Безопасность VoIP-контента. Текущая ситуация, анализ угроз и тенденции рынка

Ю. С. *Крюков*
kryukov@inbox ru

Окончание.
Начало см. в №2, 2008.

Механизмы и стандарты безопасности

Ниже мы рассмотрим стандарты и механизмы безопасности для протоколов SIP и H.323.

SIP-дайджест

Этот алгоритм «дайджест-аутентификации» *(digest authentication;* RFC-2617) в настоящее время наиболее востребован как инструмент защиты, применяемой совместно с SIP. Полученный из развития аналогичного дайджест-алгоритма для HTTP алгоритм SIP-дайджест-аутентификации позволяет производить аутентификацию SIP-абонентов (пользовательских агентов, прокси-серверов или серверов-регистрации). Алгоритм базируется на передаче «общего секрета», который состоит из контрольной суммы поверх nonce (уникальной комбинации для каждой сессии) и параметров (пользовательского имени, пароля, nonce, SIP-метода, Request URI). SIP-дайджест не осуществляет обмен паролями. Общий секрет хэшируется с использованием MD5 или SHA-1 (IETF рекомендовано использование SHA-1).

SIPS

SIPS (SIP поверх SSL/TLS[1]) защищает такие данные, как SIP URI и IP-адрес, от сниффинга и манипуляции сообщениями. Схема URI немного отличается от обычной SIP URI: sips:this_is_me@sip.com. SIPS шифрует соединение между SIP-абонентом и SIP URI и сетевой точкой (пользовательским агентом, прокси-сервером, DNS-сервером) через SSL/TLS, однако из-за SSL/TLS SIPS передается через TCP вместо UDP. Заданный по умолчанию номер порта для TCP поверх TLS-5061. Пользовательская аутентификация в этом случае проводится с использованием SIP-дайджеста, который хэширует SIP-сообщение (цифровая подпись).

SRTP

Так как RTP- и RTCP-протоколы не предлагают механизмов защиты против сниффинга и манипуляции VoIP-данными, был разработан протокол SRTP *(Secure RealTime Transport Protocol;* RFC-3711), эффективный для использования в приложениях реального времени и являющийся альтернативой базирующимся на IPsec VPN-соединениям. SRTP представляет собой защищенный вариант RTP (как SRTCP для

[1] *SSL/TLS используются в SIP*

RTCP). SRTP осуществляет шифрование данных симметрично с AES[2] (Advanced Encryption Standard), тем самым снижая вероятность эффективной реализации таких угроз, как сниффинг, повторы и DoS. При передаче RTP/RTCP-пакеты инкапсулируются в SRTP/SRTCP-пакеты. Алгоритмом SRTP используются следующие механизмы защиты контента:

- шифрование медиапотока (против сниффинга);
- аутентификация отправителя (против спуфинга);
- проверка целостности (против модификаций/манипуляций);
- защита от повторов[3] (против неавторизованного доступа к конечной точке).

SRTP определяет два вида ключей: мастер-ключ (Master Key K_M) и сессионный ключ (Session Key) - (K_E для шифрования и K_A для аутентификации). K_E (минимально – 128 бит) и K_A (минимально – 160 бит) получаются из K_M посредством криптографически стойкой псевдослучайной функции (Pseudo-Random Function – PRF).

Шифрование применяется к данным RTF-потока, а обмен ключами происходит через сигнальные сообщения, означая тем самым, что требуется использование механизмов безопасной передачи сигнальных сообщений, например SIPS.

В настоящее время не существует какого-то доминирующего метода генерации и распределения маргер-ключей. Наиболее подходящим вариантом является Multimedia Internet Keying (MIKEY; RFC-3830). MIKEY описывает процедуру управления и обмена ключами (Transport Encryption Key - TEK и Transport Generation Key - TGK) для мультимедийных сессий реального времени, а также процедуру обмена другими параметрами безопасности между абонентами. В общем, MIKEY служит для обмена мастер-ключом (K_M) и параметрами безопасности. Поскольку TEK может быть модифицирован (так называемый рекеинг), K_M также может подвергнуться модификации. В зависимости от используемого основного протокола, то есть SIP/H.323, MIKEY поддерживает соединения «пользователь-пользователь» (peer-to-peer) и «пользователь - много пользователей» (one-to-many). Это означает, что конечный пользователь, использующий SIP, может установить защищенный коммуникационный линк с конечным пользователем, использующим H.323. Кроме того, MIKEY способен поддерживать различные протоколы обмена ключами и параметрами безопасности для нескольких сессий параллельно. То есть RTP- и RTCP-линки, несмотря на использование всеми участниками TEK, могут защищаться одновременно и независимо [1].

S/MIME

S/MIME (Security/Multipurpose Internet Mail Extension; RFC-2311) был разработан для осуществления процедур шифрования и аутентификации тела сообщения (MIME) электронной почты. Однако его реальное использование этим не ограничивается. В IP-коммуникациях MIME может применяться для шифрованной передачи из «конца в конец» (end-to-end) тела сообщений и, тем самым, быть пригодным для SIP. Кроме этого, SDP-параметры, детализирующие данные абонентской информации, могут быть

[2] *AES-CTR uAES-f8*

[3] *При реализации атаки с помощью повторов злоумышленник раз за разом воспроизводит посылку записанных RTP- или RTCP-пакетов. Этот тип нападений можно рассматривать как DoS-атаку. Защита от атаки повторами может осуществляться только с помощью защиты целостности данных, воплощаемой через процедуру аутентификации сообщени, которой и обладает SRTP.*

защищены с помощью S/MIME.

