А.В. АСТАФЬЕВ, Т.О. ШАРДИН

Использование криптосистемы RSA в протоколе рукопожатия для защиты данных в ходе информационного обмена в клиент-серверных приложениях

Муромский институт (филиал) ФГБОУ ВО «Владимирский государственный университет имени А.Г. и Н.Г. Столетовых», г. Муром

УДК 004.056.55

В данной статье рассмотрено использование алгоритма шифрования RSA в протоколе рукопожатия для защиты передаваемых данных между участниками информационного взаимодействия в клиент-серверных приложениях.

Введение

Основной проблемой сети Интернет на данный момент, является недостаточная защищенность приложений и сайтов, взаимодействующих с пользователем, так как по технологическим причинам трафик, передаваемый в сети Интернет, пересылается в открытом виде, что в конечном итоге дает злоумышленнику доступ к конфиденциальной информации.

По статистике, большинство клиент-серверных приложений и сайтов подвержены данной угрозе, поэтому разработчики внедряют дополнительные методы препятствующие получению конфиденциальной информации хранящейся на серверах или передаваемой в ходе информационного обмена между клиентом и сервером. Однако наиболее эффективным подходом для решения этой проблемы является применение протокола с нулевым разглашением секрета с использованием ассиметричной системы шифрования.

Использование протокола рукопожатия в клиент-серверных приложениях

В качестве примера рассмотрим одно из реализованных клиент-серверных приложений, где для защиты информации используется протокол рукопожатия. Принцип работы показан на рисунке 1:

Рис. 1. Схема клиент-серверного приложения, использующего протокол рукопожатия

На схеме видно, что обмен данным между участниками информационного взаимодействия происходит по защищенному каналу связи. Он представляет собой протокол рукопожатия, использующий ассиметричную систему шифрования RSA. Стоит отметить, что перед получением данных клиент проходит идентификацию на сервере по открытому ключу и при успешном ответе сервера переходит ко второму этапу, вводу парольной фразы. Участники информационного взаимодействия изначально обговаривают все параметры подключения.

В результате этих действий возможность перехвата информации третьими лицами становится практически невозможным, так как весь процесс идентификации проходит в несколько этапов и в случае несовпадения одного из проверяемых параметров (ключ или парольная фраза) доступ к данным будет закрыт. Также для предотвращения попытки подбора

идентификационных данных, необходимо вести правила состава паролей и ключей, а также их смены.

Анализ устойчивости приложения

Использование одного протокола рукопожатия, включающего в себя проверку клиента и шифрования передаваемых данных, является недостаточным, так как при низкой криптостойкости алгоритма шифрования возможна попытка подбора необходимых параметров для получения конфиденциальной информации злоумышленником. Криптосистема RSA в данном протоколе является одной из устойчивых криптосистем способных противостоять криптоанализу, но только лишь при использовании для генерации ключей больших простых чисел. Например, при генерации 5-значных простых чисел для формирования пары ключей повышается криптостойкость данного алгоритма. Пример лабораторного расчета показан на рисунке 2:

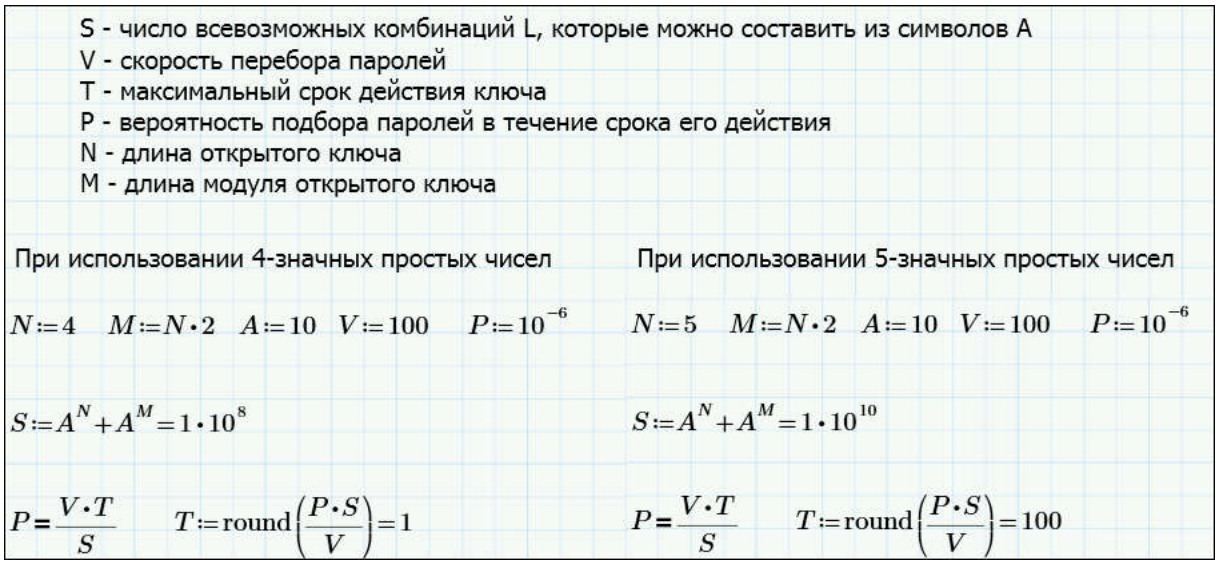

Рис. 2. Пример расчета криптостойкости используемого алгоритма шифрования

На данном рисунке видно, что время на подбор ключа при использовании 5-значных чисел составит 100 дней, без учета подбора пароля. Также при попытке вторжения в информационный обмен, злоумышленник при передаче парольной фразы получит следующее:

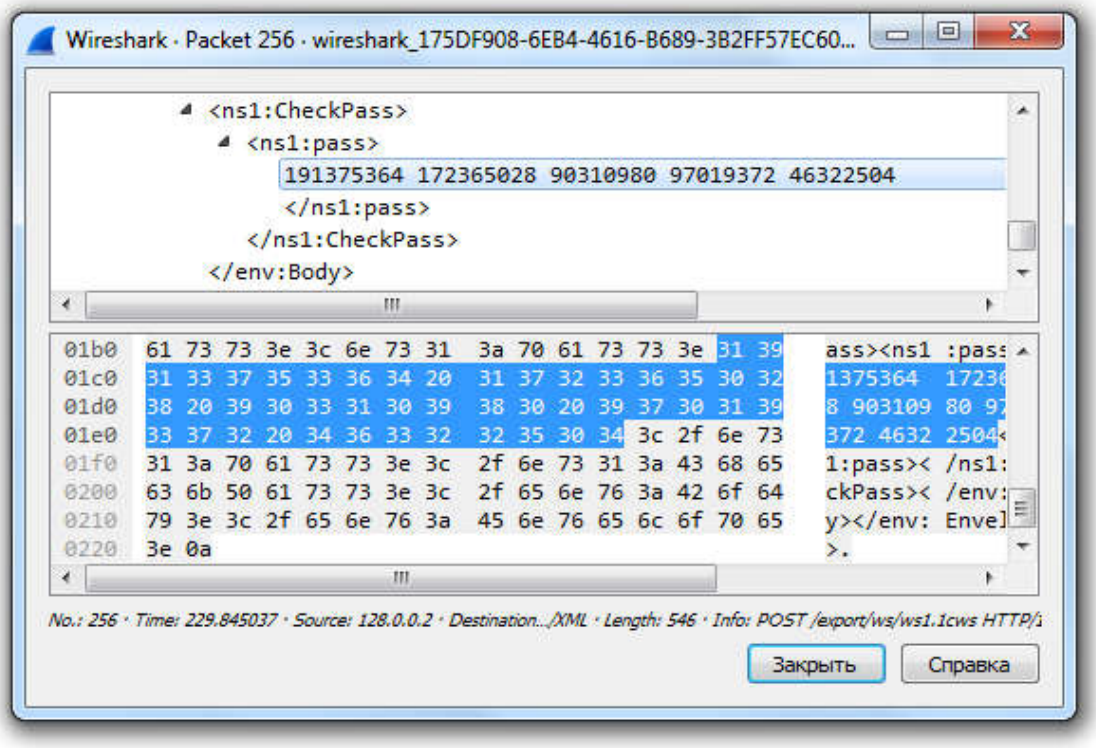

Рис. 3. Попытка перехвата парольной фразы.

