УДК 004.056.53, 004.056.55

А.В. Астафьев, канд.техн. наук, доцент, ФГБОУ ВО МИ(Ф)ВЛГУ (Муром, Россия)
(e-mail: alexandr.astafiev@mail.ru)

Т.О. Шардин, магистрант, ФГБОУ ВО МИ(Ф)ВЛГУ (Муром, Россия)
(e-mail: tima.shardin@mail.ru)

РЕАЛИЗАЦИЯ ТЕХНОЛОГИИ БЕЗОПАСНОГО ОБМЕНА ДАННЫМИ НА ОСНОВЕ ПРОТОКОЛА РУКОПОЖАТИЯ ДЛЯ СИСТЕМ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ

В данной работе рассмотрена технология безопасного обмена данными на основе протокола рукопожатия для систем промышленной автоматизации. Приведены угрозы клиент-серверных приложений, на основе которых был сделан вывод о необходимости использования и дальнейшей реализации защищенного канала связи, для осуществления безопасного обмена данными. В процессе работы проанализированы существующие методы интеграции и автоматизации процесса на промышленных предприятиях. По результатам проведенного сравнительного анализа, в качестве интеграции клиента и сервера была выбрана CMS Wordpress с использованием плагина интернет-магазина WooCommerce и 1С. Были рассмотрены прямые аналоги протокола рукопожатия, выделив достоинства и недостатки использования в данном приложении каждого сравниваемого метода, в качестве защищенного канала связи был выбран протокол рукопожатия, так как он показал больше всего преимуществ, чем приведенные аналоги. В протоколе рукопожатия использовалась ассиметричная система шифрования RSA. Сервер генерировал пару ключей, открытый ключ находился у клиента, закрытый – у сервера, идентификация клиента проводилась по открытому ключу и контрольной фразе, о которой изначально договаривались участники обмена. Если на каком-либо этапе идентификации данные не совпадали или была произведена попытка вторжения третьих лиц в информационный обмен, клиент не получал никаких данных от сервера. В конечном итоге представлены схемы работы протокола рукопожатия, криптосистемы RSA и общая схема реализованного приложения. Данная разработка показала эффективное использование и была внедрена на предприятии по производству мебельной продукции.

***Ключевые слова**: системы промышленной автоматизации, протокол рукопожатия, безопасность клиент-серверных приложений.*

DOI: 10.21869/2223-1560-2018-22-2-27-33

Ссылка для цитирования: Астафьев А.В., Шардин Т.О. Реализация технологии безопасного обмена данными на основе протокола рукопожатия для систем промышленной автоматизации // Известия Юго-Западного государственного университета. 2018. Т. 22, № 2(77). С. 27-33.

***

В настоящее время большинство крупных предприятий сталкиваются с существенными трудностями по улучшению управляемости компании. Например уменьшение времени выполнения процессов электронного документооборота с последующей возможностью их отслеживания. Эти факторы влияют на качество исполнения этих процессов. Одним из способов реализации подобных задач является внедрение автоматизированной системы, выполняющей вышеуказанные функции. Однако попытка решения задачи внедрения такой системы наталкивается на существенные сложности, связанные с отсутствием на рынке адекватного предложения, либо это предложение не рентабельно для компании по тем или иным причинам.

Стоит учитывать, что сеть Интернет является открытой информационной средой и по техническим причинам большинство трафика передается открытым способом, что дает злоумышленнику возможность получать доступ к конфиденциальным данным. Поэтому, информация, передаваемая через данную систему на предприятие, не должна быть доступна третьим лицам. Этот критерий является одним из главных, поэтому найти среди имеющихся решений оптимальное, является в некоторых случаях невозможным.

Данная технология позволит сотрудникам промышленного предприятия обеспечить быструю синхронизацию данных. В ходе информационного взаимодействия необходимо использовать защиту при передаче данных с помощью защищенного канала связи для того, чтобы предотвратить перехват информации злоумышленником, которую в дальнейшем он может модифицировать и тем самым нанести ущерб, что повлечет за собой существенные материальные потери.

На этапе анализа клиент-серверных приложений в соответствии с ГОСТ-53114-2008 [1] были выделены основные угрозы, по которым возможен перехват конфиденциальных данных в ходе информационного взаимодействия между клиентом и сервером. Основные угрозы и меры по их предотвращению представлены в таблице 1.

