Эрик Байрс

IT-безопасность в промышленности. Глубокий анализ пакетов данных для SCADA-систем

В статье рассматривается специфика обеспечения IT-безопасности в промышленной среде, приводятся примеры реальных угроз. Представлена технология DPI как основное средство обнаружения вредоносного программного обеспечения; приведён пример оборудования, реализующего данную технологию.

Введение

Мировая промышленность, объекты транспортной отрасли и энергетики в настоящее время испытывают трудности с обеспечением должного уровня IT-безопасности. Эта сфера, вбирающая в себя многочисленные критически важные приложения, в основном использует типовые SCADA-системы и промышленные АСУ со стандартизированными протоколами обмена данными. Многие из этих систем проектировались десятки лет назад, когда понятия IT-безопасности не существовало вовсе.

Современные сетевые технологии уже плотно вошли в промышленную инфраструктуру, позволяя получить сквозной доступ к информации в сети на всех уровнях – от полевого до административного. С одной стороны, лёгкий доступ к информации повышает эффективность системы, а с другой стороны, возрастает её уязвимость со стороны различных сетевых угроз (несанкционированный доступ, вирусы, хакерские атаки). Эта проблема требует немедленного решения, но, учитывая большую продолжительность жизненного цикла промышленных систем, рассчитывать на быстрое появление и распространение защищённых SCADA-систем, промышленных систем управления и соответствующих протоколов не приходится.

Между тем решения для устранения бреши в безопасности промышленных систем существуют. Одним из них является применение специальных брандмауэров для SCADA-систем, использующих технологию глубокого анализа пакетов данных (Deep Packet Inspection – DPI) и способных обеспечить контроль над трафиком системы управления. Данная статья раскрывает понятие глубокого анализа пакетов (DPI) в системах управления и показывает различие между промышленными брандмауэрами и известными их офисными аналогами. Также она представляет варианты применения DPI IT-специалистами для блокирования вредоносного и несанкционированного трафика, избегая непосредственного вмешательства в работу системы управления. А приведённый в статье пример показывает, как судоходная компания применила брандмауэры с технологией DPI для Modbus-протокола с целью защитить систему управления судоходными каналами.

Необходимость в новых технологиях безопасности

За последние 10 лет промышленные системы освоили такие сетевые технологии, как Ethernet и TCP/IP. Эти технологии широко используются в промышленных АСУ и SCADA-системах, создавая условия для более эффективной работы предприятий и делая системы контроля более доступными для пользователей. Но наряду с преимуществами они принесли и проблему: объединение информационных сетей на разных уровнях предприятия в единое сквозное информационное пространство значительно повышает уязвимость системы со стороны внешних атак, сетевых «червей», вирусов и хакеров. Проблему усугубляет то, что сетевые протоколы, используемые промышленными АСУ и SCADA-системами, разрабатывались без учёта каких-либо требований по обеспечению безопасности. Если они и предлагают некоторые меры по ограничению негативного поведения в сети, то эти меры крайне примитивны и легко обходятся. А если кому-либо разрешено читать данные с контроллера, то он может выключить или перепрограммировать его.

Данная ситуация не изменится, по крайней мере, ещё лет десять. Промышленные системы контроля и управления редко заменяются и модернизируются, их срок эксплуатации составляет от 10 до 20 и более лет. Функ-

ционал таких систем определяется заранее и не меняется, и уязвимость промышленных АСУ и SCADA-систем, ранее введённых в эксплуатацию, не может быть устранена соответствующими патчами, как это делается в ОС Windows. Поэтому пройдут многие годы, прежде чем новые, более безопасные системы контроля и управления получат распространение. И в течение этих лет множество промышленных систем контроля и управления будут беззащитны перед вредоносными действиями даже непрофессиональных хакеров. А если злоумышленник или вредоносное программное обеспечение (ПО) может получить доступ к промышленной системе, то может быть выведено из строя большинство контроллеров, нарушен технологический процесс, нанесён вред дорогостоящему оборудованию, возможно создание условий для возникновения аварий и т.д.

Решением данной проблемы является технология глубокого анализа пакетов DPI, позволяющая контролировать всю передаваемую информацию в системе с высокой точностью. Это относительно простое решение. Оно не требует полной замены дорогих уже существующих SCADA-систем и контрольно-управляющего оборудования.

Что такое традиционный офисный брандмауэр?

