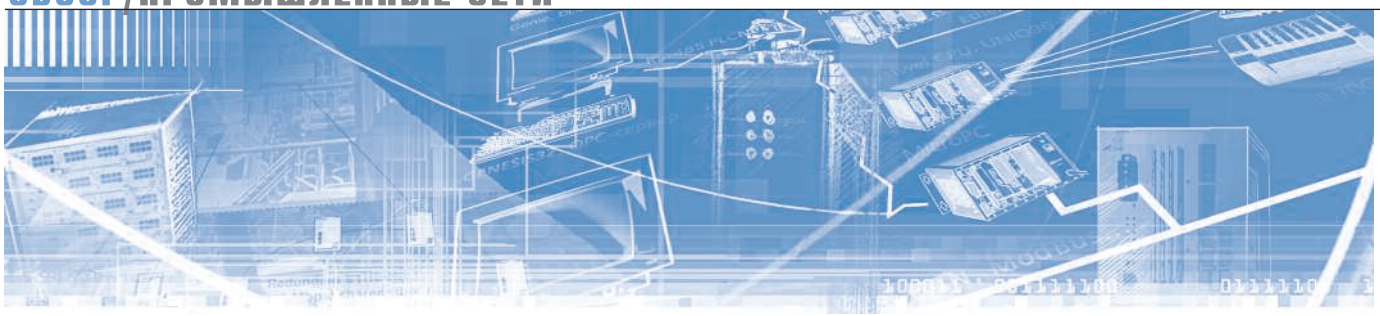


Сергей Воробьёв

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

Часть 3

Данный материал служит продолжением цикла статей, посвящённых многоуровневой защите промышленных Ethernet-сетей на базе принципа “Defense in Depth”. В статье рассмотрены ряд базовых уязвимостей промышленных протоколов IEC 104, GOOSE и DNP3, а также методы их защиты на базе глубокой инспекции трафика.

Введение

С каждым годом растёт опасность кибератак на объекты энергетической инфраструктуры. Современные АЭС, ТЭЦ, электрические подстанции, оснащённые сложными электронными системами, всё чаще становятся объектами внимания киберзлоумышленников. Таких случаев в мире, к сожалению, уже немало [1]. Последствия, к которым приводят подобные инциденты, могут быть самыми разными, начиная от банального воровства, заканчивая вмешательством в технологические процессы и функциональность объектов. При этом в условиях внедрения новых концепций и подходов, таких как Smart Grid и IIoT (Industrial Internet of Things), комплексная защита сетевой инфраструктуры промышленного объекта становится очень актуальной задачей.

В данной части статьи рассмотрим уязвимости протоколов IEC 104, GOOSE и DNP3, которые используются в энергетике для организации информационного обмена между различными системами, а также обеспечение их защиты при помощи промышленного DPI-брандмауэра Tofino Xenon.

IEC 104

IEC 104 (IEC 60870-5-104/МЭК 60870-5-104) – современный и гибкий протокол связи, который используется преимущественно в энергетике и является одним из международных стандартов

