менные проблемы науки и образования. – 2013. – № 6; URL: www.science-education.ru/113-11808

10. Михеева Т.И., Интеллектуальная транспортная геоинформационная система ITSGIS / Т.И. Михеева, С.В. Михеев, О.К. Головнин // Современные проблемы безопасности жизнедеятельности: интеллектуальные транспортные системы : материалы IV Международной научно-практической конференции (Казань, 25–26 февраля 2016 г.). – Казань : ГБУ «Научный центр безопасности жизнедеятельности», 2016. – С. 362–368. – ISBN 978-5-85247-837-5.

Т.И. Михеева, К.А. Молодыко

МЕТОД ЗАЩИТЫ ПАКЕТОВ ДАННЫХ РОЕВОЙ РОБОТИЗИРОВАННОЙ СИСТЕМЫ. МЕТОД АУТЕНТИФИКАЦИИ И ОТСЧЕТА ПАКЕТОВ

(Самарский университет, ИнтелТранС)

Первостепенной задачей при реализации роевой системы является обеспечение безопасности соединения, пакетов данных и сети, в которой ведется прием-передача. Для реализации роевой системы как взаимодействующее множество, в которое можно добавить элемент или подмножество необходим алгоритм распознавания свой-чужой. Основой такого алгоритма являются идентификация агента являющегося множеством или агента состоящего во множестве и проверка аутентификации и достоверности переданных им данных [1-3].

Метод сигналосообщения агентов разработан на принципах систем авторизации пользователей. Агент адресат должен сформировать запрос на соединение, по заданной форме в протоколе аутентификации, после чего данный пакет кодируется алгоритмом циклического избыточного кода и посылается агенту адресанту. На каждом шаге получения пакета от агента адресата проверяется правильность формирования аутентификационной информации и заголовка пакета. Агент может стать частью роевой системы, в случае если правильно сформированы пакеты данных, при передаче не была нарушена аутентификация и пройдена идентификация без блокировки. В конце каждого пакета данных ведется отсчет принятых и обработанных пакетов [4, 5].

Заголовок с аутентификацией представлен на рисунке 1.

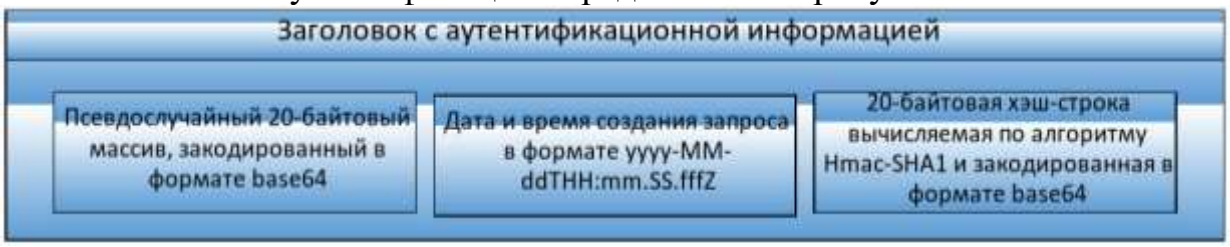

Рис. 1. Заголовок с аутентификацией

Аутентификационный заголовок пакета данных (ECNC-Auth) состоит из случайного 20-байтового массива (Nonce), закодированного в формате base64, даты и время создания запроса (Created) в формате «yyyy-MM-

ddTHH:mm:ss.fffZ» и 20-байтовой хэш-строки (Digest), вычисляемой по алгоритму Hmac-SHA1 и закодированной в формате base64 [5, 6].

Хэш-строка представляет собой результат работы алгоритма Hmac-SHA1 на конкатенации битовых массивов (рисунок 2):

1. двоичное представление поля Nonce (20 байт);
2. текстовое значение поля Created;
3. текстовое значение метода POST;
4. текстовое значение uri, без пробелов;
5. содержимое пакета, представляющее собой структурированные данные;
6. длина бит данных в пакете.

Рис. 2. Данные для вычисления Хэш-строки

Аутентификационный заголовок считается корректным, если вычисленное адресантом значение дайджеста совпадает с переданным в заголовке, а GMT-время, переданное в поле Created, отличается от времени адресанта не более чем на 10 секунд [5, 7, 8].

Агент адресат и агент адресант ведут отчет пакетов данных (рисунок 3). Адресат, формируя пакет данных, добавляет в конец автоинкрементное 32-битное целое, идентификатор запросного пакета, уникальный, в пределах сеанса обмена (CID) и отклик адресанта на последний принятый от сервера пакет (SIDResp). Адресант, формируя пакет данных, добавляет в конец автоинкрементное 32-битное целое, идентификатор запросного пакета, уникальный, в пределах сеанса обмена (SID) и отклик (CIDResp), который должен быть равен CID принятого запросного пакета. Отклик CIDResp является дополнительным подтверждением приёма пакета адресантом.

