Иван Лопухов

Обеспечение безопасности OPC для АСУ ТП

Бытует мнение, что промышленные системы управления имеют слабый потенциал быть атакованными вредоносным ПО и/или хакерами. Данное мнение ошибочно: любая система, сделанная в масштабе серийного производства, может стать мишенью для хакерских и вирусных атак. В статье рассматривается один из основных стандартов построения промышленных систем управления – технология OPC, рассказывается о предпосылках и возможных решениях для обеспечения безопасности OPC-данных. Практические аспекты и вопросы тестирования упомянутых средств безопасности будут описаны в следующей статье.

Введение

Информационные сети стали важной частью АСУ ТП и систем диспетчерского управления и сбора данных (SCADA-систем), нуждающихся в централизованном управлении и мониторинге. Традиционно системы распределённого управления и SCADA-системы проектируются изолированными от других корпоративных сетей. Они имеют естественную эффективную защиту от киберугроз благодаря использованию специализированного оборудования и протоколов передачи данных.

Сейчас происходит активное слияние корпоративных и промышленных сетей. К примеру, из-за потребности в удалённом доступе к данным, удалённом администрировании многие сети АСУ ТП стали доступны из корпоративных сетей. Компании также стремятся к снижению своих затрат за счёт построения многозадачных сетей, общих магистральных сетей, единой IT-службы. И самое главное, повсеместное использование офисных компьютеров и коммуникационного оборудования сильно повлияло на развитие любых отраслей промышленности. Стандартизированные подходы и технологии позволяют более эффективно управлять бизнесом, а сквозной доступ к данным внутри всей организации делает управление более гибким.

В то время как компании пожинают плоды этих инициатив, многие из них сталкиваются с опасностями, вытекающими из чересчур свободного доступа к данным большого числа пользователей. Соединяя вместе корпоративную сеть с АСУ ТП и давая доступ к ней пользователям, клиентам, поставщикам и другим, мы серьёзно повышаем уязвимость сети АСУ ТП и создаём угрозу конфиденциальности её данных. Система становится более открытой для вредоносного ПО, компьютерных вирусов и хакеров. Системным администраторам приходится поддерживать баланс между доступностью и безопасностью сети.

Уменьшение поверхности атаки

Один из наиболее эффективных путей к урегулированию конфликта между потребностью в доступности данных и необходимостью в защите персональных данных и процессов – это минимизация количества интерфейсов и протоколов, связывающих сеть АСУ ТП с внешней сетью. Единственное доверенное соединение, передающее все необходимые данные, снижает не только затраты на администрирование, но и риск атаки или проникновения вредоносного ПО. Этот путь известен как уменьшение поверхности атаки.

Таким образом, первейшая задача системного администратора – выбор соответствующей коммуникационной технологии, которая будет универсальной для системы контроля и корпоративной системы. Вариантов много, например, протокол Modbus TCP или HTTP, а вместе с ними протокол OPC – без сомнения, один из самых распространённых универсальных способов доступа к данным промышленных систем автоматизации.

Аббревиатура OPC (OLE for Process Control), сейчас официально называемая OPC Classic, обозначает наиболее известный стандарт промышленной интеграции. Он применяется в огромном количестве промышленных приложений от человеко-машинных интерфейсов (HMI) на рабочих станциях, систем аварийной защиты (SIS), распределённых систем управления (DCS) на полевом уровне и до корпоративных баз данных, систем планирования ресурсов предприятия (ERP), прочих бизнес-ориентированных систем корпоративного уровня.

При всей привлекательности OPC неясным остаётся вопрос обеспечения требований безопасности данным протоколом. Эта статья – попытка дать разъяснения по данному вопросу, показать, что его использование может быть достаточно безопасным. С помощью многоуровневой OPC-совместимой системы

защиты возможно создание высоконадёжных в плане безопасности систем, не требующих чрезмерных затрат на поддержку и администрирование.

Использование многоуровневых средств защиты

Вслед за уменьшением поверхности атаки следует второй шаг – построение многоуровневой системы безопасности. Данная концепция, часто называемая защитой в глубину, позволяет управлять рисками с помощью различных стратегий защиты.