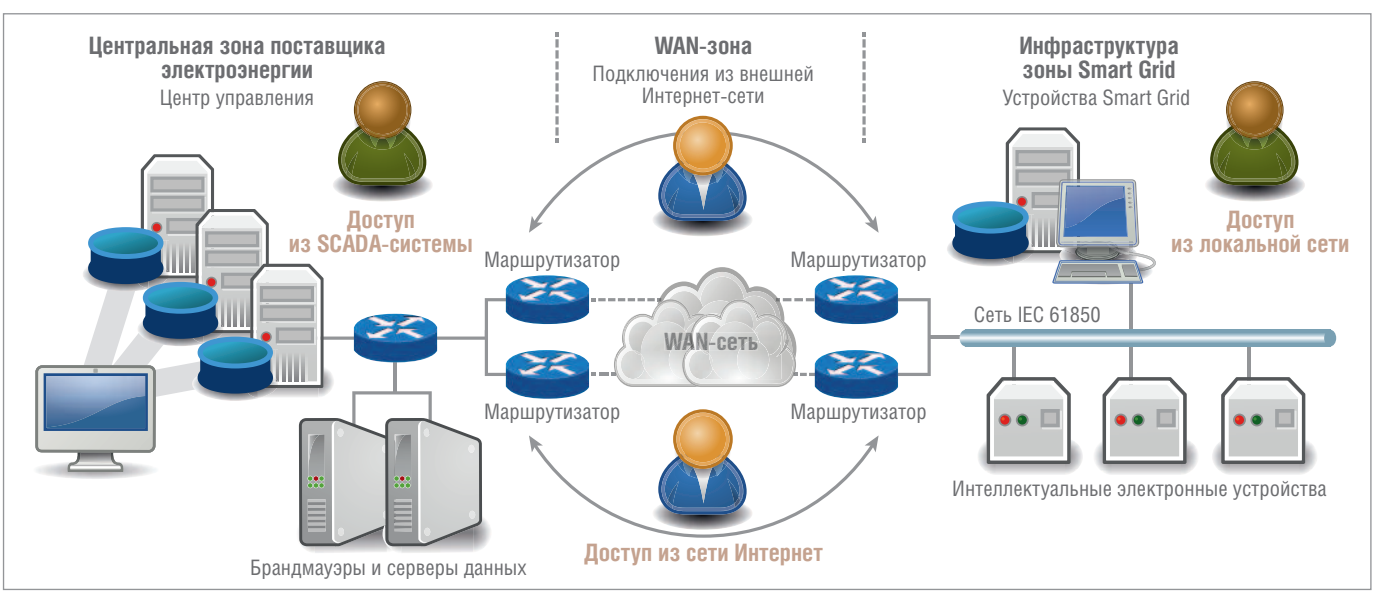


Рис. 1. Пример сетевой архитектуры подстанции

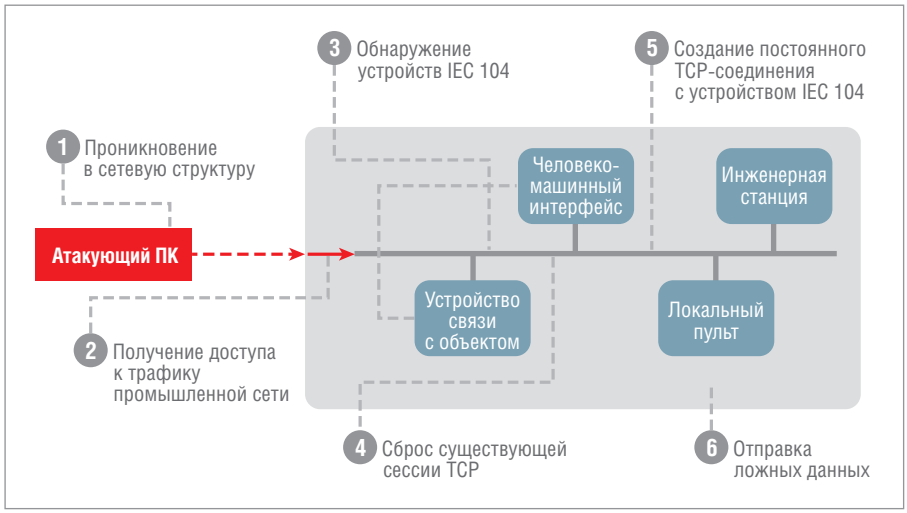


Рис. 2. Пример атаки на протокол IEC 104

IEC 60870. Он предназначен для информационного обмена между энергосистемами, а также для получения данных от измерительных преобразователей. Протокол определяет профиль связи для отправки базовых сообщений телемеханики между двумя системами через сеть, работающую на базе стека протоколов TCP/IP, что позволяет одновременно передавать данные между несколькими устройствами и службами (рис. 1).

В ряде документов было описано, что организация безопасности IEC 104 является проблематичной [2, 3], так как в протоколе довольно много слабых сторон, связанных с отсутствием шифрования данных и недостаточной проверкой подлинности. Фактически, имея доступ к сети, можно захватывать и передавать ложные данные. Проблемы безопасности протокола связи IEC 104 можно определить следующим образом:

- отсутствие поля контрольной суммы;
- отсутствие встроенных механизмов безопасности на канальном уровне и уровне приложений;
- отсутствие возможности увеличения длины пакета – протокол IEC 104 подразумевает передачу только 255 байтов информации в любой момент времени, это косвенно ограничивает количество битов, которые могут быть использованы для реализации функций безопасности во время передачи данных.

Не так давно IEC (Международная электротехническая комиссия) опубликовала стандарт безопасности IEC 62351, который описывает меры по защите серии протоколов IEC 61850. В их числе описаны методы для аутентификации и шифрования, которые направлены на увеличение уровня защищённости протокола от возможных кибератак, таких как «человек посередине», инжекция трафика и т.п. Но, к сожалению, меры, которые описаны в IEC 62351, являются сложнореализуемыми и достаточно редко внедряются, особенно на уже существующих объектах.

Уязвимости протокола IEC 104

Многие промышленные протоколы, включая IEC 104, не имеют механизма аутентификации, а также у них отсутствует механизм шифрования. Это потенциально добавляет возможность изменять данные в пакетах со служебной информацией.

На рис. 2 показан сценарий атаки, в результате которой атакующий ПК может вклиниться в поток данных и изменить значимые параметры. Если разбить подобный сценарий на этапы, то получается следующая последовательность:

Этап 1 – проникновение в сетевую структуру. Этот шаг может быть осуществлён как изнутри сети, так и из-за её пределов. Фактически это сбор информации о сети путём использования таких методов, как разведка (Foot printing), сканирование и т.д. Для противодействия подобной деятельности необходимо правильно сконфигурировать средства защиты на границе сети [4]. Например, не отключённый порт в Ethernet-коммутаторе – это типичная возможность проникнуть в сетевую структуру.

Этап 2 – получение доступа к трафику промышленной сети. Основной целью этого этапа является получение доступа к контролю служебного трафика. Это может быть реализовано путём проведения атак канального уровня, например, «человек посередине» или отравление ARP-кэша. Более подробно описано в [5].

Этап 3 – обнаружение устройств IEC 104. Основная цель данного этапа – это обнаружение подключённых устройств, которые работают по протоколу IEC 104. Это можно сделать одним из двух способов – пассивным или активным. Пассивный подразумевает прослушивание и анализ всех полученных пакетов. Активное обнаружение – это отправка как целенаправленных запросов, так и сканирование сетевого пространства на предмет наличия устройств, работающих с протоколом IEC 104.

Этап 4 – сброс существующей сессии TCP. IEC 104 создан специально для работы по стеку протоколов TCP/IP. TCP-соединения используются для всех коммуникаций протокола IEC 104. Одновременно к главной контролирующей станции, мастер-устройству, могут подключаться несколько подчинённых устройств, но для передачи данных может использоваться только одно активное соединение. Для внедрения ложной команды в существующее соединение необходимо, чтобы действующее TCP-соединение было прервано. В дальнейшем атакующий ПК должен создать постоянное TCP-соединение.

Этап 5 – создание постоянного TCP-соединения с устройством IEC 104. Для отправки данных необходимо обеспечение непрерывного соединения с целевым устройством. В противном случае данные будут отклонены принимающей стороной, так как порядок передачи данных будет нарушен.

Этап 6 – отправка ложных данных. На этом этапе целевое атакуемое устройство уже известно, как и пул адресов контрольных точек. Фактически необходимо создать корректное сообщение IEC 104.

