РАЗРАБОТКА OPC WEB СЕРВЕРА ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ МЕЖДУ ПРОГРАММНО-ТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ

THE DEVELOPMENT OF OPC WEB SERVER FOR SECURE DATA TRANSFER BETWEEN HARDWARE AND SOFTWARE COMPLEXES

V. Kochetkov

Summary. this article deals with the problems of secure data transmission from software and hardware systems (PTC) within technological networks, as well as the use of OPC DA protocols present in most complexes for data transmission. The OPC DA/ HDA family of protocols, are vulnerable because they are based on DCOM (a Component Object Model extension used to communicate objects on different computers on the network), require 135, 139, 445, and 593 ports open to public access. These ports are operated by various kinds of network worms, there are a large number of exploits (exploits) available on the Internet. The solution in this situation is to develop a client that is installed directly on the server (local access to DCOM) and sends data through the open port in the firewall via HTTP. The use of" white lists " of IP addresses, different types of data encryption provide additional protection of the client-server connection and the transmitted data.

Keywords: HTTP, XML, OPC DA, OPC tag, multithreading, DCOM, encryption, Blowfish.

Кочетков Виталий Викторович
Ведущий инженер электронщик, АО «Интер РАО — Электрогенерация» филиал «Верхнетагильская ГРЭС»
kochetkov_vv@interrao.ru

Аннотация. В данной статье затрагиваются проблемы безопасной передачи данных с программно-технических комплексов (ПТК) внутри технологических сетей, а также использование для передачи данных протоколов OPC DA, присутствующих в большинстве комплексов. Семейство протоколов OPC DA/ HDA, являются уязвимыми, так как базируются на DCOM (расширение Component Object Model, используется для связи объектов на различных компьютерах в сети), требуют открытых для общего доступа 135, 139, 445 и 593 портов. Данные порты эксплуатируются разного рода сетевыми червями, существует большое количество эксплойтов (exploits), доступных в интернет. Выходом в данной ситуации является разработка клиента, устанавливаемого непосредственно на сервер (локальный доступ к DCOM) и отдающем данные через открытый в брандмауэре порт по протоколу HTTP. Использование "белых" списков IP адресов, разного вида шифрования данных создают дополнительную защиту соединения клиент — сервер и предаваемых данных.

Ключевые слова: HTTP, XML, OPC DA, OPC тэг, многопоточность, DCOM, шифрование, Blowfish.

Введение

За последние годы, с увеличением производительности процессоров и значительном прорыве в схемотехнике в целом, произошёл рост внедряемых в России Автоматизированных Систем Управления Технологическими Процессами — далее АСУ ТП. Контроллеры управляют работой Газотурбинных установок, перекачивающих станций, станций химводоочистки. Как правило контроллеры являются частью программно-технического комплекса (ПТК), в который помимо всего прочего входит программное обеспечение, предназначенное для сбора, обработки и хранения данных. Функционал ПТК определяется на этапе проектирования, и претерпевает некоторые изменения на этапе пуско-наладки. После того как объект сдан, внести какие-либо коррективы или дополнения без заключения нового договора часто бывает затруднительно (лицензионные соглашения, сохранение гарантии организации, производящей внедрение и наладку, отсутствие собственного квалифицированного персонала). А необходимость во внесении корректив и дополнений возникает достаточно часто. Например, парогазотурбинная установка далее ПГУ, аттестовалась в режим работы НПРЧ — Нормированное Первичное Регулирование Частоты [1]. Условием участия энергоблоков электрических предприятий в НПРЧ является выгрузка определённого набора данных, и отправка через интернет в Оперативно-Диспетчерское Управление — ОДУ. Другой вариант, несколько энергетических предприятий обязывают выгружать данные в единый производственно-технический отдел — ПТО, для осуществления контроля производственных процессов в том числе УРУТ — удельный расход условного топлива. Разные предприятия имеют разный состав оборудования и программного обеспечения, заключить договора на доработку на все предприятия не всегда возможно, например, устаревшее оборудование или финансово затратно.

