Безопасность АСУТП

Е.М. Литвинов (Компания Digital Security)

Рассмотрены возможные сценарии атак на объекты АСУТП. Причем вместо «классических» сценариев, когда атака начинается на корпоративную сеть с целью попасть в технологическую сеть, приведены возможные сценарии, когда векторы атак начинаются с уровня датчиков/полевых шин.

Ключевые слова: кибератака, датчики, полевые шины, информация из открытых источников, беспроводные технологии, промышленные коммутаторы.

Начнем с очевидного и неочевидного, а именно с того, что важную информацию можно получить из открытых источников. В сети Internet выложены презентации различных докладов, раскрывающие структурные схемы различных критически важных и потенциально опасных объектов, например АЭС. Читатели легко могут это проверить. Кроме того, автор держал в руках буклет известной зарубежной компании — производителя средств коммуникации промышленного назначения, в котором описывались типовые решения по построению АСУТП на базе ее продукции. Также в проспекте были приведены достаточно детальные схемы построения АСУТП на различных объектах: ГЭС, ТЭЦ и др. Информация была дополнена данными о том, какое именно оборудование применялось для построения технологической сети.

Рис. 1

Возможно, кто-то не воспринимает всерьез риски, которые влечет за собой публикация информации в открытых источниках. Для пояснения ситуации рассмотрим два примера.

Предположим на «безобидном» слайде презентации отмечено, для передачи данных о радиационной обстановке АЭС используется радиоканал. Данная информация в значительной степени облегчает задачи как прослушивания трафика, так и подмены трафика для потенциального злоумышленника.

Другая презентация демонстрирует состав сейсмической сети мониторинга некоторого промышленного объекта. На схеме отмечено, что показания с сейсмодатчиков, которые расположены за пределами охраняемого периметра, поступают в центр сбора информации. В свою очередь, с этим узлом связан блок аварийных защит. Таким образом, злоумышленник может подключиться к сейсмодатчикам, изменить и/или подменить их показания и спровоцировать аварийный останов промышленного объекта. К радиоактивному загрязнению это не приведет, но последующий запуск энергоблока может быть затруднен.

Как следствие, обретает значимость обеспечения безопасности АСУТП и такой ее аспект, как «физическая безопасность».

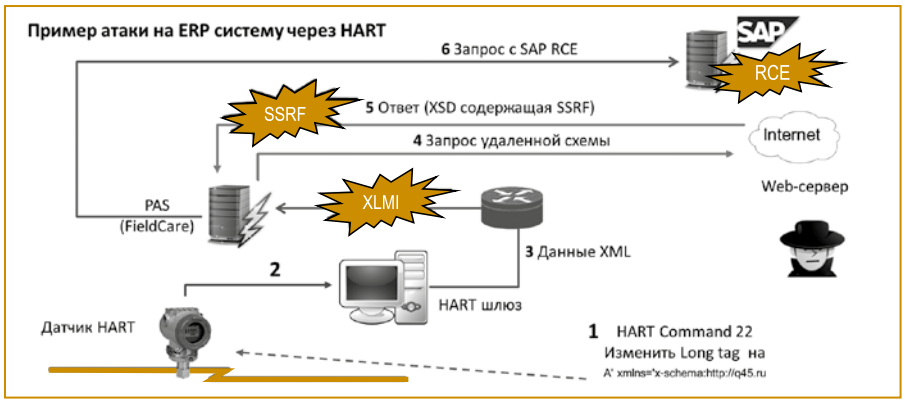

Рис. 2. Пример атаки на EPR-систему через HART-датчик, где RCE – Remote code execution, SSRF – Server-Side Request Forgery, XSD – язык описания структуры XML документа, PAS – Plant Asset Management , XMLI – программный интерфейс для работы с XML