Также стоит упомянуть, что отправленная команда IEC 104 обычно генерирует несколько ответных сообщений. Например, если мастер-устройству потребуется совершить модификацию на одном из оконечных устройств, то для этого необходимо отправить адресату сообщение типа «управляющая команда». Принимающая сторона должна ответить на это сообщение. Далее происходит генерация и отправка нескольких ответных сообщений в процессе и после выполнения команд. С первого приближения может показаться, что данный сценарий является достаточно сложным для реализации. Но в сети

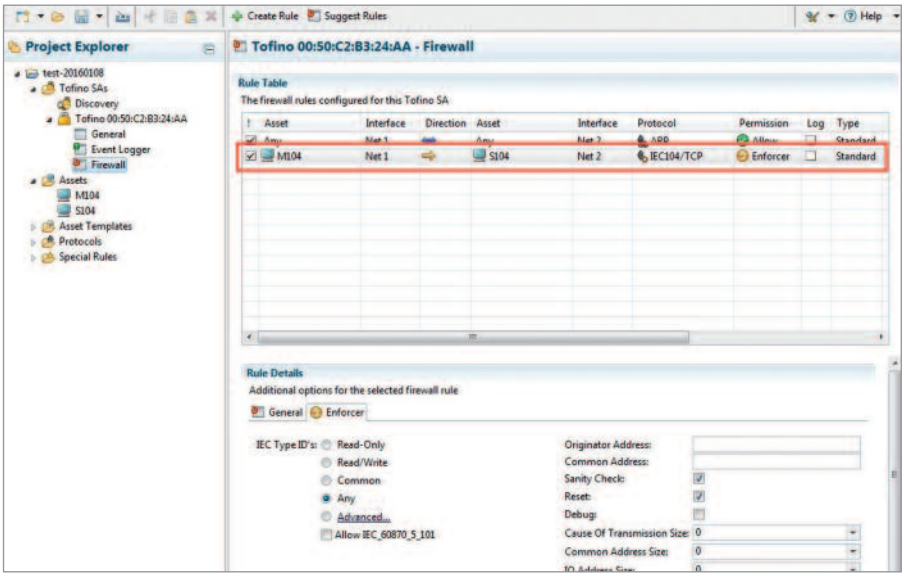


Рис. 3. Настройка DPI-фильтра для протокола IEC 104

Internet уже опубликовано достаточно много исследований и примеров различных сценариев атак на протокол IEC 104 [2].

Отсутствие механизмов защиты протокола IEC 104 от атак различных уровней может привести к тому, что критически важные инфраструктурные объекты и системы могут столкнуться с достаточно серьёзными угрозами кибератак.

IEC 104 Enforcer LSM

Модуль IEC 104 Enforcer LSM является дополнительным загружаемым модулем в устройство Tofino Xenon и предназначен для глубокой инспекции трафика (DPI – Deep Packet Inspection) протокола IEC 60870-5-104. Как было обозначено ранее, протокол IEC 104 не обладает достаточным уровнем защиты, механизмы аутентификации и шифрования отсутствуют, в связи с чем подход с глубокой аналитикой трафика и настройкой комплексных фильтров – это один из методов, который позволит существенно повысить уровень безопасности.

На рис. 3 представлен графический интерфейс среды Tofino Configurator модуля IEC 104 Enforcer LSM. Помимо точного задания адресатов путём указания связки MAC/IP-адрес пользователю доступны следующие настройки DPI-фильтра:

- Type ID определяет допустимые идентификаторы ID для входящего трафика протокола IEC 104; возможно создание различных типов групп: Read Only, Read/Write, Common и т.д.;
- Ordinator Address – перечень устройств, которые могут отправлять пакеты;
- Common Address – перечень устройств, которые принимают пакеты;
- Sanity Check – проверка трафика на полное соответствие спецификации;
- Reset – отправка сообщения TCP-reset в случае, если пакет не был пропущен.

Настроив фильтр при помощи данных параметров, можно существенно снизить риск возникновения нештатной ситуации для различных оконечных устройств.

GOOSE

GOOSE (Generic Object-Oriented Substation Event) является также протоколом, который особенно востребован в энергетике, в частности, на подстанциях. Как и IEC 104, он является стандартом МЭК 61850 и описан в главе МЭК 61850-8-1. Фактически это надёжный сервис, предназначенный для обмена сигналами между устройствами релейной защиты и автоматики (РЗА).

Архитектура современных систем РЗА построена с применением центральной шины процесса – Process Bus (рис. 4), которая обеспечивает коммутационную связь устройств, входящих в состав системы РЗА [6].

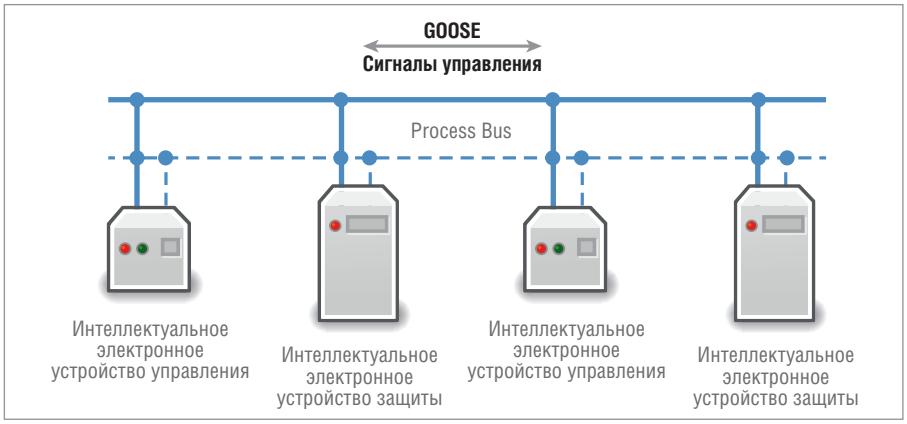
Как и все описанные ранее протоколы, GOOSE использует в качестве транспорта Ethernet-сеть. При этом GOOSE-протокол использует механизм многоадресных сетевых рассылок на канальном уровне модели OSI и служит для передачи данных реального времени.

