УДК 656:[681.5:004]

АСПЕКТЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМЫ ПРИОРИТЕТНОГО ДВИЖЕНИЯ ЧЕРЕЗ ПЕРЕКРЕСТКИ ТРАНСПОРТНЫХ СРЕДСТВ ОПЕРАТИВНОГО НАЗНАЧЕНИЯ

Согоян А.Л.

Брестский государственный технический университет, г. Брест

ДТП с участием транспортных средств (ТС) оперативного назначения несут значительные последствия: гибель людей; потери здоровья сотрудников служб; необходимость их лечения и реабилитации; значительная задержка времени реагирования на экстренный вызов (ТС не приедет на вызов, вместо него необходимо отправить другое ТС); затраты на восстановление (если это возможно) или покупку нового специализированного автотранспортного средства [1].

Один из подходов для обеспечения безопасного передвижения ТС оперативного назначения, движущихся с включенными проблесковыми маячками является использование геонавигационной системы совместно с системой управления светофорами [2].

Функционирование системы основано на том, что каждое ТС экстренного назначения оснащено GPS/GSM терминалом. При включении проблесковых маячков водителем автоматически активируется передача данных GPS по протоколу навигационного оборудования NMEA о расположении ТС по GPRS каналу на сервер управления светофорными объектами.

Для обеспечения безопасной передачи данных на сервер управления светофорами каждый GPS/GSM терминал должен поддерживать шифрование передаваемых данных, например, по алгоритму AES-128.

Криптографический алгоритм AES-128 обеспечивает безопасную передачу данных между GPS/GSM терминалом и сервером управления светофорными объектами.

Если в качестве GPS/GSM терминала используется мобильное устройство, такое как планшет или смартфон, то возможности шифрования увеличиваются, благодаря использованию криптографических программных пакетов и библиотек. Появляется возможность реализовать аутентификацию транспортного средства оперативного назначения на сервере управления светофорными объектами.

Для защиты от повторной отправки перехваченных злоумышленником данных производится сравнение времени на сервере со временем в зашифрованных данных с GPS/GSM терминала ТС оперативного назначения. В случае значительного расхождения, данные не принимаются, а информация об отправителе и полученные данные добавляются в журнал событий, после чего происходит уведомление администратора о попытке повторной отправки данных злоумышленником.

Для надежного безопасного взаимодействия GSM устройство терминала обеспечивается статическим IP адресом. При добавлении транспортного средства в список ТС оперативного назначения, поддерживаемых системой управления светофорами, администратор указывает уникальный идентификационный номер устройства и статический IP адрес. Данные с IP адресов, не включенных в список транспортных средств, игнорируются, но записываются в журнал событий с последующим уведомлением администратора.

Сервер получает зашифрованные данные с GPS терминала ТС оперативного назначения, расшифровывает их. В качестве переданных данных выступают: уникальный идентификатор, географические координаты расположения ТС, направление движения, скорость движения. Оперируя расположением и направлением движения ТС оперативного назначения, сервер производит вычисления светофорных объектов располагаемых по ходу движения оперативного транспорта. На вычисленные светофорные объекты впереди движения ТС подается запрещающий сигнал для всех полос и всех направлений движения. Вся информация о полученных данных и действиях в системе вносится в журнал событий.

Серверная часть системы должна представлять собой два физических сервера: 1) сервер, который непосредственно централизованно управляет светофорными объектами в городе; 2) сервер, обеспечивающий взаимодействие с GPS/GSM устройствами транспортных средств оперативного назначения.

Сервер 1 и сервер 2 физически соединяются между собой. Сервер 1 не имеет доступа к сети интернет, локальным сетям, за исключением сети светофорных объектов. Кроме порта для соединения с сервером 2, все порты на сервере 1 отключены файрволом, в том числе отключена служба ICMP. На сервере 2 также отключены все порты, кроме порта для взаимодействия с терминалами ТС и порта обмена данными с сервером 1.

Внедрение системы приоритетного проезда перекрестков для ТС служб оперативного назначения требует внимательного отношения к компьютерной безопасности. Взаимодействие элементов системы должно происходить по защищенным каналам связи с использованием шифрования и аутентификации. Стабильная, надежная работа серверной части может быть обеспечена при грамотной настройке политик безопасности каждого из серверов.

Работа выполнена при поддержке Европейского гранта «Grant Agreement Number 2013-4550/001-001» по проекту Be-Safe – Белорусская сеть безопасных дорог 544181-TEMPUS-1-2013-1-IT-TEMPUS-JPCR.

Список цитированных источников

1. U.S. DOT (2003). Fatality Analysis Reporting System (FARS) Web-Based Encyclopedia Queries for Emergency Use Crash Statistics.
2. Согоян, А.Л. Система приоритетного движения на перекрестках «Зеленая волна» для транспортных средств оперативного назначения: сб. материалов V Международной научно-технической конференции OSTIS-2015 / А.Л. Согоян, В.Н. Шуть. – Минск: БГУИР, 2015. – С. 309–314.

УДК 004.04

РЕАЛИЗАЦИЯ ОТКАЗОУСТОЙЧИВОСТИ ВЫСОКОНАГРУЖЕННЫХ СИСТЕМ

Шахно М.И.

Брестский государственный университет имени А.С. Пушкина, г. Брест
Научный руководитель: Козинский А.А., к.пед.н., доцент

При разработке высоконагруженных веб-систем возникает множество технических проблем. Одной из таких проблем является организация отказоустойчивости системы. Отказоустойчивость решается на различных уровнях. Практическими приёмами организации отказоустойчивости является организация кластера серверов (веб-серверов, контейнеров сервлетов), а также репликация (в памяти, базе данных).

Рассмотрим один из приёмов организации отказоустойчивости веб-серверов, который предполагает организацию на уровне архитектуры.

При отправке HTTP-запроса (см. [1], [2]) к сервису, его принимает и обрабатывает веб-сервер. Сервер может являться узлом кеширования (не всегда), а так же узлом, где хранится статический контент приложения. HTTP-запрос на выполнение каких-либо логических действий (обработка запросов к базе данных; обработка вычислений и др.) попадает в узел, где происходит балансировка нагрузки.

Узел балансировки нагрузки передает этот запрос на выполнение одному из подузлов. В нашем случае одному из контейнеров сервлетов. Контейнер сервлетов, выполнив требуемую логическую часть, передает результат запросившему сервису. Пример организации описанного подхода представлен на рис. 1.

Представленная архитектура значительно усложняется при наличии сложного масштабируемого вычислительного кластера. Такой кластер служит для обеспечения вычисления сложноструктурированных данных.

Репликация – это прием синхронизации различного рода данных. Например, данных активной сессии между узлами.