Для понимания того, как работает технология DPI, важно представлять себе принцип работы обычного офисного брандмауэра. Это устройство, которое «слушает» и контролирует входящий трафик или трафик между подсетями. Оно перехватывает трафик и анализирует его в соответствии со списком предопределённых наборов правил (Access Control List – ACL). Все сообщения, которые не удовлетворяют спискам ACL, не пропускаются брандмауэром.

Традиционный офисный брандмауэр использует списки ACL для проверки трёх первых полей сообщения Ethernet:

1) адрес отправителя сообщения (IP-адрес источника);
2) адрес получателя сообщения (IP-адрес приёмника);
3) протокол уровня приложения, содержащийся в IP-сообщении, определяемый по номеру виртуального порта (порт получателя).

Проверку адресов отправителя и получателя понять легко. Проверяя IP-адрес, брандмауэр исключает пересылку сообщений от отправителей или к получателям, не указанным в списках ACL. Пока участники сети используют разрешённые адреса, они могут обмениваться данными через брандмауэр.

Порт получателя требует больше объяснений. Такой порт не является физическим портом, подобно 10/100/1000Base-TX или USB. Это специальные номера, содержащиеся в каждом сообщении протоколов TCP и UDP. Они используются для идентификации протокола уровня приложений, информацию от которого содержит сообщение. К примеру, протокол Modbus TCP использует порт 502, а протокол Всемирной паутины HTTP использует порт 80. Номера портов зарегистрированы в департаменте Internet Assigned Numbers Authority (IANA) международной организации Internet Corporation for Assigned Names and Numbers (ICANN) и никогда не изменяются.

В завершение рассмотрения данного вопроса приведём примеры.

Если нужно разрешить только Web-трафик (протокол HTTP) от клиента с IP-адресом 192.168.1.10 к Web-серверу с адресом 192.168.1.20, то следует в список ACL добавить такую строку:

Allow Src=192.168.1.10 Dst=192.168.1.20 Port=HTTP.

После загрузки списка ACL с этим правилом будут пропускаться только сообщения, удовлетворяющие всем трём указанным критериям.

Если требуется заблокировать весь трафик Modbus TCP, проходящий через брандмауэр, то нужно определить правило, запрещающее все пакеты, содержащие номер 502 в поле заголовка пакета в качестве порта получателя.

Специфика сетевых протоколов АСУ и SCADA-систем

Проблема принципа работы традиционных брандмауэров заключается в том, что они абсолютно однозначны. Используя такой принцип, можно либо разрешить определённый протокол, либо запретить его. Более детальное управление внутри протокола невозможно.

Причина этого в том, что протоколы, используемые в АСУ и SCADA-системах, не поддаются детализации. С точки зрения номера порта получателя, сообщения с чтением данных выглядят как обновление ПО. Таким образом, разрешая прохождение сообщений с чтением данных с устройства операторского интерфейса для ПЛК через стандартный брандмауэр, вы автоматически разрешаете программирование контроллеров. А это серьёзное упущение, с точки зрения безопасности.

Для примера, весной 2009 года парламент Соединенных Штатов опубликовал сообщение для крупнейших энергетических компаний с такими словами: «Уязвимость была обнаружена и подтверждена внутри процесса обновления программного обеспечения, используемого в системах управления критически важных объектов CIKR (Critical Infrastructure and Key Resources) ... необходима разработка плана для защиты объектов CIKR. Шаги, направленные на устранение уязвимости с обновлением ПО, включают блокировку обновлений ПО соответствующими правилами брандмауэра».

К сожалению, брандмауэры, представленные на рынке, не способны различать команды от SCADA-системы. Как результат, «блокировка обновлений ПО соответствующими правилами брандмауэра» ведёт к блокировке всего трафика SCADA-системы. Так как трафик SCADA-системы считается критически важным, большинство инженеров просто полностью разрешают его, несмотря на возможные проблемы с безопасностью.

Технология DPI для обеспечения безопасности в глубину

Очевидно, что брандмауэру следует глубже разбираться в протоколах для того, чтобы точно определять, какой протокол для чего используется. И это как раз то, что позволяет делать технология DPI. После того как традиционные правила брандмауэра применены, брандмауэр с поддержкой DPI исследует контент внутри TCP/IP-сообщения и применяет более детальные правила. Он спроектирован так, чтобы понимать специфические протоколы SCADA-системы и применять фильтры к полям и значениям этих полей, что и позволяет детально контролировать систему. В зависимости от протокола эти поля могут включать команды (такие как чтение или запись регистра), объекты (например, объект «двигатель»), сервисы (получить/записать значение) и диапазоны адресов ПЛК (рис. 1).