В отличие от SIP, где шифрование применяется на базе «точка - точка» (hop-by-hop), не защищая информацию тела сообщения, передаваемого по SIP-сети, S/MIME предлагает шифрование «из конца в конец». Таким образом, информация тела сообщения может быть расшифрована только конечным пользователем посредством ассиметричной криптографии. Обмен публичными ключами в этом случае может быть реализован с помощью SIP или через сертификаты.

H.235

Стандарт H.323 v.4 (ITU-T) в структуре подстандарта H.235 для защищенной реализации H.323 изменен до H.235.9. Сегодня в H.323 v.6 расширены процедуры безопасности. Наиболее значительным из проведенных расширений является поддержка SRTP [7]. К текущим процедурам безопасности можно отнести:

- проведение базовой аутентификации пользователей (с помощью симметричной криптографии);
- аутентификацию посредством сертифицированных публичных ключей;
- метод обмена ключами Diffie-Hell-man (DH) - DH-ключи согласуются с публичными ключами, представляющими симметричные ключи для проведения процедуры аутентификации.

В настоящее время известно об одной уязвимости в H.323, делающей возможным его нецелевое использование посредством ASN.1 parsing в первой фазе обмена данными H.225 (initial call setup). Кроме этого, можно отметить сложность набора протоколов и большое число производителей, реализующих процедуру (ASN.1/PER[4] кодирования/декодирования) [2], что также повышает риск эффективного исполнения потенциальных угроз.

Для получателя существует возможность проверки RTP-пакетов с помощью Media Anti-Spam на подлинность заявленного отправителя.

ZRTP

ZRTP, разработанный Аилом Циммерманом и представленный ZFone, создан для реализации взаимодействия между конечным SIP-оборудованием различных производителей и проведения процедуры аутентификации между сторонами соединения. ZRTP является расширением RTP и описывает ключевое соглашение/принятие для использования с SIP и SRTP без необходимости применения разделенных секретов или независимой инфраструктуры публичных ключей (Public Key Infrastructure – PKI), используя вместо них для проведения идентификации голосовые аутентификационные дайджесты.

В течение процедуры установления соединения ZRTP осуществляет обмен ключами на основе алгоритма Diffie-Hellman внутри RTF-потока (иными словами, ZRTP-пакеты внедряются в RTF-пакеты). DH-обмен начинается с генерации общего секрета, на основе которого получается мастер-ключ для SRTP-сессии, передаваемый уровню SRTP. Последний из мастер-ключа получает сессионный ключ, осуществляя защиту от атак повтором с помощью аутентификационной числовой последовательности.

[4] *PER: Packet Encoding Rules*

AES используется для шифрования полей полезной нагрузки (непосредственных данных) и SRTP-пакетов, включая заголовки, посредством метода аутентификации SHA-1. Протокол опирается на предположение, что запрашиваемое соединение устанавливается с помощью такого механизма обмена сигнальными сообщениями, как SIP. Каждое использование SRTP идентифицируется с помощью уникальных данных (ZRTP Identification Data – ZID) – случайного 96-битового значения, которое создается для инсталляции Zfone. Если предварительно оговорено использование распределенных секретов, работа ZID происходит с учетом этой договоренности.

SPIT filtering

Для противодействия. SPIT-атакам используется SPIT filtering, функционирование которого основывается на использовании механизма создания белых/черных списков. Каждый VoIP-абонент обладает списком желательных/нежелательных абонентов. Использование белого списка является очень эффективной, но непрактичной мерой, так как некоторые абоненты не могут вступить в запрашиваемое соединение не будучи занесенными в белый список. Своеобразным компромиссом между требованиями безопасности и доступности выступает использование так называемых расширенных белых списков, включающих доверенные web-источники.

Общая оценка

SIP-дайджест обладает некоторыми широко известными уязвимостями, которые легко могут быть использованы злоумышленником. Одной из наиболее потенциально опасных уязвимостей является ограниченная процедура проверки целостности сообщений (заголовок не подвергается этой процедуре) [4]. Злоумышленник способен изменить сообщение или с помощью реализации MitM-сниффинга получить уникальные пользовательские идентификаторы, изменить их и переслать серверу. Кроме того, так как большинство реализаций позволяют использовать уникальные пользовательские идентификаторы в течение некоторого периода времени, злоумышленник может реализовать повторную пересылку, то есть атаку повторением. С учетом этого, злоумышленник в состоянии также осуществить собственную регистрацию в качестве легитимного пользователя. Доступно и перенаправление данных разговора на собственное оконечное устройство. Отметим, что не всеми методами реализации запросов поддерживается алгоритм дайджеста.

Транзакционная модель реализации запросов CANCEL и ACK в SIP обладает слабой аутентификацией. С точки зрения общих задач безопасности это весьма и весьма посредственно. Методы реализации запросов используют режим hop-by-hop и таким образом могут реализовываться на любом из пунктов (серверов) в сигнальной цепочке. Маловероятно, что каждый из задействованных серверов реализует процедуры безопасности, ассоциированные с другими пунктами, что в целом делает проведение аутентификации запросов малореальной. Кроме того, числовые последовательности этих двух запросов должны быть точно такими же, как и для тех запросов, с которыми они ассоциированы (изменение числовой последовательности приводит к потери ассоциативности).

Недостаточность проводимой для CANCEL и ACK аутентификации делает возможным эффективную реализацию угрозы «инъекции». Злоумышленник может фальсифицировать запросы CANCEL, приводящие к расторжению установленной пользовательской сессии, и злонамеренные ACK-сообщения (уникальные пользовательские данные в ACK-сообщениях идентичны используемым в предыдущем) [7]. В [7] предложен метод противодействия описанным выше возможностям с помощью «связывания» критически значимых полей заголовка, гарантирующего целостность последнего криптографическими методами, не давая злоумышленникам внести в него изменения.