Таблица 1

Основные угрозы клиент-серверных приложений

Основные части клиент-серверного приложения	Угрозы	Контрмеры
Серверная часть программного обеспечения	Доступ к административным разделам извне	Контроль IP адресов
		Защита административного раздела от третьих лиц
	Выявление слабых паролей	Ведение правил состава пароля и их смены
Клиентская часть программного обеспечения	Недостаточная защищенность сеанса (отсутствие таймаута)	Ограничение времени работы сеанса
	Выявление слабых паролей	Ведение правил состава пароля и их смены
Взаимодействие клиента с сервером	Вторжение третьих лиц в информационный обмен (перехват информации)	Использование защищенных протоколов передачи информации

Как видно из таблицы, для того чтобы обеспечить безопасное взаимодействие клиента с сервером, необходимо использовать различные защищенные протоколы передачи информации. В ходе реализации программного обеспечения за основу был взят протокол рукопожатия [4].

На данный момент существует несколько готовых программных продуктов для интеграции и автоматизации процесса на промышленных предприятиях. Рассмотрим эти решения на примере 1С и CMS интернет-магазина, выделим основные достоинства и недостатки, по результатам которых можно сделать вывод о том, какое именно решение выгоднее использовать для осуществления поставленной задачи:

1. 1С-Битрикс – система управления веб-проектами, программный продукт для создания корпоративных сайтов и интернет-магазинов.

2. CMS Joomla с использованием плагина VirtueMart – позволяет получить полностью рабочий интернет-магазин.

3. CMS WordPress с использованием плагина WooCommerce – как и предыдущий вариант позволяет создать интернет-магазин без материальных вложений.

Сравнительный анализ приведенных аналогов представлен в таблице 2.

Таблица 2

Сравнительный анализ аналогов

<table>
<tr><th>Достоинства использования</th><th>Недостатки использования</th></tr>
<tr><td colspan="2">1С-Битрикс</td></tr>
<tr><td rowspan="5">Единственная система, где поддерживается интеграция сайта с 1С напрямую</td><td>Требуется покупка редакции 1С-Битрикс</td></tr>
<tr><td>Требуется покупка или разработка шаблона для интернет-магазина</td></tr>
<tr><td>Необходима первоначальная синхронизация 1С и 1С-Битрикс (настройка сайта, настройка обмена данными)</td></tr>
<tr><td>Высокая стоимость использования данного решения</td></tr>
<tr><td>Требуется реализация протокола рукопожатия для безопасного обмена данными</td></tr>
<tr><td colspan="2">CMS Joomla + VirtueMart</td></tr>
<tr><td>Бесплатная и доступная CMS</td><td>Требуется реализация протокола рукопожатия для безопасного обмена данными</td></tr>
<tr><td>Бесплатный плагин VirtueMart</td><td rowspan="2">Готовые решения интеграции реализованы под старые версии 1С или не поддерживаются</td></tr>
<tr><td>Существуют готовые решения интеграции сайта с 1С</td></tr>
<tr><td colspan="2">CMS WordPress + WooCommerce</td></tr>
<tr><td>Бесплатная и доступная CMS</td><td rowspan="2">Требуется реализация протокола рукопожатия для безопасного обмена данными</td></tr>
<tr><td>Бесплатный плагин WooCommerce</td></tr>
<tr><td>Существуют готовые решения интеграции сайта с 1С</td><td rowspan="2">Готовые решения интеграции реализованы под старые версии 1С или не поддерживаются</td></tr>
<tr><td>Данная связка модулей уже используется на сайте заказчика</td></tr>
</table>

В результате сравнительного анализа было принято решение использовать последний вариант интеграции. При своих достоинствах именно оно подходило больше всего, так как оно уже использовалось на предприятии.

На практике процесс передачи информации по защищенному каналу связи зачастую связан с использованием протоколов, основанных на различных криптосистемах. В ходе реализации приложения за основу был взят следующий метод:

Протокол рукопожатия [4] – криптографический протокол, основанный на симметричном взаимном обмене информацией между участниками информационного взаимодействия по схеме запрос – ответ (рис. 1).

Используя криптосистему RSA в данном протоколе, позволяет участникам обмена изначально использовать необходимые параметры для безопасной передачи информации.

Стоит отметить, что протокол рукопожатия имеет аналоги: SSL сертификат и электронную подпись [5].

Рис. 1. Схема работы протокола рукопожатия в приложении

Для выявления достоинств и недостатков каждого аналога был проведен анализ этих алгоритмов с использованием криптосистемы RSA по следующим критериям:

1. Требование к материальным затратам – позволяет оценить, рентабелен ли данный метод при разработке приложения, требуются ли материальные затраты для поддержания алгоритма.

