Информационная безопасность АСУ ТП

Лабораторная работа №3. Анализ прошивок промышленных устройств.

1. Теория

На уровне автоматического управления АСУ ТП основными компонентами являются промышленные логические контроллеры (ПЛК) и промышленные сетевые устройства — коммутаторы, маршрутизаторы, преобразователи. Компрометация любого из данных устройств может привести к компрометации всей системы. Таким образом, важной задачей является исследование безопасности промышленных устройств. Одним из компонентов такого исследования является анализ прошивки промышленного устройства — главного программного компонента устройства. Как правило, прошивка разрабатывается под конкретную модель и поставляется производителем устройства.

Актуальную версию прошивки в некоторых случаях можно найти на сайте производителя устройства. Другим способом ее получения является снятие дампа памяти непосредственно с устройства и анализ полученного слепка. Обновление прошивки устройства, как правило, происходит вручную, зачастую с помощью специального программного обеспечения и с использованием проприетарного протокола.

Файл обновления прошивки может быть сжат, зашифрован, иметь цифровую подпись. Первым этапом исследования является определение возможности распаковки прошивки. Удобным инструментом для этого является ПО binwalk (https://github.com/ReFirmLabs/binwalk). Оно помогает установить структуру файла, проанализировать энтропию файла, установить архитектуру команд, и многое другое.

В случае, если binwalk поддерживает формат сжатия данных, эти данные также можно разархивировать с помощью binwalk. Если формат сжатия данных неизвестен, и при этом файл не зашифрован, следующим шагом становится ручной анализ структуры файла обновления прошивки. Как правило, в заголовке файла должна содержаться основная информация о файле — размер заголовка, размер данных, информация о модели, дата создания, и другая. Установление этих полей и восстановление структуры файла обновления прошивки вручную может быть нетривиальной задачей.

Вторым этапом исследования является реверс-инжиниринг прошивки. Основная цель реверс инжиниринга — поиск уязвимостей в сетевых функциях и в функциях безопасности (авторизация, взаимодействие с паролями и так далее).

Целью данной лабораторной работы является знакомство с первым этапом анализа безопасности прошивок промышленных устройств — анализом структуры файлов обновления прошивок промышленных устройств.

2. Задание

1. Для приведенных в разделе 3 лабораторной работы промышленных устройств провести анализ файлов обновления прошивок. Конечной целью анализа является нахождение участков файла, содержащих код. Данный анализ должен включать в себя:
   1.1. Анализ энтропии файла. Построение графика изменения энтропии файла в зависимости от смещения данных от начала файла.
   1.2. Анализ структуры файла, распаковка файла (в случае возможности автоматической распаковки).
   1.3. Определение участков файла (файлов), содержащих код.
   1.4. Анализ архитектуры команд.
   1.5. Поиск строк, содержащих чувствительные данные (например, пароли).
2. Составить отчет о проделанной работе. Отчет должен содержать в себе:
   2.1. Краткое описание исследуемого устройства, его назначение.
   2.2. Подробное описание результатов выполнения пункта 1 лабораторной работы.

3. Список устройств

Вариант	Устройство
1	KNX Wiser
2	Moxa ioLogik E2210
3	Advantech Adam-6100PN

Номер варианта определяется как $(Nmod3 + 1)$, где N — номер студента в списке группы.