SIP обладает множеством различных механизмов обеспечения безопасности, упомянутых при рассмотрении SIPS. Некоторые из них напрямую интегрированы в SIP-протокол, например http-аутентификация. Эти механизмы имеют альтернативные алгоритмы и параметры. SIPS не обеспечивает реализацию процедур безопасности «из

конца в конец», а поддерживает только режим hop-by-hop, что приводит к необходимости проведения пунктами сети аутентификационных процедур друг для друга. RFC-3261 не содержит никаких механизмов достижения этого требования. Кроме того, даже если некоторые механизмы, такие как OPTIONS, были использованы для достижения соглашения об аутентификации, достигнутое соглашение будет уязвимо для атак Bidding-Down[5]. В стандарте RFC-3329 определены три поля заголовка для реализации согласования механизмов безопасности в SIP, между пользовательским агентом SIP и следующим в цепочке SIP-сервером. В целом, существуют пять механизмов безопасности:

- TLS;
- http-дайджест;
- IPsec с IKE;
- неавтоматический ключевой IPsec без IKE;
- S/MIME.

В настоящее время в рамках IETF существует два проекта, касающихся процедур обеспечения безопасности на участках «из конца в середину» (end-to-middle), «середина - середина» (middle-to-middle) и «из середины в конец» (middle-to-end): End-to-middle Security in the Session Initiation Protocol (SIP) [10] и A Mechanism to Secure SIP information inserted by Intermediaries [11]. Требования безопасности между двумя подходами несколько отличаются, однако SIP End to Middle Security [10] и SIP Intermediate Security [11] ориентированы на решение одинаковых фундаментальных проблем обеспечения безопасности в SIP [9].

Протокол SRTP реализован по принципу «из конца в конец», то есть его использование не зависит от существующей сетевой инфраструктуры, а, значит, подходит для общественных сетей. Применяемый криптоаназиз, в целом, уменьшен за счет повторного использования мастер-и сессионного ключей. Из-за низкого использования ресурсов применение SRTP не оказывает никакого воздействия на качество предоставления VoIP-сервисов.

Механизмы противодействия атакам повторной передачи SRTP реализует с помощью «списков повторов», которые содержат перечень идентификаторов ранее полученных и подтвержденных (доверенных) пакетов. Это позволяет получателю производить соответствующий сравнительный анализ данных перечня с получаемыми в настоящее время пакетами. Такой механизм требует наличия у IP-телефона соответствующего размера памяти.

Аутентификация и подтверждение целостности получаемых RTP-сообщений реализуется с помощью HMAC-SHA-1 с K_A. Однако из-за недостатков HMAC-SHA-1 экспертами рекомендуется использование SHA-256, несмотря на нестандартизованность такого решения. Рекомендуется также использовать шифрование полезных данных RTP с последующим расчетом цифрового отпечатка (fingerprint) зашифрованных данных.

SRTP поддерживает безопасные RTF-сессии в течение фазы установления соединений, предшествующей обмену SRTP-пакетами. Однако фундаментальные данные (идентификатор вызова, от кого и к кому устанавливается соединение, как оно проходит, с использованием каких кодеков и пр.) передаются в открытом виде, что дает

[5] *Вариант атаки «man-in-the-middle», при котором злоумышленник изменяет сообщения, дабы убедить стороны соединения в том, что на обеих сторонах поддерживаются только слабые алгоритмы.*

возможность злоумышленнику эффективно реализовать угрозы типа MitM, спуфинг или фишинг[6]. Таким образом, требуется использовать защитные механизмы (осуществлять кодирование SIP-пакетов) в течение всего времени установления соединения.

SRTP также уязвим для атак Bid-Down (MitM), при которых злоумышленник вынуждает использовать более низкий уровень шифрования (например, AES-128 вместо AES-256) путем удаления информации AES-256 в INVITE-сообщении [3].

При использовании S/MIME возникает одна проблема: в настоящее время нет организации, управляющей распределением сертификатов, то есть не существует глобальной инфраструктуры PKI. Кроме того, установление S/MIME безопасных соединений является продолжительным процессом.

Единственная известная в настоящее время уязвимость протокола H.323 связана с дефектом ASN.1 parsing, имеющим место в первой фазе обмена H.225-данными. H.235 призван изменить эту ситуацию. Можно также отметить сложность набора протоколов и большое число производителей, реализующих процедуру (ASN.I/PER[87] кодирования/декодирования) [2], что повышает риск эффективного исполнения потенциальных угроз.

Несмотря на то что ключевой обмен не защищен против MitM-атак, связь, организованная с помощью ZRTP, является, в целом, безопасной, так как обладает криптографической стойкостью. Однако уязвимости ZRTP вполне могут быть использованы ресурсоемкими злоумышленниками. Именно поэтому некоторыми экспертами предлагается внести в протокол ряд изменений.

IAX, используемый Asterisk-серверами, является основой построения PBX-серверов от Digium. Он используется для реализации VoIP-соединений между Asterisk-серверами и между сервером и клиентами, также использующими протокол IAX. В настоящее время наиболее широко распространена вторая версия протокола IAX-IAX2.

IAX2 очень рациональный, полный и в то же время простой протокол, являющийся опосредованным к используемым кодекам и числу потоков. Таким образом, он фактически может применяться в качестве транспорта для любого типа данных. IAX2 использует единый UDP-поток данных, обычно инициализируемый на порте 4569 для организации связи между конечными точками, а также передачи сигнальной информации и данных. Голосовой трафик передается внутриполосно, что делает IAX2 более коммуникабельным для межсетевых экранов (МЭ) и отличает от SIP, эксплуатирующего внеполосную передачу RTP-потоков.

