2. IEC 62443-3-2. Security for industrial automation and control systems. Part 3-2: Security risk assessment for system design. – IEC, 2020. – 63 p.

3. ГОСТ Р ИСО/МЭК 27005. Менеджмент рисков информационной безопасности–2010. – Москва: Стандартинформ, 2011. – 48 с.

4. ГОСТ Р ИСО/МЭК 31010. Методы оценки риска–2011. – М.: Стандартинформ, 2012. – 70 с.

Асратян Р.Э.

Использование технологии SSL/TLS для создания защищенных сетевых каналов в распределенных системах

Аннотация: Рассмотрены принципы организации защищенного сетевого взаимодействия на основе использования технологии SSL/TLS для создания защищенных сетевых каналов через общедоступную сеть. В отличие от технологии VPN, описываемый подход предполагает подключение средств информационной защиты на верхнем («транспортном») уровне стека протоколов модели OSI, что позволяет более точно «сфокусироваться» на потребностях конкретного протокола приложения: HTTP/SOAP, т.е. на защите взаимодействий web-клиентов и web-сервисов.

Ключевые слова: распределенные системы, Интернет-технологии, информационная безопасность, SSL/TLS, web-сервисы, разграничение прав доступа

Многие современные распределенные информационные системы включают десятки и даже сотни рабочих станций и серверов, взаимодействующих через общедоступную глобальную сеть. Задача организации безопасных взаимодействий в таких системах уже давно вышла «на первый план» [1-2]. Обычный способ решения этой задачи заключается в использовании технологии VPN (Virtual Private Network), позволяющей реализовать защищенный «туннель» через общедоступную сеть [3]. Так как средства криптозащиты подключаются в VPN на нижнем уровне иерархии протоколов OSI (как правило, не выше

«сетевого»), эта технология отличается высокой универсальностью и способна обеспечить безопасное взаимодействие для любого из протоколов уровня «приложения» (HTTP, SMTP, POP3 и т.п.) [4].

Однако разработчики распределенных систем до сих пор сталкиваются с серьезными сложностями в области информационной безопасности. Это во многом связано с дефицитом готовых технических решений для таких задач, как разграничение прав доступа к информационным ресурсам, аутентификация информационных запросов и проверка подлинности серверов. Это приводит к появлению многих «частных решений» этих задач, приспособленных к особенностям конкретных проектов, что увеличивает трудозатраты и риск появления «брешей» в информационной защите.

В данной работе рассматривается новый подход к организации безопасных взаимодействий в распределенных системах, основанный на построении защищенных сетевых каналов с помощью технологии SSL/TLS [5]. В отличие от VPN, данный подход строго ориентирован на поддержку систем, опирающихся на технологию web-сервисов [6] для обслуживания информационных запросов. Подход основан на предположении, что технологии, более точно «сфокусированные» потребностях распределенных систем имеют больше возможностей в продвижении в сторону готовых технических решений, чем технологии, претендующие на универсальность.

Описываемый подход опирается на соединение двух сетевых технологий: SSL/TLS и технологии прокси-серверов. Структура защищенного канала проиллюстрирована на рисунке 1. Как видно из рисунка, канал включает две компоненты: клиентский шлюз и серверный шлюз.

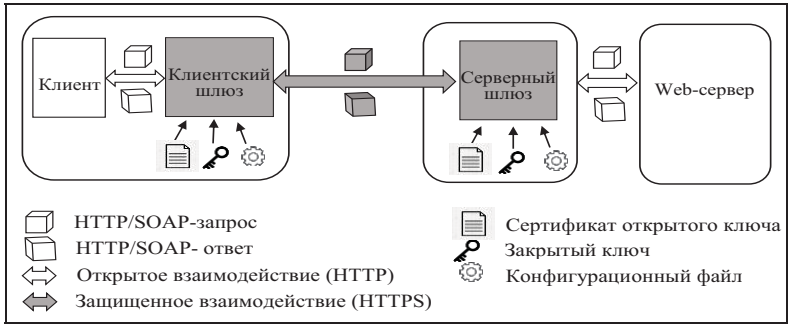

Рисунок 1 – Структура защищенного канала

Основное назначение клиентского шлюза заключается в решении следующих задач:

- «перехват» исходящих от клиента HTTP/SOAP-запросов в режиме прокси-сервера,
- анализ заголовков запросов,
- установка защищенного соединения с серверным шлюзом с применением технологии SSL/TLS и проверка подлинности серверного шлюза на основе сертификата открытого ключа,
- передача запроса серверному шлюзу и получение HTTP/SOAP-ответа по защищенному соединению,
- передача HTTP/SOAP-ответа клиенту.

Основное назначение серверного шлюза включает решение следующих задач:

- установление защищенного соединения с клиентским шлюзом по его запросу с применением технологии SSL/TLS,
- получение HTTP/SOAP-запроса от клиентского шлюза по защищенному соединению,
- 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 HTTP/SOAP-запроса,
- получение HTTP/SOAP-ответа от web-сервиса по открытому соединению и передача его клиентскому шлюзу по защищенному соединению.

Разграничение 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. Например, если в конфигурационном файле указано, что вызывать функцию MyFunction сервиса MyService имеют право только клиенты с реквизитами

C=Russia, L=Moscow, O=Titan, OU=dir*,

то доступ к этой функции будет разрешен только служащим московской организации Titan, сотрудником подразделения с названием, начинающимся на «dir» (directorate, direkciya и т.п.).

Описанный защищенный канал был реализован в среде операционной системы Linux на языке C++ с использованием библиотек поддержки SSL/TLS: libssl и libcrypt. И клиентский и серверный шлюзы приспособлены к работе в режиме фоновых программ («демонов»). Во время работы каждый из шлюзов занимает всего около 1 мегабайта оперативной памяти. Область наиболее эффективного применения канала включает распределенные системы, построенные на основе сетевой архитектуры ".NET" [7] в среде Linux (например, в интегрированной среде разработки MonoDevelop).

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 (20 января 2021 г. Пенза). – 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. *Baka P, Schatten J.* SSL/TLS under lock and key: a guide to understanding SSL/TLS cryptography. – Keyko books, 2020. – 132 p.

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.

Саломатин А.А.

Методы противодействия отслеживанию браузерных отпечатков пользователей

Аннотация: Рассматриваются методы противодействия отслеживанию браузерных отпечатков пользователей. Проанализированы различные группы мер, позволяющие препятствовать корректному отслеживанию браузерных атрибутов и изменять их значения таким образом, что сформированный отпечаток браузера не сможет верно идентифицировать пользователя. Приведены примеры способов осуществления мер в каждой группе. Отдельное внимание уделено оценке эффективности применения данных методов на сущности, полученные с помощью инструмента «fingerprint3.js». На основе проведенного исследования становится возможным осуществление практического эксперимента по идентификации пользователя с учетом применения методов, препятствующих получению полного и верного идентификатора пользователя. Развитие методов противодействия отслеживания браузерных отпечатков особенно важно для сложных систем, обслуживающих большое количество субъектов доступа.