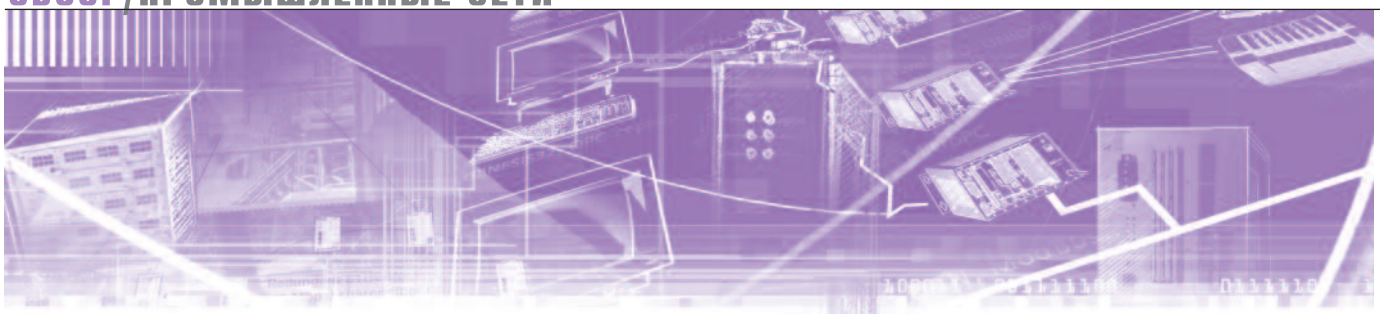

Сергей Воробьёв

“Defense in Depth” в действии. Уровень 4: защита промышленных протоколов

Часть 2

Данный материал продолжает цикл статей, посвящённых многоуровневой защите промышленных Ethernet-сетей на базе принципа “Defense in Depth”. В статье рассмотрен ряд базовых уязвимостей промышленного протокола EtherNet/IP, а также методы его защиты, основанные на глубокой инспекции трафика.

Введение

Как было упомянуто в [1], тщательная и глубокая проверка данных (DPI), передаваемых по промышленной Ethernet-сети, является узконаправленным механизмом защиты, который позволяет нейтрализовать угрозы, направленные на оконечные устройства, функционирующие на базе широко известных промышленных протоколов. В данной части статьи рассмотрим более подробно популярный протокол EtherNet/IP, методы его защиты на базе DPI, а также её реализацию на базе промышленного DPI-брандмауэра Tofino Xenon и модуля Tofino EtherNet/IP Enforcer LSM.

Протокол EtherNet/IP

EtherNet/IP – это промышленный протокол, который фактически адаптирует известный протокол CIP (Common Industrial Protocol) для использования в сетях Industrial Ethernet. При этом, если мы рассматриваем любые аспекты управления, контроля и обеспечения безопасности, то необходимо углубиться не только в заголовки протокола EtherNet/IP, но и в структуру протокола CIP, представляющую собой достаточно сложную для понимания объектно-ориентированную модель.

Как и в случае с Modbus TCP [1], EtherNet/IP – это протокол CIP (Common Industrial Protocol), который «упакован» в Ethernet-пакет. Но в отличие от Modbus CIP является достаточно гибким протоколом для приложений промышленной автоматизации, он включает в себя комплексный набор сервисов для систем АСУ ТП: сбор параметров, контроль, синхронизация и т.д. И для общего понимания организации защиты необходимо уяснить базовые принципы работы протокола. Рассмотрим протокол CIP более подробно.

Протокол CIP

CIP-протокол изначально был представлен ассоциацией ODVA (Open DeviceNet Vendors Association), в которую входят более чем 300 участников из различных стран. Он позволяет создать единую коммуникационную систему в масштабах как отдельного производственного процесса, так и предприятия

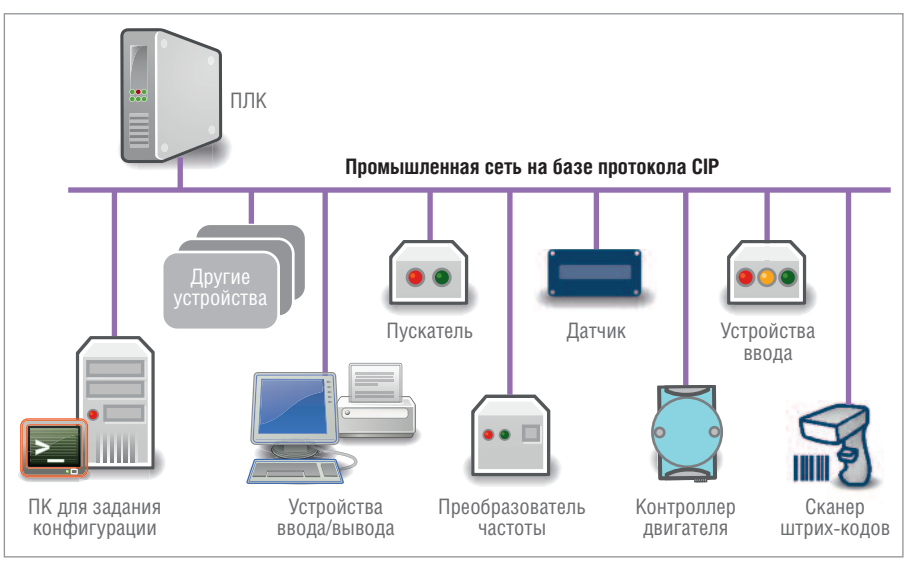

Рис. 1. Группа промышленных устройств, использующих протокол EtherNet/IP и CIP для взаимодействия

