Э. В. Слончак, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732

ОРГАНИЗАЦИЯ IP-ТЕЛЕФОНИИ В СЕТИ ПРЕДПРИЯТИЯ

Аннотация. *В статье рассмотрены способы организации и функционирования современной IP-телефонии, а также методы ее защиты. Результатом работы стала модель компьютерной сети предприятия с применением технологии Voice over IP (VoIP) с обеспечением необходимого уровня защиты голосового трафика при передаче по незащищенным каналам связи.*
Ключевые слова: *IP-телефония, GRE-туннель, IPSEC, SIP.*

Введение. В связи с увеличивающейся долей удаленной работы огромное количество компаний переходят на современные сервисы общения. IP-телефония — один из таких сервисов. Если раньше аналоговая телефония (Public Switched Telephone Network, PSTN) использовалась повсеместно и IP-телефония рассматривалась как нечто экзотическое, то на сегодняшний момент современные провайдеры, издавна предоставляющие данные услуги, отмечают снижение спроса на аналоговую связь, так как IP-телефония дешевле в эксплуатации и обладает большим функционалом. Также немаловажным фактором для предпринимателя является защита от утечки данных [1]. В связи с этим вопрос защиты голосового трафика, передаваемого средствами VoIP, становится особенно актуальным. Одним из примеров подходов к защите трафика IP-телефонии является формирование прямого защищенного канала между корреспондентами [2], также для защиты можно использовать метод шифрования телефонных разговоров с помощью протоколов TLS (Transport Layer Security) и SRTP (Secure Real Time Protocol) [3]. Однако ни один из предложенных подходов не дает должного уровня защиты голосового трафика для операционной системы Cisco IOS, так как организация его безопасной работы на сетевом оборудовании Cisco имеет особенности, знание которых необходимо учитывать при его имплементации в корпоративную сеть.

Проблема исследования. Защита IP-телефонии является достаточно сложным и комплексным процессом, поэтому были выделены несколько задач:

1. Изучить теоретические особенности функционирования IP-телефонии.

2. Сравнить современные протоколы IP-телефонии.

3. Проанализировать методы защиты VoIP-трафика.

4. Смоделировать компьютерную сеть организации, использующую в технологии VoIP, в программном эмуляторе.

Материалы и методы. Методами данного исследования стали: наблюдение, сравнение, эксперимент, измерение и абстрагирование. Для эмуляции компьютерной сети было выбрано программное средство Cisco Packet Tracer 8.1.1.

Результаты. IP-телефония — это общий термин для обозначения технологий, продуктов и услуг, использующих соединения с коммутацией IP-пакетов для поддержки голосовых вызовов, голосовой почты, видеозвонков, видеоконференций, факсимильной связи и обмена мгновенными сообщениями (IM).

Традиционно телефонные коммуникации осуществлялись по выделенным каналам PSTN. С использованием Интернета звонки передаются в виде пакетов данных по общим линиям, что позволяет избежать платы за пользование каналов PSTN. IP-телефония работает путем преобразования голосовых вызовов, факсов и другой информации в цифровые сигналы, которые проходят через современные IP-сети. IP-телефония была представлена в 1991 г. с созданием первого специализированного приложения Speak Freely [4]. Современная IP-телефония работает на различных протоколах:

1. **SIP** (Session Initiation Protocol) — это протокол прикладного уровня, определенный стандартом IETF и описанный в RFC 3261, который работает по модели клиент-сервер и использует URL и URI из HTTP, схему кодирования текста и стиль заголовка из SMTP. Сервис SIP использует служебные протоколы SDP (Session Description Protocol) для описания сессии и RTP (Real Time Transport Protocol) для передачи голоса и видео по IP-сети [5].

2. **H.323 —** стандарт ITU, который позволяет аналоговым телефонам в PSTN взаимодействовать с компьютерами, подключенными к Интернету. В основе определяемой стандартом архитектуры находится специальный шлюз, который соединяет Интернет с телефонной сетью и переводит сообщение из одного протокола в другой. Шлюз использует протокол H.323 на стороне Интернета и протоколы PSTN на стороне аналоговой телефонии [6].

