convolutional neural network based on the inner ear principle to automatically assess human's emotional state // E3S Web of Conferences. – 2020. – Vol. 224. – P. 1-10.

DOI: 10.25728/iccss.2022.95.50.035

Асратян Р.Э.

Подход к созданию защищенных сетевых туннелей в распределенных системах на основе Cryptographic Message Syntax (CMS)

Аннотация: Рассмотрен новый подход к построению защищенных каналов (туннелей) через общедоступную сеть, основанный на использовании технологии Cryptographic Message Syntax (CMS) для инкапсуляции информационных запросов в структуру т.н. «защищенного сообщения». Показано, что, в отличие от известных подходов, предложенная организация защищенного туннеля позволяет ему гибко настраиваться на работу с любой криптосистемой, поддерживающей стандарт CMS, прямо в ходе работы без какой-либо доработки и/или конфигурирования.

Ключевые слова: распределенные системы, VPN, информационная безопасность, web-сервисы, разграничение прав доступа, маршрутизация запросов

Так как почти все современные территориально-распределенные информационные системы используют Интернет для организации взаимодействия удаленных друг от друга рабочих станций и серверов, задача защиты данных в общедоступной сети уже давно находится в центре внимания разработчиков [1, 2]. Разумеется, возможно интегрировать крипто-средства и защищенные сетевые протоколы непосредственно в клиентские и сервисные компоненты системы. Однако такое решение весьма трудоемко, а цена ошибки в данной области может быть высока. Поэтому, обычный способ решения этой задачи заключается в использовании технологии VPN (Virtual Private Network), в качестве готового решения, позволяющего реализовать защищенный «туннель» через общедоступную сеть [3, 4]. Так как средства криптозащиты

подключаются в VPN на нижнем уровне иерархии протоколов OSI (на «сетевом» или «транспортном»), эта технология отличается высокой универсальностью: «выгодополучателями» оказываются все сетевые службы и протоколы уровня приложения – от WWW и электронной почты до Удаленного рабочего стола.

Тем не менее, разработчики распределенных систем до сих пор сталкиваются с серьезными сложностями в области информационной безопасности. Это в основном связано с дефицитом готовых технических решений для таких задач, как разграничение прав доступа к информационным ресурсам, аутентификация информационных запросов и проверка подлинности серверов, организация доступа к серверам, «спрятанным» в т.н. частных локальных сетях предприятий. Это приводит разработчиков к необходимости создавать множество «частных решений» этих задач, приспособленных к особенностям конкретных проектов, что увеличивает трудозатраты и риск появления «пробелов» в информационной защите.

В данной работе рассматривается новый подход к организации безопасных взаимодействий в распределенных системах, основанный на построении защищенных сетевых туннелей с помощью технологии CMS [5]. В отличие от традиционных, данный подход является строго специализированным: он ориентирован на поддержку систем, использующих технологию web-сервисов [6, 7] для обслуживания информационных запросов. Именно эта специализация позволяет дольше продвинуться в сторону готовых технических решений по сравнению с универсальными технологиями.

Описываемый подход опирается на соединение двух сетевых технологий: CMS и технологии прокси-серверов. В основу CMS заложено понятие (и соответственный программный класс) «подписанного сообщения» (SignedCms), представляющее собой своего рода защищенный контейнер для хранения информации и обеспечения ее аутентичности и конфиденциальности. С этой целью класс SignedCms оснащен необходимыми функциями-членами для загрузки в него произвольных данных, формирования и проверки электронных подписей, шифрования и расшифровки данных. Важным свойством CMS является его способность использовать любую криптосистему, поддерживающую этот стандарт (выбор

криптосистемы осуществляется динамически и целиком определяется используемым сертификатом открытого ключа). Защищенный туннель, опирающийся на CMS, в полной мере «наследует» эту гибкость в выборе крипто-средств (рисунок 1).