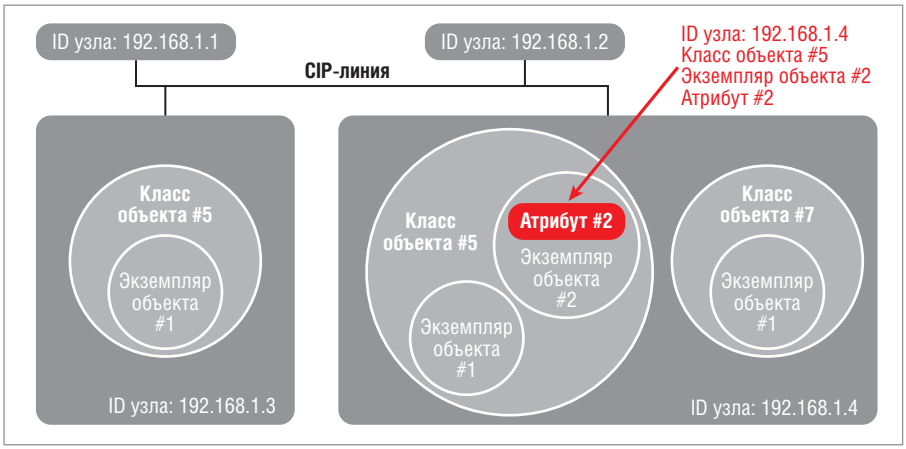

Рис. 2. Пример адресации CIP-объектов

в целом. В настоящий момент CIP-протокол может быть упакован в различный «транспорт»: DeviceNet, ControlNet, CompoNet – это всё различные варианты исполнения протокола CIP [2].

Если рассматривать структуру промышленной сети на базе протокола CIP, то в её основе находится ряд CIP-объектов. По иерархии это объектно-ориентированный подход с созданием абстрактной модели сети.

Физически сеть состоит из CIP-узлов, в качестве которых может выступать очень широкий круг устройств от ПЛК до датчика (рис. 1). CIP-узел (CIP-node) является набором объектов, где объект – это абстрактное представление физической части конкретного устройства [2] и сопоставляется с логическим объектом на основе каждого устройства, поэтому всё, что не описано в виде объекта, не видно через протокол CIP. Каждый объект (Object) принадлежит к одному из классов (Class), которые имеют один и тот же набор атрибутов. Каждый класс имеет уникальный идентификатор в диапазоне от 1 до 65535. Иногда необходимо более одной «копии» класса внутри устройства. Каждая такая «копия» обозначается как экземпляр данного класса (Instance). Объекты имеют связанные с ними переменные данных. Они называются атрибутами (Attribute) конкретного объекта (рис. 2). Обычно атрибуты предоставляют статус или управляют работой объекта. Каждому атрибуту объекта присваивается идентификатор в диапазоне от 0 до 255. Существует два типа атрибутов, а именно атрибуты экземпляра и класса. Экземпляр конкретного объекта является представлением этого объекта внутри класса. Каждый экземпляр имеет тот же набор атрибутов, но свой собственный набор значений атрибутов, что делает каждый экземпляр уникальным. Экземпляры имеют уникальный идентификатор (в диапазоне 1–65535).

Узлы и объекты, из которых создаётся CIP-сеть, используют стандартную схему адресации, включающую следующие элементы:

- *Node ID* назначается каждому узлу сети CIP;
- *идентификатор класса (Class ID)* назначается каждому классу объекта в сети;
- *идентификатор экземпляра (Instance ID)* назначается определённому экземпляру класса;
- *идентификатор атрибута (Attribute ID)* назначается атрибуту класса или объекта;
- *Service Code* идентифицирует конкретное поведение класса или объекта.

В класс могут входить объекты, которые контролируют группу аналоговых входов, а экземпляр может быть конкретным аналоговым входом для передатчика уровня. Примером же атрибута, или, другими словами, свойства для этого экземпляра может быть статус, используемый для указания наличия ошибки при превышении рабочего диапазона напряжения источника входного сигнала.

Каждый объект поддерживает набор сервисов (служб) по умолчанию и в некоторых случаях набор пользовательских сервисов. Сервис – это функция, поддерживаемая объектом. Например, сервис Get Attribute All позволяет запросить значения всех атрибутов для конкретного экземпляра объекта.

С точки зрения организации сети CIP представляет схему, в которой осуществляется соединение между несколькими конечными точками. Но для удовлетворения требований к задержкам используются два разных типа передачи данных. Они ещё называются неявными (implicit) и явными (explicit) сообщениями.

В протоколе EtherNet/IP для implicit-сообщений используется протокол UDP (номер порта 2222), который обеспечивает минимальный уровень задержки, для explicit-сообщений используется протокол TCP (номер порта TCP 44818) для случаев, когда необходимо надёжное соединение, например между ПЛК и HMI.

При этом одна из главных задач EtherNet/IP – установка соединения с использованием стандартных команд, в частности, команды Register Session, которая должна быть выполнена до любого обмена CIP-сообщениями. После установления сеанса обновляются различные поля в заголовке EtherNet/IP, такие как длины пакетов и типы данных соединения, которые относятся к последующему CIP-пакету.

Уровень CIP-данных более сложный, но соответствует стандартному формату. Он может включать в себя различную функциональность, но всё в пределах прикладного уровня согласно модели OSI. Сильной стороной протокола является его способность группировать точки данных через представление объекта. Например, если программируемый логический контроллер имеет аналоговый выходной сигнал, то он представлен через объект. При необходимости HMI может использовать данный объект для извлечения данных и настройки аналоговых выходных точек в ПЛК [3].

Угрозы безопасности для протокола EtherNet/IP

Как уже было описано в [1], сетевые протоколы, такие как Ethernet/IP, никогда не предполагали наличия функций обеспечения безопасности сети. Большинство промышленных протоколов, как и бóльшая часть спецификаций EtherNet/IP и CIP, были разработаны в то время, когда безопасность систем АСУ ТП не рассматривалась, в принципе.