---

[6] *Phiihing - это мошенничество с целью хищения личных данных. При phishing-атаках мошенники под фальшивыми предлогами пытаются вынудить вас раскрыть важные личные данные, такие как номера кредитных карточек, пароли, данные о банковском счете и т. д. Phishing-атаки могут проводиться лично, по телефону или в сети через нежелательные сообщения электронной почты или всплывающие окна.*

[7] *PER: Packet Encoding Rules.*

Таблица 3. Обзор протоколов безопасности для VoIP

Механизмы безопасности	Конфиденциальность	Целостность	Аутентификация	Контроль доступа	Ответственность	Анонимность
SIP-дайджест	-	-	+	+	+	-
SIPS	+	+	(+)	-	-	-
S/MIME (тело сообщений)	(+)	(+)	(+)	(+)	(+)	(+)
SRTP	(+)	(+)	(+)	-	-	
H.235	+	+	+	-	-	-
ZRTP	(+)	(+)	(+)	-	-	-
IAX2	+	+	-	-	-	(+)
Skype	(+)	(+)	-	-	-	-

Базовая структура IAX разработана для мультиплексирования сигнальной информации и мультимедийных потоков в единый UDP-поток, циркулирующий между двумя компьютерами. Протокол IAX является бинарным, предназначенным для уменьшения объема служебной информации в отношении передаваемого голосового контента. Общая эффективность использования пропускной способности была отодвинута на второй план, выдвигая в качестве приоритетной цели формирования IAX-протокола обеспечение эффективной полосы пропускания для индивидуальных голосовых вызовов. Создание единого UDP-потока и манипуляции с ним являются более простыми задачами для пользователя, расположенного позади МЭ. Кроме этого, IAX2 может использовать механизмы шифрования (AES-128) для защиты голосовых данных и сигнальной информации, тем самым поддерживая возможность реализации безопасных соединений.

Skype-пользователи, по существу, имеют возможность осуществлять телефонные вызовы и пользоваться видеосвязью с помощью своего компьютера, программного обеспечения Skype и ресурсов сети Интернет. В основе Skype-соединения лежит инсталлируемое пользователями бесплатное программное обеспечение, при этом установление такого соединения возможно не только со Skype-пользователями, но и с абонентами сетей мобильной и традиционной телефонии. В настоящее время Skype-приложение является бесплатным и может быть загружено с web-сайта компании, однако само программное обеспечение является собственностью разработчика, сохраняющего его закрытым. Главное отличие Skype от других VoIP-приложений заключается в том, что оно использует прямое (peer-to-peer) соединение, в то время как более традиционной является клиент-серверная модель. Директория Skype-пользователей полностью децентрализована и распределена среди сетевых узлов, что означает возможность осуществления легкого масштабирования до очень больших размеров (сегодня насчитывается более 100 миллионов пользователей) без необходимости дополнительных капитальных затрат. Сегодня обсуждение реальной опасности Skype-трафика приобрело значительные масштабы, выходя далеко за пределы непосредственной безопасности Skype, и оказало большое влияние на VoIP-культуру в целом, что в сумме констатировало формирование нескольких дизайнерских принципов:

- весь Skype-трафик шифруется по умолчанию, пользователю недоступно отключение опции;
- на основе имеющихся данных предполагается, что Skype использует надежные алгоритмы шифрования;
- пользователи не вовлечены в процесс шифрования и не имеют никакого отношения к открытой ключевой инфраструктуре.

Констатация вышеизложенных принципов оказала большое влияние на существующий рынок, заставив других производителей предлагать сопоставимые, конкурентоспособные продукты.

Реализация концепции безопасности

В настоящее время VoIP-сети содержат широкий спектр различных компонентов: телефоны, менеджеры вызовов, шлюзы, серверы, маршрутизаторы и т.д. Существующая VoIP-инфраструктура требует воплощения определенных требований безопасности, которые формируются из двух фундаментальных составляющих общих требований безопасности сетей и специфических требований безопасности, актуальных исключительно для VoIP-сетей и сервисов.

В следующих разделах мы коснемся некоторых базовых принципов защиты и сформулируем общие рекомендации по созданию безопасных VoIP-сетей с учетом специфики VoIP-приложений.

Стандарт сетевой безопасности

Создание защищенной VoIP-сети должно начинаться с использования стандартных механизмов защиты, традиционно используемых для сетей передачи данных. Дополнительные меры безопасности, использование которых применительно к VoIP-сетям является столь же необходимым, обуславливается спецификой самих VoIP-сетей и приложений, для которых характерны специфические и уникальные угрозы безопасности. Необходимым и основным условием создания безопасной VoIP-сети является глубоко продуманное сетевое планирование с учетом требования предоставления услуг с определенным качеством (Quality-of -Service - QoS).

Важно понимать, что восприятие VoIP-сетей и услуг с точки зрения реализации концепции безопасности не должно осуществляться через призму других IP-приложений.

В то время как безопасность сетей передачи данных, прежде всего, сосредоточивается на защите данных сетевого уровня (например, посредством VLAN и МЭ), реализация безопасности ассоциированных с VoIP компонентов требует использования мультиуровневого подхода, включающего идентификацию физических устройств (телефонов, шлюзов и серверов) и сетевых точек доступа вместе с их авторизацией. Необходимо предусмотреть механизмы защиты сессионного и транспортного уровней, так как именно для этих уровней существует вероятность эффективной реализации таких угроз, как DoS и MitM. Наконец, 7-й уровень эталонной модели ISO-OSI - уровень приложений - должен быть защищен от вирусов, SPIT-атак, мошенничеств и других характерных атак.