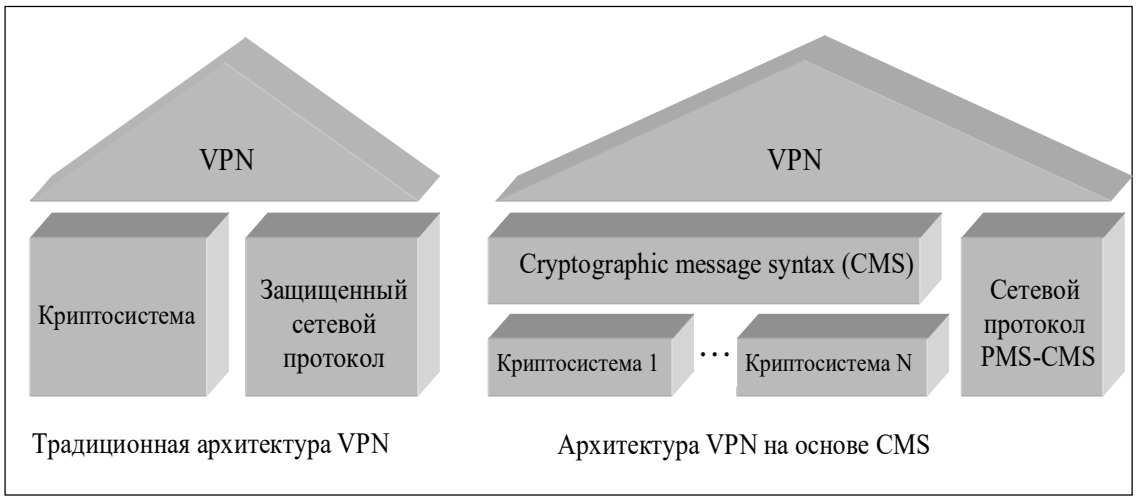

Рисунок 1 – Архитектурные решения для реализации VPN

Структура защищенного туннеля приведена на рисунке 2. Как видно из рисунка, его основу составляют два шлюза: клиентский (CG) и серверный (SG). Каждый шлюз представляет собой постоянно активную программу, размещенную или на рабочей станции, или на выделенном сервере. Основное назначение клиентского шлюза включает выполнение следующих функций:

- «перехват» исходящих от клиента HTTP/SOAP-запросов в режиме прокси-сервера,
- анализ заголовков запросов и выбор удаленного SG на основе имени адресуемого web-сервера (высокоуровневая маршрутизация запросов),
- установка защищенного соединения с выбранным SG и проверка подлинности серверного шлюза на основе сертификата открытого ключа,
- инкапсуляция информационного запроса в объект SignedCms, формирование электронной подписи CG, шифрование его открытым кличем SG, передача объекта серверному шлюзу и получение от него другого объекта SignedCms, содержащего результат обработки запроса,

