ПРОГРАММНОЕ СРЕДСТВО ОБЕСПЕЧЕНИЯ АУТЕНТИФИКАЦИИ СООБЩЕНИЙ

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

Мишулков А. В.

Ярмолик В. Н. – д-р. техн. наук, профессор

В настоящее время время широко используются системы, предоставляющие услуги и интерфейс использования в незащищенных сетях. Это обязывает к обеспечению защиты таких видов систем от несанкционированного доступа, изменения передаваемой информации, атак со стороны злоумышленников.

Для решения данной задачи применяются различные методы и протоколы, большинство которых были глубоко рассмотрены и проанализированы. Главным недостатком данных методов является высокая сложность реализации и использования, а как следствие интеграции с уже существующими системами. В рамках данного доклада представляется программное средство обеспечения аутентификации сообщений, решающее проблемы обеспечения защиты, сложности интеграции и расширяемости, а также модификации методов аутентификации сообщений для специфических случаев.

Ниже представлена архитектура программного средства, каждый модуль которой расширяем и легко заменяем (без перекомпиляции приложения), что позволяет его достаточно легко модифицировать в специфических случаях. Например, для хранения ключей безопасности и прочей конфигурационной информации в каком-либо облачном сервисе достаточно реализовать и заменить лишь модуль предоставления конфигурации.

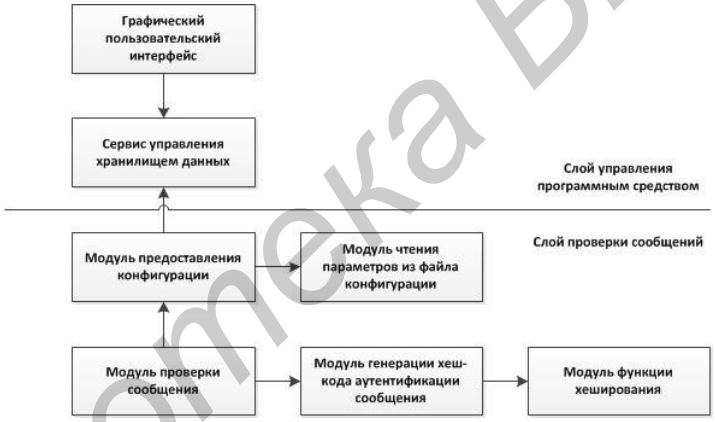

Рис. 1 – Архитектура программного средства

В качестве метода аутентификации сообщений предлагается использовать хеширование с использованием секретного значения (рисунок 2), в частности HMAC (hash-based message authentication code) ввиду следующих преимуществ данного подхода:

- возможность использовать имеющиеся хеш-функции без изменений, в частности, хеш-функций, которые уже есть в программном продукте, и их код уже доступен;
- сохранение первоначалльной производительности исполнения хеш-функции без каких-нибудь значительных ухудшений;
- использование и обработка ключей более простым способом;
- легкая сменяемость базовой хеш-функции в том случае, если более быстрая и более безопасная хеш-функция будет доступна позже.

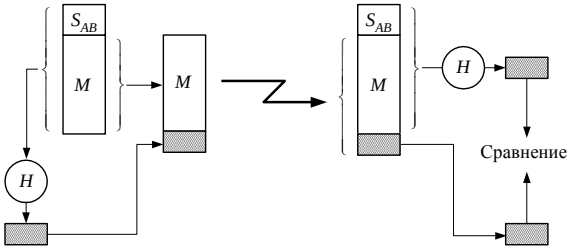

Рис. 2 – Схема работы алгоритма хеширования с использованием секретного значения

Предложена и разработана эффективная реализация схемы аутентификации на основе хеширования с использованием секретного значение, что позволило повысить производительность алгоритма. Улучшение заключается в использовании функции сжатия, результат которой используется в качестве вектора инициализации начальных состояний для алгоритма функции хеширования. В данной реализации алгоритма генерации хеш-кодов сообщений выполняется лишь одно дополнительное хеш-преобразование в отличии от трех в стандартной реализации. Это реализация особенно целесообразна, если большинство сообщений, для которых вычисляется MAC, короткие.

В качестве стандартной реализации функции хеширования для генерации хеш-кода сообщения используется функция SHA-256, являющаяся на данный момент одной из наиболее криптостойких и используемых.

Были проведены фунциональное тестирование и испытания скорости работы модуля аутентификации сообщений, входящего в состав программного средства. Результаты испытаний свидетельствуют, что производительность алгоритмов безопасности удовлетворяет критерием скорости и безопасности.

Таким образом, было разработано программное средство аутентификации сообщений, которое позволяет создавать безопасные веб-сервисы, защищенные от несанкционированного доступа и изменений передаваемой информации при работе как с клиентскими приложениями, так и серверными. Также разработанное программное средство позволяет гибко конфигурировать настройки безопасности в зависимости, которые могут изменяться в зависимости от требований и условий использования конкретного веб-ориентированного сервиса..

Список использованных источников:

1. Шнайер, Б. Прикладная криптография / Б. Шнайер. – Москва: Триумф, 2002. – 480 с.
2. Ярмолик, В. Н. Теория информации / В. Н. Ярмолик // Уч. метод. пособие для студентов специальности I – 40 01 01 "Программное обеспечение информационных технологий" дневной и дистанционной форм обучения. – Минск: БГУИР, 2004. – 118 с.: ил.