3. **SCCP** (Skinny Client Control Protocol) — это фирменный протокол компании Cisco для сигнализации сеансов связи с корпоративной системой связи Cisco Unified Communications Manager (CUSM). В качестве агента вызова в протоколе используется продукт Cisco CallManager, который также выступает в качестве сигнального прокси для событий вызова, инициированных по другим общим протоколам, таким как H.323 и SIP для передачи голоса. SCCP разработан как протокол связи для аппаратных конечных точек и других встроенных систем со значительными ограничениями процессора и памяти [7].

Сравнение международных стандартов IP-телефонии представлено в табл. 1.

Таблица 1

Сравнение протоколов SIP и H.323

Характеристика / протокол	*H.323*	*SIP*
Архитектура	Монолитная	Модульная
Масштабируемость	Ограниченная	Расширенная
Гибкость	–	+
Обмен сообщениями	–	+
Сложность	Сложный	Умеренно сложный
Формат сообщений	Двоичный	ASCII-формат
Совместимость с интернетом	Не совместим	Совместим
Архитектура	Построен на телефонных системах	Зависит от подключения к Интернету

Главная проблема защиты сервисов IP-телефонии заключается в том, что телефоны и личности существуют виртуально, что означает, что пользователи могут брать свои VoIP-телефоны с собой и работать из любого места. Кроме того, это означает, что пользователи могут использовать для звонков SIP-приложения, также известные как программные телефоны.

Телефонные VoIP-услуги имеют множество преимуществ в плане безопасности по сравнению с традиционными телефонными системами:

- контроль использования тарифного плана в режиме реального времени;
- строгое соблюдение правил бесплатных звонков;
- шифрование звонков для предотвращения подслушивания;
- надежные функции голосовой почты с доставкой по электронной почте.

Современные VoIP-сервисы используют пограничные контроллеры сессий (Session Border Controller, SBC) для обеспечения оптимальной безопасности и производительности, которые действует как межсетевой экран, поддерживающий производительность и логическую маршрутизацию вызовов. Операторы поддерживают высокие стандарты для исправления уязвимостей безопасности и обновления прошивки производителя, что обеспечивает более высокий уровень конфиденциальности, безопасности и надежности для бизнеса.

Сформулируем основные угрозы безопасности VoIP:

- *Отказ в обслуживании (Denial of Service, DoS)* — тип атаки, который лишает сеть ресурсов и приводит к прерыванию телефонного обслуживания. Для центра обработки вызовов это может ухудшить качество звонков, задержку и время работы.
- *Мошенничество с платными звонками* требует доступа к звонкам на внешнюю линию из вашей телефонной системы. Злоумышленники могут набирать дорогие международные номера, которые влекут за собой дорогостоящие платные звонки.
- *Фишинг* — тип атаки, направленный на пользователей, которые доверяют своему определителю номера. Жертвы разглашают

информацию о внутренней IP-сети, пароли или другие конфиденциальные данные.

• *Перехват вызовов* — тип атаки, при котором злоумышленники используют незащищенные сети для перехвата незашифрованного SIP-трафика.

• *Спам* — ящики голосовой почты, которые часто используют ограниченный или «частный» определитель номера, также является мишенью для робозвонков и других телефонных афер.

• *Вредоносные программы*, которые используют злоумышленники для получения учетных данных по телефону или электронной почте, открывают больше возможностей для проникновения в сеть компании и утечки конфиденциальных бизнес-данных.

VoIP-атаки могут быть бесшумными и незамеченными в течение нескольких месяцев из-за недостаточно квалифицированной защиты сервиса IP-телефонии. Для шифрования вызовов используются протоколы TLS и SRTP, которые работают вместе для обеспечения высокого уровня безопасности каждого вызова. Незашифрованные сети подвержены подслушиванию. В отличие от этого, зашифрованные данные бесполезны для тех, кому удастся записать их передачу. Важно шифрование, которое осуществляется от телефона до поставщика услуг. Данные должны быть зашифрованы на всех возможных уровнях [8].

Для наибольшей совместимости SIP не шифруется. Поскольку IP-телефония использует стек IP, шифрование управляется транспортным уровнем. Когда оно включено, сеанс вызова VoIP и сопутствующие данные вызова недоступны для похитителей данных.

