УДК 004.056.5

ВОПРОСЫ МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ СЕТЕВОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ

В. В. Рева
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Аннотация. Статья посвящена вопросам модернизации защиты сетевого канала передачи данных. Использованы эмпирические и аналитические методы исследования, системный подход, а также группировка и сравнение. Анализируется современное состояние проблемы. Рассматриваются возможности обеспечения безопасности портов, защиты беспроводной и виртуальной локальных сетей, предотвращения спуфинга, DHCP-атак и кражи портов. Обозначены уязвимости сети передачи данных. Разработаны способы модификации систем защиты при атаках разного вида. Такой подход представляется уникальным, т. к. отечественные авторы исследуют безопасность отдельных протоколов и технологий.

Ключевые слова: сетевая передача данных, спуфинг, DHCP-атака, DDoS-атака, интернет вещей, IoT, локальная сеть, кибератака, MAC-флуд.

ISSUES OF MODERNIZATION OF THE SYSTEM OF PROTECTION OF THE NETWORK DATA TRANSMISSION CHANNEL

Vladislav V. Reva
Don State Technical University, (Rostov-on-Don, Russian Federation)

Abstract. The article is devoted to research in the field of modernization of the protection of the network data transmission channel. The work uses empirical and analytical research methods, a systematic approach, as wellas methods of grouping and comparison. The current state of the problem is analyzed. The possibilities of port security, protection of wireless and virtual local area networks, prevention of spoofing, DHCP attacks and port theft are considered. The vulnerabilities of the data transmission network are indicated. Methods of modification of protection systems in case of attacks of various types have been developed. This approach seems to be unique, because domestic authors investigate the security of individual protocols and technologies.

Keywords: network transmission, spoofing, DHCP attack, DDoS attack, Internet of Things, IoT, local area network, cyber attack, MAC flood.

Введение. Распространение мобильных гаджетов предъявляет новые требования к каналам связи. Ставятся и решаются вопросы построения сетевых каналов передачи данных [1]. Такие каналы устанавливают соединения между двумя устройствами, участвующими в обмене данными. Множество организаций рассматривают меры безопасности сетевой модели стека (магазина) сетевых протоколов (англ. open systems interconnection model, OSI) от уровня приложений до степени защиты IP (от англ. international protection rating — международный класс защиты). Однако зачастую остается без внимания канал передачи данных. Это приводит к атакам и компрометациям. В данной работе рассмотрены вопросы безопасности и модернизации сетевого канала передачи данных.

Основная часть

Методы защиты сетевых каналов передачи данных. Сетевые каналы передачи данных задействуют в экономике, обороне, науке и других сферах.

В [1] рассматриваются проблемы создания сетей связи, подчеркивается важность

совершенствования работы в данном направлении.

Автор статьи [2] поднимает вопрос безопасности сетевых каналов передачи данных в часто атакуемой сфере — банковской.

В работе [3] выявлены уязвимые места и способы защиты модели OSI в Cisco. Очень популярная концептуальная модель взаимодействия открытых систем OSI позволяет им взаимодействовать по стандартным протоколам.

В [4] представлено исследование одного из самых распространенных протоколов WLAN (от англ. wireless local area network — беспроводная локальная сеть).

В [5] оцениваются возможности DDoS-атак (от англ. denial of service — отказ в обслуживании) в отношении интернета вещей (IoT). IoT собирает данные, которые можно проанализировать для автоматизации последующих действий или решений.

В [6, 7] описана еще одна технология беспроводной локальной сети — Wi-Fi, обсуждаются вопросы ее безопасности.

Общая проблема перечисленных работ — недостаточное внимание повышению эффективности противодействия кибератакам в сетях передачи данных. Отметим, что для каналов в этом смысле риски очень высоки. Ниже перечислены наиболее распространенные виды атак.

1. ARP-спуфинг. Подмена ARP (от англ. address resolution protocol — протокол определения адреса) позволяет злоумышленнику маскироваться под законный хост, а затем перехватывать кадры данных в сети, изменять или останавливать их. Часто используется для запуска других атак. Это может быть отказ в обслуживании, перехват сеанса или данных между двумя компаниями или людьми («человек посередине»).