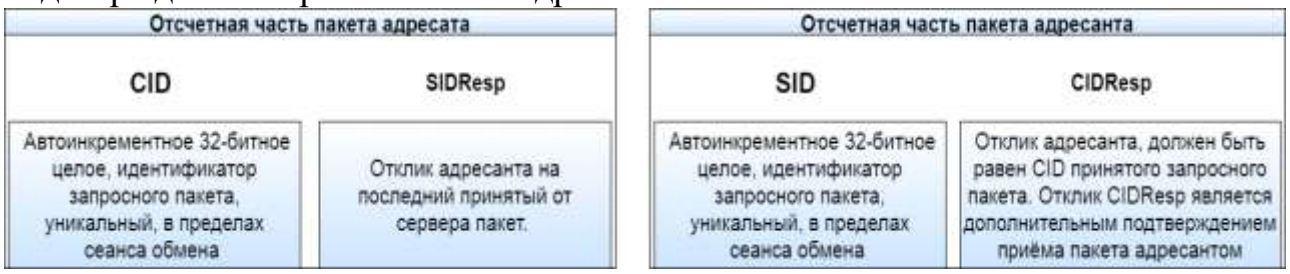

Рис. 3. Отсчетные части пакетов данных агентов

Вероятность успешной атаки на рой, используя уязвимость ложных сообщений, зависит от используемых в протоколе алгоритмов, для вычисления хэш-функции и проверки подписи сообщения [9, 10].

В качестве метода идентификации предлогается алгоритм Фейга-Фиата-Шамира, основанный на протоколе доказательства без разглашения. Хэш-

функция вычисляется по алгоритму SHA1, проверка целостности информации выполняется по алгоритму Hmac. Помехоустойчивость системы обеспечивается использованием циклического избыточного кода CRC. Данная система позволяет изменять алгоритмы на более стойкие без изменения структуры системы [5, 10].

Литература

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2-х кн.: Кн. 1. – М.: Энергоатомиздат, 1994. – 400 с.
2. Герасименко В.А., Малюк А.А. Основы защиты информации: Учебник для высших учебных заведений Министерства общего и профессионального образования РФ – М.: МИФИ, 1997. – 538 с.
3. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Основные положения: принят и введен в действие Постановлением Госстандарта России от 6 апреля 2000 г. № 95-ст. 12 с.
4. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Основные положения: принят и введен в действие Постановлением Госстандарта России от 30 июня 2000 г. № 175-ст
5. Тараскин М.М., Царегородцев А.В. Защита информации в организациях: методика исследования угроз, уязвимостей и рисков – М.: Академия ФСБ России, 2012.
6. Интеллектуальная транспортная геоинформационная система ITSGIS. Ядро / Т.И. Михеева, С.В. Михеев, О.К. Головнин, А.В. Сидоров, Е.А. Савинов. – Самара : Интелтранс, 2016. – Т.1. – 171 с. – ISBN 978-5-9906857-4-1.
7. Михеева, Т.И. Интеллектуальная дислокация дорожных знаков на электронной карте // Т.И. Михеева, С.В. Михеев, А.В. Сидоров // М.: Мир дорог.– 2003. № 72. – С. 44-47.
8. Михеева, Т.И. Информационная технология автоматической дислокации геообъектов транспортной инфраструктуры на улично-дорожной сети // Т.И. Михеева, А.В. Сидоров, О.К. Головнин / Перспективные информационные технологии (ПИТ-2013) //Труды межд. научно-техн. конф. – Самара: Изд-во Самарск. науч. центра РАН, 2013. – С.236-241.
9. Михеев, С.В. Модели транспортных потоков в интеллектуальных транспортных системах / Т.И. Михеева, С.В. Михеев, И.Г. Богданова // Современные проблемы науки и образования. – 2013. – № 6; URL: www.science-education.ru/113-11808.
10. Михеева Т.И., Интеллектуальная транспортная геоинформационная система ITSGIS / Т.И. Михеева, С.В. Михеев, О.К. Головнин // Современные проблемы безопасности жизнедеятельности: интеллектуальные транспортные системы : материалы IV Международной научно-практической конференции (Казань, 25–26 февраля 2016 г.). – Казань : ГБУ «Научный центр безопасности жизнедеятельности», 2016. – С. 362–368. – ISBN 978-5-85247-837-5.