Т. О. Шардин
Научный руководитель: доцент кафедры ФПМ, к.т.н. А.В. Астафьев
Муромский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, Владимирская область, г. Муром, ул. Орловская, д.23
E-mail:tima.shardin@mail.ru

Обзор и анализ методов проверки подлинности абонентов в клиент-серверных приложениях

В настоящее время большинство систем предоставляют возможность сетевого взаимодействия, позволяя пользователям производить обмен информацией между различными сервисами. Однако, в некоторых случаях, корректность передаваемых данных крайне важна, поэтому разработчики данного программного обеспечения принимают меры по защите передаваемых данных, тем самым защищая их от злоумышленников. Зачастую это реализуется методом проверки подлинности абонентов. В связи с этим анализ, разработка новых и совершенствование существующих методов проверки подлинности абонентов является актуальной научно-технической задачей.

Целью исследования является обзор и анализ методов проверки подлинности абонентов, используемых в клиент-серверных приложениях для защиты передаваемой информации.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор методов проверки подлинности.
2. Анализ выбранных методов.
3. Выводы о проделанной работе.

Обзор методов проверки подлинности. На практике, процесс проверки подлинности зачастую связан с использованием различных криптографических систем. Большинство специалистов сделали вывод, что наилучшие результаты достигаются при использовании алгоритмов, основанных на передаче ключевых сообщений.

В ходе исследования были рассмотрены следующие методы:

SSL сертификат — это стандартная интернет технология безопасности, которая используется, чтобы обеспечить зашифрованное соединение между веб-сервером (сайтом) и браузером. SSL сертификат позволяет использовать https протокол. Это безопасное соединение, которое гарантирует, что информация которая передается от вашего браузера на сервер остается приватной, то есть защищенной от хакеров или любого, кто хочет украсть информацию [1].

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость) [2].

Протокол записи — это уровневый протокол. На каждом уровне сообщения включают поля для длины, описания и проверки. Протокол записи принимает сообщения, которые нужно передать, фрагментирует данные в управляемые блоки, разумно сжимает данные, применяя MAC (message authentication code), шифрует и передаёт результат. Полученные данные он расшифровывает, проверяет, распаковывает, собирает и доставляет к более верхним уровням клиента [3].

Анализ методов проверки подлинности. В результате анализа были выявлены следующие достоинства и недостатки данных алгоритмов и методов по следующим критериям, приведенных в таблице:

Таблица 1 – Результаты анализа.

Вид	Не требует материальных затрат	Возможно хранить на носителях информации	Необязательно хранить в тайне от посторонних лиц	Присутствует выбор шифрования между клиентом и сервером	Для получения необходим центр сертификации	Невозможно подделать
SSL сертификат	-	-	+	-	-	-
ЭЦП	-	+	-	-	-	+
Протокол записи	+	-	+	+	+	-

Выводы о проделанной работе. В результате проведенного исследования было выяснено, что наиболее оптимальным методом проверки подлинности абонентов является использование протокола записи, так как его применение повысило бы отказоустойчивость и всю работу в целом, а также для его реализации не требуется никаких материальных затрат.

Литература

1. Цифровые SSL сертификаты [Электронный ресурс] // Habrahabr.ru : интернет портал URL: https://habrahabr.ru/company/tuthost/blog/150433 (дата обращения: 28.03.2016).

2. Электронная подпись [Электронный ресурс] // Википедия : свободная энцикл. URL: https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C (дата обращения: 28.03.2016).

3. Протокол записи [Электронный ресурс] // Википедия : свободная энцикл. URL: https://ru.wikipedia.org/wiki/SSL#.D0.9F.D1.80.D0.BE.D1.82.D0.BE.D0.BA.D0.BE.D0.BB_.D1.80.D1.83.D0.BA.D0.BE.D0.BF.D0.BE.D0.B6.D0.B0.D1.82.D0.B8.D1.8F (дата обращения: 29.03.2016).

4. Молдовян А.А., Молдовян Д.Н., Левина А.Б. Протоколы аутентификации с нулевым разглашением секрета - Санкт-Петербург: СПб: Университет ИТМО, 2016. - 55 с.