В результате механизмы для обеспечения конфиденциальности, целостности или доступности передаваемой информации не были включены в спецификацию.

Эти моменты были не раз упомянуты в различных исследованиях и при разборе реальных событий [3]. Фактически ситуация такова, что если сотрудник предприятия имеет доступ к передаче данных с ПЛК по протоколу EtherNet/IP, то, скорее всего, у него есть возмож-

ность отключить либо перепрограммировать ПЛК.

Пример подобных атак был продемонстрирован на примере ПЛК Allen-Bradley серии ControlLogix [3]. В процессе атаки сперва был установлен сеанс EtherNet/IP между компьютером и ПЛК, а затем, используя CIP-объект, атакующий ПК смог изменить ряд параметров в устройстве, таких как IP-адрес, сетевая маска и DNS-серверы. Аутентификация для данных действий не требовалась, только создание нового сеанса EtherNet/IP. Объект CIP не является вредоносным по своей природе, но он может быть использован злоумышленником для вредоносных действий.

Используя подобную технику атаки, несложно догадаться, что атакующий ПК может прослушивать активный сеанс и добавлять в последовательность передаваемых данных различные CIP-пакеты, например, для изменения IP-адреса ПЛК, с которым происходит обмен, тем самым прерывая сессию. Отсутствие в протоколе EtherNet/IP аутентификации оставляет достаточно явную «дыру» для возможных атак.

Но, наверно, более опасной является способность атакующего ПК инициировать обновление прошивки. EtherNet/IP – это протокол, который обладает очень гибкими возможностями, что, с одной стороны, повышает возможности управления, а с другой стороны, позволяет сделать критические изменения конфигурации, причём для этого необходимо лишь использование стандартного обмена CIP-сообщениями. Подобная уязвимость была также продемонстрирована на примере ПЛК ControlLogix [3]. Но такие уязвимости протокола не являются недоработкой, так как изначально спецификация EtherNet/IP не предполагала это. Анализ всех подобных уязвимостей приводит к вопросу: какой механизм аутентификации можно было бы добавить в спецификацию для предотвращения отправки вредоносных сообщений CIP? И это уже область для будущих исследований и разработки дополнительных стандартов.

Но иногда возникает ситуация, когда угрозы связаны не с ограничениями спецификации протокола EtherNet/IP, а, скорее, с его реализацией. Эти проблемы часто проявляются, когда стек EtherNet/IP не организует должным образом проверку на изменённые фреймы.

Также существует заблуждение, что изменённые пакеты могут исходить только от злоумышленника, хакера и т.п., но это далеко не так. Например, некорректно спроектированный человеко-машинный интерфейс (HMI) может привести к логической ошибке типа «один за единицу» (off-by-one error) в поле длины EtherNet/IP. Это приведёт к тому, что процесс, который запущен на сервере или ПЛК, будет неправильно использовать длины полей данных. В итоге можно констатировать, что неправильная структура EtherNet/IP-фрейма также может нанести существенный вред.

Методы защиты EtherNet/IP

Проблемы безопасности промышленных протоколов, которые уже сейчас являются частью существующих стандартов и повсеместно используются, скорее всего, останутся в ближайшие 10–15 лет. В настоящее время ведутся обсуждения по добавлению новых функций безопасности в спецификации, но процесс внедрения, вероятно, растянется на многие годы. И даже ког-

да эти изменения в стандартах будут приняты, с учётом специфики внедрения обновлений на промышленных объектах обновления тех же самых ПЛК будут далеко не быстрыми. Ведь, как правило, срок эксплуатации ПЛК на производстве может составлять 10, 20 или более лет. И даже смена политик безопасности существующих протоколов в SCADA и ICS (Industrial Control System) не может быть обеспечена с помощью патчей, так как функциональность этих протоколов определяется в глобальных масштабах, требующих изменений самих стандартов.

Пройдёт ещё много лет до того, как будут широко использоваться более новые, более безопасные промышленные протоколы и устройства. Это оставляет миллионы существующих промышленных устройств управления открытыми для возможных атак. Если атакующий ПК или червь смогут получить доступ к системе АСУ ТП, то это может привести к тому, что промышленный протокол, в нашем случае EtherNet/IP, может быть использован для отключения или перепрограммирования большинства ПЛК.

Получается, что необходим метод защиты уже существующих промышленных протоколов, устройств и систем, независимо от будущих улучшений спецификаций. В IT-мире есть две основные технологии, обеспечивающие безопасность трафика в проводных сетях. Это шифрование и фильтрация пакетов. Если рассматривать EtherNet/IP на базе этих технологий, то получается следующая картина.

Шифрование данных и VPN

Более подробно о технологиях шифрования и VPN было написано в [4]. VPN обеспечивает три ключевые возможности:

- **конфиденциальность:** VPN-сервер шифрует данные, проходящие между двумя конечными точками;
- **аутентификация:** VPN-сервер аутентифицирует каждую конечную точку;
- **целостность:** VPN-соединения обеспечивают неизменность сообщений при передаче между отправителем и получателем.

Данный метод в целом является очень перспективными, но криптография в настоящее время страдает от ряда ограничений. Например, протокол EtherNet/IP является критичным по времени, и для каждого пакета, входящего в VPN-туннель, потребуются дополнительные вычислительные ресурсы для шифрования и дешифрования пакета. Для таких устройств, как ПЛК с ограниченными ресурсами центрального процессора, это может привести к значительным задержкам. Кроме того, VPN не обеспечивает проверку данных. Если авторизованный VPN-узел отправляет ложные данные в туннель, на другом конце туннеля эти данные появятся без изменений.