Для защиты IP-телефонии от злоумышленников необходимо пользоваться следующими рекомендациями:

• политика надежных паролей;

• обновление операционной системы и прикладного программного обеспечения;

• использование виртуальной частной сети (Virtual Private Network, VPN) с шифрованием для удаленных сотрудников;

• шифрование беспроводного трафика Wi-Fi;

• перманентный анализ журналов вызовов;

• ограничение количества звонков и блокировка частных звонков;

• отключение неактивных учетных записей;

• внедрение удаленного управления устройствами для возможности удаленного стирания со скомпрометированного устройства;

• обучение пользователей методам безопасности.

На рис. 1 представлена модель сети организации с двумя филиалами, между которыми необходимо установить защищенный VPN-канал, для передачи данных IP-телефонии.

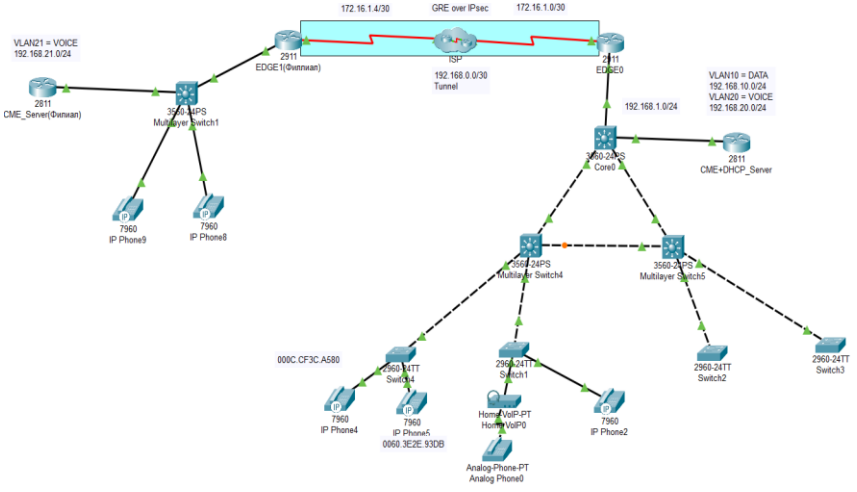

Рис. 1. Модель сети организации

В сеть компании внедрена IP-телефония, защита организована посредством VPN-туннеля с использованием протокола GRE. VoIP-траффик между филиалами шифруется посредством IPsec.

На рис. 2 и 3 продемонстрированы смоделерованная процедура звонка из одной сети в другую, а также передача зашифрованных данных протоколом IPsec.

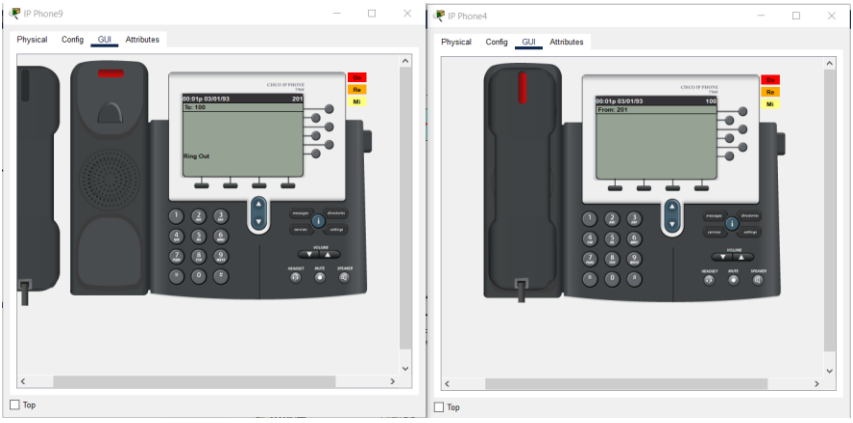

Рис. 2. Звонок в другой филиал

EDGE1(Филлиал)

Physical Config CLI Attributes

IOS Command Line Interface

```
EDGE1#show crypto ipse
EDGE1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: EDGE1_EDGE0_Map, local addr 172.16.1.5

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 0
   #pkts decaps: 16, #pkts decrypt: 16, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.5, remote crypto endpt.:172.16.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x87CA8D85(2278198661)

     inbound esp sas:
      spi: 0xC1945A1A(3247725082)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: FPGA:1, crypto map: EDGE1_EDGE0_Map
        sa timing: remaining key lifetime (k/sec): (4525504/3550)
        IV size: 16 bytes
        replay detection support: N
```

Ctrl+F6 to exit CLI focus Copy Paste

Top

Рис. 3. Шифрование передаваемого VoIP-трафика

Заключение. В результате проведенной работы была смоделирована защита IP-телефонии средствами современных протоколов туннелирования и шифрования. Также в статье были рассмотрены теоретические особенности функционирования IP-телефонии и проанализированы современные протоколы. В статье предложены методы защиты IP-телефонии, позволяющие снизить угрозы, связанные с передачей голосового трафика. Один из предложенных подходов, связанный с защитой конфиденциальности был реализован в среде эмуляции.