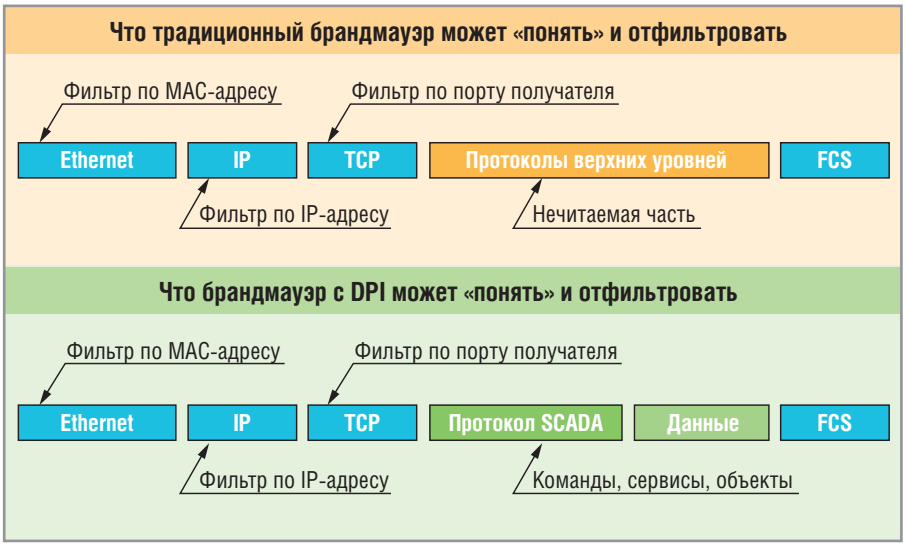

Рис. 1. Сравнение возможностей по фильтрации трафика традиционным брандмауэром и брандмауэром с DPI (традиционный брандмауэр не понимает протокола передачи данных SCADA-системы, поэтому соответствующий трафик можно только запретить или разрешить целиком)

К примеру, брандмауэр с возможностью глубокого исследования протокола Modbus (Hirschmann EAGLE Tofino, Honeywell Modbus Read-only Firewall, Schneider ConneXium Tofino Firewall) способен определять, какого типа сообщения (чтение, запись) содержатся в посылке, и отфильтровать сообщения с записью информации. Хороший DPI-брандмауэр также способен производить инспекцию сообщений на предмет их необычного формата или необычного поведения (например, 10 000 ответных сообщений на единственный запрос). Такой «неправильный» трафик характерен для сетевых атак и вредоносного ПО и должен быть заблокирован.

Защита SCADA-систем с помощью DPI на практике

Детальный контроль АСУ и SCADA-систем может значительно улучшить защищённость и надёжность системы. Для примера рассмотрим реальную судоходную управляющую компанию. Она использует ПЛК в управлении всеми мостами и шлюзами для обеспечения безопасного движения транспортных средств и речных судов.

Компания столкнулась со следующей проблемой: ряду рабочих станций требовался постоянный доступ к данным с ПЛК. Однако только специальные станции управления должны иметь возможность посылать команды и вообще влиять на работу контроллеров. Обычные пароли или брандмауэры не обеспечивают тонкую настройку системы и, соответственно, нужный уровень безопасности.

Решение проблемы состояло в применении брандмауэра с DPI-технологией для Modbus-трафика между станциями управления и ПЛК. Брандмауэр позволяет пропускать только команды чтения информации с рабочих станций на контроллеры (рис. 2), за исключением ряда защищённых станций управления. Все удалённые команды программирования Modbus от сторонних операторов рабочих станций блокируются. Всего 54 брандмауэра было установлено в 24 точках системы, что позволило с 2008 года надёжно защитить систему от возможных инцидентов.

Как технология DPI противостоит вирусам и вредоносному ПО

Ещё лет 5 назад технология DPI рассматривалась как интересное дополнение к системе. Сейчас благодаря текущему поколению вирусов типа Stuxnet, Duqu, Conficker она является необходимостью для защищённых АСУ и SCADA-систем.

Сегодняшние разработчики вредоносного ПО знают, что брандмауэры и другие средства сетевой безопасности способны отфильтровать неопознанный или неразрешённый протокол сразу. Они в курсе, что если в сети используются обычные протоколы типа HTTP, Modbus и MS-SQL, то появление нового протокола сразу обратит на себя внимание системного администратора или межсетевого экрана. Поэтому разработчики вредоносного ПО пытаются уйти вглубь, то есть спрятаться внутри трафика тех протоколов, которые уже используются в атакуемой сети. К примеру, многие современные «черви» сейчас прячут свой внешний трафик внутри протокола HTTP так, что внешне его сообщения выглядят совершенно обычно.