Стратегия многоуровневой защиты обладает рядом преимуществ. Главное из них в том, что если первый уровень защиты нарушен, то следующий, использующий другой метод защиты, создаст дополнительную помеху, способную предотвратить проникновение угрозы. Менее очевидное, но даже более важное преимущество в том, что атаки могут быть разноплановыми, а каждый уровень защиты должен быть оптимизирован с учётом определённого типа вредоносных действий. К примеру, защита от компьютерного вируса требует техник, отличающихся от защиты от злонамеренных действий сотрудников компании. Таким образом, ключ к улучшению каждого уровня защиты в глубину состоит в том, чтобы удостовериться, что данный уровень находится в контексте той информации или процесса, который он призван защищать.

Пример защиты в глубину коммерческого банка

Система безопасности банка представляет собой хороший пример защиты в глубину системы управления. Что же делает банк более защищённым, чем частный дом или круглосуточный магазин? Банк использует множество средств безопасности для обеспечения максимальной защиты сотрудников, клиентов и активов. Уровней безопасности не только много, но каждый из них направлен на защиту от отдельного типа угроз в той части системы, где он применён. К примеру, каждый банк имеет железные двери, бронированные окна, охрану, защищённые ключи, сейфы и сигнализацию. Двери – эффективное и простое средство. Сами по себе они либо позволяют войти каждому, либо закрыты для всех, вне зависимости от того, кем входящий человек является и как себя ведёт.

Уровнем выше дверей – охрана банка. Она проверяет поток посетителей банка, контролирует права доступа и поведение людей, используя ряд установленных критериев.

Следующий уровень – электронная система контроля доступа и сигнализации. В ней используется система профилей посетителей с аутентификацией по ключам, отпечаткам пальцев, паролям, распознаванию лица и т.д.

Эта упрощённая модель показывает, что каждый уровень безопасности не просто создаёт дополнительную защиту, а соответствует модели угроз, сформированной для каждого уровня.

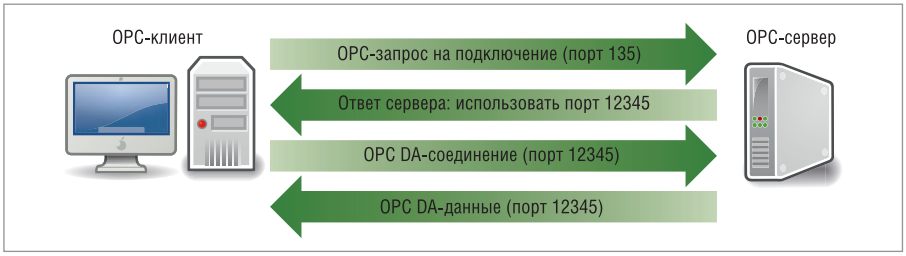

Рис. 1. Динамическое назначение виртуальных портов OPC-сервером

Безопасность промышленной системы управления

Как же обстоят дела с безопасностью в АСУ ТП? По аналогии с банком роль охраны и сигнализации тут выполняют системы обеспечения сетевой безопасности и безопасности приложений соответственно.

К примеру, межсетевой экран функционирует наподобие охраны. Отдельные протоколы в сети либо пропускаются, либо запрещаются им в зависимости от списка правил. Так же как охрана может обладать опытом, существуют межсетевые экраны, более глубоко «разбирающиеся» в протоколах SCADA-систем и обеспечивающие дополнительную фильтрацию на основе контекста и поведения трафика.

Аналогично OPC-сервер с хорошим уровнем безопасности при подключении клиента может контролировать доступ только к определённым данным. Попытки доступа к запретным данным должны быть пресечены и запротоколированы.

Как в примере с охраной и сигнализацией банка, межсетевой экран, обеспечивающий сетевую безопасность, и OPC-сервер, отвечающий за безопасность приложения, являются необходимыми. Межсетевой экран может заблокировать миллионы сообщений неустановленного формата на сервер, являющихся частью DoS (Denial of Service) атаки. В то же время проверка и авторизация пользователей может предотвратить атаку внутри сети.