Передача информации GOOSE-сообщениями реального времени накладывает жёсткие ограничения на время доставки пакетов (до 4 мс).

В качестве устройств коммутации трафика применяются промышленные Ethernet-коммутаторы, которые адаптированы к передаче больших по объёму GOOSE-сообщений. Как правило, если коммутатор имеет сертификацию IEC 61850, то приоритет передачи GOOSE-сообщений установлен на максимальный уровень по умолчанию. При этом никакой аутентификации и шифрования в базовой реализации GOOSE-протокола не предусмотрено. Имея доступ к шине процесса, можно передать любую ложную информацию.

Но в отличие от многих других протоколов ситуация с GOOSE не такая плачевная: в стандарте МЭК 62351 «Защита информации и данных» 6-я глава которого посвящена безопасности профилей обмена данными МЭК 61850 (GOOSE), описано использование цифровой подписи, которая подтверждает целостность данных и однозначно определяет отправителя сообщения. Согласно МЭК 62361 цифровая подпись формируется по RSA-алгоритму и применяется не ко всему сообщению, а к его хэш-сумме, вычисленной по алгоритму SHA-256 [6].

Но если проанализировать, какие задержки будет вносить данная реализа-



Условное обозначение: Process Bus – центральная шина процесса.

Рис. 4. Пример использования протокола GOOSE

SEZAM

ТАМ, ГДЕ ИБП БЕССИЛЬНЫ

Сетевой защитный модуль SEZAM

Параметры

- вход 220, 380 В
- мощность 3, 5, 10, 15 кВт
- рассеиваемая энергия импульсов перенапряжения до 20 кДж

Защита от

- повышенного напряжения
- импульсов от 4,5 до 10 кВ и разрядов молнии
- последствий обрыва нулевого провода
- преднамеренных электромагнитных воздействий

ProSoft®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU

ция, то можно констатировать, что будет теряться весь смысл идеологии протокола: время доставки существенно возрастёт, особенно при программной реализации.

GOOSE Enforcer LSM

GOOSE Enforcer – это очередной загружаемый модуль, который предназначен для инспекции GOOSE-трафика в реальном времени. Скорость работы достигает 2000 пакетов в секунду. При этом Tofino Xenon с установленным модулем поддерживает возможность работы в сети с несколькими ведущими и ведомыми устройствами.

По умолчанию любой пакет GOOSE с MAC-адресом назначения, не входящим в диапазон широковещательной или многоадресной рассылки, автоматически блокируется с последующим информированием. Также все GOOSE-пакеты с исходным MAC-адресом, который не находится в списке разрешённых, автоматически блокируются.

Для каждого настраиваемого соединения могут быть установлены следующие параметры DPI-фильтра:

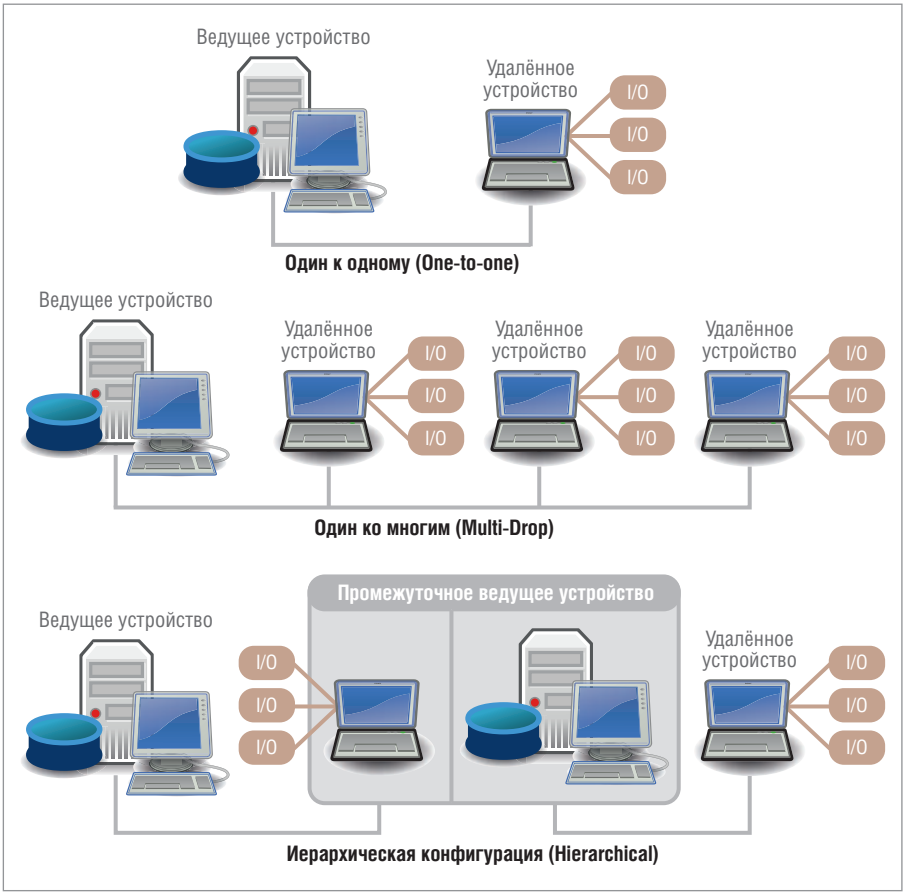
- проверка правильности протокола на предмет соответствия стандарту МЭК 61850-8-1;
- первичная проверка пакета данных на предмет наличия отправителя;
- проверка последовательности пакетов с одинаковым ID.

Настроив необходимые правила, можно обеспечить защиту протокола, временны́е задержки при этом будут в рамках штатной работы протокола.

