АЛГОРИТМЫ ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

Румас Р. А.
Кафедра телекоммуникаций и информационных технологий
Белорусский государственный университет
Минск, Республика Беларусь
E-mail: antanana71@gmail.com

В статье рассмотрены алгоритмы однонаправленной передачи данных в компьютерных сетях на основе архитектуры, обеспечивающей однонаправленную передачу данных на аппаратном уровне. Одной из проблем работы средств однонаправленной передачи данных является отсутствие в публичном доступе алгоритмов от существующих производителей, что препятствует исследованию и развитию этих решений. Предложенные алгоритмы направленные на решение задачи передачи файлов данных и событий информационной безопасности между различными информационными системами.

Введение

Вопрос защиты критических важных объектов информатизации (КВОИ) становится актуальнее на фоне развития сферы кибербезопасности [1-2] и необходимости взаимодействия объектов информационной инфраструктуры КВОИ с центрами кибербезопасности в рамках выполнения требований законодательства. Для решения указанной задачи целесообразно использовать надежные решения – средства однонаправленной передачи данных, исключив несанкционированный доступ на КВОИ. Решения однонаправленной передачи данных, предлагаемые на рынке, не раскрывают свои алгоритмы, что усложняет внедрение и адаптацию данных технологий в новых областях. В статье представлен набор алгоритмов для однонаправленной передачи файлов данных и событий информационной безопасности, которые обеспечивают передачу данных на физическом уровне через оптическую гальваническую развязку [3]. Основной задачей является обеспечение безопасной передачи данных в формате UDP-пакетов между информационными системами, исключая несанкционированный доступ.

I. Методы исследования

Архитектура системы состоит из двух прокси-серверов: отправляющего и принимающего. Прокси-серверы соединены через физический однонаправленный канал, включающий два медиаконвертера и оптический сплиттер, что позволяет передавать исключительно UDP-пакеты [4]. На каждом из серверов реализуются специализированные алгоритмы для обработки и передачи данных в зависимости от типа информации. Все предложенные алгоритмы разрабатывались с учетом требований к безопасности, скорости передачи и минимизации потерь данных.

II. Алгоритм передачи файлов данных

Вопрос передачи файлов данных между информационными системами является одним из актуальных, поэтому рассмотрим соответствующий алгоритм.

Прокси-сервер реализовывает две основные функции:

получение (передача) файлов данных непосредственно привычными двунаправленными протоколами из информационной системы, например FTP или SMB;

однонаправленная передача файлов данных через оптическую гальваническую развязку с прокси-сервера отправителя на прокси-сервер получатель.

Рассмотрим более подробно алгоритм однонаправленной передачи файлов данных.

1. На прокси-сервере отправителе работает программное обеспечение (ПО), которое проверяет в заранее определенной папке наличие файлов данных;
2. На прокси-сервере получателе запускается модуль ПО, например udp-receiver [5], который начинает прослушивать UDP-пакеты и ожидать получения пакетов через однонаправленный канал передачи данных;
3. В случае наличия файлов данных для передачи (на прокси-сервере отправителе) запускается модуль ПО, например udp-sender [5], который запускает процесс однонаправленной передачи файла данных через оптическую гальваническую развязку, используя транспортный протокол UDP из-за отсутствия обратной связи и невозможности установления TCP-соединения;
4. На прокси-сервере получателе после начала получения потока UDP-пакетов происходит сборка пакетов, проверка контрольных сумм и восстановление исходного файла;
5. После успешного получения и формирования файла данных на прокси-сервере получателе, оператор может получить передаваемый файл привычным двунаправленным протоколом, например FTP или SMB.

Если обнаруживается потеря пакетов, используется, например, метод прямой коррекции

ошибок (FEC) или повторная передача поврежденного файла данных, инициируемая оператором в ручном режиме по результатам анализа принятого файла.

Для решения вопроса с проверкой целостности файлов данных, которые передаются через однонаправленный канал данных, дополнительно можно использовать передачу файла с контрольными данными, например название передаваемого файла, хэш-сумма, размер. Указанная информация позволит прокси-серверу получателю проверить целостность принимаемого файла данных и иную техническую информацию.

III. Алгоритм передачи событий информационной безопасности

Для передачи событий информационной безопасности (ИБ), например журналы событий систем или средств защиты информации, рассмотрим формализованный протокол syslog для передачи событий ИБ в режиме реального времени. Используются легковесные UDP-сообщения, которые содержат ключевые параметры события, включая метку времени, идентификатор события и краткое описание.

С учетом того, что однонаправленная передача данных обеспечивается на транспортном протоколе UDP, на котором в том числе работает syslog без необходимости преобразования пакетов, рассмотрим следующий алгоритм.

1. События ИБ поступают UDP-пакетами от источников, например от объектов информационной инфраструктуры КВОИ, на прокси-сервер отправитель. В свою очередь прокси-сервер отправитель реализует функционал по пересылке получаемых UDP-пакетов через ПО, например iptables для ОС Linux;
2. Пересылаемые UDP-пакеты с прокси-сервера отправителя через оптическую гальваническую развязку поступают на прокси-сервер получателя;
3. Прокси-сервер получателя реализует функционал по пересылке получаемых UDP-пакетов через ПО, например iptables для ОС Linux, на систему централизованного сбора событий ИБ, например SIEM-систему.

Каждый из алгоритмов был адаптирован под специфику передаваемых данных, что делает возможным применение предложенных решений в различных сферах.

IV. Заключение

Рассмотрены алгоритмы однонаправленной передачи файлов данных и событий информационной безопасности для обеспечения надежной и безопасной работы, например при взаимодействии объектов информационной инфраструктуры критически важного объекта информатизации с центрами кибербезопасности. Представленные алгоритмы применимы в защищенных сегментах сетей, где необходимо обеспечить в том числе кибербезопасность и защиту от несанкционированного доступа на аппаратном уровне.

Список литературы

1. О кибербезопасности : Указ Президента Респ. Беларусь, 14 фев. 2023 г., № 40 // Нац. реестр правовых актов Респ. Беларусь. – 2023. – 1/20733.
2. О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 [Электронный ресурс] : приказ ОАЦ при Президенте РБ, 25 июля 2023 г., № 130 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – 2023. – 7/5425.
3. Воротницкий Ю. И., Румас Р. А. Оптическая гальваническая развязка при однонаправленной передаче данных // Квантовая электроника [Электронный ресурс] : материалы XIV Междунар. науч.-техн. конф., Минск, 21–23 нояб. 2023 г. / Белорус. гос. ун-т ; редкол.: М. М. Кугейко (гл. ред.), А. А. Афоненко, А. В. Баркова. – Минск : БГУ, 2023. – 1 электрон. опт. диск (CD-ROM). – ISBN 978-985- 881-530-1. – С. 302–305.
4. Воротницкий Ю. И. Архитектура аппаратно-программного средства однонаправленной передачи данных в компьютерных сетях / Ю. И. Воротницкий, Р. А. Румас // Доклады БГУИР. 2023. Т. 21, No 3. С. 96–101. http://dx.doi.org/10.35596/1729-7648-2023-21-3-96-101.
5. Udpcast. Command line tool [Электронный ресурс]. – Режим доступа: https://www.udpcast.linux.lu/cmd.html. – Дата доступа: 01.10.2024.