– производительность промежуточного узла;
– загруженность промежуточного узла;
– дополнительные затраты времени отправителем на разбиение исходных данных на блоки, шифрование каждого из блоков, установление сессий с каждым из промежуточных узлов;
– затраты времени конечным адресатом на склейку пришедших блоков.

Следовательно в случаях, когда необходимо увеличить криптостойкость системы к MITM-атакам, целесообразно делить исходные данные на большее число пусть и небольших блоков. В противном случае число разбиений исходных данных должно быть в пределе 2-4, что позволит избежать сильного замедления работы системы.

Еще одной немаловажной характеристикой данной системы является производительность каждого из узлов в зависимости от размера передаваемого через него блока. Эта зависимость также не является линейной. Узел способен обработать большее количество байтов информации в единицу времени, если она передается большими блоками. Это связано с тем, что для обработки каждого из блоков информации необходимо устанавливать защищенную сессию с другим узлом сети и инициализировать криптосервисы для обработки полученного блока.

Дополнительным параметром при оценке эффективности разработанной системы является также величина затраченных ресурсов для передачи данных по средствам peer-to-peer сети. Узлы данной сети могут быть использованы не только для ретрансляции зашифрованных блоков данных между адресатами, но и для дополнительных задач, которые решаются при помощи построения peer-to-peer сети. Таким образом нельзя сказать, что зависимость затрат электроэнергии (или интернет-трафика) прямопропорциональна числу одновременно работающих узлов сети. Узел такой сети изредка будет использоваться для ретрансляции (или же передачи/получения) блоков данных, а в оставшееся время будет вести себя как будто это приложение и не было установлено.

На основании проведенных исследований установлено, что разработанную систему целесообразно применять в случаях, когда ключевым параметром является безопасность передачи данных, а скорость передачи при этом не имеет такого весомого значения, так как она всегда будет заметно ниже, чем у классических методов.

Список использованных источников:

1. Trappe, Wade (2005). Introduction to Cryptography with Coding Theory. New York: Pearson. p. 257.
2. Network Forensic Analysis of SSL MITM Attacks – NETRESEC Network Security Blog. Retrieved March 27, 2011.

МОДЕЛИ КАЧЕСТВА КЛИЕНТСКОЙ И СЕРВЕРНОЙ ЧАСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Резванов А. В.

Бахтизин В. В. – к-т. техн. наук, профессор

В настоящее время вопрос оценки качества веб-приложений является актуальным, т.к. в современной экономике веб-приложение может выступать в качестве дополнительного канала связи между промышленными предприятиями, организациями и их клиентами (B2C) или для связи между предприятиями (B2B).

При оценке качества веб-приложения его можно разделить на клиентскую часть и серверную часть. Клиентская часть включает файлы гипертекстовой разметки HTML, стили CSS и код JavaScript. Серверная часть включает код на таких языках программирования, как Java, C#, PHP, Python и других.

Оценка качества веб-приложений может быть основана на международных стандартах качества, таких как стандарт ISO/IEC 25010:2011 [1]. В данном стандарте 8 характеристик качества. При этом некоторое подмножество этих характеристик является более важным для клиентской части, в то время как другое подмножество более характерно для серверной части.

Для клиентской части важными характеристиками являются функциональная пригодность, совместимость, удобство использования, надежность и сопровождаемость (рис. 1).

Для серверной части важными являются функциональная пригодность, эффективность функционирования, совместимость, надежность, защищенность, сопровождаемость и мобильность (рис. 2).

Жирным шрифтом выделены наиболее важные характеристики.

Надежность клиентской части включает подхарактеристику завершенности, в то время как для серверной части кроме завершенности имеют значение такие подхарактеристики как готовность, отказоустойчивость и восстанавливаемость.

