СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

М. В. Сокол

Белорусский государственный университет, г. Минск;
masha.sokal.gmail.com
науч. рук. – В. В. Краснопрошин, д-р тех. наук, проф.

Задача, рассматриваемая в настоящей работе, возникла в сфере компьютерной безопасности. Исходная постановка задачи такова: имеется система управления железнодорожным транспортом и узлами, являющаяся критической инфраструктурой. Требуется создать для нее надежную систему защиты информации с учетом особенностей критических инфраструктур. В работе определяется методология создания системы защиты информации для критической инфраструктуры, выбираются механизмы защиты информации с учетом ограниченных ресурсов устройств и высокой распределенности критической инфраструктуры.

Ключевые слова: критическая инфраструктура; моделирование; система защиты информации.

ВВЕДЕНИЕ

В настоящее время все области деятельности человека и общества компьютеризированы и автоматизированы. Одной из наиболее актуальных задач является задача автоматизации и бесперебойного функционирования критических инфраструктур. Они представляют собой сложные системы, которые занимаются генерацией электроэнергии, добычей полезных ископаемых, телекоммуникациями, транспортом, и т.д. Безопасное функционирование таких инфраструктур имеет первостепенное значение для национальной безопасности и экономики. Отсутствие стандартизированного решения проблемы безопасности для критических инфраструктур можно объяснить их большой распределенностью, разнообразием используемых устройств и соединений, необходимостью работы в режиме реального времени.

В данной работе предлагается подход к реализации системы защиты информации для критической инфраструктуры на примере системы управления железнодорожным транспортом. Метод включает в себя построение общей и компонентной модели распределенной системы, их поэтапную защиту и оптимизацию работы системы безопасности. Также предлагается набор криптографических методов защиты информации, подходящих для работы на устройствах с ограниченными ресурсами.

1. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И ПОСТАНОВКА ЗАДАЧИ

Проблемы безопасности в критических инфраструктурах обусловлены сильной взаимосвязанностью различных критических инфраструктур друг с другом и компонент каждой из них, использованием устройств с разными характеристиками, отсутствием стандартизированной методики разработки системы защиты информации для критических инфраструктур.

В качестве примера критической инфраструктуры взята система управления железнодорожными узлами и транспортом. Она поддерживает правильный и безопасный обмен сообщениями между центром управления и оборудованием путей и поездов.

Объектами железнодорожной системы устройства на путях и на борту поездов, центральная база данных, система блокировки железнодорожных путей, сервер-менеджер обновлений и конфигурации, сервер железнодорожного депо. Требуется обеспечить безопасность связи, жизненного цикла устройства, сервера и базы данных.

2. МЕТОДИКА РАЗРАБОТКИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Основным подходом к обеспечению безопасности критических инфраструктур является моделирование. Критическую инфраструктуру можно рассматривать как распределенную информационную систему. Чтобы обеспечить безопасность такой системы, предлагается построить две модели: общую и компонентную[1]. Проанализировав эти модели, выявив в них уязвимости и произведя защиту на каждом уровне детализации, можно построить систему защиты информации.

На общем уровне модель системы в формальном виде можно записать кортежем:

$$\mathrm{C} = (A, T, M, K, Ch), \qquad (1)$$

где A – архитектура, T – сетевые технологии, M – управление, K – основные действующие лица, Ch - каналы связи.

Конфигурация распределенной системы определяется значением каждого элемента кортежа. Можно выделить пять возможных вариантов архитектур распределенных систем: клиент-серверная, сервис-ориентированная, архитектура одноранговых сетей, grid-архитектура, облачная архитектура. К типам сетевых технологий можно отнести объектную, компонентную, веб-сервисов, многоагентную. P2P, облачную технологии. Управление может централизованным, частично централизованным и децентрализованным. На основе такого определения распределенных систем выделяются их классы, каждому из которых подхо-

дят определенные механизмы безопасности. Это позволяет осуществить защиту системы в целом, не рассматривая детально.

Формальную модель системы на компонентном уровне можно записать кортежем:

$$C = (R, N, Pr), \quad (2)$$

где R – ресурсы, N — узлы, Pr — процессы.

К ресурсам относятся программные или аппаратные ресурсы системы: данные, сервисы, узлы сети, коммуникационные каналы сети. Узлами системы являются подключенные к ней устройства: клиенты, серверы, устройства хранения данных. Процессом в системе является любой программный код, исполняемый на узлах сети или передаваемый по ее коммуникационным каналам.

