Безопасность (и/или) АСУТП

В.С. Белов, А.А. Брызгин (Group-IB)

Отмечена необходимость повышения уровня взаимодействия и взаимопонимания между специалистами по автоматизации и информационной безопасности. Перечислены типовые этапы ручного анализа файла прошивки ПЛК, позволяющего выявить скрытые механизмы управления устройством.

Ключевые слова: АСУТП, ПЛК, кибератака, анализ файла прошивки, реверс-инжиниринг.

Безопасность ТП критична для большинства промышленных систем, поскольку воздействие на эти процессы может повлечь за собой не просто компрометацию учетных записей, раскрытие чувствительных данных или финансовые потери. Следствием таких воздействий может быть остановка обеспечения важными ресурсами и даже экологические и социальные катастрофы.

Ключевым моментом, определяющим безопасность современной промышленной системы, можно назвать то, что во времена «начальной автоматизации» никто не задумывался об обеспечении защищенности узлов управления промышленных систем. Решения были громоздки, дороги и недоступны для удаленного изучения. Подобная ситуация наблюдалась и с компьютерными системами, и сетями до тех пор, пока червь Морриса не привлек внимание к компьютерной и сетевой безопасности.

2 ноября 1988 г. в США более 6 тыс. узлов сети Internet (на тот момент - ARPANET) фактически утратили работоспособность на значительное время. Причиной этого стала программа аспиранта Корнелльского университета Роберта Морриса.

Разрушительное действие программы объяснялось не злым умыслом Морриса, а ошибкой в алгоритме, но ситуация имела далеко идущие последствия.

Именно этому инциденту мы обязаны появлением индустрии информационной безопасности, а также структуры CERT (Cyber Emergency Response Team) – команды реагирования на инциденты кибербезопасности, одна из которых (единственная коммерческая в РФ) работает в Group-IB.

В случае безопасности технологий промышленной автоматизации подобный переломный момент наступил лишь в 2010 г. с появлением первого вредоносного файла Stuxnet, нацеленного на АСУТП иранских обогатительных станций. ПО содержало высококачественный код, эксплоиты повышения привилегий, а также ранее неизвестные 0day-эксплоиты, имело возможности самораспространения в сети и с помощью флеш-накопителей. Появление червя Stuxnet заставило во многом пересмотреть взгляды на безопасность АСУТП, комплексный подход к которой до этого практически не рассматривался. Хотя даже сейчас, когда «эхо Stuxnet'а» затихло, и было выявлено еще несколько мощных вредоносов для систем автоматизации уровня ТП, подход к безопасности многих вендоров все еще остается на уровне 90-х гг. XX века.

Взаимодействие специалистов по автоматизации и информационной безопасности

Кроме того, существует и проблема коммуникаций между специалистами по компьютерной безопасности и технологиям автоматизации. Существенно затрудняет взаимопонимание разность приоритетов в классической триаде безопасности (Конфиденциальность, Целостность, Доступность). Классические «безопасники» по привычке используют «КЦД», специалисты же по автоматизации резонно предпочитают «ДЦК», так как остановка большинства элементов в серьезном ТП может нанести ущерб, несравнимый с разглашением даже очень важных сведений. Внеплановая остановка доменной печи зачастую приводит к необходимости возводить новую печь, ну а к чему приведет задержка при открытии/закрытии задвижек на опасном химическом или ядерном производстве не хочется даже думать. Диалога же о приоритезации характеристик информации не происходит, каждый остается при своем мнении, а системы автоматизации продолжают зиять сквозными дырами.

Специалисты по автоматизации искренне и совершенно справедливо удивляются, когда для защиты коммуникаций по небезопасному протоколу им предлагают поставить «в разрыв» некое устройство, которое неизбежно снизит надежность системы в целом, а для встраивания которого, систему, а значит и весь ТП придется приостанавливать. Ведь именно надежности и непрерывности ТП добиваются многие годы.

Вносят свой вклад во всеобщее непонимание и разработчики систем автоматизации, отказывающиеся дорабатывать прошивки и протоколы и непонимающие своей главенствующей роли в битве с уязвимостями в системах автоматизации ТП.

Кроме того, даже те специалисты по безопасности, для которых защита ТП является профильной деятельностью, не всегда хорошо ориентируются в разновидностях систем автоматизации. Одному из авторов на профильной конференции довелось модерировать секцию, посвященную безопасности АСУТП, и участвовать в горячей полемике. Участник конференции предлагал прогнать специалиста по безопасности за то, что тот не смог расшифровать аббревиатуру «АСУЗ».