Выходом из такой ситуации может быть написание собственной автоматизированной информационной системы — АИС, которую в процессе эксплуатации можно будет адаптировать под любые новые условия (автогенерация отчётов, автоматическая выгрузка данных).

```
<soap:Body>
  <ReadResponse xmlns="http://opcfoundation.org/webservices/XMLDA/1.0/">
    <ReadResult
      RcvTime="2003-05-27T00:15:36.6400000-07:00"
      ReplyTime="2003-05-27T00:15:36.7500000-07:00"
      ServerState="running"
    />
    <RItemList>
      <Items
        ItemName="Simple Types/UInt"
        Timestamp="2003-05-27T00:15:36.7343750-07:00">
        <Value xsi:type="xsd:unsignedInt">4294967295</Value>
      </Items>
      <Items
        ItemName="Simple Types/Int"
        Timestamp="2003-05-27T00:15:36.7343750-07:00">
        <Value xsi:type="xsd:int">2147483647</Value>
      </Items>
      <Items
        ItemName="Simple Types/Float"
        Timestamp="2003-05-27T00:15:36.7343750-07:00">
       <Value xsi:type="xsd:float">3.402823E+38</Value>
      </Items>
    </RItemList>
  </ReadResponse>
</soap:Body>
```

Рис. 1. Пример XML пакета OPC XML-DA при передаче трёх тегов.

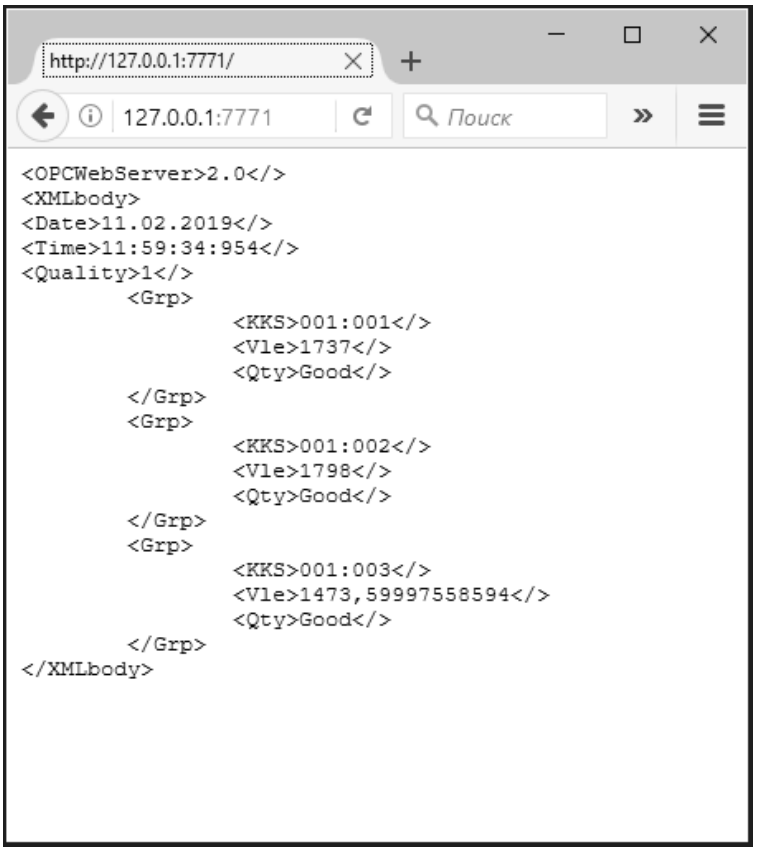

Рис. 2. Пример XML пакета разрабатываемого клиента при передаче трёх тегов.