Существует мнение, что наиболее перспективным использованием криптографических технологий является аутентификация устройств, а не шифрование потока данных [3]. Но, к сожалению, вопросы, касающиеся надёжного управления ключами или сертификатами для управляющих устройств, таких как ПЛК, по-прежнему остаются открытой темой для исследований.

Глубокая инспекция пакетов (DPI)

Deep Packet Inspection (DPI) – это расширение традиционной технологии межсетевого экрана, которая может обеспечить аналитику и управление трафиком EtherNet/IP. Более подробно о базовых принципах DPI было написано в [1].

DPI позволяет брандмауэру углубляться в сообщение, чтобы точно понимать, для чего используется протокол.

Далее мы рассмотрим, как на основе технологии DPI можно анализировать структуру сообщений EtherNet/IP-пакетов и как это позволяет обеспечить безопасность сети.

Анализ протокола EtherNet/IP для использования DPI

Основная задача устройства, которое осуществляет DPI-анализ протокола, – это понять базис структуры протокола и правильно выявить ложные данные. Понимание структуры протокола важно для оценки характеристик каждого поля в сообщении и взаимодействия этих полей. Например, значение поля "Length" в сообщении EtherNet/IP в первом приближении не несёт никакой критичной информации. Но это поле задействовано при выполнении часто используемого сервиса Get Attribute All, который позволяет получить служебную информацию об объекте, например, текущее значение аналоговых выходных сигналов. Но что именно поле "Length" означает? Это минимум или максимум? Сигнализирует ли выход за пределы его значения о возможной атаке? Будет ли изменение этого параметра влиять на CIP-объекты или сервисы? Как это поле связано с другими полями? Это всё вопросы для проверки DPI.

Получается, что если в процессе DPI-анализа можно определить конкретный байт или поле, из-за которого возникла проблема, то есть большая вероятность, что удастся блокировать ошибочные значения полей данных, при этом сохранить легитимное управление. Однако для этого необходимо понимать структуру протокола, а также проводить подробный его анализ.

Структура заголовка EtherNet/IP

Структура заголовка EtherNet/IP имеет очень важное значение, так как содержит данные для дальнейшей инкапсуляции сообщений протокола CIP. Заголовок EtherNet/IP имеет фиксированную длину в 24 байта. Максимальный размер пакета, включая заголовок, составляет 65535 байт и представляет собой прямой порядок байтов (табл. 1).

Поле команды (Command) описывает действия, которые могут выполняться на этом уровне. Создание сеанса происходит по команде RegisterSession и может быть отменено с помощью команды UnregisterSession. Существуют также различные команды запросов, такие как ListInterfaces и ListIdentity. Эти команды предоставляют клиентскому программному обеспечению базовую информацию об устройстве, с которым он пытается связаться. Наиболее важными командами являются SendRRData и SendUnitData, которые включают значимые параметры для анализа CIP-данных. Сообщения CIP хранятся внутри EtherNet/IP-пакетов с командами SendRRData и SendUnitData. Поле Command является обязательным для DPI-анализа, оно позволяет ограничить круг коммуникаций и возможных путей связи.

Поле длины (Length) также очень важно, оно определяет общую ожидаемую длину пакета минус размер заголовка EtherNet/IP (24 байта по умолчанию). Таким образом, если фактический размер полезных данных пакета меньше или превышает указанную длину, возникает проблема с пакетом, и это один из признаков ошибочных данных.

Следующее за полем длины поле – дескриптор сессии (Session handle). Оно

уникально для сессии и, как правило, находится в ответе на команду RegisterSession, сгенерированную, например, из ПЛК. Этот дескриптор используется для всего сеанса связи.

Поле состояния (Status) используется получателем, чтобы указать, успешно ли выполнена запрошенная команда инкапсуляции (Encapsulation Message). Ноль обозначает успешную команду, значения выше нуля указывают на то, что произошла ошибка и данный пакет будет проигнорирован.

Поле контекста отправителя (Sender Context) заполняется отправителем и возвращается получателем без изменения. Во многих случаях команды без ожидаемого ответа просто игнорируют это поле.

Наконец, флаг опций (Options), если содержит ноль, то не используется, если его значение не равно нулю, пакет должен быть отброшен.

Поле данных команды (Command Specific Data) играет большую роль в формате инкапсулированного сообщения CIP. Этот раздел содержит фиксированную структуру, известную как общий формат пакета (Common Packet Format, CPF). Он содержит 16-битное поле, представляющее количество элементов для последующего просмотра. Элемент имеет два типа: адрес и данные. На практике первоначально указывается элемент адреса, после чего следует элемент данных.

Структура CIP-сообщений

Структура CIP-сообщения имеет несколько статичных полей, которые содержат набор CIP-сегментов, включая сегменты порта, логические сегменты, сегменты сети, символов, данных и ключевые сегменты (рис. 3). В дополнение к этому всегда существует сервис CIP, выполняющий некоторые действия над сегментом логического класса. В некоторых случаях сообщение CIP может быть объектом диспетчера соединений с использованием сервиса Forward Open для установления связи. В других случаях это может быть базовый CIP-сервис атрибута Get Attribute All.