DNP3

Протокол DNP3 был разработан компанией Westronic, Inc. (сейчас GE Harris) ещё в начале 1990-х годов. На данный момент протокол также является достаточно популярным в сфере электроэнергетики и в нефтегазовой промышленности. Фактически протокол определяет правила, по которым промышленные устройства общаются между собой. DNP3 – это удобный инструмент передачи данных из одной точки в другую, для обмена данными команд и процессов. Более подробно о протоколе написано в [7].

С точки зрения организации взаимодействия между устройствами, в спецификации протокола DNP3 описана поддержка трёх режимов связи между ведущим устройством (Master Unit) и удалёнными устройствами (Outstation Devices) [8].



Условное обозначение: I/O – модули ввода-вывода.

Рис. 5. Базовые сетевые конфигурации протокола DNP3

Первый режим – это одноадресная транзакция, когда ведущее устройство отправляет сообщение с запросом на удалённое устройство с конкретным адресом. Например, ведущее устройство отправляет запрос на считывание величины силы тока или управляющее сообщение на переключение реле. Удалённое устройство, в свою очередь, отправляет ответ.

Следующий режим взаимодействия – это широковещательные запросы, когда ведущее устройство отправляет сообщение всем удалённым устройствам в сети, например, сообщение Write, которое сбрасывает показания всех датчиков силы тока. Устройства Outstation не отвечают на широковещательные запросы.

Третий режим связи – это незапрашиваемые ответы от удалённых устройств. Подобные ответы обычно используются для предоставления периодических обновлений или предупреждений.

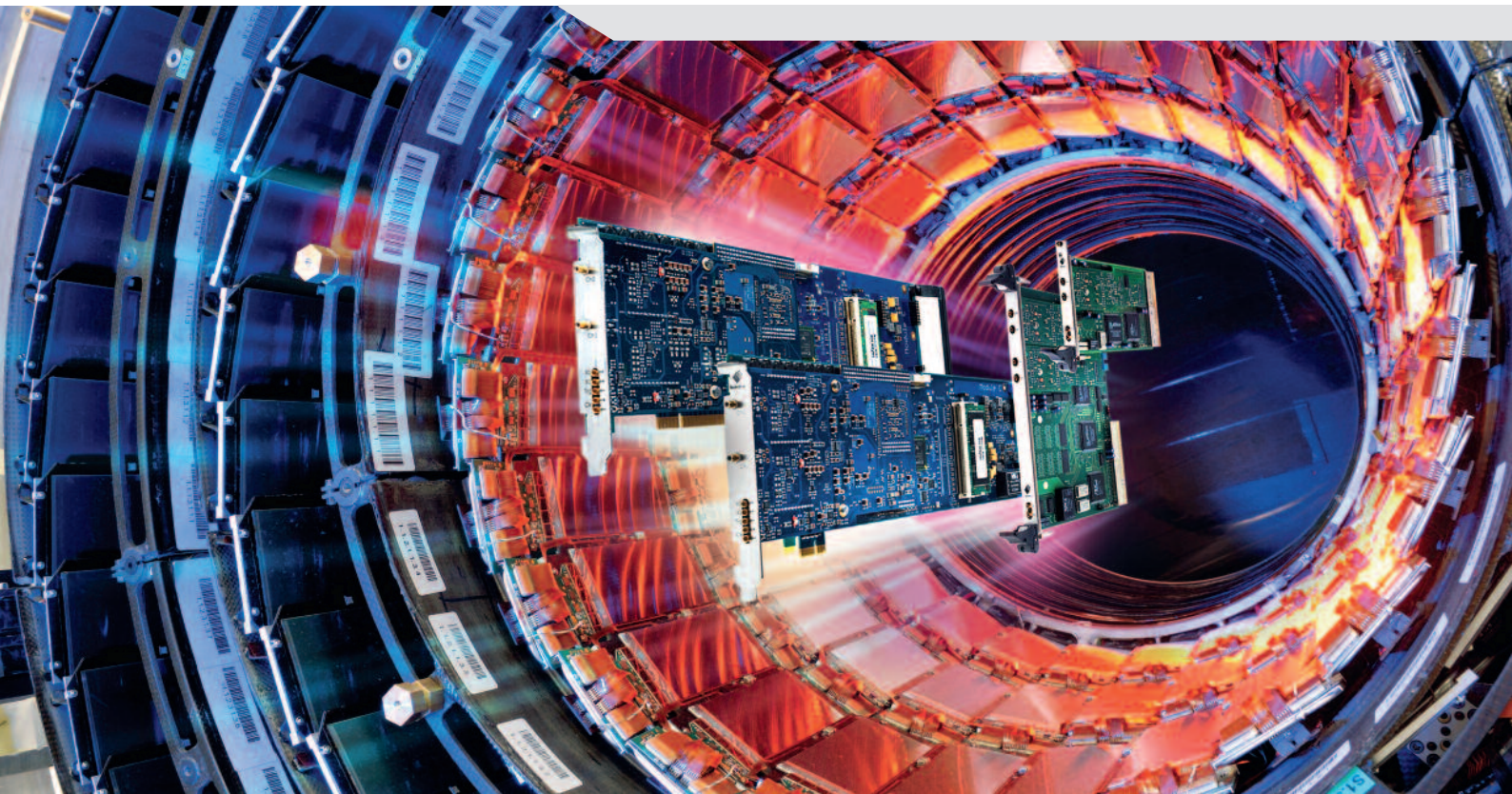
Обозначенные режимы позволяют, с одной стороны, построить гибкую структуру обмена информацией, но с другой стороны, добавить «прозрачности» в обмен данных, ведь изначально такие инструменты, как авторизация и аутентификация, также не были определены для протокола.

Протокол DNP3 поддерживает множество сетевых конфигураций. Три общих конфигурации показаны на рис. 5. В конфигурации «один к одному» ведущее и удалённое устройства совместно используют выделенное соединение. Конфигурация «один ко многим» строится по схеме, когда одно ведущее устройство обменивается данными с несколькими удалёнными устройствами. Каждое из удалённых устройств получает все запросы от ведущего устройства, но отвечает только на сообщения, адресованные непосредственно ему. Также протоколом предусмотрена иерархическая конфигурация, когда устройство действует как удалённое в одном сегменте и ведущее в другом сегменте.