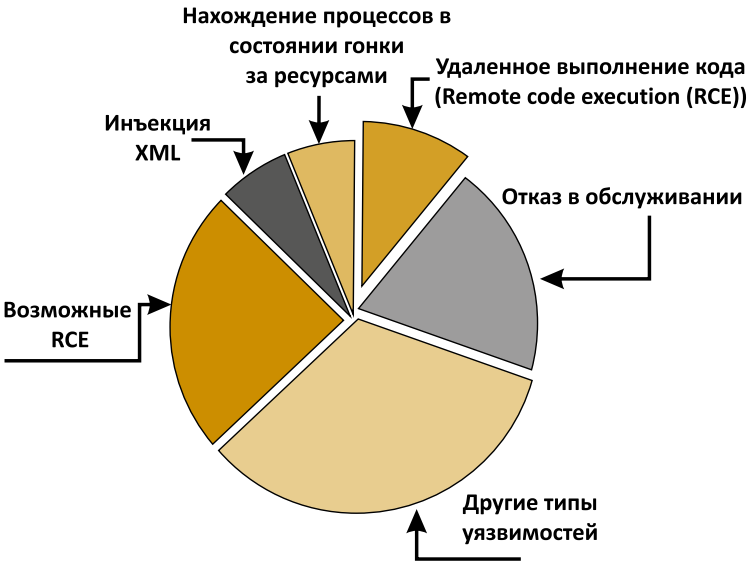

Рис. 3. Число уязвимостей по типам

Таблица. Виды уязвимостей при использовании мобильных приложений

Тип приложения	*Угрозы*
Пульт управления	- отказ в обслуживании или компрометация сервера - отсутствие на стороне сервера проверки данных с точки зрения промышленного процесса - компрометация хранимых данных, потенциально ведущая к изменению интерфейса или функциональности (для ЧМИ приложение) - отказ в обслуживании клиента
Клиент для OPC/MES или система архивации	- утечка информации о процессе через уязвимость протокола - отказ в обслуживании или компрометация сервера - обман оператора для сокрытия сигнала тревоги
Удаленное управление SCADA	- компрометация процесса через уязвимость в протоколе или приложении - отсутствие на стороне сервера проверки данных с точки зрения промышленного процесса - компрометация процесса через уязвимость сервера - отказ в обслуживании или компрометация клиента

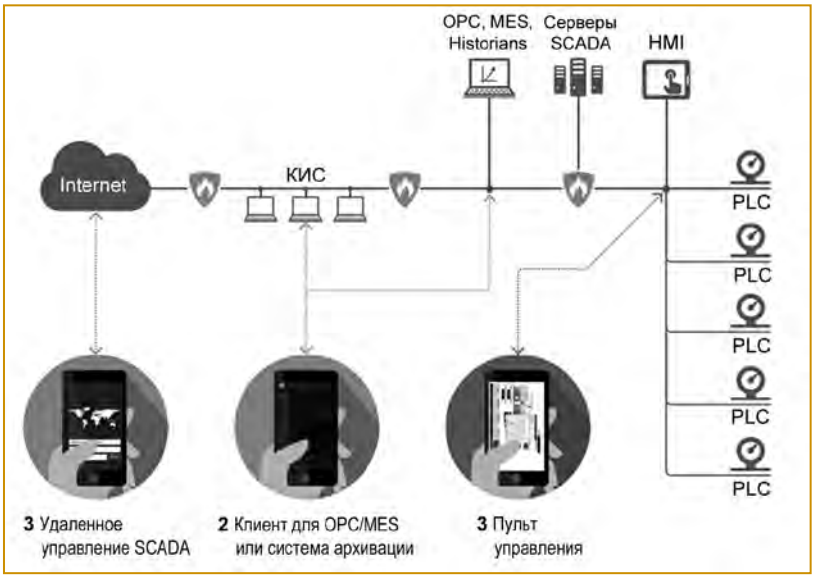

Рис. 4. Уязвимости в случае применения мобильных/беспроводных технологий

Датчики как причина уязвимостей АСУТП

Говорить о том, что АСУТП сегодня полностью изолированы от внешнего мира, несколько ошибочно [1]. На рис. 1 показано, что на трубопроводах могут применяться различные датчики, к которым можно получить непосредственный доступ, поскольку они находятся за охраняемым периметром. Могут использоваться различные беспроводные технологии (Wireless HART, ISA100.11a). Как известно, к беспроводному датчику реально подключиться, находясь на расстоянии от этого устройства. В этом случае злоумышленнику нет необходимости проникать через забор, а достаточно оказаться рядом с беспроводной сетью, чтобы иметь возможность подсоединиться к технологической сети.

Продолжая тему датчиков, вспомним, что их внутренняя структура включает несколько разных микроконтроллеров, а также микросхемы внешней памяти. Фактически это означает, что датчик имеет достаточную вычислительную мощность, чтобы в случае его заражения выступить уже в качестве отдельного вычислительного узла, который сможет заражать другие датчики или как-то влиять на ТП.

Для подтверждения того, что современные «умные» датчики таят в себе опасность, в рамках компании Digital Security было проведено исследование, посвященное атакам через HART-датчик, которые можно развить до уровня ERP-систем [2]. На рис. 2 представлен возможный сценарий атаки как на технологическую, так и на корпоративную сеть со стороны полевых шин/датчиков.

Сначала злоумышленник подключается к удаленному HART-датчику и меняет в нем некоторые установки. Далее эти параметры через HART-шлюз попадают в PAS-систему. Для файервола и для PAS это будут валидные данные, но PAS-система может их трактовать, как команду на запрос удаленной схемы/данных. Ответ на этот запрос может уже содержать SSRF. А это позволит развить атаку уже до корпоративной сети предприятия. Также в ходе этого исследования было изучено программное обеспечение, которое работает с различными датчиками (рис. 3).

В ходе исследования было выявлено более 500 уязвимостей из более чем 700 исследованных устройств. Порядка 30% уязвимостей могут привести к выполнению произвольного кода/команд. Имеется возможность «подделать» устройства нижнего/полевого уровня, что может вызывать изменение ТП. Уязвимости в XML позволяют расширять атаку до корпоративной сети.