СПИСОК ЛИТЕРАТУРЫ

1. Морриси П. IP-телефония — звено в системе корпоративной безопасности / П. Морриси. — Текст : электронный // Сети и системы связи. — 2006. — № 2. — URL: https://www.elibrary.ru/item.asp?id=15539010& (дата обращения: 20.05.2022).
2. Ковцур М. Протоколы обеспечения безопасности IP-телефонии / М. Ковцур. — Текст : электронный // Первая миля. — 2012. — № 5. — URL: https://www.elibrary.ru/item.asp?id=15539010& (дата обращения: 20.05.2022).
3. Степкина Т. А. Рекомендации по защите внутрикорпоративной сети IP-телефонии от несанкционированного доступа к конфиденциальной информации / Т. А. Степкина. — Текст : электронный // Альманах мировой науки. — 2016. — № 5. — URL : https://www.elibrary.ru/item.asp?id=26210322 (дата обращения: 20.05.2022).
4. VoIP (voice over Internet Protocol) / A. S. Gillis. — URL: https://www.techtarget.com/searchunifiedcommunications/definition/VoIP (date of the application: 20.05.2022). — Text : electronic.
5. Протокол SIP Протокол инициирования сеанса. — Текст : электронный. — URL: https://russianblogs.com/article/88951639769/ (дата обращения: 20.05.2022).
6. Internet Telephony Protocol | H.323. — URL: https://www.techtarget.com/searchunifiedcommunications/definition/VoIP (date of the application: 20.05.2022). — Text : electronic.
7. SCCP на Asterisk 11 без прошивки телефона CISCO серии 7960. — Текст : электронный. — URL: https://voxlink.ru/kb/asterisk-configuration/sccp-na-asterisk-11-bez-proshivki-telefona-cisco-serii-7960/ (дата обращения: 20.05.2022).

8. Is VoIP Secure? The Ultimate Guide to VoIP Security & Call Encryption Ethnography / Cameron Johnson. — URL: https://www.nextiva.com/blog/voip-security.html/ (date of the application: 20.05.2022). — Text : electronic.

Д. А. Ромейко, Т. И. Паюсова
Тюменский государственный университет, г. Тюмень

УДК 004.056

ОБЗОР ВОЗМОЖНОСТЕЙ СРЕДЫ METASPLOIT FRAMEWORK

Аннотация. *В данной статье приведены материалы, которые позволят студентам, изучающим информационную безопасность, освоить теоретические основы тестирования на проникновение. Понимание основ эксплуатации уязвимостей помогает студентам осознать важность и необходимость комплексной системы защиты, позволяющей снизить риск наличия недекларированных возможностей. Результатом работы стала серия лабораторных работ, посвященных эксплуатациям уязвимостей.*

Ключевые слова: *metasploit framework, эксплойт, payload, kali linux, metasploitable3, meterpreter, reverse shell, msfvenom, уязвимость, кибератака.*

Введение. Тестирование на проникновение позволяет ответить на вопросы о том, как злоумышленники могут вмешиваться в информационную инфраструктуру. Используя инструменты пентеста, «белые хакеры» и эксперты по информационной безопасности могут проникнуть в систему и проверить наличие сетевых и прикладных дефектов и уязвимостей на любом этапе разработки или развертывании.

Одним из инструментов пентеста является проект Metasploit Framework. Это платформа с открытым исходным кодом, которая позволяет выполнять тестирование системы на проникновение с помощью командной строки или графического интерфейса.

Проблема исследования. Статистика «Лаборатории Касперского» показывает, что в организациях наиболее серьезными последствиями кибератак являются невозможность доступа к критически важной бизнес-информации (59% российских компаний