Виртуальные локальные сети (VLAN)

В качестве возможного решения проблемы обеспечения информационной безопасности для корпоративных сетей можно рекомендовать развертывание двух независимых VLAN-сетей: одной - для трафика данных, а другой - для голосового трафика. При этом идеально было бы выделить две независимые подсети с различным диапазоном адресов в соответствии с RFC-1918 (Ю.x.x.x, 172.16.X.X и 192.168.X.X). Кроме того, развертывание раздельных DHCP-серверов позволяет легче обнаружить сетевое вторжение и обеспечить защиту с использованием средств межсетевого экранирования.

Логическое разделение гарантирует невозможность одновременной атаки на сеть данных и VoIP-сеть. Одни вирусы не могут быть использованы, злоумышленником для обеих сетевых составляющих. Также описываемая архитектурная модель значительно усложняет злоумышленнику осуществление сниффинга, перехвата или подслушивания трафика.

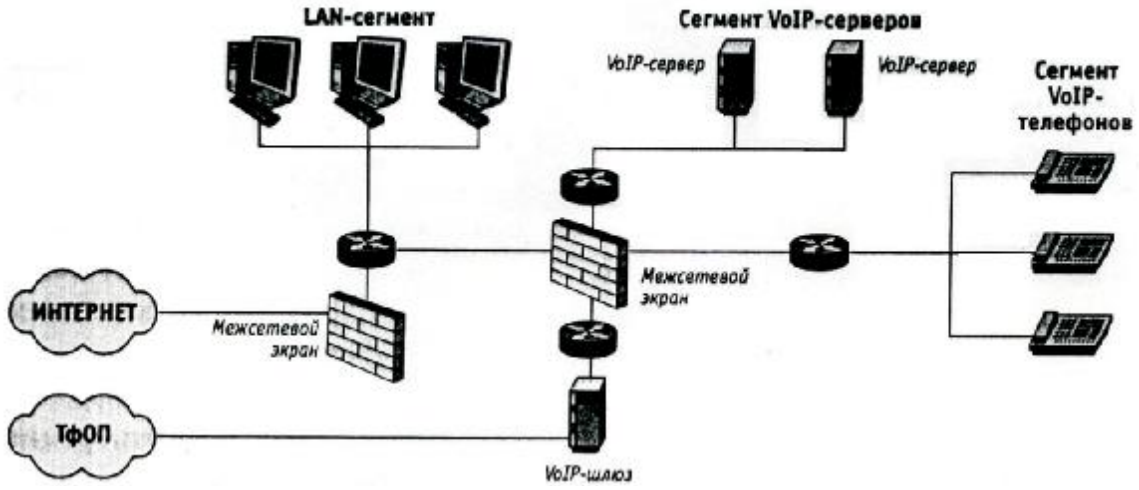

Рис. 2. VLAN и межсетевое экранирование

Другим преимуществом является возможность введения приоритетных классов для управления качеством обслуживания. В этом случае голосовой трафик может обслуживаться с более высоким приоритетом, чем данные.

В VoIP VLAN используются исключительно телефоны, что дает возможность сетевому администратору отслеживать состояние своей сети и своевременно определять использование доверенных ресурсов в мошеннических целях.

Благодаря разделению и независимой обработке трафика данных и голосового трафика исключается вероятность возникновения коллизий, так как исключено «соревнование» трафика, что, в свою очередь, увеличивает качественные характеристики запрашиваемых сервисов (за счет уменьшений очереди/времени ожидания). Аудиопотоки очень чувствительны к временным характеристикам, так что описанный недорогой подход разделения трафика позволяет существенно улучшить предоставление VoIP-сервисов в существующей сетевой инфраструктуре.

Вместе с тем, несмотря на то что описанная VLAN представляет изящный путь решения проблемы информационной безопасности, полное разделение составляющих сетевого трафика без VLAN-маршрутизации проблематично по ряду причин [12]:

- софтфоны рабочих станций сети данных требуют обеспечения доступа к VoIP-серверам в VoIP-сетях;
- клиентам, совместно использующим общий ресурс, необходимо иметь возможность прямого набора телефонного номера из контакта в приложении (например, Lotus Notes или Outlook);
- VoIP-сервер связан с каталогом услуг, таким как LDAP или ADS.

Однако VoIP-инфраструктура некоторых предприятий, использующих большое число различных устройств (VoIP-серверов, VoIP-шлюзов, VoIP-телефонов, софтфонов, СП-

систем и др.), связанных друг с другом, слишком сложна для VLAN. Эти проблемы могут быть решены расположением VoIP-сервера одновременно в сети трафика данных и голоса.

Рисунок 2 иллюстрирует возможное построение сетевой инфраструктуры с использованием двух МЭ: одного - для сетей передачи данных, а другого - для телефонной сети. Первым обеспечивается передача пакетов из сети Интернет во внутреннюю сеть для сеансов, инициированных пользователем внутренней сети. Второй МЭ управляет трафиком телефонов, VoIP-серверов и VoIP-шлюзов.

Шифрование

Шифрование используется для обеспечения конфиденциальности и аутентификации в телефонной связи. Реализация безопасных телефонных соединений возможна с использованием SRTP, шифрования RTP-контента и информации сигнализации с TLS. Использование TLS, являющегося альтернативой IPsec, обеспечивает надежную защиту против хакерских атак, в то время как SRTP обеспечивает защиту против подслушивания.

IPsec используется для шифрования сообщений установления соединения и сообщений управления, являясь эффективным средством защиты информации и противодействия подслушиванию. IPsec может использоваться в «туннельном режиме» (tunnelling mode) вместо «транспортного режима» (transport mode), так как туннелирование закрывает IP-адреса источника и получателя, чем обеспечивает защищенное от анализа трафика соединение. Однако использование IPsec предполагает его поддержку на устройствах и менеджерах вызовов[8].

Кроме того, возможно возникновение проблем взаимодействия с некоторыми устройствами управления и мониторинга, не поддерживающими шифрование. Существует и проблема с NAT. IPsec использует порт 500, который обходит мульти-туннели VoIP через NAT.

