Защита канального уровня промышленных Ethernet-сетей

С.С. Воробьев (Компания ПРОСОФТ)

Рассмотрены киберугрозы канального уровня, которые могут возникнуть в промышленных Ethernet-сетях - MAC- и ARP-spoofing, VLAN hopping, STP attack, DHCP starvation. Предложены возможные методы организации защиты на базе принципа Defense in Depth и управляемых коммутаторов.

Ключевые слова: киберугрозы, угрозы канального уровня, защита промышленной Ethernet-сети, Defence in Depth.

Введение

Принцип Defense in Depth является многоуровневым механизмом обеспечения защиты промышленной Ethernet-сети [1]. Каждый этап подразумевает различные типы анализа и защиты. Например, защита периметра промышленной сети — это в первую очередь защита от внешних угроз. Она реализуется при помощи промышленного IP-брандмауэра, работающего на уровне L3 модели OSI [1, 2]. Однако угрозы, связанные с безопасностью промышленной сети, могут возникать из внешней сети и исходить из внутренней, в которой находятся устройства, функционирующие исключительно на уровне L2 модели OSI. А ведь на уровне L2 свои правила, устройства здесь оперируют исключительно фреймами. И если не знать и не контролировать того, что происходит на уровне L2, то даже некорректная работа собственного внутреннего оборудования или программного обеспечения может привести к проблемам и сбоям. Например, неконтролируемая широковещательная рассылка (broadcast) может заполонить и перегрузить сегмент сети, атаки типа VLAN hopping могут привести к несанкционированному доступу к различным узлам, а MAC flooding может превратить управляемый коммутатор в обычный узел (hub). При этом IP-брандмауэр, который функционирует на уровне L3 и работает исключительно с IP-адресами, будет функционировать в штатном режиме и никак не просигнализирует о наличии угрозы.

Для решения данной проблемы и нейтрализации угроз канального уровня необходимо использовать устройство, которое функционирует на уровне L2 модели OSI и позволяет анализировать трафик. Таким устройством может стать брандмауэр уровня L2 [1] либо коммутатор с расширенной политикой безопасности. Правильная настройка коммутаторов может защитить сеть от множества угроз. Рассмотрим возможные угрозы канального уровня и механизмы защиты на примере промышленного коммутатора серии RSP35 от Hirschmann с установленной операционной системой HiOS.

Угрозы канального уровня: что защищаем?

Канальный уровень (Data Link Layer) является вторым по счету как в модели OSI, так и в модели TCP/IP. Передача данных осуществляется при помощи фреймов размером 64...1518 байт. Существуют также вариации меньше 64 (Runts) и больше 1518 (Jumbo) байт. Адресация осуществляется на основе MAC-адресов, а в качестве основного инструмента, позволяющего собрать информацию о подключенных устройствах, выступает протокол ARP (Address Resolution Protocol — протокол определения адреса). С первого взгляда все просто: установили коммутаторы, произвели их первоначальную настройку, сеть в итоге работает, а безопасность перекладывается на более высокие уровни, где уже задействованы мощные L3-брандмауэры. При этом многие администраторы просто не уделяют должного внимания тем процессам, которые происходят именно на втором, канальном уровне. В рамках промышленной сети это может негативно отразиться на работе технологических процессов, ведь основное число устройств функционирует именно на втором уровне. А там все не так просто, в первую очередь это связано с тем, что многие протоколы второго уровня, например ARP и STP, разрабатывались без какой-либо привязки к безопасности. Например, при базовой конфигурации коммутатора не требуется никакой дополнительной информации, чтобы при помощи ARP-запроса узнать MAC-адрес хоста по известному IP-адресу. В итоге в первую очередь необходимо защитить используемые L2-протоколы путем правильной настройки коммутаторов. Современные промышленные коммутаторы имеют в своем арсенале достаточно инструментария для защиты именно второго, канального уровня.

Но для правильной конфигурации необходимо также понимать логику работы атакующих ПК и технологию потенциальных угроз. Рассмотрим самые популярные из них.

ARP- и MAC-spoofing или угроза мирному протоколу

ARP-протокол используется для определения физического MAC-адреса при условии известного IP-адреса получателя. Работу протокола можно описать следующими действиями.