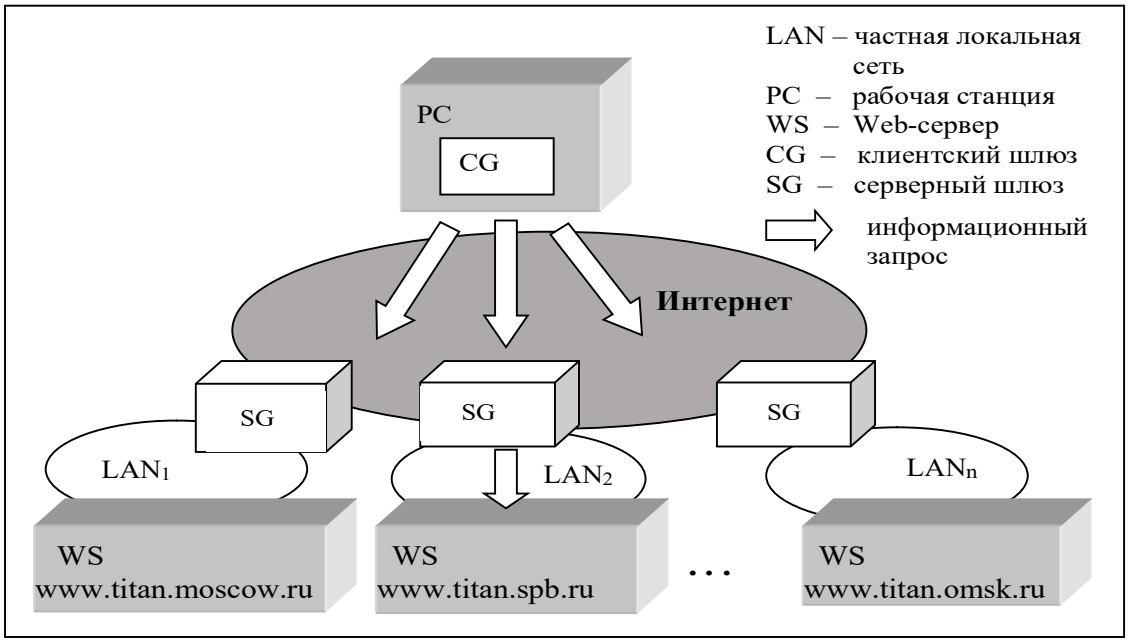

Рисунок 2 – Высокоуровневая маршрутизация запросов в туннеле

- расшифровка, проверка электронной подписи SG в полученном объекте, извлечение из него результата обработки запроса и передача последнего клиенту.

Основное назначение серверного шлюза включает выполнение следующих функций:

- установление защищенного соединения с клиентским шлюзом по его запросу и передача ему сертификата открытого ключа,
- получение объекта SignedCms, содержащего информационный запрос, от клиентского шлюза,
- расшифровка, проверка электронной подписи CG в полученном объекте и извлечение из него информационного запроса,
- проверка права клиента на доступ к адресуемому web-сервису или к отдельной сервисной функции на основе сертификата открытого ключа, полученного от клиентского шлюза,
- установление открытого сетевого соединения с web-сервисом и передача ему полученного информационного запроса,
- получение результата обработки запроса от web-сервиса по открытому соединению,
- инкапсуляция результата обработки запроса в объект SignedCms, формирование электронной подписи SG, шифрование

его открытым кличем CG и передача объекта клиентскому шлюзу и передача его клиентскому шлюзу по защищенному соединению.

Важно отметить, что конверсия имени адресуемого web-сервера в IP-адрес осуществляется лишь после доставки запроса в SG. Поэтому, сложная ситуация, в которой web-серверы в различных частных локальных сетях имеют одинаковые «серые» адреса, не вызывает никаких проблем.

Проверка прав доступа к web-сервисам или отдельным функциям-членам осуществляется на основе сопоставления реквизитов владельца клиентского сертификата открытого ключа с контрольными значениями реквизитов, указанными в конфигурационном файле серверного шлюза.

Литература:

1. *Салимова Ш.А.* Кибербезопасность в России: актуальные угрозы и пути обеспечения в современных условиях / Достижения вузовской науки 2021: Сборник статей XVII Международного научно-исследовательского конкурса, Пенза, 20 января 2021 года. – Пенза: «Наука и Просвещение», 2021. – С. 207-214.

2. *Жаранова А.О.*, *Птицына Л.К.* Анализ влияния распределенности на качество функционирования комплексных систем защиты информации / Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020): Сборник научных статей IX Международной научно-технической и научно-методической конференции. – СПб: СПБГУТ, 2020. – С. 324-327.

3. *Акушуев Р.Т.* Принцип работы VPN и его особенности // Modern Science. – 2020. – № 7. – С. 312-314.

4. *Хант К.* TCP/IP. Сетевое администрирование. – СПб.: Питер, 2007. – 816 с.

5. Request for Comments: 5652. Cryptographic Message Syntax, 2009. – URL: https://datatracker.ietf.org/doc/html/rfc5652 (дата обращения 10.10.2022).

6. *Шапошников И.В.* Web-сервисы Microsoft .NET. – СПб: БХВ-Петербург, 2002. – 336 с.

7. *Мак-Дональд М., Шпушта М.* Microsoft ASP.NET 3.5 с примерами на C# 2008 и Silverlight 2 для профессионалов. – М.: Вильямс, 2009. – 1408 с.