионной. Современные версии USB-ключей развивают концепцию [2] и позволяют разработчику выполнить произвольный алгоритм внутри электронного ключа. В дополнение к рассмотренным методам защиты применяются запутывание кода (англ. obfuscation) и комбинирование упакованного кода с кодом, который его восстановит. На основе проведенного анализа, подтверждаемого в том числе сторонними исследованиями [3], оптимальным является комбинация из нескольких способов защиты. Например, применение USB-ключа в связке с запутыванием кода.

Список литературы

1. Software Management: Security Imperative, Business Opportunity [Электронный ресурс] URL: https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf (дата обращения: 05.04.2019).

2. Senselock [Электронный ресурс]. URL: http://senselock.ru/index.php (дата обращения: 05.04.2019).

3. Liutkevicius A. Assessment of Dongle-based Software Copy Protection Combined with Additional Protection Methods // Electronics and Electrical Engineering. 2011. № 6 (112). P. 111–116.

ЗАЩИТА ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ РАСПРЕДЕЛЕННЫМ АКУСТИЧЕСКИМ ДАТЧИКОМ НА ОСНОВЕ КОГЕРЕНТНОГО РЕФЛЕКТОМЕТРА

Д.Н. Курбыко, В.Н. Урядов

Надежность работы системы связи, т. е. ее способность в течение длительного времени выполнять заданные функции по передаче информации с установленной нормами достоверностью – то, к чему стремится и потребитель, и поставщик услуг, и оператор сети связи. Всем известно, что аварию легче предотвратить, чем устранить. Для этого надо своевременно обнаружить признаки ее наступления. Чтобы ВОЛС функционировала без прерывания связи, службы эксплуатации должны проводить комплекс мероприятий для сведения к минимуму вероятности повреждения кабельной инфраструктуры. Помочь им в этом вопросе может распределенный акустический датчик «Дунай» на основе когерентного рефлектометра. Принцип действия распределенного акустического датчика «Дунай» схож с тем, как функционирует радар или обычный оптический рефлектометр: в тестируемую линию вводится мощный зондирующий световой импульс, и анализируются характеристики отраженного и рассеянного назад излучения. В отличие от других приборов распределенный акустический датчик на основе когерентного рефлектометра благодаря чувствительности к фазовой модуляции в волокне [2] позволяет измерять распределение акустических воздействий по всей длине волокна. Датчик акустических воздействий на основе когерентного рефлектометра (COTDR) позволяет обнаружить проведение практически любых работ вблизи ВОЛС, а тем более манипуляции с оптическим кабелем. Кабельная инфраструктура волоконно-оптических сетей связи должна быть рассчитана на многолетнюю эксплуатацию и неоднократные модернизации систем связи в течение всего срока ее эксплуатации, обычно составляющего 25 лет. При отсутствии ошибок проектирования правильная организация эксплуатации – залог успешной работы ВОЛС. Чтобы предотвратить возможные обрывы кабеля на наиболее ответственных (с точки зрения объемов трафика) и проблемных (с точки зрения случайных обрывов при строительных работах) участках ВОЛС, целесообразно использовать распределенный датчик акустических воздействий на основе когерентного рефлектометра