Сетевое устройство посылает запросы ARP, в которых содержится вопрос: «IP-адрес x.x.x.x — это вы? Прекрасно! Присылайте ваш MAC-адрес» (https://xakep.ru). Пакеты рассылаются на все узлы в сегменте сети, и каждый исследует ARP-запрос и отсылает ответ в случае совпадения. Данный принцип работы является уязвимым, а атаки, которые это используют, имеют общее название spoofing — подмена. Они сводятся к подмене настоящего MAC-адреса устройства адресом злоумышленника. При правильно реализованной атаке это приводит к захвату фреймов и перехвату информации.

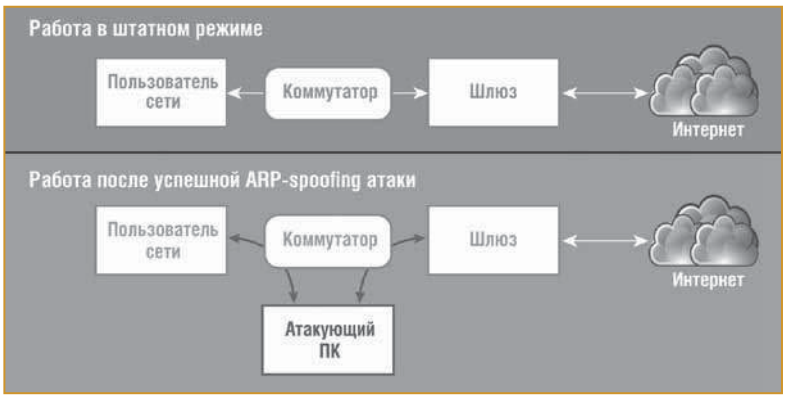

Рис. 1. Пример ARP-spoofing атаки

Виды атак

— *MAC-spoofing*. Это атака канального уровня, заключается она в том, что на сетевой карте изменяется MAC-адрес, и это заставляет коммутатор отправлять на порт, к которому подключен злоумышленник, пакеты, которые до этого он видеть не мог.

— *ARP-spoofing*. Цель данной атаки состоит в том, чтобы послать хосту специально подготовленный ответ, в котором IP-адрес будет сопоставлен ложному MAC-адресу. Результатом данной атаки будет отсылка пакетов не к узлу A (изначальному конечному устройству), а к узлу B. При этом жертва даже не будет знать, что посылает пакеты не по тому адресу. Такой процесс называют часто отравлением ARP-кэша (рис. 1) (https://xakep.ru).

Как защититься?

Подобные атаки достаточно широко известны, построить против них грамотную защиту можно при помощи настройки политики безопасности (Port Security) каждого конкретного порта коммутатора, то есть закрыть доступ к порту всем чужим устройствам. Реализация может быть различной, начиная от банального отключения неиспользуемых портов, что является важным и обязательным действием, и заканчивая настройкой управления доступом в соответствии с IEEE 802.1x.

При правильной настройке Port Security устройство позволяет передавать данные только от желаемых отправителей. Когда эта функция включена, коммутатор проверяет идентификатор VLAN и MAC-адрес отправителя до принятия решения по передаче пакета данных. В итоге коммутатор отбрасывает пакеты данных от других отправителей и регистрирует это событие. Операционная система HiOS, установленная в коммутаторах Hirschmann RSP35, позволяет настроить: число статических и динамических MAC-адресов на каждый порт, параметры отправки SNMP-трапа при регистрации несанкционированного подключения, а также активацию функции Auto Disable, которая позволяет полностью выключить порт при подключении чужого устройства. Правильная настройка Port Security коммутатора делает реализацию атак типа MAC- и ARP-spoofing значительно сложнее. При этом наличие возможности ограничения числа динамических MAC-адресов сводит к минимуму воздействие атаки типа MAC-flooding, цель которой — переполнение CAM-таблицы (Content Addressable Memo) коммутатора (CAM-table overflow).

Другим возможным инструментом настройки Port Security является управление доступом в соответствии с IEEE 802.1x. Это стандарт, который используется для аутентификации и авторизации пользователей и рабочих станций в сети передачи данных (http://habrahabr.ru). При помощи данного инструмента можно предоставить права доступа к различным блокам и сервисам сети, в нашем случае это определенные порты коммутатора.