При этом хорошему специалисту по безопасности ПО для успешного выполнения задач анализа

Рис. 1. Найдена одна Web-панель управления, требующая авторизации

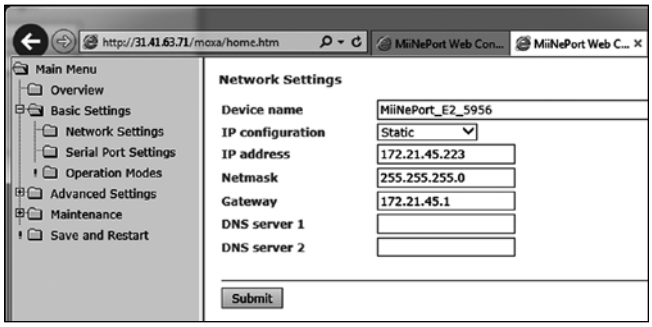

Рис. 2. Найдена другая Web-панель управления. Авторизации не требуется

защищенности прошивок и протоколов совершенно необязательно знать терминологию, а в большинстве случаев и функционал защищаемых систем. И этот пример наглядно иллюстрирует сложности работы на пересечении двух отраслей, площадь которого (пересечения) постоянно растет.

Уязвимое звено

Одним из основных элементов, отвечающих непосредственно за реализацию ТП, и в то же время, одной из ключевых точек входа проверки на уязвимость АСУТП, является ПЛК.

Основные проблемы, связанные с безопасностью ПЛК:

• отсутствие стандартизации: ПЛК построены на базе разных платформ, с использованием разных операционных систем;

• для контроля над ПЛК обычно достаточно нахождения с ним в одном сегменте сети. Зачастую подсистема авторизации в ПЛК не представлена вовсе (рис. 1 и 2), либо присутствуют стандартные/легкоугадываемые реквизиты доступа. Для получения доступа к ПЛК бывает достаточно знать его сетевой адрес и протокол взаимодействия с ним либо просто запустить сервисную утилиту под конкретный ПЛК;

• поскольку ПЛК могут находиться в труднодоступных, опасных местах и/или на значительном удалении от обслуживающего персонала, практикуется вынесение функционала обновления компонентов системы в Web-панель управления и HMI-интерфейсы. Фактически это может означать полную доступность ПЛК любому человеку через Internet.

Для иллюстрации рассмотрим поиск ПЛК на предмет потенциально доступных во внешней сети устройств в публичной базе знаний Shodan. Введем в строку поиска название вендора либо модель контроллера, и поисковик предложит определенное число доступных во всем мире устройств с FTP, HTTP либо SSH-доступом к ним. Большой вопрос, какая часть из этих устройств встроена в рабочие системы, а какая является публичными демонстрациями и ловушками-honeypot, однако изучить настройки контроллера и механизмы обновления прошивок сегодня может даже неподготовленный пользователь. Для подготовленного злоумышленника есть и более изощренные способы поиска и изучения ПЛК.

Согласно информации авторитетного ресурса по исследованию информационных «дыр» cvedetails.com, а также проекта Metasploit, специализирующегося на предоставлении информации об уязвимостях, помощи в создании сигнатур для IDS, создании и тестировании эксплойтов, современные ПЛК могут иметь разного рода уязвимости, в том числе, удаленного отказа в обслуживании. То есть удаленный злоумышленник может отправить специально сформированный пакет, что повлечет за собой временное прекращение нормальной работы контроллера.

Но наиболее критичными воздействиями на контроллер являются его удаленная перезагрузка, отключение либо переконфигурирование, модификация прошивки.

Анализ файлов прошивок ПЛК

Основной методикой поиска расширенных команд управления системой, заложенных производителем является реверс-инжиниринг ОС контроллера.

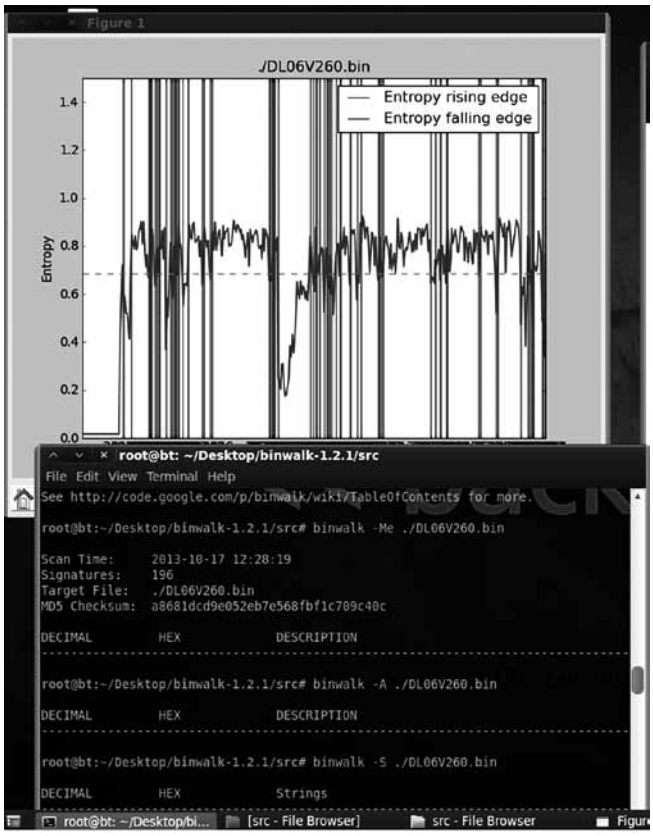

Рис. 3. Анализ исследуемой прошивки в программе Binwalk

Его результатом может быть выявление скрытых команд управления устройством, скрытых служб либо недокументированных сервисных учетных записей. Иногда файлы ОС устройства предоставляются на официальном сайте вендора в свободном доступе, иногда их можно извлечь только с запущенного реального устройства.