Мобильные/беспроводные технологии

Отдельной угрозой для современных АСУТП могут служить решения на основе мобильных/беспроводных технологий, предлагаемые крупнейшими вендорами (рис. 4). Все многообразие уязвимостей в этом случае можно разделить на три основных группы (таблица):

— мобильные приложения, позволяющие управлять SCADA удаленно;

— OPC/MES-клиенты, позволяющие подключаться к технологической сети, находясь в корпоративной сети;

— мобильные пульты управления, позволяющие подключаться к технологической сети и, например, изменять настройки ТП.

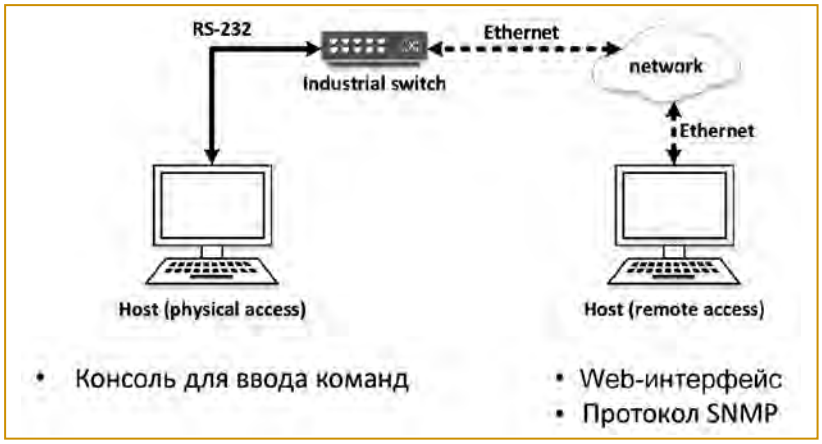

Рис. 5. Возможности подключения для конфигурирования и обновления прошивки

В ходе исследования было рассмотрено 20 приложений для ОС Android, которые так или иначе взаимодействуют с инфраструктурой АСУТП. При этом не было найдено ни одного приложения без недостатков и/или уязвимостей.

Промышленные коммутаторы

В завершение остановимся на еще одном возможном векторе атак, который на первый взгляд не является очевидным. Атака может начаться со стороны промышленных коммутаторов.

Были изучены изделия двух известных зарубежных компаний. Условно назовем их А и Б. На рис. 5 показаны возможные способы подключения к данным коммутаторам.

Промышленный коммутатор фирмы А работает под управлением ОС VxWorks вер. 5.4.2. На текущий момент последняя версия ОС VxWorks 7. В версии 5.4.2 используется линейное адресное пространство, отсутствуют механизмы защиты от эксплуатации бинарных уязвимостей. Для данной версии ОС существует не менее 10 зарегистрированных CVE. Отсутствует защита от переполнения в стеке и динамической памяти.

Ситуация с изделием фирмы Б несколько лучше, поскольку он работает под более свежей версией ОС — 6.1. Но здесь также отсутствуют механизмы защиты от эксплуатации бинарных уязвимостей.

Однако при непосредственном подключении к данным промышленным коммутаторам через RS-232 имеется беспрепятственная возможность обновить прошивку. Отсутствует проверка подлинности прошивки. А это открывает прекраснейшую возможность для реализации эшелонированной атаки как на технологическую сеть, так и на корпоративную. Не стоит исключать сценарий, согласно которому во время транспортировки злоумышленник может подменить прошивку с оригинальной на модифицированную для реализации атаки MiTM (непосредственно на коммутаторе) без видимых внешних эффектов благодаря достаточно мощным CPU, применяемым в данных коммутаторах.

Предусмотрена возможность подключиться к данным коммутаторам через Ethernet с помощью протокола SNMP v1 и изменить те или иные настройки. В коммутаторе фирмы А может использоваться и более защищенный SNMP v3, но по умолчанию включен SNMP v1.

Заключение

В заключение отметим, что современные АСУТП представляют собой достаточно сложную и в какой-то мере открытую систему. Сегодня начинают применяться различные smart-датчики, которые помимо измерения физической величины могут производить самодиагностику. Применяются различные беспроводные технологии, которые позволяют снизить стоимость построения технологической сети; удаленные каналы как для мониторинга, так и для управления технологической сетью. С одной стороны, все это способствует увеличению эффективности работы АСУТП, но с другой, — это открывает дополнительные возможности для злоумышленников.

Список литературы

1. *Евдокимов Д.С.* Разработка эксплойтов для АСУТП: двойная игра // Автоматизация в промышленности. 2015. №2.
2. *Юшкевич И., Большев А.* SCADA и мобильники: оценка безопасности приложений, превращающих смартфон в пульт управления заводом Исследовательский центр Digital Security. 2017. https://dsec.ru/upload/medialibrary/492/49277618bcf63a2550f21561cf81a968.pdf.

Литвинов Егор Михайлович *– ведущий специалист по безопасности АСУТП компании Digital Security. Контактный телефон +7 (495) 223-07-86.*