Данный способ является более сложным, требующим наличия сервера аутентификации (RADIUS-сервер), аутентификатора (в нашем случае это коммутатор), а также клиентского ПО 802.1x на рабочей станции конечного пользователя. Аутентификатор и конечные устройства взаимодействуют через протокол аутентификации EAPoL (Extensible Authentication Protocol over LANs). При подобной настройке управления доступом к портам контролируется доступ к сети с подключенных конечных устройств.

VLAN — это про безопасность?

Создание сети при помощи VLAN (Virtual Local Area Network) — логических (виртуальных) локальных компьютерных сетей является одним из самых популярных способов разделения сети на сегменты. Существует механизм уровня L2 — IEEE 802.1Q и L3 — IEEE 802.1v. Самый популярный — это механизм второго уровня на базе портов коммутатора. Он встречается практически в каждой сети. Все очень просто: порты коммутатора помещаются в разные VLAN. Далее при прохождении фрейма через порт в него дописывается специальный тег, который как раз и позволяет определить номер VLAN. Фактически создаются несколько виртуальных коммутаторов внутри одного. Создается иллюзия, что никакая атака не пройдет. Но, к сожалению, это только иллюзия. Атаки, связанные с VLAN, — это самый популярный тип атак, носят они название VLAN hopping (http://habrahabr.ru) — перепрыгивание. Атаки данного типа предполагают получение доступа в VLAN, который изначально был нереализуем для атакующего ПК.

Виды атак

VLAN-spoofing или атака на DTP-протокол. Данная атака работает преимущественно на коммутаторах Cisco [3] и возможна из-за того, что коммутаторы с поддержкой протокола Cisco DTP (Dynamic Trunking Protocol) могут автоматически согласовывать тип порта (access или trunk). Не вдаваясь в подробности данной атаки, отметим, что, используя протокол

Рис. 2. Пример атаки типа VLAN hopping/Double tagging attack

DTP и «недонастроенный» коммутатор, атакующий ПК может получить доступ ко всем VLAN, присутствующим на коммутаторе.

Атака при помощи Native VLAN. Native VLAN — это достаточно архаичное понятие в стандарте 802.1Q, обозначающее VLAN, к которой коммутатор относит все фреймы, идущие без тега, то есть трафик внутри Native VLAN передается нетегированным. Фактически коммутатор, видя, что к нему пришел нетегированный фрейм, помещает его автоматически в Native VLAN и далее передает его в место назначения. Попадая на другой коммутатор, фрейм без тега помещается в его Native VLAN и т. д. Таким образом возможно получить доступ к ряду хостов. По умолчанию Native VLAN — это VLAN 1.

Double tagging attack. Данная атака также связана с уязвимостью многих коммутаторов, которые поддерживают стандарт 802.1Q. Для дальнейшего пояснения назовем порт, к которому подключены оконечные устройства или хосты, access, а порты коммутатора, которые подключены к другим коммутаторам, trunk. Механизм данной атаки заключается в том, что на access-порт коммутатора приходит фрейм с двумя тегами, один из которых соответствует Native VLAN данного коммутатора, а другой тег соответствует VLAN, в которую хочет попасть атакующий. И если в trunk-соединение между коммутаторами включена Native VLAN (по умолчанию она, как правило, включена), то коммутатор передаст данный пакет со вторым тегом, отбросив первый (рис. 2) [3].

Как защититься?

Разделение сети при помощи VLAN может быть безопасным, правильно настроенная конфигурация коммутатора в части VLAN, отличная от начальной «из коробки», позволит увеличить безопасность сети и грамотно разделить потоки данных. Сформулируем ряд рекомендаций, которые позволят сделать сеть, в которой присутствуют VLAN, безопаснее.

1. При создании сети с VLAN необходимо поместить все используемые порты коммутатора в различные VLAN, отличные от ID 1.
2. Не использовать Native VLAN вообще.
3. Использовать принудительное тегирование всех фреймов.
4. Помещать порты между коммутаторами в отдельную VLAN.
5. Настроить порты, задействованные для передачи между коммутаторами, на прием только тегированных фреймов.
6. Для управления коммутаторами рекомендуется создать отдельную VLAN.
7. Создать DUMMY VLAN для неиспользуемых портов либо отключить их, используя механизм Port Security.
8. Отключить протокол DTP для устройств Cisco.