На рис. 3 показаны поля сервиса Forward Open, которые инициируют создание сессии, а также предоставляют параметры сетевого подключения для двух обменивающихся устройств. CIP-сервис резервирует самый старший бит для обозначения того, является ли пакет запросом или ответом. Следующие 7 бит используются для указания типа CIP-сервиса. Один и тот же номер сер-

Таблица 1

Структура заголовка EtherNet/IP

Состав	Название поля	Тип данных
Заголовок для инкапсуляции	Команда	UINT
	Длина	UINT
	Дескриптор сессии	UINT
	Статус	UINT
	Контекст отправителя	ARRAY of Octet
	Флаг опций	UDINT
Данные команды	Инкапсулированные данные	ARRAY of Octet

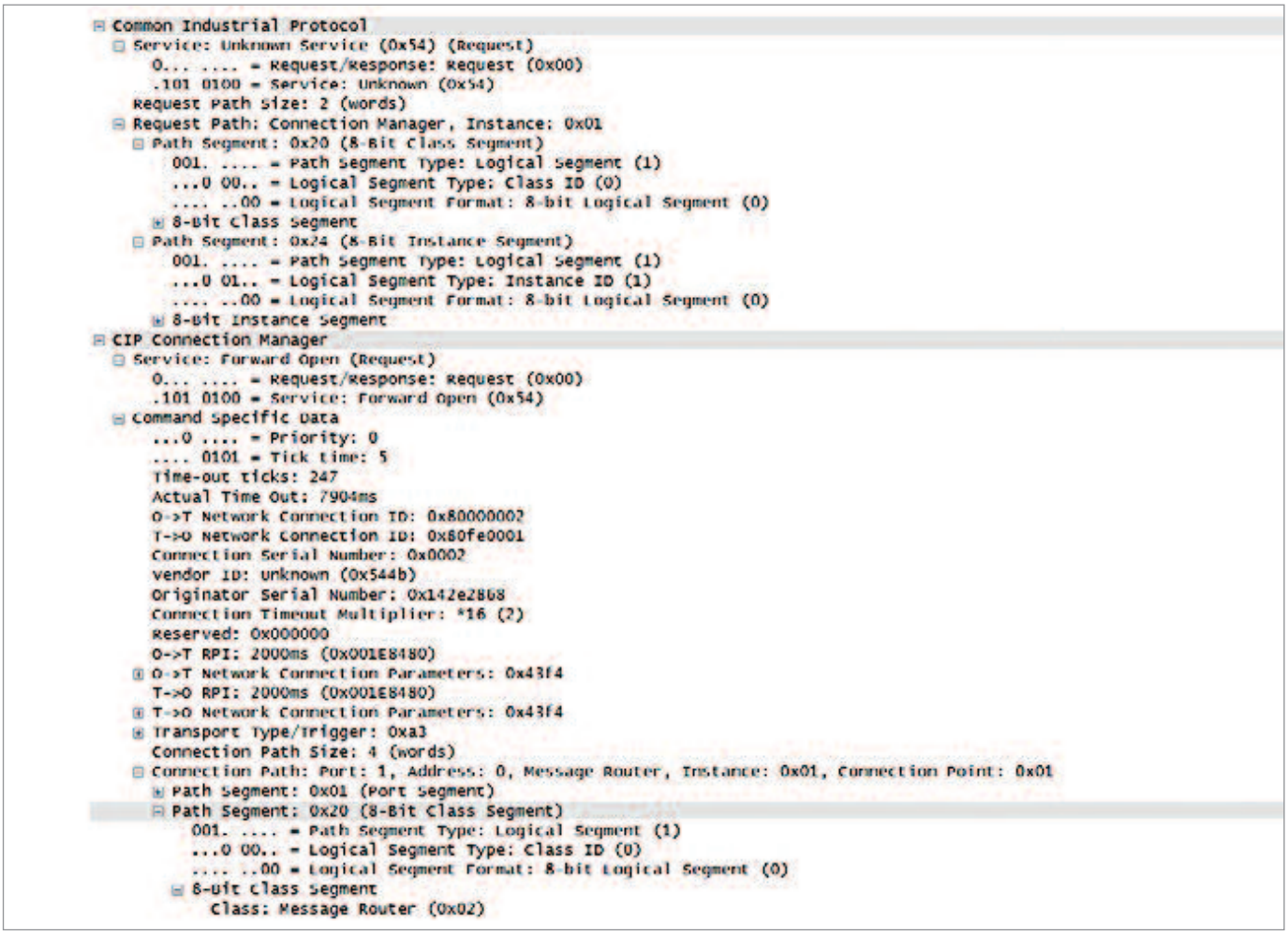

Рис. 3. Структура CIP-сообщения

виса может указывать на совершенно разные функции для разных объектов. Подобное повторное использование номеров сервисов усложняет принятие решений о фильтрации и представляет собой достаточно сложную задачу для реализации DPI для этого протокола.

Следующим за полем сервиса является размер пути запроса в словах (Connection Path Size). На рис. 3 значение равно 2, что означает 4 байта (2×2). Это поле содержит набор сегментов, которые в конечном счёте необходимо анализировать и фильтровать.

Но для реализации DPI основное поле, которое представляет интерес, – это класс логических объектов (Logical Object Class), причём наиболее важным является кодирование логического сегмента (Logical Segment). Логический сегмент представляет собой 8-битное поле с тремя старшими битами, обозначающими тип логического сегмента, в данном случае 001. Следующие 3 бита обозначают логический тип (рис. 4). Наконец, последние 2 бита используются для определения размера сегмента.

Также существует специальный тип CIP-сообщения, он называется пакетом с несколькими сервисами (Multiple Service Packet). В основном он используется для уменьшения задержки между запросами и обычно присутствует при запуске или завершении сессии. Этот тип сообщений позволяет таким устройствам, как HMI, встраивать ряд CIP-сообщений в один заголовок EtherNet/IP. Пакет Multiple Service действует на объект маршрутизатора сообщений (Message Router Object) и содержит список смещений, где начинается первый элемент CIP, затем второй и т.д. (рис. 5). В нём не указан максимальный размер списка смещений. Устройство, которое получает одно из этих сообщений, разбивает каждое инкапсулированное CIP-сообщение и отвечает по схеме «один ко многим». Передача больших наборов данных при помощи сообщений Multiple Service Packet может быть весьма продуктивна, с точки зрения экономии трафика, но в данных сообщениях существуют весьма значимые отличия от стандартного формата пакета. Эта особенность сказывается на DPI подобных пакетов, заставляя реализовывать дополнительный анализ.