Большинство пользовательских VoIP-решений, к сожалению, не поддерживает шифрование, что приводит к достаточно простому для злоумышленника прослушиванию VoIP-соединения или даже изменения его содержимого. Существует несколько открытых решений, облегчающих злоумышленнику процедуру сниффинга VoIP-соединений. Некоторые надежды на получение безопасного VoIP-соединения можно связывать с использованием закрытых патентованных кодеков, однако, как показывает практика, закрытость решений еще не гарантирует их надежности. Некоторые производители используют сжатие для повышения уровня защищенности, но важно понимать, что настоящая безопасность связи может быть достигнута только с использованием шифрования и криптографической аутентификации, которые узко доступны на потребительском уровне.

Аутентификация

В отличие от PSTN-систем, где каждый телефонный аппарат определяется телефонным номером (ID), соответствующим физическому расположению телефонной линии, к которой аппарат подключен, VoIP-системы назначают телефонам IP-адреса. Так как

[8] *SRTP доступен на аналоговых телефонных адаптерах Analog Telephone Adapters (ATA), производимых некоторыми компаниями, например Sipura/Linksys. SRTP также доступен для Gizmo Project для софтфонов (PC/лаптопы, реализующие телефон).*

подобная архитектура предполагает возможность эффективной реализации spoof-атак (при этом злоумышленник присваивает себе чужой ресурс), необходимо принудительное проведение процедуры определения идентичности потенциальных подписчиков при аутентификации в режиме «пользователь - пользователь» (peer-to-peer). Однако такая реализация достаточно сложно применима на практике, так как секретная информация, требующаяся для каждой аутентификации, не может быть легко распределена между пользователями, выдвигая необходимость применения РК1-подхода.

Конфиденциальность связи между VoIP-пользователями - главная задача обеспечения защищенности коммуникаций, так как общедоступные открытые IP-сети являются целью злоумышленников, легко способных реализовать MitM-атаку, чтобы получить доступ к частной информации участников соединения. Поэтому для любого VoIP-соединения требуется проведение соответствующих процедур шифрования и аутентификации.

С тех пор как VoIP-системы, например VoIP-шлюзы или VoIP-серверы, стали составлять основу осуществляемых сотрудниками компании речевых соединений, эффективная в их отношении реализация угроз безопасности ставит под сомнение общую функциональность корпоративной VoIP-сети и ее компонентов, а значит, требует защиты от НСД центральных VoIP-систем. Следовательно, все сетевые пользователи и администраторы должны проходить аутентификацию, проводимую центральной аутентификационной службой, которая связана с системой МЭ, реализующей контроль доступа к сетевым ресурсам.

Средство межсетевого экранирования

МЭ являются стандартным инструментом защиты сетей передачи данных, проверяя каждый пакет, проходящий из доверенной сети или в нее. Базирующиеся на SIP и H.323 услуги IP-телефонии используют UDP-пакеты и входящие TCP-соединения. Однако в большинстве случаев конфигурации используемых в компаниях МЭ не позволяют протекать VoIP-контенту. Кроме того, из-за динамического распределения портов по запросу МЭ не способны эффективно фильтровать VoIP-трафик. При этом совсем не важно, какой сетевой протокол (SIP или H.323) используется. В обоих случаях требуется реализация stateful-фильтрации[9] протекающего трафика и его ассоциирование с номером порта. Подобный тип МЭ способен запоминать ранее пройденный трафик и анализировать данные прикладного уровня, содержащиеся в пакетах. Более того, подобные экраны способны анализировать адрес отправителя и отвергать пакеты, получаемые от нежелательных источников.

Шлюзы прикладного уровня (Application Level Gateways – ALG[10]) являются альтернативой использованию МЭ. Так как они «понимают» VoIP-протокол, для них

[9] *Stateful-фильтрация (фильтрация с учетом контекста) - отслеживание текущих соединений и пропуск только тех пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений. Такие типы сетевых экранов позволяют эффективнее бороться с различными видами DoS-атак и уязвимоапями некоторых сетевых протоколов. Кроме того, они обеспечивают функционирование таких протоколов, как H.323, SIP, FTP и т. п., использующих сложные схемы передачи данныхмежду адресатами, плохо поддающиеся описанию статическими правилами и, зачастую, несовместимые со стандартными (stateless) сетевыми экранами.*

[10] *ALG является специфическим инструментом прикладного уровня, адаптированным для работы с определенным протоколом на прикладном уровне и осуществляющем фильтрацию сообщений в соответствии с заданной политикой безопасности. ALG спосо-I бен модифицировать сообщения.для приведения их в соответствие с используемой политикой безопасности.*

возможно осуществление анализа данных прикладного уровня, то есть непосредственно полезной нагрузки, заключенной в анализируемом пакете. ALG обладает программным обеспечением, которое является анализатором для ASN.1-данных (H.323, кодируемый в ASN.l), SIP, MGCP и SDP, осуществляет временную запись состояний сигнальных протоколов и динамически открывает/закрывает порты в соответствии с состоянием сессии.

По сравнению со stateless и stateful межсетевыми экранами ALG предлагает наивысший уровень безопасности, так как открывает UDP-порты только для актуальных соединений, а не предлагает открытие диапазона портов.

Несмотря на существующий на рынке перечень коммерческих предложений по ALG для VoIP-протоколов, большинству существующих сегодня средств межсетевого экранирования недоступна эффективная обработка VoIP-протоколов, таких как SIP. Кроме того, у производителей, использующих протоколы собственной разработки, существует проблема с динамическим открытием диапазона портов и отсутствует поддержка NAT. Пограничный контроллер сессий (Session Border Controllers - SBC) является новым поколением МЭ, призванных решить большинство существующих проблем взаимодействия VoIP-протоколов и средств межсетевого экранирования. SBC контролирует сигнальный и медиатрафик (видео, данные, голосовую информацию).