Далее, на примере коммутатора Hirschmann RSP35 рассмотрим механизм настройки. Необходимо сделать три простых шага: 1) создать необходимые VLAN; 2) определить правила для исходящего из порта трафика; 3) определить правила для входящего в порт трафика.

При определении правил для исходящего трафика необходимо указать по каждому порту действия коммутатора перед отправкой фрейма:

— T — порт находится в данном сегменте VLAN, фреймы посылаются с тегом;

— U — порт находится в данном сегменте VLAN, фреймы посылаются без тега;

— F — порт не находится в данном сегменте VLAN.

Соответственно, в зависимости от подключенного к порту устройства нужно установить необходимые настройки. Если порт подключен к соседнему коммутатору, и необходимо передать тегированный трафик, то устанавливаем значение T. Если к порту подключен хост, который не умеет работать с VLAN, но пакет должен быть передан, то устанавливаем значение U. Если передавать трафик данного VLAN в этот порт не нужно, устанавливаем F.

При определении правил для входящего трафика необходимо также заполнить простую таблицу, выполнив два действия. Для начала надо поместить порты коммутатора в различные VLAN и указать: с каким трафиком будет работать данный порт, с тегом или без тега. Если порты соединяют два коммутатора, их необходимо поместить в отдельные VLAN, указав при этом работу исключительно с тегированным трафиком.

При этом такие настройки, как принудительное тегирование всех фреймов, обязательное помещение каждого порта в VLAN, уже присутствуют в коммутаторах Hirschmann изначально, что существенно упрощает процесс настройки. В итоге правильно настроив VLAN на коммутаторах, можно сделать сеть

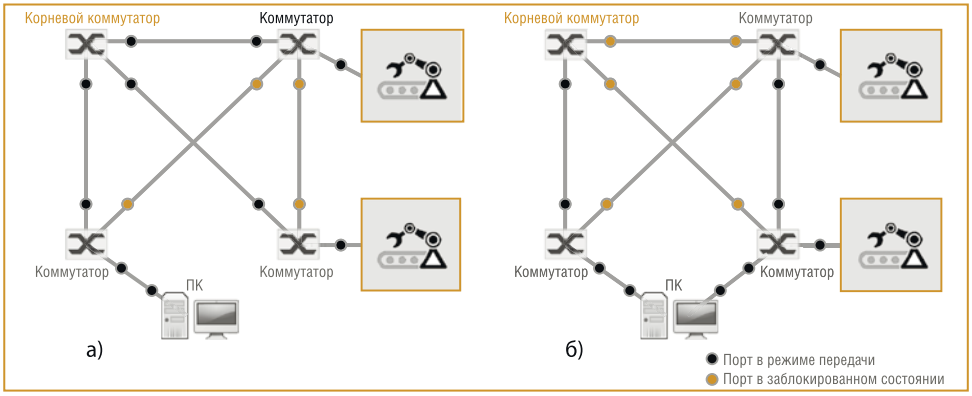

Рис. 3. Пример атаки на xSTP-протокол: а – конфигурация сети при штатной работе xSTP-протокола, б – конфигурация сети после успешной атаки

намного безопаснее.

Резервирование в промышленной сети — необходимость, а как с безопасностью?

Резервированные соединения являются обязательной частью промышленной Ethernet-сети. Сеть должна быть доступна и работоспособна в любой момент времени, иначе может произойти какая-либо нештатная ситуация. Для промышленных сетей, как правило, используются механизмы резервирования, функционирующие на втором, канальном уровне модели OSI. Одни из самых популярных протоколов — это группа xSTP (Spanning Tree Protocol), в которую входят STP, RSTP (Rapid STP) и MSTP (Multiple STP). Основной задачей xSTP является устранение петель в топологии из-за наличия избыточных соединений. Решается эта задача путем выбора корневого пути и блокировки избыточных соединений. В результате работы протокола строится минимальное остовное дерево, которое и будет являться рабочей топологией. Для обмена информацией между собой и формирования структуры дерева коммутаторы используют специальные пакеты BPDU (Bridge Protocol Data Units). Конфигурационные пакеты регулярно рассылаются корневым коммутатором на широковещательный адрес, который прослушивают все коммутаторы с включенным xSTP.