Реализация DPI для EtherNet/IP

Как отмечалось ранее, архитектура уровней EtherNet/IP и CIP не является фиксированной и содержит много динамических составляющих. При создании сеанса используется набор команд с различными результатами и динамическими полями.

Для реализации эффективного механизма DPI необходимо обратить внимание на два ключевых фактора. Первым являются действия по проверке пакетов

	Logical Type		
Class ID	0	0	0
Instance ID	0	0	1
Member ID	0	1	0
Connection Point	0	1	1
Attribute ID	1	0	0
Special	1	0	1
Service ID	1	1	0
Extended Logical	1	1	1

	Logical Format		
8-bit logical value	0	0	
16-bit logical value	0	1	
32-bit logical value	1	0	
Reserved for future	1	1	

Рис. 4. Тип и формат CIP-сообщения

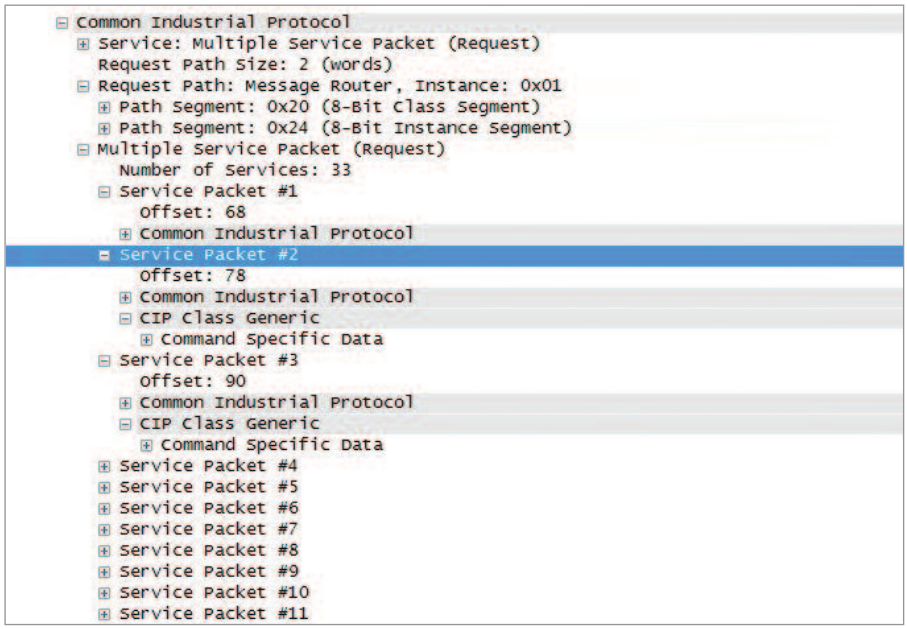

Рис. 5. CIP-пакет с несколькими сервисами (Multiple Service Packet)

относительно спецификации протокола. Это необходимо для обеспечения правильного отображения структуры и значений в пакете. Во-вторых, необходимо определить, какие поля или действия будут иметь значимый смысл, с точки зрения пользователя. Далее они будут определены как фильтруемые.

Начнём с проверки «правильности» пакета. Обычно подобные проверки могут существенно снизить атаки типа «отказ в обслуживании» (DoS). Результатом же подобной атаки может стать ПЛК, который просто не отвечает. Чтобы предотвратить подобную атаку, проверка должна выполняться в тандеме, как на уровне EtherNet/IP, так и на CIP. Эта проверка правильности также должна учитывать направленность пакетов для определения запросов и ответов, поскольку они различаются по формату. Как отмечалось ранее, есть бит, указывающий, запрос это или ответ, поэтому пакеты могут быть сопоставлены с адресами источника и получателя и TCP-портами. Пакеты также могут быть проверены на правильность длины, допустимые пути запроса с использованием сегментов данных, действительность CIP-сервисов и т.д.

С точки зрения пользователя, подобная проверка должна быть реализована отдельно от оконечного устройства, например, на отдельном брандмауэре. При этом такая проверка работоспособности протокола должна быть опциональной, потому что в некоторых случаях поставщик оборудования может не полностью придерживаться официальной спецификации.

Следующая область для фильтрации – это те поля, которые могут быть определены пользователем. Поскольку CIP – это объектно-ориентированная система с различными сервисами, действующими на объекты, имеет смысл фильтровать поля, которые обозначают, какой объект и сервис вызываются. Пользователь всегда может указать объекты и сервисы, которые безопасны для брандмауэра, и блокировать все остальные. Например, чтобы предотвратить изменение злоумышленником параметров CIP-объекта, пользователь может удалить этот объект из своего «белого» списка разрешённых объектов и сервисов. Затем DPI-брандмауэр должен идентифицировать этот объект в пакете и сравнить его с разрешённым списком. Если сервис или CIP-объект явно не разрешены, брандмауэр заблокирует этот пакет.

Спецификация ODVA описывает набор общих сервисов и необязательных объектов, которые могут быть привязаны к объекту. Она также позволяет поставщику группировать определённые сервисы. Эта группировка даёт возможность реализовать список фильтров только для чтения или для чтения-записи. В качестве примера можно группировать все атрибуты Set {Single, All} для команд записи, тогда как атрибуты Get Attribute {Single, All} можно сгруппировать для команд только для чтения.

Ситуация становится более сложной при просмотре конкретных объектов. Если мы снова посмотрим CIP-сервис 0×54 Forward Open, привязанный к конкретному объекту CIP, то точно такое же

значение 0×54 на другом объекте может означать сервис Write Set Value.

Это означает, что недостаточно группировать сервисы CIP в целом, необходимо объединить CIP-сервисы и их связанные объекты вместе, чтобы разработать абстрактную группу функций. Преимущество создания подобной группы объектов и сервисов заключается в том, что пользователю предоставляется эффективный способ защиты потока передачи данных EtherNet/IP.