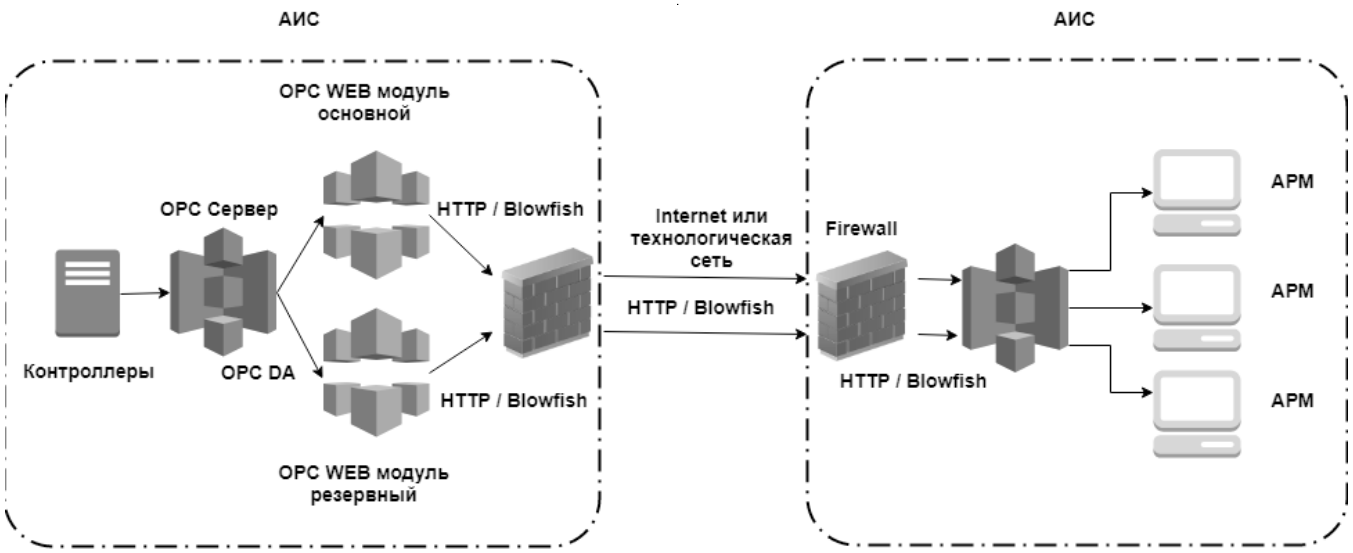

Рис. 3. Передача данных из одной АИС в другую через технологическую сеть.

Рассмотрим критерии OPC WEB сервера для сбора и передачи данных:

- Должен поддерживать интерфейс обмена данными с ПТК.
- Должен поддерживать многопоточность.
- Должен содержать интерфейс для обмена данными по протоколу HTTP.
- Иметь возможность сохранять данные в формате обмена данными CSV.
- Модуль сбора данных обязательно должен иметь резервирование.
- Для обеспечения безопасности должен уметь фильтровать TCP — соединения по белому списку.
- Иметь возможность шифровать данные, передаваемые по сети.

OPC WEB сервер должен обладать возможностью сбора данных с разных программно-технических комплексов, в том числе и с устаревших. Проведя исследование, выяснилось, что 92 процента ПТК, имеют установленный OPC DA [4] сервис. Данный сервис как нельзя лучше подходит для сбора данных. Разработка клиента OPC DA неплохо описана в статье Федоренко Д. Ю. [2], автор описывает простой клиент, способный получить список установленных OPC серверов. Используя один из интерфейсов (синхронное чтение, асинхронное чтение), просматривать данные только с одного OPC сервера за один раз. Наш же OPC WEB сервер, согласно критерию, приведённому выше должен получать данные одновременно с неограниченного количества OPC серверов за раз, для чего предполагается разработка класса описывающего интерфейс сбора данных по протоколу OPC DA. Создавая новый экземпляр класса для каждого OPC сервера, и инициализируя его внутри отдельного потока, получаем возможность сбора данных, где отдельные сервера не будут зависеть друг от друга, и неисправность одного, не повлияет на работоспособность других.

Для передачи данных в нашу автоматизированную информационную систему используем протокол HTTP, аналогично OPC XML-DA [3] (XML-Data Access), который не доступен в большинстве программно-технических комплексов, но имеет ряд положительных качеств, например, большинство программистов смогут подключиться к серверу по HTTP протоколу и получить данные из XML (не нужен высококвалифицированный программист), нет нужды разбираться в спецификациях протоколов обмена и распределения адресов данных. Другой особенностью нашей реализации передачи данных по HTTP является более сжатый формат передачи данных. Размер пакета данных при передаче 100 тегов в OPC XML-DA будет в несколько раз больше смотрим рисунки № 1 и № 2, что скажется на времени передачи данных по сети и как результат время обновления данных в АИС увеличится, что негативно скажется на качестве и достоверности данных.

Выгрузка данных в csv файл нужна в том случае, если возможен обрыв связи между АИС и OPC WEB сервером, например, находятся на большом расстоянии друг от друга и данные проходят через большое число коммутаторов, и при этом ПТК не имеет встроенного средства выгрузки данных в csv формате (например, в Ovation от Emerson возможно выгружать данные только по 10 минут с дискретностью 1 секунда). В случае обрыва связи, данные можно будет подгрузить в АИС из OPC WEB сервера. Периодичность сохранения должна настраи-

Рис. 4. Страница настройки OPC клиента.