Особенности обеспечения сетевой безопасности

Для понимания вопросов сетевой безопасности важно знать, что большинство TCP/IP-протоколов, таких как Modbus TCP, содержат стандартизированный идентификатор (номер порта) в каждом сообщении, который необходим для идентификации сообщения как части протокола более высокого уровня. Простая идентификация протокола позволяет межсетевому экрану блокировать или пропускать его сообщения. К примеру, для блокировки всего трафика Modbus TCP межсетевой экран должен найти и заблокировать все сообщения, содержащие присвоенный Modbus TCP идентификатор в соответствующем поле.

Отдельный OPC-сервер не использует фиксированные номера TCP-портов. Вместо этого он динамически присваивает новые номера TCP-портов для каждого процесса, используемого в коммуникации с OPC-клиентами. Те, в свою очередь, в каждой сессии должны определить присвоенные им номера путём запроса их у сервера. После этого OPC-клиенты устанавливают новое TCP-соединение с OPC-сервером, используя полученный номер порта. OPC-серверы могут использовать любые номера портов в диапазоне от 1024 до 65535, что делает технологию OPC Classic фактически несовместимой с традиционными межсетевыми экранами (рис. 1).

С одной стороны, можно оставить открытыми на межсетевом экране все порты с 1024 до 65535, но это всё равно, что посадить спящую охрану в банке. С другой стороны, стремление к блокировке всех портов парализует работу OPC-сервера. Тем не менее, даже динамическое распределение номеров портов не отменяет возможности защиты OPC-сервера с помощью межсетевого экрана. Специализированные межсетевые экраны с поддержкой технологии OPC Classic способны автоматически отслеживать и управлять доступом к динамически открываемым портам (врезка «Как работает межсетевой экран для OPC-сервера?»). Они спроектированы для интегра-

ции в существующую сеть без её остановки и внесения изменений в конфигурации OPC-сервера и клиентов.

Пример такого решения – межсетевой экран Eagle Tofino производства Byres Security, подразделения компании Belden. Программный модуль Tofino OPC Enforcer устанавливается на данную аппаратную платформу и служит специализированным межсетевым экраном для OPC-сервера (врезка «Возможности и применения Eagle Tofino»). Аппаратно-программный комплекс Eagle Tofino интегрируется в работающую сеть АСУ ТП без внесения в неё изменений и простоя системы. Это простое решение для выделения OPC-сервера в безопасную зону согласно рекомендациям стандартов ANSI/ISA99, NERC CIP и IEC.

Особенности обеспечения безопасности приложений

Возвращаясь к аналогии с банком, мы видим, что как только посетитель вошёл в банк и миновал охрану, он попадает к банковскому служащему, который занимается денежными транзакциями. Его задача – не просто проводить транзакции, но и проверять права на их проведение у конкретных держателей счетов. OPC-серверы разных производителей OPC используют при подключении протокол DCOM, известный как объектный RPC (ORPC), фактически выполняющий роль охраны на входе в банк, и не предоставляют расширенных функций безопасности, выполняемых служащими банка.

Обеспечение безопасности приложений по отношению к OPC-серверу должно учитывать особенности технологии OPC и архитектуру OPC-сервера. Данные от OPC-сервера распространяются по всей сети предприятия, поэтому правильная защита в глубину является критически важной. Без неё возникает чрезмерное количество потенциальных угроз, влекущих за собой серьёзные последствия для безопасности системы, производства и окружающей среды.

Во многих инсталляциях OPC-серверов безопасность отдана на откуп корпоративному межсетевому экрану и настройкам DCOM. В то же время при использовании этих средств остаётся ряд известных уязвимостей. И даже корректная настройка всей системы не обеспечивает необходимого уровня безопасности. Дело в том, что корпоративные межсетевые экраны и служба Windows DCOM не инспектирует OPC-данные. Эффективную защиту могут обеспечить только те средства безопасности, которые спроектированы в соответствии со спецификацией OPC и подстроены под конкретный протокол.

Функции безопасности OPC-сервера

Любой OPC-сервер или продукт имеет возможность реализовать один из трёх уровней безопасности: отключена, DCOM и OPC-безопасность. Каждый уровень предлагает больше средств контроля и безопасности на основе проверки прав доступа того, кто подключается.

- *Безопасность отключена.* Это значит, что права запуска и подключения к OPC-серверу есть у всех, а права подключения есть у всех клиентов. OPC-

Как работает межсетевой экран для OPC-сервера?