Вирус Stuxnet – это отличный пример маскировки опасного ПО внутри «невинного» протокола. Он спроектирован для функционирования внутри протокола RPC (Remote Procedure Call) и предназначен как для заражения новых жертв, так и для коммуникаций в режиме точка–точка между заражёнными машинами (рис. 3).

RPC – это идеальный протокол для атаки АСУ и SCADA-систем, так как

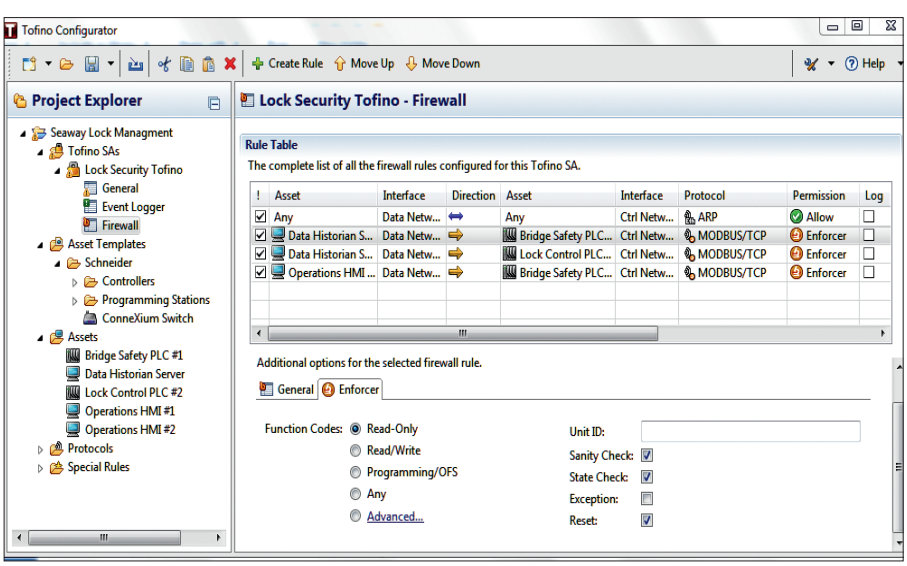

Рис. 2. Правила брандмауэра пропускают только команды чтения между модулем Data Historian и ПЛК; дополнительные фильтры позволяют также проверять команды Modbus на соответствие спецификации протокола