Без использования протокола рукопожатия и алгоритмов шифрования, при передаче парольной фразы, для доступа к данным, злоумышленник получил бы искомую фразу:

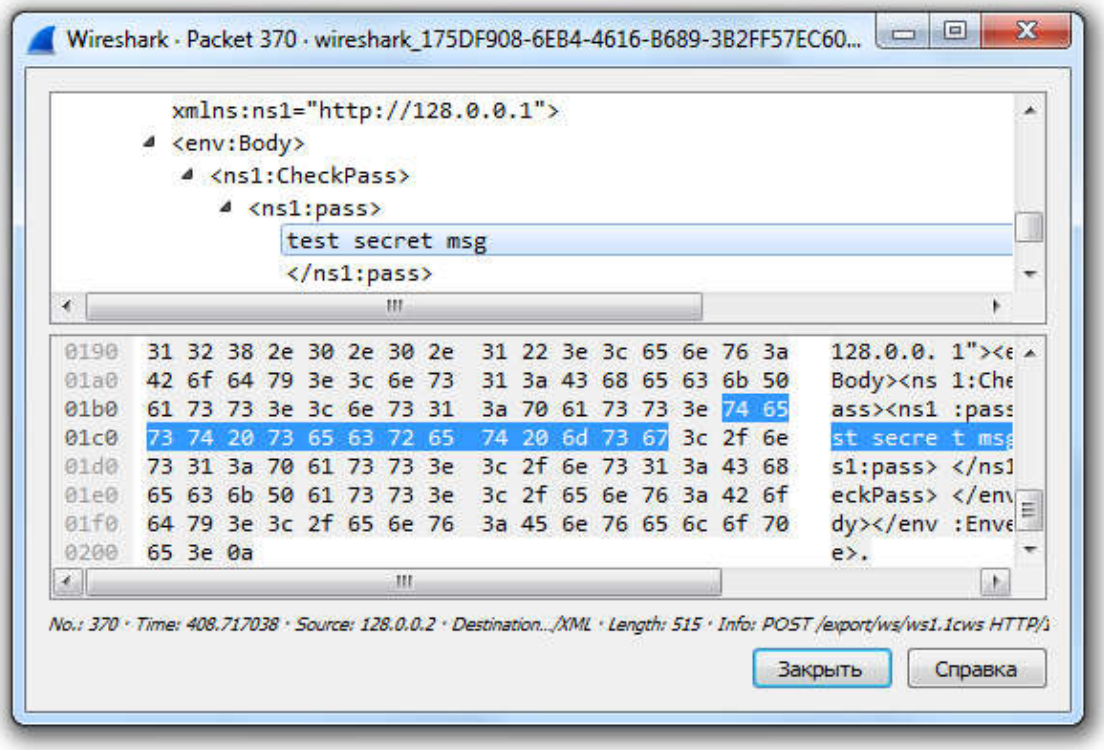

Рис. 4. Перехват парольной фразы без использования шифрования

Заключение

Таким образом, использование протокола рукопожатия с использованием криптосистемы RSA в клиент-серверных приложениях позволит предотвратить возможный перехват конфиденциальной информации при обмене между клиентом и сервером.

Литература

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

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 - Санкт-Петербург: СПб: Университет ИТМО, 2016. - 55 с. - экз.

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

6. Astafiev A.V. the method of combining the results of localization algorithms for character and bar code labels / Astafiev A.V., Orlov A.A., Provotorov A.V. // 2015 International Conference "Stability and Control Processes" in Memory of V.I. Zubov (SCP) 2015. С. 617-618.

7. Provotorov A. Development of methods for determining the locations of large industrial goods during transportation on the basis of RFID / Provotorov A., Privezentsev D., Astafiev A. // Procedia Engineering. 2015. Т. 129. С. 1005-1009.