В итоге, зная, что в сети используются протоколы xSTP, можно успешно провести на нее атаку и перехватить весь трафик сегмента [4].

Атака STP

STP attack. Атака данного типа возможна по той же причине, что и атака на сеть, использующую протокол ARP. Протоколы xSTP никак не защищены. Цель подобной атаки — это разорвать связующие звенья дерева, дестабилизировать CAM-таблицы, а также удерживать сеть в непрерывном состоянии повторного выбора корневого коммутатора. Это можно сделать путем создания ложных BPDU-фреймов несуществующего коммутатора. В итоге можно удерживать сеть в состоянии непрерывного выбора корневого моста, и любой широковещательный трафик станет причиной широковещательного шторма, насыщая сеть фреймами и приводя ее в неработоспособное состояние. Другой возможный сценарий — это стать корневым коммутатором, что приведет к захвату всего трафика сегмента (рис. 3).

Как защититься?

Существует несколько достаточно несложных методов для защиты сети с xSTP-протоколами от атаки. Во-первых, необходимо уйти от первоначальных настроек коммутатора. Коммутатор выходит с фабрики в конфигурации, которая способствует легкому внедрению в уже существующую сеть. В нем, как правило, один из xSTP-протоколов по умолчанию включен на всех портах, обычно это RSTP. Так сделано для удобства, но в целях обеспечения безопасности данную конфигурацию необходимо изменить.

Для успешной STP-атаки у атакующего ПК должен быть доступ к порту, на котором включен xSTP-протокол, для дальнейшей передачи фреймов с ложными BPDU. Следовательно, реализация подобных атак становится намного труднее, если установить запрет на доступ со стороны оконечных устройств и хостов к портам коммутатора, на которых включен xSTP-протокол. Реализуется это путем выключения xSTP на портах, которые не участвуют в построении общей топологии, а также путем настройки Port Security. Данные действия значительно усложнят возможность описанной ранее атаки.

Еще один подход заключается в переходе от xSTP-протоколов к более современным протоколам резервирования. Такими на сегодняшний день являются протоколы кольцевого резервирования, которые обеспечивают быстрое время восстановления

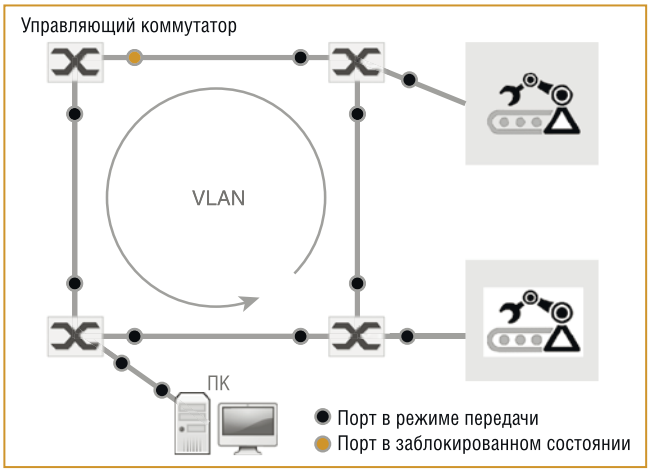

Рис. 4. Резервирование сети при помощи кольцевой топологии

(< 200 мс), например, стандартизованный MRP (Media Redundancy Protocol). При использовании данного протокола организация связи имеет более высокую защиту. Если рассматривать тот же MRP, то администратором вручную задается управляющий коммутатор (Ring Manager) с четким указанием портов, а при создании служебного канала обмена информацией между коммутаторами автоматически создается отдельная VLAN с уже настроенной политикой доступа (рис. 4). Допускается одновременное использование MRP и протоколов резервирования группы xSTP. В итоге, настроив правильно протоколы резервирования и Port Security, можно увеличить степень защиты сети, сохранив при этом ее отказоустойчивость.