Если объединить подобную фильтрацию по объектам и сервисам вместе с проверкой протокола по спецификации, то получится мощный инструмент по обеспечению безопасности протокола. А если развить идею объединения объектов и сервисов, то этот список фильтрации может быть формируемым пользователем. Например, для конкретного процесса может иметь смысл разрешить функцию только для чтения на объекте TCP/IP, но разрешить возможность чтения и записи на объектах аналогового вывода. Эта гибкость позволит пользователю настраивать фильтрацию систем на основе пары клиент/сервер.

Tofino EtherNet/IP Enforcer LSM

Чтобы разобраться в тонкостях промышленных протоколов, необходимы достаточно глубокие знания. Зачастую у специалистов, которые эксплуатируют готовую систему АСУ ТП, нет информации, какие конкретные объекты или сервисы использует их система. Для облегчения данной задачи должно быть средство, которое позволит создать правила фильтрации простым и удобным способом.

Одно из таких средств – промышленный брандмауэр Tofino Xenon с установленными модулями глубокого анализа трафика. Более подробно о брандмауэре Tofino Xenon рассказано в [1]. За анализ трафика EtherNet/IP отвечает модуль Tofino EtherNet/IP Enforcer LSM, который позволяет достаточно просто настроить правила его фильтрации. Рассмотрим его более подробно.

Пользователю доступен графический интерфейс (рис. 6), который предназначен для создания требуемой конфигурации брандмауэра. При этом начальной точкой конфигурации становится создание стандартных IT-правил на базе списков доступа. Затем пользователь может указать те правила, где необходимо, чтобы брандмауэр выполнял более глубокий анализ. Таким образом, можно управлять как правилами DPI, так и стандартными IT-правилами.

На рис. 6 показан набор правил. В этом примере HMI физически расположен в сети Supervisory (подключён к одному интерфейсу брандмауэра), тогда как ПЛК размещён в сети управления (подключён к другому интерфейсу брандмауэра). Поскольку пакеты проходят через интерфейсы на брандмауэре, устройство проверяет пакеты по тем правилам, которые были обозначены. Также следует обратить внимание на то, что в дополнение к правилу EtherNet/IP существуют правила для трафика, проходящего между двумя устройствами, например, для того чтобы разрешить другие протоколы, такие как FTP и HTTP.

Но одно поле, которое может потребовать дополнительного объяснения, – это поле “Direction”. Как известно, SPI-брандмауэр [1] пропускает через устройство пакеты, предназначенные для установленной сессии соединения. Эта же функциональность присутствует в устройстве Tofino Xenon, что позволяет пользователю явно указать, какие устройства задействованы в соединениях и в каком направлении можно установить соединения, не требуя указания дополнительных правил для ответов.

Выделенное правило на рис. 6 – это то, что соответствует трафику EtherNet/IP, исходящему из HMI и входящему в ПЛК. В данном случае брандмауэр автоматически разрешает ответы от ПЛК на HMI без каких-либо дополнительных правил.

Применяя функциональность DPI со встроенным редактором, пользователь получает дополнительные преимущества. К ним относится возможность создания своих правил для протокола EtherNet/IP. Настройки реализуются в своём редакторе ACL (Access Control List – список управления доступом) и требуют просто добавления дополнительной конфигурации к уже существующим правилам.

На рис. 6 показан редактор DPI-правила для EtherNet/IP, выбранного ранее. Редактор автоматически предоставляет пользователю все параметры для выбранного правила. Основные параметры, связанные с функциональностью DPI для этого правила, отображаются в правой части этого редактора. Например, здесь отображена опция “Sanity Check” которая как раз и позволяет проверить трафик на правильность по стандартизованной спецификации. В левой части редактора представлен интерфейс для настройки правил, связанных с протоколом CIP. Редактор позволяет создавать правила на основе сервисов и объектов CIP (рис. 7).