ваться отдельно. Отличительной особенностью нашего OPC WEB сервера сбора данных от OPC XML-DA, является возможность резервирования, модули сбора данных могут быть запущены в паре как основной и резервный, которые работают параллельно, и при потере связи с одним АИС продолжит получать данные с другого, смотрим рисунок № 3.

Для обеспечения безопасности сервера и передаваемых данных OPC WEB сервер предполагается устанавливать локально, на сервер АИС, подключенный к контроллерам. Выход в технологическую сеть закрыть брандмауэром, в котором запретить подключения на все порты, кроме порта назначенного OPC WEB серверу (по умолчанию это порт 7771), смотрим рисунок ниже. По этому порту сервер сможет отдавать полученную с контроллеров информацию по протоколу HTTP.

Таким образом, мы предотвратим возможность заражения серверов сетевыми вирусами, и эксплуатацию уязвимостей DCOM при помощи эксплойтов. Для большей надёжности создадим "Белый" список, в который занесём IP адреса только тех компьютеров сети, которым разрешим обмен информацией с нашим OPC WEB сервером, все остальные подключения будут сбрасываться. При необходимости можно ввести дополнительный журнал, в который программа сможет записывать попытки нелегального подключения: время, IP адрес, количество попыток подключения. Фильтруя соединения по списку, всё равно остаётся вероятность подключения злоумышленника к нашим серверам, это так называемый спуфинг (spoofing attack от английского подмена). Это ситуация, когда человек или программа маскируется под другую программу (компьютер в сети), фальсифицируя данные о себе. В этом случае злоумышленник может получить доступ к данным. Такая проблема решается за счёт использования шифрования передаваемых данных, например паролем, ключом или сертификатом смотрим рисунок № . 5.

Теперь даже если злоумышленник используя разные ухищрения, подключится к серверу, его соединение будет сброшено, так как запросы от него будут не леги-

Рис. 5. Страница настройки безопасности сети.

тимными (OPC WEB сервер не распознает запрос, определит, что тот не зашифрован и согласно включенной опции “шифрование передаваемых данных”, закроет соединение). Нам предоставляется два криптографических алгоритма: Blowfish и AES, и один способ кодирования информации Base64. Фактически никакой защиты информации Base64 в себе не несёт, и при необходимости может быть легко вскрыт, по этой причине лучше использовать один из двух криптографических алгоритмов на выбор. Естественно все компьютеры, которые будут получать данные по сети от OPC WEB сервера, так же должны поддерживать данные криптографические протоколы.

Выводы и дальнейшие перспективы исследования.

Как показывает практика, автоматизированные информационные системы склонны к централизации. Локальные АИС сбора данных с разных технологических точек, объединяют в технологические сети, например для передачи полученных данных в единую информационную систему для хранения и обработки. С появлением сетей, появляются и риски заражения серверов и неправомерного доступа к информации, кругом лиц не имеющим на то права. Информационные системы электростанций не являются исключением, поэтому программное обеспечение для безопасной передачи данных по технологическим сетям будут развиваться. Обрастать криптографическими протоколами и методами контроля достоверности данных. Одновременно с этим будет увеличиваться количество поддерживаемого технологического оборудования, данные с которых необходимо передавать по компьютерным или радиосетям (промышленный WI-FI, радиорелейная связь). Из всего выше сказанного, можно сделать выводы, что OPC WEB сервер будет востребован на предприятиях с развитой информационной структурой (цеха автоматизированных систем управления технологическими процессами). Где необходима надёжная и безопасная система сбора и передачи коммерческих данных (учёт расхода газа, электроэнергии, горячей воды), всё, где обрывы связи и потери данных могут принести к многомиллионному ущербу.

ЛИТЕРАТУРА

1. Резервы активной мощности Единой энергетической системы России — стандарт СТО 59012820.27.010.001–2018, утвержденного приказом АО «СО ЕЭС» от 15.02.2018 № 32 http://so-ups.ru/fileadmin/files/laws/standards/st_rezerv_activ_150218.pdf
2. Федоренко Д. Ю. Программирование OPC клиентов на C++ и C#.
3. OPCFoundation — спецификация OPC XML-DA http://opcgate.ru/downloads/OPC%20XMLDA%20Specification.pdf
4. OPCFoundation — спецификация OPC DA http://opcgate.ru/downloads/OPC%20DA%20Specification.pdf
5. Панасенко Сергей. Алгоритмы шифрования. Специальный справочник. БХВ-Петербург 2009 г.

Журнал «Современная наука: актуальные проблемы теории и практики»

Ставропольская ГРЭС