Узлы являются основными объектами модели. Каждому узлу соответствуют определенные ресурсы, которые он использует, и каналы, по которым он взаимодействует с другими узлами. Детальное рассмотрение каждой компоненты позволяет защитить систему с учетом особенностей ее составляющих.

3. РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

На первом этапе строится общая модель системы. В данной модели клиент-серверная архитектура, компонентная технология связи и централизованный способ управления. Для решения проблемы аутентификации и управления ключами в такой модели рекомендуются инфраструктуры протокола Kerberos и открытых ключей. Можно выделить основные действующие лица системы и связи между ними. К первым относятся системные администраторы, центр управления, устройства на железнодорожных путях, бортовые устройства, железнодорожное депо. Администраторов с центром управления связывает локальный проводной канал, устройства с центром управления – защищенное беспроводное интернет-соединение.

Для построения системы защиты информации строится нужно защитить каждый компонент в отдельности.

К ресурсам системы R относятся: R1 – данные, хранящиеся в базе данных; R2 – пересылаемые сообщения и обновления; R3 – коммуникационные каналы; R4 – программное и аппаратное обеспечение системы.

К узлам системы N относятся: N1 – персональные компьютеры системных администраторов; N2 – серверы-менеджеры конфигураций; N3 – сервер блокировки железнодорожных путей; N4 – база данных; N5 – устройства на железнодорожных рельсах; N6 – устройства на борту поезда; N7 – сервер железнодорожного депо.

Основными процессами в системе являются: P1 – обновление устройств; P2 – отправка сообщений-команд; P3 – отправка сигнальных сообщений от устройств, сбор данных и построение текущей конфигурации; P4 – добавление устройства; P5 – аутентификация устройства; P6 – удаление устройства.

Для каждой компоненты можно определить задачу:

$$Z = (C, K, M), \tag{3}$$

где C – компонента системы, а именно, какой-либо ресурс R, узел N, процесс P, K – критерий обеспечения безопасности компоненты, M – множество методов защиты данных, которые позволяют решить задачу.

Нахождение решения каждой такой задачи в системе обеспечивает безопасноть системы. Защита ресурсов обеспечивается шифрованием и криптографическими протоколами. Узлы защищаются путем их физической изоляции, шифрования хранимых данных и поддержания безопасной передачи данных в каналах. Основную сложность представляет организация безопасного выполнения процессов.

На основе всех требующихся механизмов безопасности была разработана архитектура модуля системы безопасности, представленная на Рис.1.

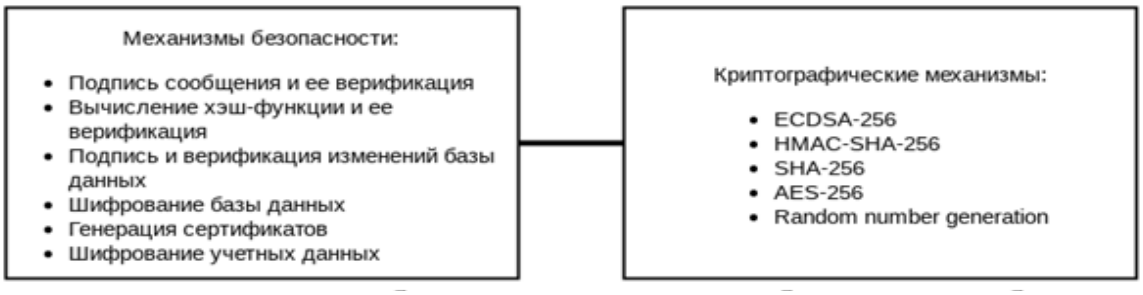

Рис. 1. Архитектура модуля системы защиты информации

Механизмы безопасности были протестированы на эмуляторе Raspberry Pi1 и Pi3, что показало доступность данных методов для использования на устройствах критической инфраструктуры. Модель критической инфраструктуры управления железнодорожными узлами и составами была проэмулирована программно. По результатам тестирования разработанного модуля системы безопасности в рамках модели система защиты информации выполняет свои функции.

Библиографические ссылки

1. *Галибус Т. В., Краснопрошин В. В.* Концептуальное моделирование и организация механизмов защиты информации в распределенных системах // Информатика январь-март 2016. 11 с.