Адекватные средства межсетевого экранирования должны быть способны контролировать сигнальную информацию, NAT VoIP и управлять медиасессией.

Системы обнаружения и предотвращения вторжения

Системы обнаружения и предотвращения вторжений (Intrusion Detection Systems и Intrusion Prevention -IDS/IPS) быстро становятся неотъемлемой частью большинства систем безопасности, ориентированных на использование МЭ. Они блокируют злонамеренные пакеты и защищают от вторжения сетевую систему. Однако не достаточно четко и правильно сконфигурированные системы обнаружения и предотвращения вторжений могут существенно понизить качество сетевых сервисов, так как способны ошибочно маркировать нормальные пакеты как злонамеренные и препятствовать их прохождению. Например, обычные UDP-пакеты небольшого размера могут быть восприняты такой системой, как UDP-флудинг при реализации DoS-атаки. Это в состоянии повлечь за собой ретрансляцию, которая станет причиной снижения качества предоставляемых услуг. То есть необходимо использование адаптированных для VoIP пограничных IPS.

NAT и STUN

NAT – типичная сетевая опция, заключающаяся в переводе частных сетевых адресов в публичные. NAT-маршрутизаторы передают пакеты только тех соединений, которые инициированы из доверенной сети, и отклоняют пакеты, спонтанно поступающие в доверенную сеть из внешней. Поступающие входящие голосовые пакеты UDP переадресовываются на порт получателя, однако ассоциирование с получателем происходит динамически и может быть реализовано различными путями.

Другая проблема связана с интерпретацией исходящих вызовов, поскольку NAT способен осуществлять передачу пакетов третьего уровня, тогда как TCP оперирует с четвертым. NAT изменяет IP-адрес источника (в IP-заголовке) и порт источника (в UDP- или TCP-заголовке).

В то же время информация об IP-адресе и UDP-порте остается неизменной в пределах части передачи сигнальных сообщений, что требует сохранения внутреннего IP-адреса как адреса отправителя в IP-заголовке исходящего пакета. Результат - безответность вызовов ввиду невозможности маршрутизации внутреннего IP-адреса. Публичный (внешний) IP-адрес должен быть передан получателю. Серийное туннелирование (Serial Tunnelling - STUN; RFC 3489) помогает решить эту проблему: конечные точки доступа могут получить публичный IP-адрес и связать NAT со шлюзом. Для этого STUN-клиент (например, VoIP-телефон) посылает на STUN-сервер запрос, в ответ на который ему определяется клиентский мандат (имя пользователя и пароль). Затем клиент посылает второй запрос, указывая данный мандат с целью получения от расположенного перед STUN-сервером NAT-шлюза информации NAT-связи. STUN-сервер извлекает из сообщения IP-адрес источника и IP-порт источника и передает их в ответном сообщении STUN-клиенту. Впоследствии соответствующие VoIP-приложения меняют публичные IP-адреса на внутренние IP-адреса и вставляют их в заголовок. Дальнейшие запросы позволяют клиенту идентифицировать тип NAT. На сегодняшний день STUN поддерживается многими моделями VoIP-телефонов и провайдерами.

Таким образом, по возможности нужно найти компромисс между необходимостью использования NAT или таких механизмов, как STUN или TURN.

Софтфоны или аппаратные IP-телефоны?

Телефон, являющийся самым традиционным и распространенным элементом VoIP-сетей, к сожалению, также может стать целью атаки злоумышленника.

С точки зрения обеспечения безопасности и надежности связи к использованию софтфонов нужно подходить очень взвешенно. Так как софтфоны нарушают традицию разделения голоса и данных (что в общем случае – весьма положительный момент технологической динамики), они уязвимы для различных вирусов и червей, имеющих множество точек входа в систему, на которой базируется софтфон. К этим точкам входа относятся операционные системы, собственно приложение IP-телефонии и используемые услуги. В отличие от традиционных аппаратных IP-телефонов, которые размещаются в VoIP сегменте VLAN, софтфоны относятся к сегменту сети данных и поэтому подвержены всем характерным для этого сегмента атакам. Кроме этого, традиционные аппаратные IP-телефоны базируются на фирменных операционных системах, составляющих собственность разработчика, и способны предоставлять ограниченный перечень сервисов.

Большинство традиционных аппаратных IP-телефонов использует закрытые протоколы, такие как Unistim (Nortel), SCCP (Cisco) или H.323 с собственными расширениями (Avaya). Использование собственных фирменных протоколов в общем случае является более безопасным решением, поскольку эти протоколы не составляют открытую информацию, а, значит, потенциальным нарушителям трудно провести их анализ с целью выявления возможных уязвимостей и их последующего использования. Также учтем, что традиционные аппаратные IP-телефоны - гораздо менее достижимая цель для потенциальных нарушителей, так как они ориентированы на выполнение более узкого спектра задач и обладают менее сложным программным обеспечением.

Рекомендуется использование телефонов, предлагающих сильные механизмы защиты (аутентификацию и/или шифрование) для информации сигнализации и медиаданных.

Сетевые устройства

Необходимо использовать криптостойкие пароли. Если для сетевого администрирования используется HTTP или TELNET, соединение между клиентом и сетевым устройством должно быть безопасным с использованием SSL/TLS или SSH.

Операционные системы

В общем случае VoIP-системы используют операционные системы общего назначения, традиционно имеющие множество уязвимостей. При этом основным принципом реализации информационной защиты в таких условиях является запрещение использования/закрытие всех неиспользуемых в операционной системе VoIP-системы (VoIP-сервера или IP PBX) сервисов.