Сетевое взаимодействие строится из нескольких уровней, которые позволяют обеспечить гибкость и контролировать не только значимые данные, но и состояние соединения и потока данных. При создании протокола DNP3 в качестве основы была взята модель OSI, но с учётом специфики было выделено три значимых уровня, не включая физический. Это канальный уровень (Data

SPECTRUM

Высокоскоростные инструментальные платы Spectrum



Для широкого спектра решений по сбору данных и генерации сигналов

PCI/PCI-X и PCI Express

- Свыше 200 моделей плат
- До 16 синхронных каналов
- Разрешение от 8 до 16 бит
- Частота опроса до 1 ГГц
- Встроенная память до 4 Гбайт
- Тактирование и многомодульная синхронизация

6U CompactPCI

- Около 80 вариантов модулей
- До 16 каналов
- Разрешение до 16 бит
- Частота опроса до 500 МГц

3U PXI

- Более 45 моделей
- Соответствие стандарту PXI
- Межмодульная синхронизация
- Тактирование 10 МГц
- Память до 512 Мбайт

Программное обеспечение

- Собственное ПО SBench 6
- Поддержка ОС Windows, Linux
- Разработка систем сбора и записи данных по ТЗ заказчика
- Индивидуальное консультирование по выбору оборудования для конкретных применений

LXI-системы сбора сигналов

- Более 60 моделей
- Соответствие стандарту LXI
- Число каналов 2–48
- Частота опроса до 500 МГц
- Разрешение от 8 до 16 бит
- Полоса частот от 100 кГц до 250 МГц

Link), псевдотранспортный (Pseudo-Transport) и прикладной (Application).

Канальный уровень фактически отвечает за адресацию между узлами DNP3 и обнаружение ошибок, псевдотранспортный предназначен для разбиения данных на фрагменты и последующей их сборки, и, наконец, прикладной уровень определяет набор типов данных и операций, посредством которых обеспечивается взаимодействие.

Протокол DNP3 может передаваться по различным физическим средам, включая последовательные интерфейсы. Однако современные устройства и SCADA-системы обычно используют DNP3 в промышленных Ethernet-сетях. Реализация подобного подхода получила негласное наименование DNP3/TCP. Однако при её реализации фактически никак не была затронута модель трёхуровневого сетевого взаимодействия.

Другими словами, три уровня DNP3 размещаются непосредственно поверх стека протоколов TCP/IP [8]. Из этого следует, что уязвимости протокола DNP3 распространяются на любые «транспортные» реализации, будь то это Ethernet, либо RS-485, а вариант DNP3/TCP подвержен ещё и уязвимостям канального уровня [5].

Уязвимость протокола DNP3

В целом уязвимости, которые могут касаться DNP3-протокола, можно разделить на три категории:

- уязвимости, которые присутствуют в спецификации;
- уязвимости, которые присутствуют непосредственно в устройствах;
- уязвимости, которые используют недостатки базовой сетевой инфраструктуры.

Уязвимости устройств, как правило, проявляются при ошибках конфигурации и программирования, например, переполнение буфера. Уязвимости сетевой инфраструктуры связаны, скорее, со слабыми политиками общей сетевой инфраструктуры безопасности.

Но самые сложные для идентификации и контроля – это уязвимости, которые присущи спецификации протокола.

DNP3 был разработан без учёта вопросов безопасности. Он подвержен ряду классических угроз, начиная от прослушивания и спуфинга данных, заканчивая модификацией и созданием перебоев в передаче информации. Например, атака типа Reset Data может привести не только к повторной инициализации данных в удалённом Outstation-устройстве до значений, не совместимых с состоянием системы, но и повлиять на работу других устройств.

Но всё-таки большинство атак на протокол DNP3 основывается на способности перехватывать, изменять и/или создавать ложные DNP3-сообщения. Ведь реализация обмена по DNP3 на базе спецификации, как правило, не предполагает таких операций, как шифрование, аутентификация и авторизация. Оконечные устройства, работающие с протоколом DNP3, просто предполагают, что все сообщения корректны [8].

Рассмотрим наиболее распространённые подходы при проведении атак.

Passive Network Reconnaissance (пасивная сетевая разведка): атакующий ПК либо вредоносное ПО с соответствующим доступом захватывает и анализирует DNP3-сообщения. Подобный сце-

EtherWAN

EX77900

28-портовый управляемый коммутатор L3
Промышленное исполнение
Кольцевое резервирование с быстрым восстановлением (<15 мс)

ПРОМЫШЛЕННОЕ СЕТЕВОЕ ОБОРУДОВАНИЕ

для АСУ ТП, сетей безопасности и видеонаблюдения

- Многопортовые коммутаторы Gigabit Ethernet, в том числе PoE
- Резервирование линий связи для отказоустойчивости
- Оптимизированная передача промышленных протоколов и IP-видео
- Удлинители Ethernet до 2,6 км (cat. 3, 5, телефонный провод)
- Преобразователи сред Ethernet
- Диапазон рабочих температур –40...+75°C для монтажа вне помещений
- Грозозащита Ethernet и VDSL

ED3575

Управляемый коммутатор
6×Fast Ethernet + 2×1 GbE SFP
2×VDSL-удлинитель Ethernet
Резервирование RSTP, α-Ring

EX73900

Управляемый коммутатор L3
12×1 GbE + 4×1 GbE SFP
Резервирование RSTP, α-Ring
Маршрутизация динамическая, статическая