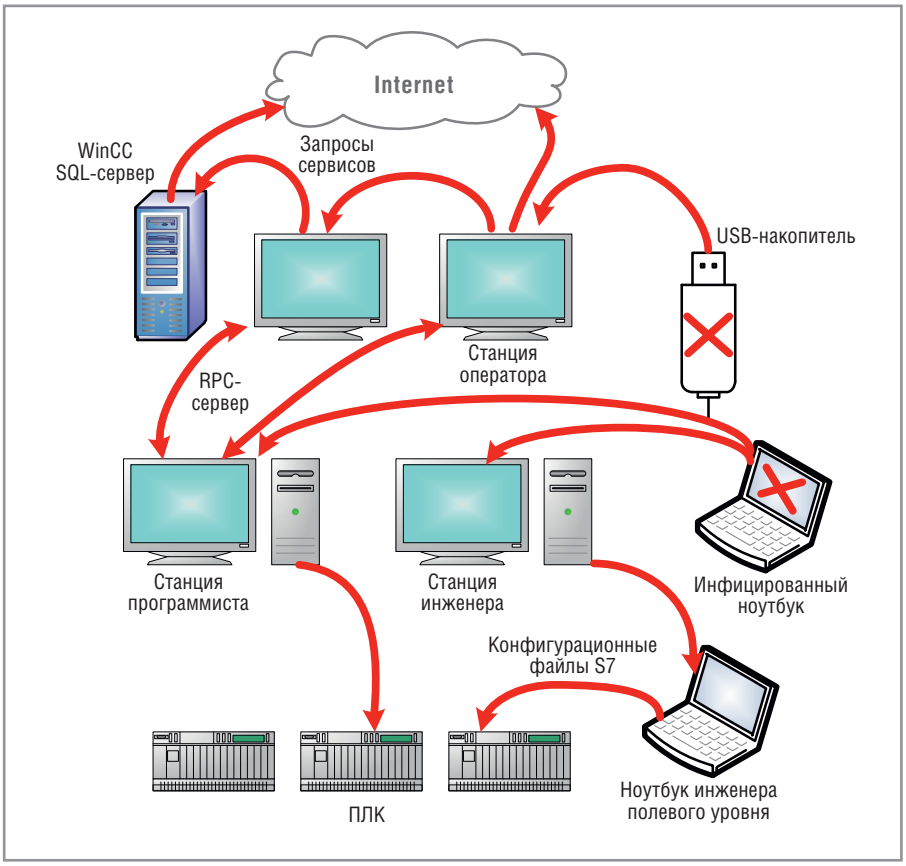

Рис. 3. Вирус Stuxnet распространяется многими путями, включая использование протокола RPC как вектора; технология глубокого анализа пакетов данных DPI в состоянии зарегистрировать нестандартное использование протокола и запретить большинство путей распространения вируса

он широко применяется в современных системах контроля и управления. Для примера, технология OPC (OLE for Process Control), являющаяся сегодня самой используемой в промышленной интеграции объектов, базируется на технологии DCOM (Distributed Component Object Model), которая также задействует протокол RPC.

Более того, серверы управления и рабочие станции обычно конфигурируются для совместного использования файлов и принтеров по протоколу Microsoft SMB, который также передаётся поверх протокола RPC. И, возможно, самый значимый пример тут – все контроллеры Siemens SIMATIC PC S7 и системы на их основе, которые используют собственные форматы сообщений, также передаются поверх протокола RPC. Если бы вы были администратором сети, заражённой вирусом Stuxnet, единственное, что бы вы заметили, – небольшое увеличение трафика RPC-протокола, что едва ли послужило бы поводом для тревоги. Даже если бы вы что-то заподозрили, то едва ли вы бы что-то обнаружили, имея в арсенале лишь стандартный брандмауэр. Простая блокировка всего RPC-трафика привела бы к остановке всех связанных с данным протоколом сервисов на предприятии. Без средств анализа состава трафика протокола RPC и блокирования паразитного трафика (то есть DPI) не удастся остановить действие вредоносного ПО.

Рис. 4. Внешний вид программно-аппаратного комплекса защиты промышленного IT-контура с реализацией DPI-технологии Hirschmann EAGLE Tofino

Заключение

Технология DPI – мощный инструмент в ассортименте средств обеспечения IT-безопасности, который позволяет обнаруживать и блокировать вредоносный трафик в системах управления и SCADA-системах. Данная технология не абстрактна, она имеет вполне конкретную уже рабочую реализацию в виде модульного ПО Tofino от Byres Security, входящего в аппаратно-программный комплекс защиты Hirschmann EAGLE Tofino (рис. 4).

EAGLE Tofino способен проводить глубокий анализ более чем 50 промышленных протоколов (PROFINET, МЭК 61850, DNP и др.), анализировать трафик Modbus TCP и OPC-сервера/клиента, строить VPN-тоннели. Программное обеспечение Tofino включает более 25 предварительно настроенных профилей безопасности для ПЛК Siemens, VIPA, WAGO и т.д., позволяя обезопасить контроллеры от несанкционированного вмешательства в их программы. Более подробно об этом можно прочитать в источниках, указанных в списке рекомендуемой литературы. ●

Рекомендуемая литература

1. How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems [Электронный ресурс]. – Режим доступа : https://www.tofinosecurity.com/how-stuxnet-spreads.
2. PLC Security Risk: Controller Operating Systems [Электронный ресурс]. – Режим доступа : https://www.tofinosecurity.com/blog/plc-security-risk-controller-operating-systems.
3. Tofino Modbus TCP Enforcer LSM [Электронный ресурс]. – Режим доступа : https://www.tofinosecurity.com/products/Tofino-Modbus-TCP-Enforcer-LSM.
4. Securing Your OPC Classic Control Systems [Электронный ресурс]. – Режим доступа : http://www.opcfoundation.org/DownloadFile.aspx?CM=3&RI=781&CN=KEY&CI=282&CU=4.
5. Tofino OPC Enforcer LSM [Электронный ресурс]. – Режим доступа : http://www.tofinosecurity.com/products/Tofino-OPC-Enforcer-LSM.
6. Using Tofino to Control Stuxnet [Электронный ресурс]. – Режим доступа : http://www.tofinosecurity.com/professional/using-tofino-control-stuxnet.
7. Tofino Live Demonstration [Электронный ресурс]. – Режим доступа : http://www.youtube.com/watch?v=G4E0bxZGZL0.

Автор – технический директор компании Byres Security
Перевод Ивана Лопухова, сотрудника фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru