УДК 621.3

УЯЗВИМОСТИ НИЗКОУРОВНЕВЫХ ПРОТОКОЛОВ КАК ИНСТРУМЕНТ ДЛЯ АТАКИ НА АСУ ТП

Плешко Д.Ю.

Научный руководитель – Сапожникова А.Г.

Промышленные системы управления (ICS, АСУ ТП) за последние годы вышли на принципиально новый уровень благодаря развитию информационных технологий и сети Интернет. Однако новый виток автоматизации несет свои проблемы: некорректное применение технологий защиты и обработки данных приводит к серьезным уязвимостям.

В связи с этим промышленные системы управления все чаще становятся мишенью для злоумышленников и киберармий. На смену отдельным червям Stuxnet (2010) и Flame (2012) пришли более изощренные схемы многоступенчатых атак. Так, для распространения трояна Havex в 2014 году хакеры взламывали сайты производителей ПО для управления промышленными предприятиями (SCADA) и заражали официальные дистрибутивы SCADA-систем, которые затем устанавливались на предприятиях, что позволило злоумышленникам получить контроль над системами управления в нескольких европейских странах.

Современные АСУ ТП представляют собой сложные многоуровневые архитектуры, глубоко интегрированные с остальной инфраструктурой предприятия.

Времена, когда программируемые логические контроллеры (PLC, промышленные контроллеры) могли находиться в одном сегменте сети вместе с КИС и интернет-серверами, постепенно проходят, и сейчас высокая сегментированность и иерархичность являются неотъемлемыми свойствами АСУ ТП. Эти свойства могут создать ложное ощущение безопасности инфраструктуры, поскольку на первый взгляд двумя основными точками проникновения в сеть предприятия для атакующего являются демилитаризованная зона и КИС. Таким образом, для того чтобы получить доступ в промышленный сегмент сетевой инфраструктуры, атакующий должен преодолеть множество межсетевых экранов, систем обнаружения и предупреждения вторжений и других систем защиты. К сожалению, многоуровневая инфраструктура все еще остается уязвимой по отношению к атакам с нижних уровней, причем эти уровни зачастую защищены гораздо хуже.

В качестве примера можно рассмотреть уязвимости в инфраструктурах, в состав которых входят устройства, использующие протокол HART для обмена данными. Этот протокол (дистанционно управляемый измерительный преобразователь, адресуемый через магистраль) представляет собой промышленный стандарт передачи данных для интеллектуальных полевых приборов. Он был разработан в конце 1980-х компанией Rosemount, а сегодня используется в промышленных устройствах множества производителей, в том числе ABB, Endress & Hauser, Emerson, Honeywell и др., чаще всего – для подключения датчиков и удаленных систем ввода-вывода к PLC. При помощи шлюзов HART и HART-модемов управлять устройствами HART можно и с компьютера. Предназначенные для этого программные средства включают в себя HMI-системы (SCADA), OPC-серверы (OLE for Process Control) и системы PAS (Plant Asset management Software).

HART является типичным протоколом со схемой передачи данных типа «управляющий – управляемый» (master – slave), когда PLC или компьютер отправляют некоторую команду датчику либо системе ввода-вывода, а тот, в свою очередь, присылает ответ. В основном его применяют для настройки удаленных устройств, а также для считывания их состояния. HART может использовать различные физические среды, но самая популярная из них – токовая петля (4–20 мА). Скорость передачи по ней составляет 1200 бод, при этом цифровой сигнал может накладываться на аналоговую составляющую.

В токовой петле за сигнал отвечает не напряжение, а ток, поэтому она более устойчива к помехам, так что длина линий HART может составлять до 3 км. Данные свойства, а также способность HART работать во взрывоопасных зонах (классов 0, 1 и 2) позволяют

использовать HART-устройства на объектах критической важности, таких как электростанции, химические заводы, нефтегазовые платформы и др. Типичные места применения RTU, использующих HART, – это зоны повышенной опасности. Кроме того, благодаря высокой дальности действия устройства HART можно размещать за территорией предприятия, например, для контроля утечек и экологической обстановки на электростанциях и химических заводах, на трубопроводах, подстанциях и магистралях в нефтегазовой промышленности, на электростанциях и в других местах, где датчик должен находиться на определенном расстоянии от контроллера или HMI.

Тем не менее, из-за использования токовой петли в качестве среды передачи данных протокол HART уязвим к различного рода атакам. Во-первых, злоумышленник может, подключившись к линии HART с помощью устройства с высоким импедансом, незаметно прослушивать линию, получая таким образом информацию об инфраструктуре. Во-вторых, он может перенастроить какой-либо датчик или подделать его. Например, если атакующий изменит адрес Polling ID датчика на новый, а потом ответит управляющему устройству со старым Polling ID, то PLC или компьютер будут считать, что работают с реальным датчиком, в то время как на самом деле это датчик поддельный, имитируемый злоумышленником. Возможность подделки данных от датчиков являет собой реальную угрозу безопасности АСУ ТП. Но это далеко не весь спектр проблем, который может возникнуть из-за слабой защиты линий HART.

Современные программные средства, работающие с HART, например, OPC-серверы и PAS-системы, обладают возможностью глубокой интеграции с другими элементами инфраструктуры, в том числе с системами MES (Machine Execution System) и ERP (Enterprise Resource Planning). Эта интеграция может проходить через PAS-системы, которые взаимодействуют с устройствами на базе HART при помощи спецификации FDT/DTM. Технология FDT/DTM создана FDT Group, чтобы упростить разработку систем PAS и работу с полевыми устройствами. В основе технологии лежат COM-контейнеры и COM-объекты, взаимодействующие между собой посредством XML-сообщений. Иными словами, данные, полученные от полевых датчиков, упаковываются в XML-сообщения и передаются в PAS-систему, откуда они могут быть переданы на более высокие уровни – в MES или ERP.

Если в компоненте, работающем с датчиком, недостаточно корректно реализована (или вообще отсутствует) фильтрация входных данных, то злоумышленник может, изменив конфигурацию или подделав датчик, вызвать инъекцию XML-кода внутри PAS-системы. Это чревато серьезными последствиями, поскольку в таком случае злоумышленник проникает на верхние уровни иерархии АСУ ТП, даже если они отделены от нижних при помощи МСЭ. Инъекция кода XML может привести к атакам отказа в доступе, чтению произвольных файлов, атаке на механизмы аутентификации и даже к выполнению произвольного кода в системе. Все это в худшем случае может спровоцировать полную компрометацию инфраструктуры как на нижних, так и на верхних уровнях.

Рассмотрим пример такой атаки, приведённой на рисунке 1.

Злоумышленник, получив доступ к токовой петле (1), сначала прослушивает проходящие по ней пакеты и таким образом получает информацию об инфраструктуре и устройствах, взаимодействующих с линией. После чего он отправляет специализированный пакет, который изменит определённые параметры датчика (в данном случае – параметр long tag, длинный символьный идентификатор) таким образом, чтобы стала возможной инъекция XML-кода. Либо он может использовать вышеописанную методику и подделать датчик посредством смены Polling ID. Поскольку размер обычного пакета HART редко превышает 70 байт, атакующему необходимо подгрузить дополнительные инструкции XML. Это можно сделать через ссылку на внешний документ. Когда PAS-система начнет взаимодействовать с датчиком (2), данные, содержащие инъекцию XML, передаются на уровень выше (3), в MES или другие системы. На этом уровне внедряется ссылка на XML-документ, находящийся на внешнем или локальном Web-сервере, после чего происходит загрузка внешней схемы XML

(4). Таким образом (5) атакующий может читать произвольные файлы на сервере с MES-системой или использовать методы SSRF для расширения диапазона атаки.