PD3041

Модуль искро- и грозозащиты для VDSL

PROSOFT®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU

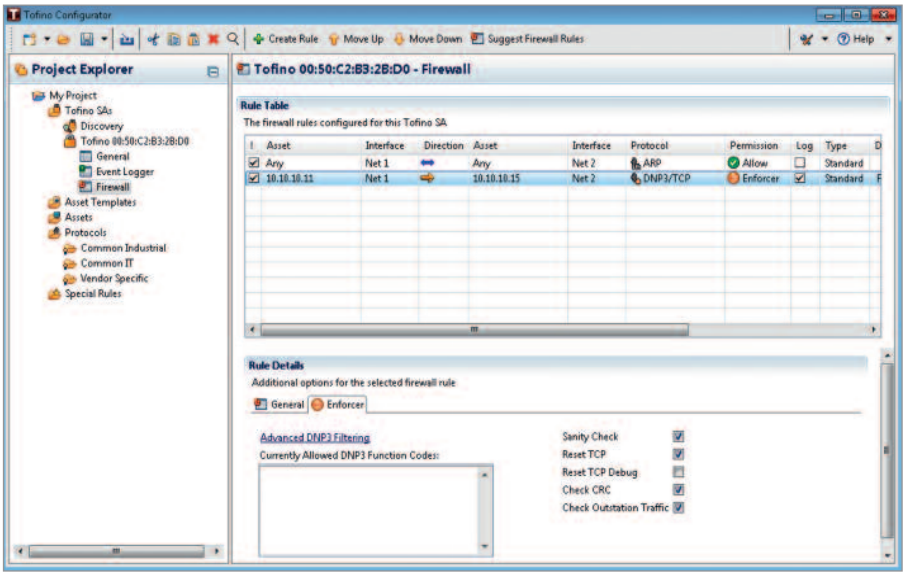


Рис. 6. Настройка DPI-фильтра для протокола DNP3

нарий позволяет получить информацию о топологии сети, функциональности устройства, адресах памяти и других данных. Эта атака может привести к тому, что будет осуществлён перехват как основных данных, так и информации о топологии сети.

Baseline Response Replay (повторение базового ответа): данная методика атаки сводится к тому, что атакующий ПК либо вредоносное ПО имитирует ответы ведущему устройству при отправке ложных сообщений на внешние устройства. При этом возможны различные варианты, начиная от прерывания ведущего устройства, заканчивая передачей ложных данных.

Rogue Interloper: атакующий ПК устанавливает устройство типа «человек посередине» между ведущим устройством и удалёнными станциями, которые могут читать, изменять и создавать DNP3-сообщения.

Используя данные подходы, можно скомпрометировать данные на каждом из трёх уровней.

Для примера рассмотрим прикладной уровень.

Прикладной уровень обеспечивает основную функциональность для систем, работающих на базе протокола DNP3, и, как правило, наибольшее количество угроз и атак связано именно с ним. Рассмотрим несколько наиболее популярных атак.

Outstation Write Attack. При реализации данной атаки происходит отправка DNP3-сообщение с кодом функции 2, который приводит к записи объектов данных в удалённое устройство. Атака может изменить информацию, хранящуюся в памяти устройства, что приведёт к ошибкам или, что более вероятно, к переполнению буфера памяти.

Clear Objects Attack. Эта атака реализуется при отправке сообщения с кодом функции 9 или 10, чтобы «заморозить» или стереть объекты данных. Атака может очистить критические данные или привести к сбою удалённого устройства. При этом подобная атака с использованием кода функции 10 является наиболее проблематичной, так как сообщение с этим функциональным кодом не требует подтверждения.

Outstation Data Reset. Сообщение DNP3 с кодом функции 15 заставляет оконечное устройство повторно инициализировать объекты данных, сбросить к их изначальным значениям, не соответствующим текущему состоянию системы.

Outstation Application Termination. Если атакующий отправит DNP3-сообщение с кодом функции 18, который используется для прекращения работы приложений, выполняющихся на удалённых устройствах, то устройство перестанет отвечать на обычные запросы от мастер-устройства.

Configuration Capture Attack. Данная атака отправляет сообщение, которое указывает на повреждение файла конфигурации. Атака заставляет ведущее устройство передать новый файл конфигурации, который затем можно перехватить. Дальнейшее развитие сценария предполагает выполнение отдельной атаки, нацеленной на изменение файла конфигурации и загрузку на целевое удалённое устройство.

Описанные типы атак являются лишь небольшой частью из возможных [8]. При этом они могут исходить как от реального злоумышленника, так и от неправильно сконфигурированного ПО или написанного кода. Для обеспечения защиты протокола необходим глубокий анализ, который позволит создать фильтры, способные обеспечить требуемую защиту.

DNP3 Enforcer LSM

Модуль DNP3 Enforcer LSM отвечает за анализ трафика протокола DNP3. Пользователю доступен графический интерфейс (рис. 6), который предназначен для создания необходимой конфигурации брандмауэра. Как и в случае с остальными модулями, анализ DNP3-трафика можно контролировать для каждого соединения.

На рис. 6 показан набор правил. Он включает ряд дополнительных возможностей по анализу протокола DNP3:

- Sanity Check – проверка DNP3-трафика на полное соответствие спецификации;
- Reset TCP – отправка сообщения TCP-reset в случае, если пакет не был пропущен;
- Reset TCP Debug позволяет генерировать отладочное сообщение при отправке сообщения сброса сессии;
- Check CRC – проверка контрольной суммы CRC, как в заголовках канального уровня, так и на прикладном уровне протокола DNP3; данная проверка реализована на аппаратном уровне и не сказывается на быстродействии брандмауэра;
- Check Outstation Traffic – проверка пакетов, исходящих от удалённых устройств (Outstation Devices).

Заключение

Концепция Defense in Depth, описанная в предыдущих статьях цикла, является одним из методов обеспечения безопасности сети промышленного объекта.

Реализация всех четырёх этапов [9] позволит существенно повысить защиту, взлом которой будет представлять очень сложную задачу для атакующего.

Глубокая проверка данных – это подход, позволяющий обеспечить защиту тех протоколов, которые в принципе не имеют механизмов защиты. Протоколы IEC 104, GOOSE и DNP3, уязвимость которых была описана в данной статье, применяются в энергетике и являются базовыми для многих промышленных предприятий.

Бездействие по организации их защиты может привести к существенному снижению уровня кибербезопасности всего промышленного объекта.

Загружаемые модули IEC 104, GOOSE и DNP3 Enforcer LSM для промышленного брандмауэра Tofino Xenon предназначены для обеспечения защиты одноимённых протоколов путём глубокой инспекции трафика и гибких параметров настраиваемого фильтра.

Правильная настройка фильтра позволит обеспечить не только всестороннюю защиту протоколов, но и создать самый грозный рубеж обороны согласно концепции Defense in Depth. ●

Литература

1. Самые громкие кибер-атаки на критические инфраструктуры [Электронный ресурс] // Режим доступа : https://habr.com/company/panda/blog/316500/.
2. Qassim Q., Jamil N., et al. Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system // International Journal of Engineering & Technology. – 2018. – Vol. 7. – № 2.14.
3. Czechowskiy R., Wicher P. Cyber Security in communication of SCADA systems using IEC 61850 // Proceedings of International Conference MEPS'15 Modern Electric Power Systems. – Wroclaw, 2015.
4. Воробьёв С. "Defense in Depth" в действии. Уровень 1: защита границы сети // Современные технологии автоматизации. – 2017. – № 4.
5. Воробьёв С. "Defense in Depth" в действии. Уровень 2: защита канального уровня // Современные технологии автоматизации. – 2018. – № 1.
6. Гусев И. Вопросы информационной безопасности современных систем РЗА [Электронный ресурс] // Режим доступа : http://digitalsubstation.com/blog/2013/12/16/voprosy-informacionnojj-bezopasnosti-sovremennykh-sistem-rza/.
7. Медведев А. DNP3 по-русски // Современные технологии автоматизации. – 2017. – № 2.
8. East S., Butts J., et al. A taxonomy of attacks on the DNP3 protocol // Revised Selected Papers of Critical Infrastructure Protection III: Third IFIP WG 11.10 International Conference. – Hanover, New Hampshire, 2009.
9. Воробьёв С. Глубокая защита промышленного сетевого периметра // Современные технологии автоматизации. – 2017. – № 4.

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

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

День решений Advantech в Москве: IoT-устройства, популярные решения и новинки оборудования

Этой осенью компания ПРОСОФТ совместно с крупнейшим поставщиком оборудования для промышленной автоматизации компанией Advantech провела семинар в столице. Аудитория познакомилась с популярными и новейшими устройствами для сбора данных и управления, встраиваемыми компьютерами и компьютерными платформами, серверным и сетевым оборудованием, а также с прорывными IoT-решениями.

Наибольший интерес вызвали устройства для удалённого сбора данных, которые можно интегрировать в различные облачные сервисы, созданные в рамках концепции Интернета вещей.

Сейчас тема применения IoT-систем в промышленности, на транспорте и инфраструктурных объектах становится всё более популярной, а возможность беспроводной передачи данных с помощью операторов сотовых сетей с удалённых объектов всё чаще привлекает заказчиков из промышленного сектора. Устройства Advantech, предназначенные именно для такой передачи данных, были представлены в рамках семинара.

Одна из презентаций познакомила слушателей с модулями беспроводной связи: обновлённым модулем WISE-4000 (Wi-Fi), а также модулями Wzzard Smart Mesh (Smart-Mesh IP) и Wzzard LoRa (Lora Private и Lora WAN), которые можно использовать как готовые решения для сбора данных с конечных устройств.

Также большой интерес и множество вопросов вызвала презентация, посвящённая встраиваемым решениям, узлам связи для Интернета вещей, на базе которых заказчик может создать своё собственное изделие, способное взаимодействовать с другими устройствами по уже существующим протоколам передачи данных.

Внимание аудитории к встраиваемым устройствам такого типа неудивительно, поскольку именно они востребованы заказчиками, которые нуждаются в современных системах управления распределёнными объектами в нефтегазовом секторе, системе ЖКХ и умных зданий, на транспорте. Такие заказчики, действующие и потенциальные, являются ключевыми для Advantech, они же составляли основную аудиторию семинара.

Отметим интерес к решениям Advantech и экспертов крупнейших операторов сетей передачи данных, которые сегодня активно работают над специализированными решениями для Интернета вещей. Семинар показал, что для Advantech открываются широкие возможности сотрудничества с такими компаниями в качестве поставщика аппаратной части интегрированных IoT-решений.

Важной частью семинара стал обзор применений оборудования Advantech в реальных проектах. Так, была рассмотрена система на базе оборудования компании по управлению крупным распределённым сельскохозяйственным объектом – промышленный Интернет вещей в действии. Автоматизированная система высокоточного земледелия обеспечивает своевременный полив, внесение удобрений, организацию оптимальной среды для качественного вызревания растений и плодов, транспортную логистику и многое другое.

Также были представлены решения для жилищно-коммунального комплекса по диспетчеризации зданий, учёту ресурсов, управлению котельными и т.д. Отметим, что ЖКХ и проекты формата «Умный дом» – ещё одна сфера, где решения Advantech широко востребованы.

Специалисты из области системной интеграции по достоинству оценили презентацию линейки компьютерных платформ и современных компонентов для сборки промышленных компьютеров. Особенно слушателей интересовал вопрос о доступности изделий Advantech в течение длительного времени, столь важный для промышленной автоматизации.

– *Широкий охват рассмотренных тем позволил нам представить заказчикам максимально полную картину решений и устройств, которые сегодня Advantech предлагает рынку, а активность и высокая вовлечённость аудитории подтвердили актуальность самого формата мероприятия – с живым общением, дискуссиями, возможностью напрямую обсудить острые вопросы»*, – так прокомментировал итоги семинара бренд-менеджер ПРОСОФТ Александр Барон. ●