2. Использование удостоверяющего центра – позволяет оценить, необходимо ли дополнительно прибегать к использованию подтверждения подлинности ключей с помощью электронно-цифровой подписи.

3. Криптостойкость использованного алгоритма шифрования в протоколе – позволяет оценить, обладает ли данный алгоритм шифрования достаточной способностью противостоять криптоанализу. Это один из важных критериев, так как при недостаточной или низкой криптостойкости, использование алгоритма для защиты информации между участниками обмена нецелесообразно.

4. Простота использования метода – позволяет оценить, понятна ли работа для пользователя, работающего с интерфейсом используемого алгоритма.

Результаты анализа сведены в таблице 3.

По результатам видно, что протокол рукопожатия является безопасным для защиты информации при использовании его в качестве технологии безопасного обмена данными. Метод обладает рядом преимуществ, а именно: выгоден по экономическим соображениям (затраты минимальные или их вовсе нет), не требует удостоверяющих центров, что позволяет использовать его любому лицу, а также прост в использовании, при этом обладая высокой криптостойкостью. Математическая модель, данного алгоритма представлена ниже на рисунке 2. Схема разработанной системы приведена на рисунке 3.

Таблица 3

Результаты сравнительного анализа

Вид	Требование к материальным затратам	Использование удостоверяющего центра	Криптостойкость использованного алгоритма шифрования в протоколе	Простота использования метода в приложениях
Протокол рукопожатия	Не требует материальных затрат	Не требует удостоверяющих центров	Обладает высокой криптостойкостью	Обладает простотой при использовании в приложениях
SSL сертификат	Требует материальные затраты	Требует удостоверяющего центра	Обладает высокой криптостойкостью	Требует дополнительного программного обеспечения
Электронная подпись	Требует материальные затраты	Требует удостоверяющего центра	Обладает высокой криптостойкостью	Обладает простотой при использовании в приложениях

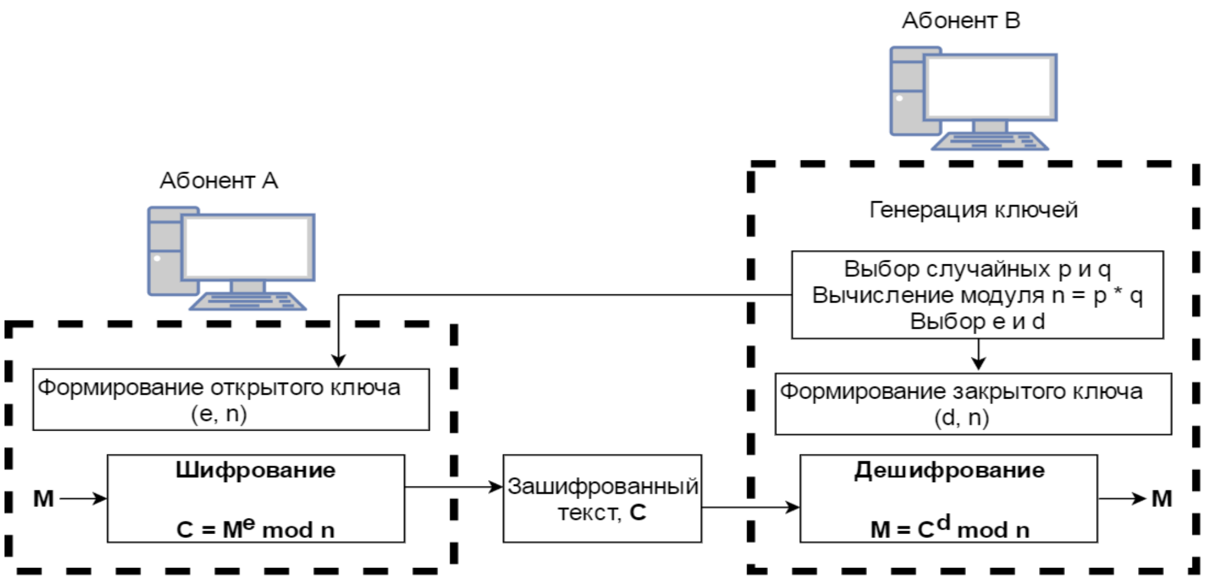

Рис. 2. Математическая модель алгоритма RSA, используемая в протоколе рукопожатия

Система представляет два связанных между собой модуля:

1. Клиентская часть – плагин на сайте под управлением CMS Wordpress. Связь с сервером происходит по протоколу SOAP.