Рис. 2. Проверка запросов на подключение

Рис. 3. Разрешение на подключение

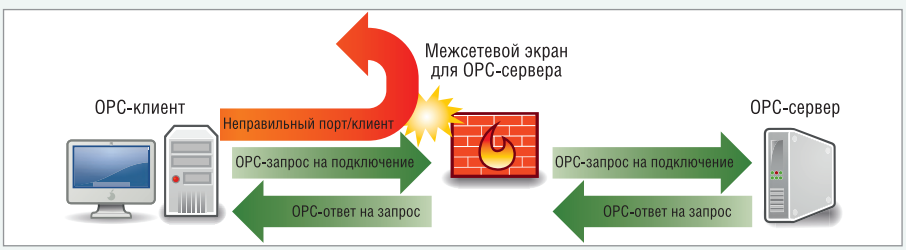

Рис. 4. Порт открыт

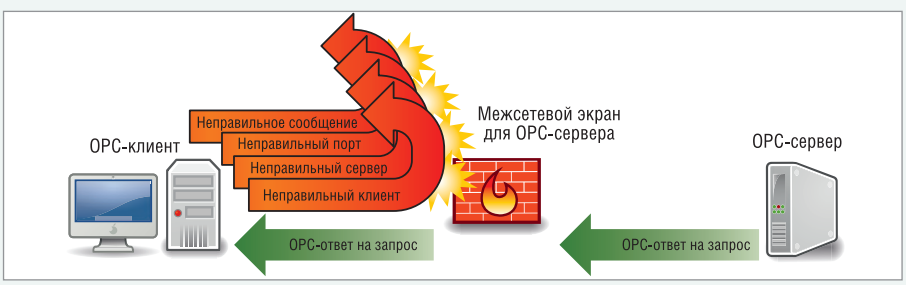

Рис. 5. Блокирование опасного трафика

На примере модуля Tofino OPC Enforcer рассмотрим пошаговую схему работы межсетевого экрана для OPC-сервера.

- Tofino OPC Enforcer перехватывает запрос на подключения от клиента к серверу OPC и проверяет следующее: является ли OPC-сервер разрешённым; разрешены ли подключения от данного клиента к серверу; правильно ли сформировано сообщение с запросом на подключение к серверу.
- Tofino OPC Enforcer перехватывает ответ от сервера и проверяет, правильно ли сформировано сообщение с ответом от сервера; послано ли оно именно тому клиенту, который его запрашивал; какой TCP-порт открыт сервером для клиента.
- Tofino OPC Enforcer немедленно открывает TCP-порт, указанный в ответном сообщении сервера, со следующими ограничениями: только для обмена данными выбранного клиента и сервера; только если клиент использует назначенный порт; только если установленная TCP-сессия начинается в указанный промежуток времени.
- Tofino OPC Enforcer блокирует опасный трафик в случае, если он получен от неавторизованного клиента или сервера, если подключение запрашивается к неправильному TCP-порту, если подключение пытается использовать чужой порт или RPC-запрос к серверу сделан неверно. ■

сервер не проверяет права доступа к любым функциям, заложенным разработчиками.

- *DCOM-безопасность.* Включён только компонент Windows DCOM. Права доступа и запуска OPC-сервера ограничены и распространяются на выделенных клиентов, равно как и права доступа для клиентских приложений. В то же время OPC-сервер не контролирует доступ к специализированным функциям безопасности. Этот уровень безопасности реализуется с помощью DCOM по умолчанию.
- *OPC-безопасность.* Поддерживает спецификацию безопасности OPC. OPC-сервер работает в качестве монитора для контроля доступа к специализированным функциям безопасности OPC. Данная опция может быть реализована самостоятельно или параллельно с DCOM.

Роли и безопасность на уровне пользователей

Спецификация безопасности OPC основана на проверке пользовательских прав доступа к серверу по специальным сертификатам. Она позволяет OPC-продуктам предоставлять специфические функции по добавлению, просмотру и чтению/записи индивидуальных параметров. В среде промышленного предприятия доступ к данным должен различаться в зависимости от должностных полномочий:

- инженерам АСУ ТП может понадобиться полный доступ к чтению и записи данных во всех точках системы;
- операторы системы могут иметь доступ только к определённым точкам или участкам системы, за которые они отвечают;
- управляющий персонал должен иметь права чтения основных параметров производительности системы.

