УДК 681.3+681.031

Н.И. Алишов, доктор технических наук,
(Национальный авиационный университет, Украина),
В.А. Марченко, кандидат технических наук, А.Н. Мищенко, аспірант
(Институт кибернетики им. В.М. Глушкова НАН Украины)

ОСОБЕННОСТИ СОЗДАНИЯ СИСТЕМ ЗАЩИТЫ VOIP С ПРИМЕНЕНИЕМ МЕТОДА КОСВЕННОГО ШИФРОВАНИЯ

В статье рассматриваются вопросы связанные с особенностью применения метода косвенного шифрования в системах VoIP. Приводятся преимущества и недостатки применения указанного метода шифрования для защиты разговоров. Представлена концептуальная схема построения системы защиты для переговоров и описаны их особенности.

Большинство известных современных алгоритмов компьютерного шифрования не отвечают условиям абсолютной безопасности по Шеннону [1]. Это определяет априорную уязвимость используемых криптосистем, так как они построены на основе алгоритмов для которых не доказана теоретическая криптостойкость.

Шеннон сформулировал основные требования, предъявляемые к надежным шифрам. В частности, ключ для нераскрываемого шифра должен обладать тремя критически важными свойствами:

- быть истинно случайным – содержать истинно случайные последовательности;
- совпадать по размеру с заданным открытым текстом – быть не меньше открытого текста;
- применяться только один раз – не допускается повторное применение ключа.

Этим требованиям отвечает схема одноразовых блокнотов (One-time pad), реализованная ранее Гильбертом Вернамом [2].

При этом условия, которым должен удовлетворять ключ, настолько сложны, что практическая реализация криптоалгоритма, отвечающего трём требованиям абсолютной криптоустойчивости, является трудно осуществимой. Современные реализации одноразовых блокнотов используются только для передачи сообщений наивысшей секретности.

Использование в качестве поточного крипто алгоритма метод одноразовых блокнотов гарантирует абсолютную надежность и криптостойкость всей системы. Авторами предложен новый подход, для компьютерной реализации принципов заложенных в одноразовых блокнотах, который назван методом косвенного шифрования [3, 4].

Основная идея метода заключается в том что у отправителя и получателя имеются одинаковые массивы данных, которые являются секретными ключами. Байты информации, подлежащие защите, заменяются (по определенному алгоритму) байтами секретного массива. Полученный новый массив байт размером исходного сообщения передается адресату. Полученный по каналу массив данных, подвергается обратному преобразованию: байты заменяется байтами секретного файла (зеркальный алгоритм). Этот метод способен обеспечить абсолютную безопасность по Шеннону, поскольку объединяет принцип одноразовых блокнотов и небольшое количество алгебраических преобразований, к тому же он легко реализуется на большинстве существующих программно-аппаратных средствах, и при его использовании можно:

- создать средства для заполнения ключа истинно случайными числами;
- вне зависимости от количества передаваемых данных, размер ключа будет равен объему передаваемой информации;
- обеспечить однократность применения ключа.

Особенностью метода косвенного шифрования является то, что при шифровании одного и того же байта открытого текста всегда получаются различные байты шифротекста. Та-

ким образом, отпадает необходимость «нормализации» шифруемых сообщений для противодействия атакам с использованием статистических методов.

Для реализации метода косвенного шифрования могут использоваться как программные средства, так и аппаратные подсистемы выполняющие шифрование/дешифрование потоков полезной информации и способные генерировать истинно случайные числа, а также содержащие средства для хранения контейнера-ключа (рис.1) с возможностью его перезаписи (замены).

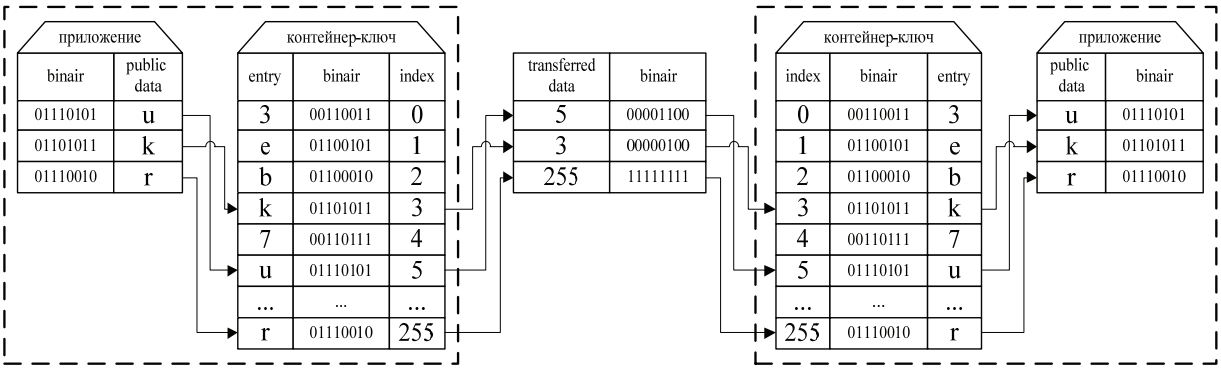

Рис.1. Общий алгоритм использования контейнера-ключа

В случае использования программных реализаций метода косвенного шифрования после установки соответствующего ПО на целевую систему необходимо дополнительно обеспечить организационную защиту помещений, где размещены эти криптосистемы.