Характеристика удобства использования клиентской части включает такие подхарактеристики, как

обучаемость (learnability), простота использования (operability) и эстетичность пользовательского интерфейса (user interface aesthetics). Кроме этого могут быть предложены дополнительные подхарактеристики удобства использования клиентской части, такие как обратная связь (feedback), сходство с аналогами (familiarity) и интерактивность (interactivity), которые учитывают специфику веб-приложений. Модель клиентской части не включает подхарактеристику доступность (accessibility) характеристики удобство использования, так как она определяется контекстом использования веб-приложения .

При анализе качества веб-приложений, помимо клиентской и серверной части, можно также оценивать качество информационного наполнения (контента) и информационной архитектуры веб-приложения, для которых также возможно создание собственных моделей качества.

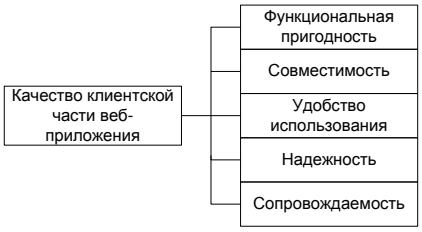

Рис. 1 – Модель качества клиентской части веб-приложения

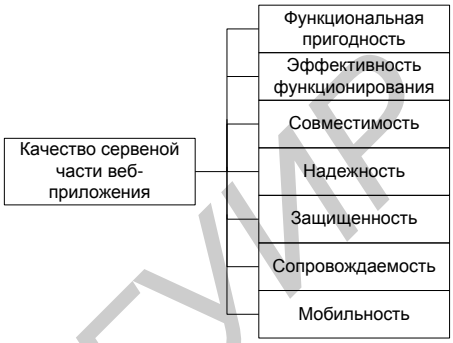

Рис. 2 – Модель качества серверной части веб-приложения

Два рассмотренных подмножества характеристик качества позволяют более полно учитывать специфику как клиентской, так и серверной части веб-приложений.

Список использованных источников:

1. ISO/IEC 25010:2011: System and Software Engineering - Systems and Software Quality Requirements and Evaluation (SQuaRE) - System and Software Quality Models, ISO Copyright Office, Geneva, March 2011
2. В. В. Бахтизин, Л. А. Глухова, С. Н. Неборский. Метрология, стандартизация и сертификация в информационных технологиях. Мн.: БГУИР, 2013.

ОБРАБОТКА ДАННЫХ СЕНСОРНЫХ УСТРОЙСТВ МОБИЛЬНЫХ ПЛАТФОРМ

Белорусский государственный университет информатики и радиоэлектроники

Селиванов И. А.

Бранцевич П. Ю. – к-т техн. наук, доцент

В докладе рассмотрены подходы к разработке методов и алгоритмов обработки данных, полученных с сенсорных устройств. Отмечается необходимость учитывать следующие параметры таких устройств: пропускная способность канала передачи данных, тактовая частота микроконтроллера, объём оперативной памяти. Данные параметры накладывают определённые ограничения на разрабатываемые алгоритмы. Также в алгоритмах нужно реализовать фильтрацию данных.

Сенсорные данные и получаемая с их помощью информация активно используются в различных направлениях жизнедеятельности человека: от промышленности и научных приборов до устройств повседневного использования. Широкое распространение на данный момент получили мобильные устройства с набором датчиков, предназначенных для получения информации об активности и жизнедеятельности человека - так называемые фитнес-трекеры и им подобные устройства.

Основными функциями таких устройств является: вычисление количества сделанного пользователем шагов; определение пройденного расстояния, подсчёт пульса. Более сложные устройства специализируются на вычислениях конкретных параметров человеческой активности в контексте его деятельности. Такими параметрами могут быть, например, фазы сна или скорость во время бега, и т.д. Некоторые устройства предназначены для спортсменов, они вычисляют параметры конкретных активностей спортсмена во время игр или тренировок – это могут быть удары в боксе или теннисе, прыжки и повороты в горнолыжном спорте.

Одним из таких устройств является сенсор PIQ[1], который позиционируется как спортивный трекер. Данное устройство содержит в себе два акселерометра, гироскоп, магнитометр, датчики температуры и давления. Все данные, получаемые с этих датчиков, могут передаваться на другие мобильные устройства