2. Серверная часть – представляет собой систему генерации ключей и дополнения для созданной базы предприятия 1С (веб-сервис). Располагается на компьютере организации.

Заключение

В результате проделанной работы, данная разработка доказала ее эффективное использование на практике. Разработка подтверждена свидетельствами о регистрации программы для ЭВМ № 2017617564, № 2017661972, а также внедрена на предприятие по производству мебельной продукции.

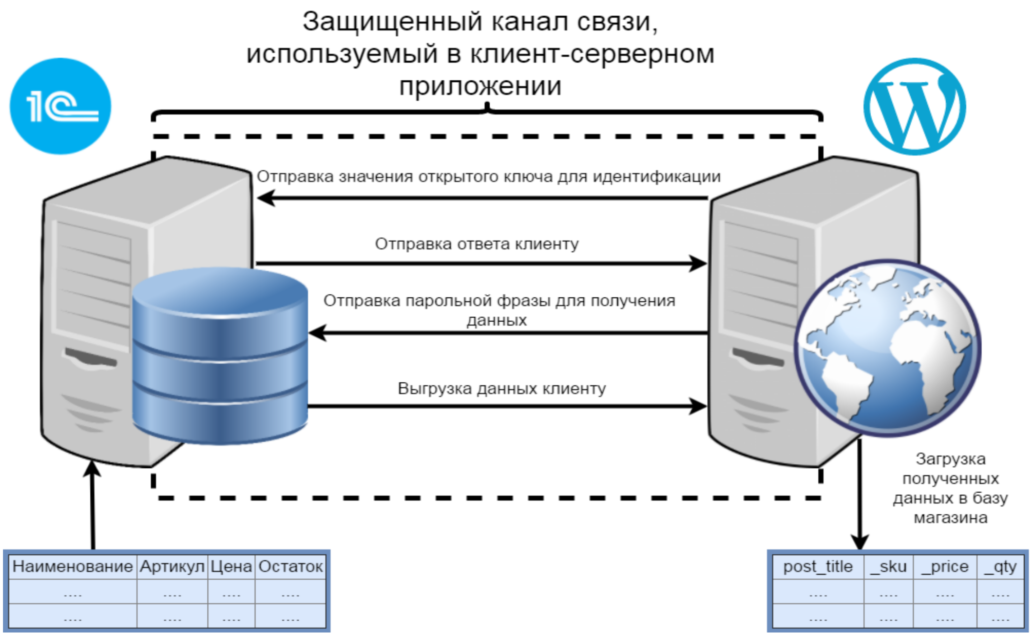

Рис. 3. Схема работы разработанной системы,
использующая реализованную технологию безопасного обмена данными

Список литературы

1. ГОСТ Р 53114–2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М., 2008.

2. Астафьев А.В., Шардин Т.О., Волков Д.А. Свидетельство РФ на программу на ЭВМ 2017 №2017617564 от 07.07.2017 «Программа аутентификации объекта информационного взаимодействия на основе протокола рукопожатия для защиты данных в системах промышленной автоматизации».

3. Астафьев А.В., Шардин Т.О., Волков Д.А. Свидетельство РФ на программу на ЭВМ 2017 №2017661972 от 25.10.2017 «Программа идентификации объекта информационного взаимодействия на основе протокола рукопожатия для защиты данных в системах промышленной автоматизации».

4. Молдовян А.А., Молдовян Д.Н., Левина А.Б. Протоколы аутентификации с нулевым разглашением секрета.: СПб.: Университет ИТМО, 2016. 55 с.

5. Водолазский В. Коммерческие системы шифрования: основные алгоритмы и их реализация. Часть 1 // Монитор. 1992. N 6-7. С. 14 – 19.

6. Воеводин В.В. [и др.]. Параллельные вычисления. СПб.: БХВ-Петербург, 2002. 608 с.

7. Jonsson J., Kaliski Jr., B.S.: On the Security of RSA Encryption in TLS. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 127–142. Springer, Heidelberg (2002).

8. Brandon Rhodes, John Goerzen, TLS/SSL, Foundations of Python Network Programming, pp. 93-114.

9. Andrew Clark, HTTP Session Security, Encyclopedia of Cryptography and Security, pp. 567-569.

10. Wiener, M.: Cryptanalysis of Short RSA Secret Exponents. IEEE Transactions on Information Theory 36(3), pp. 553–558 (1990).