Представленная криптосистема призвана обеспечить:

- качественно новый уровень криптографической стойкости шифруемой потоковой информации;
- шифрование в реальном времени больших объемов информации;
- максимальную гибкость и прозрачность в применении для обеспечения безопасности сторонних сетевых приложений.

В настоящее время всё большую популярность пользуются различного рода приложения для проведения телефонных разговоров видеоконференций, презентаций и т.п. через глобальные телекоммуникационные сети. Соответственно вопросы защиты данных в таких системах выходят на передний план, так как удобство и большая гибкость в организации подобных систем сопряжена с повышенными рисками, связанными с возможным несанкционированным доступом или прослушиванием[5].

При построении системы защиты для VoIP приложения кроме наличия общих угроз и связанных рисков дополнительно учитываются специфические риски, связанные с возможностью перехвата и прослушивания самих разговоров, а так же перехват и анализ сигнальной информации используемых протоколов, которая позволяет определить факт наличия и времени проведения переговоров.

Авторами предлагается вариант реализации метода косвенного шифрования, обеспечивающий гибкую интеграцию решению с VoIP приложениями, который заключается в создании промежуточной «прослойки», таким образом, что приложение может выйти в сеть только через этот прокси-сервер. Таким образом, достигаются две цели:

- защита полезной нагрузки VoIP;
- защита сигнальной информации стека VoIP протоколов.

К примеру, на двух ЭВМ установлены VoIP приложения и предлагаемая система защиты (рис.2), в таком случае реализуется следующая схема:

- Система защиты постоянно следит за сетевой активностью VoIP-приложения;
- VoIP-приложение инициализирует сетевое подключение к удалённой ЭВМ;

▪ Система защиты блокирует передачу информации от приложения в сеть, перенаправляет поток данных от VoIP-приложения на себя и выполняет подключение от своего имени к запрашиваемой удалённой системе. После установления соединения с удалённой криптосистемой начинается обмен потоками зашифрованной полезной информации.