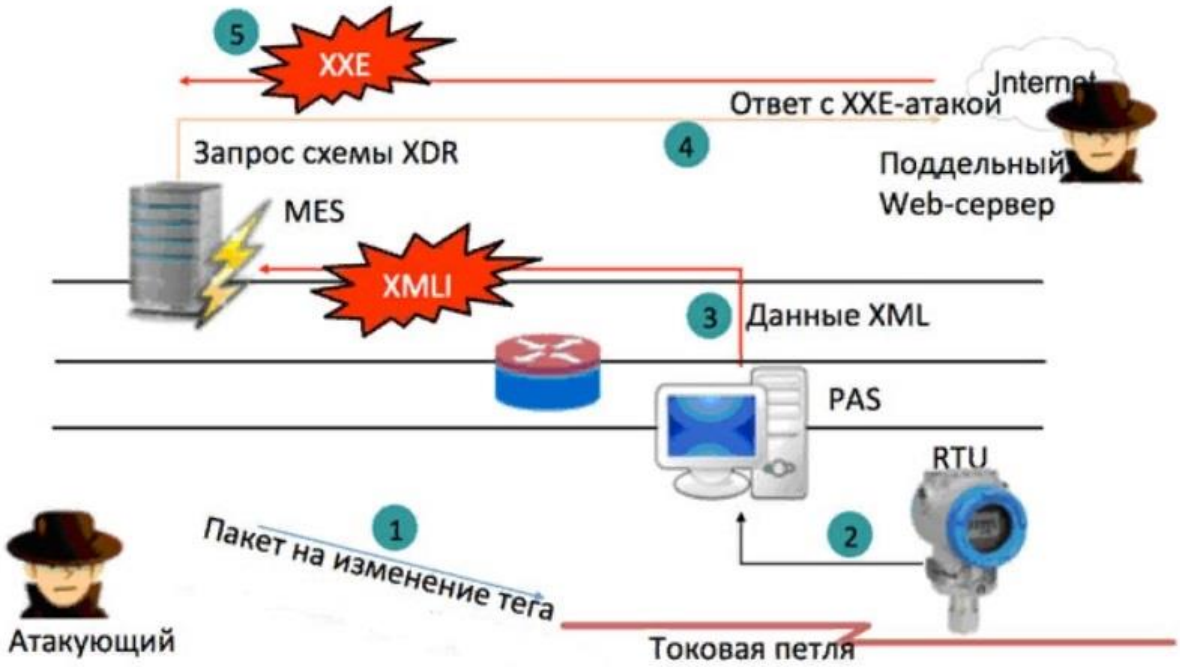

Рисунок 1. Схема хакерской атаки на нижние уровни

Так насколько сложно злоумышленнику получить доступ к линии токовой петли? Если устройства находятся вне территории предприятия, то зачастую линия HART – это три-четыре провода, которые могут быть упакованы в отдельный кабель-канал или использовать канал с другими промышленными линиями. Например, в нефтегазовом секторе такая линия может проходить параллельно с трубопроводом. Всё, что требуется от злоумышленника, – это получить кратковременный (5–10 минут) доступ к линии. Причём не обязательно нарушать её целостность – при определенных конфигурациях достаточно просто подключиться к ней.

Какими могут быть последствия такого рода атак? Помимо вышеперечисленных возможностей по подделке показаний датчиков, перехвату управления актуаторами, атакам отказа в доступе на HMI-, OPC- и PAS-системы, чтению произвольных файлов существует гораздо более страшная угроза по отношению к инфраструктуре: в случае успешной компрометации MES- или PAS-системы за счет глубокой взаимосвязи компонентов в АСУ ТП злоумышленник может перехватить контроль над всем производственным процессом, от нижних уровней до верхних.

Это становится возможным благодаря тому, что при сегментировании и изолировании различных АСУ ТП пока редко учитывается тот факт, что атака извне может произойти не только со стороны Интернета или КИС, но и с уровня промышленных протоколов или полевых устройств.

Какие меры можно принять для защиты? К сожалению, в случае использования протокола HART остается лишь гарантирование физической безопасности линий токовой петли. Кроме того, необходимым является аудит инфраструктуры АСУ ТП, в том числе и программных средств, интегрированных с HART, для того чтобы злоумышленник, даже получив доступ к токовой петле, не смог проникнуть на другие уровни и сегменты инфраструктуры.

Современные подходы к проектированию инфраструктур АСУ ТП позволили устранить старые болезни в области информационной безопасности таких систем. Тем не менее, усиливая защиту верхних сегментов системы (КИС, ДМЗ и др.), не стоит забывать и

про защиту нижних уровней, так как вектор атаки может быть направлен не только сверху вниз (из КИС/Интернета к ПЛК/полевым устройствам), но и наоборот: от промышленных шин передачи данных между полевыми устройствами – на уровни MES, ERP и в конечном итоге КИС.

Перечисленные выше факты указывают на гипотетическую возможность влияния уязвимостей низкоуровневых протоколов на решения, принимаемые на основе данных АСУ ТП, что в свою очередь свидетельствует об относительной небезопасности систем, использующих в своём составе устаревшие протоколы.

Литература

1. Казиев, В.М. Введение в системный анализ и моделирование / В.М. Казиев. – М. : ИНТУИТ, 2001. – 72 с.

2. Чичкарёв, Е.А. Системный анализ сложных систем управления / Е.А. Чичкарёв. – Пермь : ПГТУ, 2005. – 59 с.