Для правильной настройки безопасности приложения должны различать обстоятельства, при которых каждый пользователь запрашивает информацию. Создать дополнительный уровень безопасности на данном этапе может программный продукт MatriconOPC, базирующийся на спецификации безопасности OPC организации OPC Foundation. Программный шлюз контролирует права каждого пользователя на доступ, чтение и запись в конкретной точке. Такой высокоточный контроль гарантирует, что правильные данные будут переданы только соответствующим пользователям, и предотвратит несанкционированный доступ к данным на сервере.

Заключение

Инциденты, связанные с игнорированием вопросов безопасности OPC, будут возникать чаще вместе с увеличением спроса на OPC-технологии. История показывает, что причина большинства инцидентов, информацию о которых можно найти в виде отчётов в свободном доступе, заключается в неправильном использовании средств безопасности или в их отсутствии.

Специалисты АСУ ТП, знакомые с вопросами безопасности не понаслышке, кроме собственных наработок по обеспечению безопасности конкретной системы управления и отлаженной архитектуры OPC, применяют дополнительные средства безопасности, ориентированные именно на OPC-технологию. Современные средства способны обеспечить достаточный уровень безопасности существующей системы без замены и остановки работающего оборудования и глубоких знаний в области защиты в глубину. Программный шлюз данных MatriconOPC и модуль защиты OPC-данных Tofino OPC Enforcer – самостоятельные продукты, которые можно и нужно комбинировать в единой системе управления.

Реальность такова, что инциденты, связанные с безопасностью систем, не просто случаются с «другими людьми». С точки зрения дальновидности, имеет смысл подготовиться к неожиданностям заранее путём обеспечения безопасности OPC-данных до наступления последствий, которые будут дорого стоить.

Рекомендуемая литература

1. Darek Kominek, Eric Byres. Effective OPC Security for Control Systems – Solutions you can bank on [Электронный ресурс] // Режим доступа: http://www.tofinosecurity.com/effective-OPC-solutions.
2. Денисенко В.В. Компьютерное управление технологическим процессом, экспериментом, оборудованием. – М. : Горячая линия – Телеком, 2009.
3. Шахновский Г. Безопасность Систем SCADA и АСУ ТП [Электронный ресурс] // Режим доступа: http://www.security-bridge.com/biblioteka/stati_po_bezopasnosti/bezopasnost_sistem_scada_i_asutp/
4. Eric Byres. Using ANSI/ISA-99 standards to improve control system security [Электронный ресурс] // Режим доступа: http://web.tofinosecurity.com/download-the-white-paper-using-ansi-/-isa-99-standards-to-improve-control-system-security/ ●

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

Возможности и применения Eagle Tofino

Программный модуль Tofino OPC Enforcer, будучи загруженным в аппаратную платформу Eagle Tofino (рис. 6), обладает следующими уникальными возможностями:

- реализует технологию отслеживания подключений в промышленных протоколах;
- защищает протоколы OPC DA, HAD, A&E;
- автоматически отслеживает TCP-порты, номера которых присвоены OPC-сервером подключениям, и открывает эти порты на межсетевом экране Eagle Tofino;
- позволяет выявить путём специальной «санитарной проверки» OPC-запросы, сделанные не в соответствии со стандартом DCE/RPC;
- поддерживает множество клиентов и серверов одновременно;
- предлагает установить программируемую задержку для автоматического завершения подключений, срок давности которых истёк;
- просто настраивается и конфигурируется с помощью утилиты Tofino CMP.

Типовые применения:

- управление всем сетевым трафиком в системе, где используются протоколы OPC DA, HAD, A&E;
- защита передаваемых данных, которые направляются к базам данных и диспетчерским системам и от них;
- защита промышленных систем сбора данных;
- совместное применение с программным модулем Tofino VPN LCM для VPN-защиты OPC-соединений. ■

Рис. 6. Промышленный межсетевой экран Hirschmann Eagle Tofino с программным модулем обеспечения безопасности Tofino OPC Enforcer