2. MAC-флуд. У всех коммутаторов в сети Ethernet есть таблица с адресуемой памятью. В этой автоматизированной системе CAM (от англ. computer-aided manufacturing — автоматизация технологической подготовки производства) хранится информация, которой может воспользоваться злоумышленник, например:

– номера портов,

– MAC-адреса (от англ. media access Control — надзор за доступом к среде).

Таблица с адресуемой памятью имеет ограниченные размеры, атака происходит посредством пересылки MAC-адресов и последующего заполнения коммутатора с помощью ARP-спуфинга. После заполнения системы коммутатор перестает передавать данные в CAM — и начинается трансляция трафика. Ее перехватывает злоумышленник и получает данные, предназначенные для конкретного хоста.

3. Кража портов. Коммутаторы Ethernet запоминают порты. Атака с кражей портов использует эту способность коммутаторов. Злоумышленник наводняет коммутатор поддельными кадрами ARP с MAC-адресом целевого хоста в качестве адреса источника. Коммутатор «обманывают». Целевой хост находится на порту, к которому подключен злоумышленник. Он получает кадры, которые предназначались только для целевого хоста.

4. DHCP-атаки. Протокол DHCP (от англ. dynamic host configuration protocol — протокол динамической настройки узла) не является протоколом канала передачи данных. Однако в исследуемом случае полезны решения для предотвращения атак DHCP. При атаке с подменой DHCP злоумышленник может:

– развернуть мошеннический DHCP-сервер для предоставления адресов клиентам;

– предоставить хост-компьютерам ложный шлюз по умолчанию с ответами DHCP, и кадры данных с хоста направятся на ложный шлюз, где злоумышленник может перехватить весь пакет.

Практические рекомендации обеспечения безопасности сетевых каналов. Назовем несколько способов модификации систем защиты сетевых каналов передачи данных, которые могут снизить вредоносность рассмотренных типов атак.

Обеспечение безопасности порта. По умолчанию безопасность порта ограничивает количество входящих MAC-адресов до одного. При изменении MAC-адреса на порту и при его заполнении безопасность обеспечивается следующими действиями:

– закрытие порта,

– настройка порта на отключение или блокировку MAC-адресов, если превышен лимит.

Такой подход позволит избежать реализации атаки MAC-флудинга и клонирования.

Отслеживание DHCP. DHCP-спуфинг открывает возможность прослушивать запросы DHCP и отвечать на них. При успешной атаке ответ будет отражаться как авторизованный. Отслеживание DHCP — это функция коммутатора, которая позволяет предотвратить такие атаки. Специально настроенный коммутатор определит, какие его порты могут отвечать на запросы DHCP. К тому же порты будут идентифицированы как надежные или ненадежные.

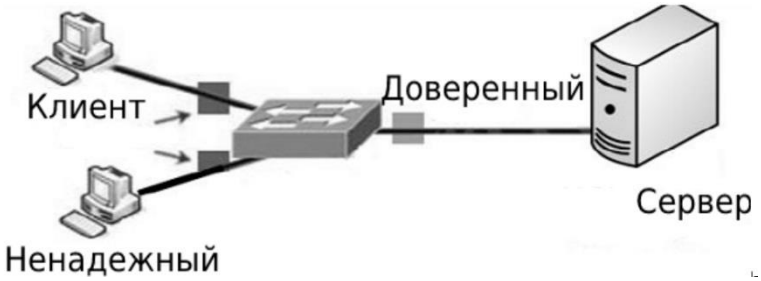

Рис. 1. Отслеживание DHCP

При такой настройке доверенными будут только те порты, которые подключаются к авторизованному серверу. И только через них можно передавать сообщения. Все остальные порты считаются ненадежными и используются только для отправки запросов (см. рис. 1).

Предотвращение ARP-спуфинга. Одно из рекомендуемых действий — использование статических записей ARP в таблице ARP-хоста. Статические записи ARP — это постоянные записи в кэше ARP. Однако данный метод непрактичен и не позволяет использовать протокол DHCP. При этом система обнаружения вторжений склонна сообщать о ложных срабатываниях.

Защита виртуальной локальной сети. Переключение VLAN (от англ. virtual local area network — виртуальная локальная компьютерная сеть) может быть выполнено двумя способами: спуфинг переключателя и двойная маркировка.

В случае с подменой переключателя предупредительные меры против атак с подменой коммутатора:

– перевод пограничных портов в режим статического доступа,

– отключение автосогласования на всех портах.

Предотвращение атак на STP. STP (от англ. spanning tree protocol — протокол остовного дерева) относится ко 2-му уровню управления. При избыточности путей он препятствует образованию петель потока данных. Поясним, что пути создаются с целью укрепления защиты, но вместе с ними могут образовываться петли потоков данных, которые часто приводят к DoS-атаке.

Предупреждение и предотвращение атак на STP обеспечивают функции root guard (англ. корневая защита) и BPDU-guard (от англ. bridge protocol data unit — блок данных протокола мостового перенаправления). Они призваны ограничить порты коммутатора, на которых согласовывается корневой мост. Первая функция оптимальна для портов, на которых происходит

подключение к коммутатору, вторая — для портов, обращенных к пользователям.

Защита виртуальной локальной сети VLAN. Опасность атак на виртуальные локальные сети заключается в том, что с переключением VLAN в одной сети можно подключиться к трафику других сетей и получить данные.

Предупредительные меры против атак с подменой коммутатора:

– перевод пограничных портов в режим статического доступа,

– отключение автосогласования на всех портах.

Атаки в беспроводной локальной сети позволяют злоумышленнику:

– подслушивать,

– выдавать себя за авторизованного пользователя,

– ограничить использование сети,

– отслеживать трафик.

В беспроводных локальных сетях все точки доступа должны быть настроены для обеспечения безопасности посредством шифрования и аутентификации клиентов. Типы схем, используемых в беспроводной локальной сети для обеспечения безопасности, следующие:

– проводная эквивалентная конфиденциальность (англ. wired equivalent privacy, WEP),

– протокол 802.11i,

– защищенный доступ Wi-Fi,

– WPA2 (от англ. Wi-Fi protected access — защищенный доступ Wi-Fi).

Заключение. В рамках представленной работы рассмотрены проблемы безопасности сетевых каналов передачи данных. Описаны методы предотвращения и устранения последствий атак. В ряде случаев возможности обеспечения безопасности ограничиваются. Тем не менее они позволяют усилить защиту сетевого канала. Безопасность системы определяется уязвимостью самого слабого звена. Таковым может быть 2-й уровень. Ему подходят предложенные меры безопасности. К тому же они значимы для защиты сети от многих типов атак.

Библиографический список

1. Кузнецов, М. А. Современные технологии и стандарты подвижной связи / М. А. Кузнецов, А. Е. Рыжков. — Санкт-Петербург : Линк, 2008. — 128 с.

2. Storck, P. Benefits of commercial data link security / P. Storck // Integrated Communications, Navigation and Surveillance Conference (ICNS) // IEEE Xplore : [сайт]. — 2013. — P. 27–38. — URL: https://ieeexplore.ieee.org/document/6548566. 10.1109/ICNSurv.2013.6548566.

3. Alcívar, P. Security in the data link layer of the OSI model on LANs wired Cisco / P. Alcívar, M. G. M. Santos // Journal of Science and Research Revista Ciencia e Investigación. — 2018. — P. 106–112. 0.26910/issn.2528-8083vol3issCITT2017.2018pp106-112.

4. Energy-efficient analysis of an IEEE 802.11 PCF MAC protocol based on WLAN / Z. Guan, Z. J. Yang, M. He, Qian Wen-Hua / Journal of Ambient Intelligence and Humanized Computing. — 2019. — № 10. — P. 1727–1737. 10.1007/s12652-018-0684-8.

5. DDoS in the IoT: Mirai and other botnets / C. Kolias, G. Kambourakis, A. Stavrou, J. Voas // Computer. — 2017. — № 50 (7). — P. 80–84.

6. Росс, Д. Wi-Fi. Беспроводная сеть / Д. Росс. — Москва : НТ Пресс, 2007. — 320 с.

7. Русаков, А. О. Методы защиты от атаки «человек посередине» в Wi-fi сетях / А. О. Русаков, Р. А. Чалый // Актуальные проблемы авиации и космонавтики. — 2016. — Т. 1. — № 12. — С. 767–769.

Об авторе:

Рева Владислав Владимирович, магистрант кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1) supervladrev@gmail.com.

About the Author:

Vladislav V. Reva, Master's degree student of Computing Systems and Information Security Department, Don State Technical University (1, Gagarina sq., Rostov-on-Don, RF, 344003), supervladrev@gmail.com.