Кроме этого, VoIP-системы, базирующиеся на операционных системах общего назначения, таких как Windows или Linux, должны использовать механизмы дополнительной защиты.

Качество обслуживания (Quality-of-service – QoS)

При построении защищенных VoIP-сетей и систем необходимо учитывать тот факт, что использование таких средств межсетевого экранирования, как stateful или ALG, может увеличить время обработки/ожидания трафика, оказывая сильное влияние на общее качество предоставляемых услуг. Также надо принять во внимание, что другие VoIP-системы, такие как VoIP-телефоны, имеют достаточно низкую вычислительную мощность, что приводит к трудности эффективной реализации шифрования для повышения общего уровня безопасности. Существует лишь несколько моделей IP-телефонов, предоставляющих возможность реализации AES-шифрования по разумной цене. В этом случае рекомендуется возложить ответственность за шифрование на центральный сетевой пункт – маршрутизатор или шлюз, который шифрует весь трафик от любого хоста или системы, используя, скажем, IPsec-туннелирование.

Необходимо отметить связь между QoS и используемыми протоколами. Например, SIP-протокол кодирует сообщения в ASCII-формате, который в некоторых случаях образует слишком большие объемы данных, не пригодные для использования в сетях с низкой пропускной способностью. Поскольку в общем пакет может превышать MTU-размер при использовании, скажем, беспроводной LAN, не исключены задержки пакетов или их потери. Для решения этой задачи целесообразно применять бинарное кодирование SIP в соответствии с рекомендациями RFC-3485 и RFC-3486.

Удаленное управление

Для реализации функций удаленного управления и аудита доступа рекомендуется использовать IPsec или Secure Socket Shell (SSH). Другая возможность состоит в использовании HTTPS с TLS. Необходимо избегать возможности получения удаленного управления IP-PBX системами от небезопасных точек. Если предоставление возможности удаленного доступа является необходимостью, целесообразно предусмотреть процедуры шифрования для запрашиваемого доступа.

Патчи

Особенно внимательны сетевые администраторы должны быть к патчам текущего ПО VoIP-систем и приложений.

Принципы минимизации VoIP-рисков

В настоящее время наиболее актуальными задачами функционирования VoIP-систем представляются обеспечение необходимого качества обслуживания и безопасность. В рамках данной статьи мы проанализировали возможные угрозы безопасности VoIP-систем и VoIP-приложений, а также продемонстрировали некоторые методы и механизмы противодействия таковым.

Таблица 4. Принципы минимизации VoIP-рисков

Потенциальная угроза	Наилучший механизм противодействия
Атака на уровне приложения	• ALG, межсетевые экраны, IDS/IPS прикладного уровня
DoS/DDoS	• IDS/IPS прикладного уровня • Антивирусная система • Изменение текущего приложения с помощью патча • VLAN • Создание домена безопасности с жесткой политикой безопасности
Подслушивание	• VPN для изоляции VoIP-трафика • Выборочное шифрование
Атаки на протоколы	• ALG и IDS/IPS
SPIT	• Строгая аутентификация, авторизация и IPsec
SIP-мониторинг, спуфинг	• Строгая аутентификация, авторизация и IPsec
Вирусы и черви	• Патчи для текущих приложений • Антивирусная система • IDS/IPS прикладного уровня • VLAN • Создание домена безопасности с жесткой политикой безопасности

SIP и RTP имеют приемлемые возможности для реализации шифрования и проведения аутентификации. H.323 также обладает потенциалом для реализации защищенных соединений. Остается вопрос реализации этих возможностей в существующем VoIP-оборудовании. Кроме этого, необходимо напомнить читателю, что работа по улучшению функционирования VoIP-оборудования и приложений постоянно ведется и в ближайшем будущем несомненно можно будет проанализировать новые возможности и механизмы защиты VoIP-контента. Приведенные в таб. 4 данные суммируют все сказанное в этой статье и определяют наиболее эффективные принципы минимизации VoIP-рисков.

ЛИТЕРАТУРА

1. BSI-VoIPSEC: Studie zur Sicherheit van Voice over Internet Protocol, pages 109-111, www.bsi.bund.de/literat/studien/VoIP/index.htm.
2. www.securityfocus.com/infocus/1782.
3. www3.ietf.org/proceedings/06mar/slides/ raiarea 1/raiarea-l.ppt.
4. Dorgham Sisalem et. al, SNOCER, Low Cost Tools for and High Available VoIP Communication Services, Towards a Secure and Reliable VoIP Infrastructure, 3rd May 2005, pp. 38-39, www.sno-cer.org/Paper/COOP-005892-SNOCER-D2-l.pdf.
5. www.ietf.org/internet-drafts/draft-guy-iax-02.txt.
6. voipsa.org/Resources/tools.php.
7. www.packetizer.com/voip/h323/whatsnew_ v6.html.
8. Anderson, Mark: VoIP Security - Uncovered; WhiteDust Security http://www.whitedust.net; Retrieved on 2006-05-26.
9. Kuhn, Walsh, Fries: Security Considerations for Voice Over IP Systems; Recommendations of the National Institute of Standards and Technology (NIST); NIST Special Publication 800-58; January 2005.
10. G. Egeland: Introduction to IPsec in IPv6; Eurescom; http://www.eurescom.de/~publicweb-deliverables/Pl 1 OOseries/Pl 113/Dl/pdfs/pirl/41_ IPsec_intro.pdf.
11. Cisco Networkers2000: http://www.cisco.com/ networkers/nwOO/pres/2403.pdf.
12. BSI-VoIPSEC: Studie zur Sicherheit van Voice over Internet Protocol, page 86, www.bsi.bund.de/ literat/studien/VoIP/index.htm.