Поступила в редакцию 08.02.18

UDC 004.056.53, 004.056.55

A.V. Astafiev, Candidate of Engineering Sciences, Associate Professor, Murom Institute (Branch) of The Vladimir State University of Alexander Grigoryevich and Nikolay Grigoryevich Stoletovykh (Murom, Russia) (e-mail: alexandr.astafiev@mail.ru)

T.O. Shardin, Undergraduate, Murom Institute (Branch) of The Vladimir State University of Alexander Grigoryevich and Nikolay Grigoryevich Stoletovykh (Murom, Russia) (e-mail: tima.shardin@mail.ru)

DATA EXCHANGE TECHNOLOGY BASED ON THE HANDSHAKE PROTOCOL FOR INDUSTRIAL AUTOMATION SYSTEM

In this paper, the technology of secure data exchange based on the handshake Protocol for industrial automation systems is considered. The threats of client-server applications, on the basis of which it was concluded that the need to use and further implementation of a secure communication channel, for the implementation of secure data exchange. In the process of work, the existing methods of integration and automation of the process at industrial enterprises are analyzed. According to the results of the comparative analysis, as the integration of client and server was chosen Wordpress using plug-ins an online store WooCommerce and 1C. Were considered direct analogues of the handshake Protocol, highlighting the advantages and disadvantages of using in this application, we compare each method, as a secure communication channel has been selected the handshake Protocol, as it showed more benefits than listed counterparts. The handshake Protocol used an asymmetric RSA encryption system. The server generated a pair of keys, the public key was at the client, the private – at the server, the client identification was carried out by the public key and the control phrase, which was originally agreed by the exchange participants. If at any stage of identification the data did not match or an attempt was made to invade third parties in the information exchange, the client did not receive any data from the server. Finally, the schemes of the handshake Protocol, RSA cryptosystems and the General scheme of the implemented application are presented. This development has shown effective use and has been implemented in the enterprise for the production of furniture products.

Key words: *industrial automation, handshake protocol, client-server applications security.*

DOI: 10.21869/2223-1560-2018-22-2-27-33

For citation: Astafiev A.V., Shardin T.O. Data Exchange Technology Based on the Handshake Protocol FOR Industrial Automation System. Proceedings of the Southwest State University, 2018, vol. 22, no. 2(77), pp. 27-33 (in Russ.).

***

Reference

1. GOST R 53114–2008 Zashhita informacii. Obespechenie informacionnoj bezopasnosti v organizacii. Osnovnye terminy i opredelenija. Moscow, 2008.
2. Astaf'ev A.V., Shardin T.O., Volkov D.A. Svidetel'stvo RF na programmu na JeVM 2017 №2017617564 ot 07.07.2017 «Programma autentifikacii ob#ekta informacionnogo vzaimodejstvija na osnove protokola rukopozhatija dlja zashhity dannyh v sistemah promyshlennoj avtomatizacii».
3. Astaf'ev A.V., Shardin T.O., Volkov D.A. Svidetel'stvo RF na programmu na JeVM 2017 №2017661972 ot 25.10.2017 «Programma identifikacii ob#ekta informacionnogo vzaimodejstvija na osnove protokola rukopozhatija dlja zashhity dannyh v sistemah promyshlennoj avtomatizacii».
4. Moldovjan A.A., Moldovjan D.N., Levina A.B. Protokoly autentifikacii s nulevym razglasheniem sekreta. Sankt-Peterburg, 2016, 55 p.
5. Vodolazskij V. Kommercheskie sistemy shifrovanija: osnovnye algoritmy i ih realizacija. Chast' 1. Monitor, 1992, no. 6-7, pp. 14 – 19.
6. Voevodin V.V. i dr.,. Parallel'nye vychislenija. Sankt-Peterburg, 2002. P. 608.
7. Jonsson, J., Kaliski Jr., B.S.: On the Security of RSA Encryption in TLS. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 127–142. Springer, Heidelberg (2002).
8. Brandon Rhodes, John Goerzen, TLS/SSL, Foundations of Python Network Programming, pp. 93-114.
9. Andrew Clark, HTTP Session Security, Encyclopedia of Cryptography and Security, pp. 567-569.
10. Wiener, M.: Cryptanalysis of Short RSA Secret Exponents. IEEE Transactions on Information Theory 36(3), pp. 553–558 (1990).