Легко обнаружить, легко атаковать

Следующий тип атак связан с наличием удобной функциональности ряда коммутаторов, которая позволяет обнаружить устройство и задать первоначальную конфигурацию. Такие протоколы, как HiDiscovery от Hirschmann фактически позволяют заменить консольный порт, с их помощью можно обнаружить устройство, определить его тип и задать первоначальные настройки.

Атака же сводится к отправке широковещательного запроса и перехвата ответного трафика, который и содержит множество полезной информации, начиная от типа устройства и заканчивая настройками параметров в сети.

Как защититься?

Защититься можно банальным отключением данных протоколов. Да, конечно, обнаружить устройство теперь станет сложнее. Но и потери важных служебных данных не произойдет.

Защитить DHCP-сервер

DHCP-сервер (Dynamic Host Configuration Protocol) — это сетевое устройство, которое позволяет автоматически получать параметры, необходимые для работы в сети со стеком протоколов TCP/IP. Работа строится по модели клиент-сервер. Клиент на этапе конфигурации сетевого устройства обращается по DHCP-протоколу к серверу и получает от него нужные параметры. С одной стороны, это позволяет избежать ручной настройки сетевых устройств, а с другой, — это делает сеть уязвимой к специфическим атакам.

DHCP-атака

DHCP starvation. Данный тип атаки сводится к тому, что атакующий отсылает DHCP-серверу большое число DHCP-запросов с разными MAC-адресами. В итоге рано или поздно весь набор свободных параметров закончится, и сервер не сможет обслуживать новых клиентов. В результате нарушается работоспособность сети.

Как защититься?

Данный вид атак не является классической атакой L2-уровня, но все-таки может нарушить работу многих устройств, в том числе и работающих на канальном уровне. Метод борьбы с подобными атаками имеет название DHCP snooping и зачастую поддерживается коммутаторами [5]. Логика работы сводится к тому, что когда коммутатор получает фрейм, в котором находится DHCP-запрос, он сравнивает MAC-адрес в запросе и адрес, который присутствует на данном порту коммутатора. Если адреса совпадают, то коммутатор отправляет пакет дальше, так как данный клиент известен. Если адреса не совпадают, то коммутатор отбрасывает пакет.

Свой–чужой, списки доступа

Списки доступа — ACL (Access Control List) являются пограничной защитой, которые жестко что-то разрешают либо что-то запрещают. Обычно список доступа разрешает или запрещает IP-пакеты, и реализуется это на базе брандмауэра. Но также существуют списки доступа на базе MAC-адресов. При этом появляется возможность создания списков доступа как на базе конкретных портов, так и на базе созданных VLAN. При создании ACL-правил устройство разрешает трафик для созданных правил, а весь остальной блокирует.

Заключение

При построении многоуровневой защиты промышленной Ethernet-сети зачастую не уделяется должного внимания угрозам второго, канального уровня модели OSI. Но угроз здесь достаточно много. Множество угроз не поддается обнаружению с помощью мощных L3-брандмауэров. Но они могут быть нейтрализованы при помощи современных промышленных коммутаторов, которые обладают очень удобными и эффективными механизмами защиты. Атаки типа MAC- и ARP-spoofing, VLAN hopping, STP attack, DHCP starvation могут быть предотвращены путем правильной настройки коммутатора. Кроме того, создание списков доступа ACL позволит не только создать добавочную защиту, но и уменьшить нежелательный трафик.

Список литературы

1. *Воробьев С.С.* Глубокая защита промышленного сетевого периметра // Современные технологии автоматизации. 2017. № 4.
2. *Воробьев С.С.* Defense in Depth в действии. Уровень 1: защита границы сети // Современные технологии автоматизации. 2017. № 4.
3. *Одом У.* Cisco CCNA, ICND2 200-101. М.: Вильямс, 2015.
4. *Томицки Л.* Атака на протокол Spanning Tree [Электронный ресурс] // Сайт Securitylab. Режим доступа: http://www.securitylab.ru/analytics/451090.php.
5. *Бражук А.* Защита внутри периметра [Электронный ресурс]//Хакер. Режим доступа: https://xakep.ru/2013/08/23/safe-among-perimetr/.

Воробьев Сергей Сергеевич *– инженер по применению АСУТП компании ПРОСОФТ.*
Контактный телефон (495) 234-06-36.
E-mail: info@prosoft.ru