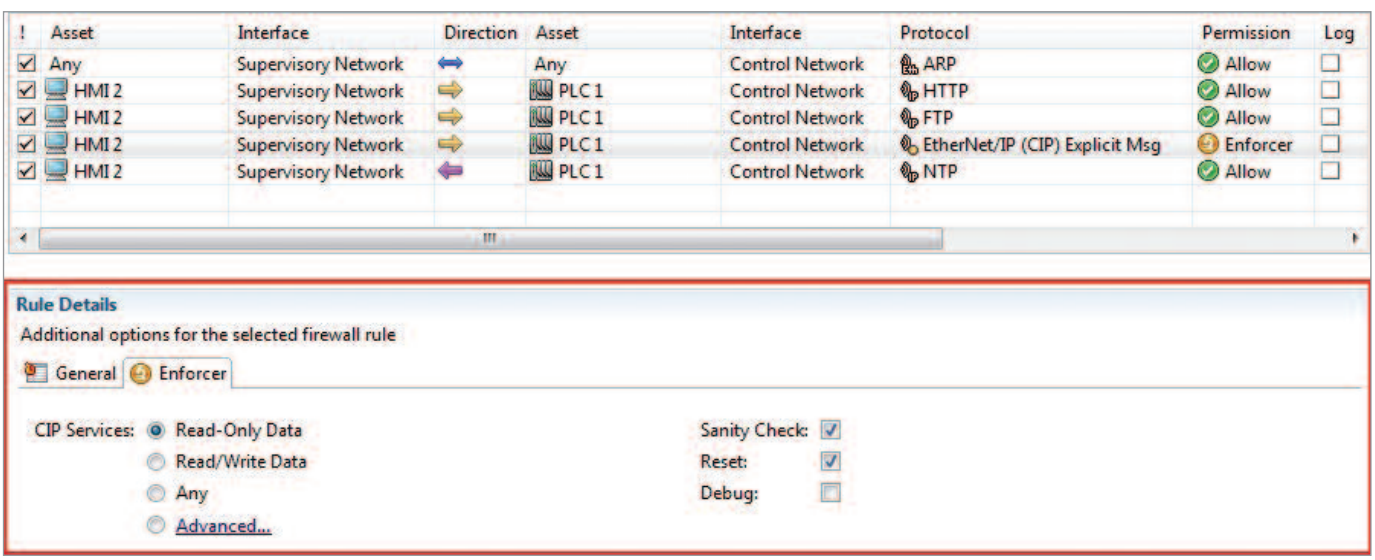

Рис. 6. Настройка DPI-фильтра для протокола EtherNet/IP

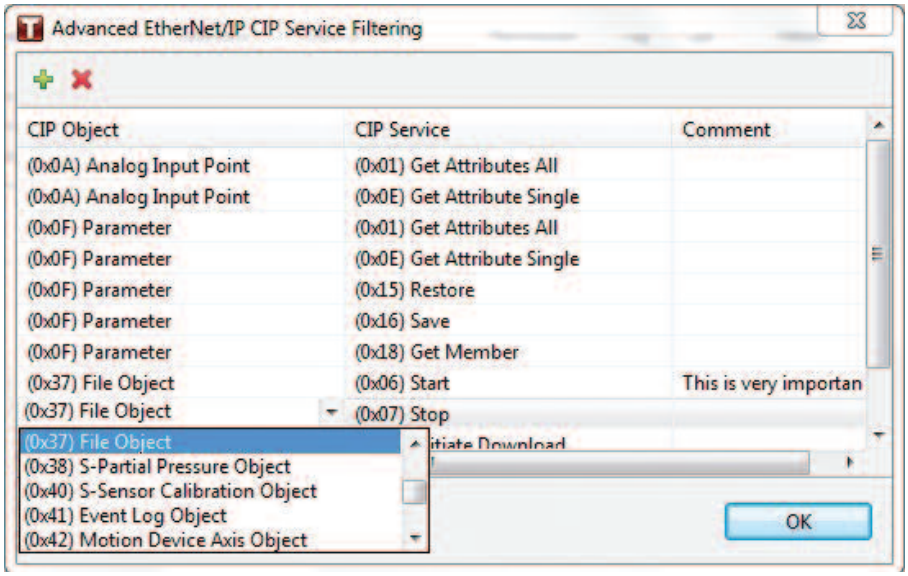

Рис. 7. Настройка расширенных параметров фильтрации DPI-фильтра для протокола EtherNet/IP

Для выбора правил CIP-объектов и связанных с ними сервисов также используется перечень стандартных объектов и сервисов CIP. При этом пользователь не ограничен предопределённым списком. Предоставляется возможность выбора произвольного идентификатора класса, а также сервисных кодов, не найденных в стандартной библиотеке конфигурации.

Заключение

Глубокая проверка данных (DPI) промышленных протоколов является очень эффективным методом защиты устройств, которые работают на базе промышленных протоколов. Но чтобы реализовать данную проверку, необходимы фундаментальные знания организации протокола. EtherNet/IP – это один из популярнейших промышленных протоколов, который позволяет привести промышленную сеть к объектно-ориентированной модели, что существенно увеличивает возможности управления. Но этот протокол также имеет ряд уязвимостей, которые появились из-за того, что он изначально не учитывал задачи обеспечения безопасности.

Одним из устройств, которые позволят обеспечить защиту протокола, является промышленный брандмауэр Tofino Xenon с установленным модулем Tofino EtherNet/IP Enforcer LSM, позволяющим не только проверить трафик на соответствие спецификации, но и настроить правила доступа для конкретных объектов и сервисов. ●

Литература

1. Воробьёв С. “Defense in Depth” в действии. Уровень 4: защита промышленных протоколов. Часть 1 // Современные технологии автоматизации. – 2018. – № 3.
2. EtherNet/IP Quick Start for Vendors Handbook [Электронный ресурс] // Режим доступа : https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00213R0_EtherNetIP_Developers_Guide.pdf.
3. Byres E., Schweigert E., Thomas M. Securing EtherNet/IP Control Systems using Deep Packet Inspection Firewall Technology [Электронный ресурс] // Режим доступа : https://www.odva.org/Portals/0/Library/Annual_Meeting_2014/2014_ODVA_Conference_Byres_Schweigert_Thomas_Securing_EtherNetIP_with_DPI_FINAL.pdf.
4. Воробьёв С. “Defense in Depth” в действии. Уровень 1: защита границы сети // Современные технологии автоматизации. – 2017. – № 4.

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Инновационные решения были представлены на «ПТА – Санкт-Петербург 2018»

5-6 июня в Северной столице состоялось традиционно значимое событие – XI Специализированная выставка-форум «Передовые Технологии Автоматизации. ПТА – Санкт-Петербург 2018». В этом году для его проведения была выбрана новая площадка – конгресс-центр «ЛЕНПОЛИГРАФМАШ».

В рамках деловой программы форума были представлены инновационные решения и компоненты для автоматизации зданий и создания цифрового производства будущего.

С экспертными докладами и презентациями выступили ведущие разработчики и производители оборудования и программного обеспечения: SIEMENS, Kawasaki Robotics, OMRON, JUNG, Embedded Systems, INTELVISION, ИНСАТ, B.E.G., BOLID, B&R, ПРОСОФТ, ADLINK Technology, Hirschmann, EtherWAN и другие.

В выставочной зоне оба дня работы форума была представлена экспозиция интеллектуальных систем и компонентов. Высокая посещаемость мероприятия подтвердила актуальность обсуждаемых на форуме вопросов в Северо-Западном регионе. ●