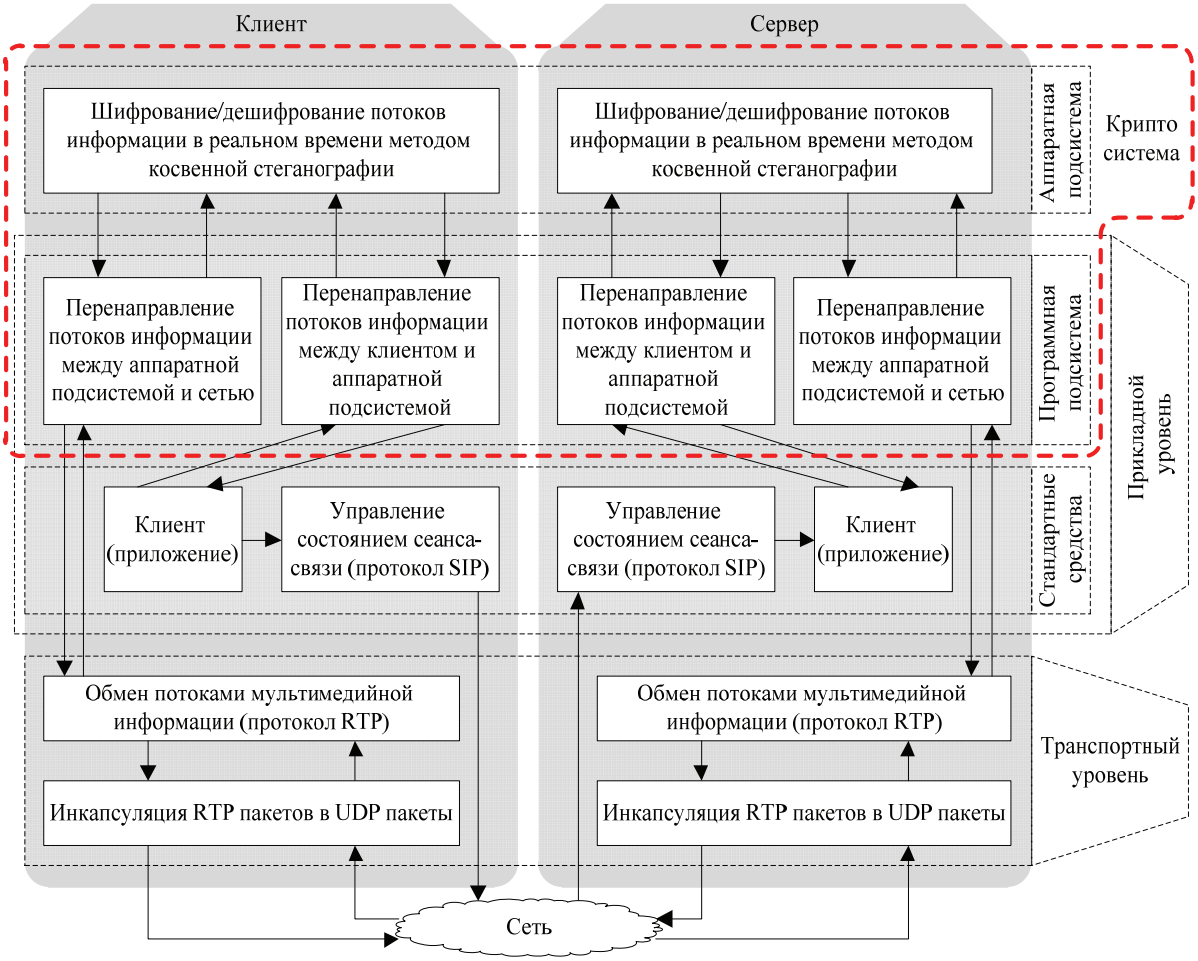

Рис. 2. Концептуальная схема функционирования системы защиты

В такой реализации криптосистема сама обеспечивает передачу данных по сети и следит за корректностью передаваемой информации. При этом защита передаваемой информации на уровне полезной загрузки (содержимое RTP пакетов или вышележащих протоколов) реализуется прозрачным шифрованием самого содержимого, а остальная информация пропускается в неизменённом виде. Таким образом, для проведения защищенного разговора достаточно установить программный или аппаратный комплекс защиты (в зависимости от применяемой реализации) на оконечные переговорные устройства(IP-телефон, ПК пользователя и т.п.) и доступ к содержимому разговора будут иметь только указанные пользователи, но при этом вся служебная информация будет оставаться общедоступной. Такая реализация позволяет применять данную систему защиты помимо VoIP систем на базе стандартного стека протокола также в проприетарных системах (Skype и подобных) в которые используемые протоколы неизвестны или недоступны их спецификации.

Для противодействия перехвату и анализа сигнальной информации системой защиты шифруется информация уже на уровне сигнальных протокол(SIP, H.323). В такой реализации системы защиты устанавливаются на входе сетей абонентов, и фактически защищается только канал между установленными системами защиты, при этом внутри сетей абонентов вся сигнальная информация передается в открытом виде. Поэтому в таком случаи необходимо использовать гибридную защиты, при которой помимо шифрования канала между сетями абонентов дополнительно шифруются сами переговоры. Гибридная реализация не защищает

от угрозы перехвата сигнальной информации, находясь внутри сети абонента, но не позволяет прослушивать сами переговоры.

Заключение

Применение предлагаемой системы защиты, использующей для шифрования метод косвенного шифрования, позволяет реализовать качественно новый уровень безопасности, обладающей криптостойкастью выше других потоковых криптосистем. Сама система потокового шифрования может работать на каналах, обладающих различными свойствами и качеством, при этом криптостойкость передаваемой информации остается на достаточно высоком уровне.

В методе косвенного шифрования алгоритм замены сегментов открытой информации на соответствующие сегменты секретного контейнера-ключа является потоковым, что делает алгоритм приемлемым для применения в системах шифрования потоковой информации. Если контейнер-ключ содержит истинно случайные числа и используется однократно, то метод обеспечивает абсолютную криптостойкость по Шеннону.

Безопасность и конфиденциальность передаваемой информации обеспечивается при помощи защитного программно-аппаратного комплекса, интегрируемого в существующие, стандартные системы интерактивного общения. Защитный программно-аппаратный комплекс состоит из двух подсистем - программной и аппаратной. Аппаратная подсистема выполняет шифрование/дешифрование в реальном времени получаемых от программной подсистемы потоков информации.

Программная подсистема устанавливается непосредственно на ЭВМ клиента. Важным достоинством программной подсистемы является гибкость её интеграции в существующие решения систем интерактивного общения, без внесения существенных изменений в текущую инфраструктуру. Именно такую функциональность обеспечивает программная подсистема защитного программно-аппаратного комплекса, шифруется только полезная медиа-информация.

Список литературы

1. Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностр. лит-ры, 1963. – 830 с.

2. Vernam G.S. Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications // Journal of the IEEE. – 1926. – V 55. – P. 109–115.

3. Алишов Н.И. Косвенная стеганография // Intern. Book Series "INFORMATION i SCIENCE & COMPUTING" (Sofia: ITHEA). – 2009. – N 11. – P. 53–58.

4. Алишов Н.И., Марченко В.А., Оруджева С.Г. Косвенная стеганография как новый способ передачи секретной информации // Комп'ютерні засоби, мережі та системи: зб. наук. пр. – К.: НАНУ, Ін-т кібернетики, 2009. – № 8. – С. 105–112.

5. Ransome J.F., Rittinghouse J. Voice over Internet Protocol (VoIP) Security. – N.Y.: Digital Press, 2004. – 432 pp.