Исследование прошивки контроллера — нетривиальная задача, поскольку заранее неизвестен ни ее формат, ни архитектура процессора, для которого она собрана, ни форматы упаковки данных внутри ОС. Практика показывает, что прошивка чаще всего находится в неизвестном либо недокументированном формате. В этом случае извлечение и иследование содержимого возможно в результате реверс-инжиниринга специализированных утилит для работы с заданным типом прошивок.

Хорошим методом для автоматизации исследования файлов прошивок контроллеров является использование утилит для автоматической обработки и извлечения встроенных упакованных контейнеров, определения типа прошивки по известной базе сигнатур, а также поиска встроенного исполняемого кода. Речь о таких утилитах, как signsrch, offzip, TrID, binwalk (рис. 3).

Типовыми шагами при ручном анализе файла прошивки являются:

- извлечение текстовых строк из прошивки;
- анализ встроенной служебной информации, которая может указывать на способы хранения данных. Наиболее популярные форматы — Ar, YAFFS2, JFFS2, SquashFS, CramFS, ROMFS, UbiFS, xFAT, NTFS, ext2fs/ext3fs/ext4fs, iHEX, SREC/S19;
- поиск служебных заголовков и идентификация алгоритмов упаковки данных;
- идентификация набора инструкций архитектуры процессора. Наиболее популярны прошивки, содержащие код с инструкциями для процессоров ARM и PowerPC;
- дизассемблирование/декомпиляция прошивки;
- восстановление символьной информации;
- исследование используемых протоколов сетевого взаимодействия;
- выявление недокументированных возможностей;
- выявление предустановленных реквизитов доступа.

Анализ прошивок большинства современных контроллеров позволяет выявить скрытый функционал, уязвимые конструкции, «вшитые» учетные данные.

Недоступность контроллеров для изучения потенциальными злоумышленниками и так называемый «воздушный зазор» между ПЛК и внешними сетями — факторы, долгое время обеспечивавшие относительную защищенность АСУТП, постепенно теряют свою актуальность. Известные атаки на АСУТП можно считать лишь первыми признаками грядущей революции в понимании необходимости защиты промышленных систем. Подход «Security through obscurity» давно себя скомпрометировал.

Путь к победе

Игнорировать наличие уязвимостей только на основании того, что система не имеет связей с внешней сетью — по меньшей мере недальновидно. Подрядчики, которые ленятся выезжать на объект для конфигурации системы; обслуживающий персонал, желающий контролировать состояние систем даже из дома; инсайдеры, чей след виден в большинстве современных атак и заражений — все эти персонажи способны «показать большой мир» промышленной системе.

Решить описанные проблемы специалисты разных предметных областей могут только сообща. Главное, регулярно собираться в формате «АСУТПшники, безопасники, разработчики систем» и обсуждать насущные вопросы и приемлемые для всех варианты решения. Терпеливо объяснять друг другу особенности своей сферы деятельности без подколов и упреков и делиться опытом. Так победим!

Белов Виктор Сергеевич *– главный специалист по анализу защищенности ПО и исследованию вредоносного кода;*
Брызгин Андрей Александрович *– руководитель направления "Аудит и Консалтинг" Group-IB.*
Контактный телефон (495) 984-33-64.
E-mail:bryzgin@group-ib.ru
http://www.group-ib.com

«Газпром добыча Астрахань» создаёт интеллектуальное месторождение с использованием передовых технологий

ООО «Газпром добыча Астрахань» внедрило технологии Emerson для сбора данных от интеллектуальных устройств на Астраханском газоконденсатном месторождении. Использование программного приложения AMS Device Manager компании Emerson обеспечивает повышенные меры безопасности ведения технологических процессов, снижение эксплуатационных затрат и позволяет повысить качество и увеличить выработку товарной продукции за счет снижения простоев технологического оборудования.

На Астраханском промысле насчитывается более 6000 интеллектуальных приборов – оборудования нового поколения, способного по стандартному аналоговому каналу предоставлять дополнительную информацию о техническом состоянии прибора. Информация, поступающая от системы диагностики, сочетается с сигналами основных измерений и поступает в промысловую базу данных с соответствующими метками достоверности. Это позволяет не только осуществлять качественный контроль над месторождением, но и принимать превентивные меры, направленные на поддержание бесперебойной работы оборудования, и использовать с высокой степенью безопасности актуальные данные в системах автоматического регулирования ТП, применяемых на месторождении.

http://www.Emerson.com и *www.emersonprocess.ru*