Волков Д.А.
Научный руководитель: к.т.н., доцент каф. ФПМ А.В. Астафьев
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail:madehim333@yandex.ru

Обзор и анализ метода аутентификации с использованием протокола с нулевым разглашением секрета Фиата-Шамира

Защита информации является неотъемлемой составной частью общей проблемы информационной безопасности, роль и значимость которой во всех сферах жизни и деятельности общества и государства на современном этапе неуклонно возрастают.

Сначала сеть Интернет проектировалась и рассматривалась как система обработки и передачи информации в военной среде. Вопрос безопасности данных и в те времена являлся особо важным, но из-за ограниченного числа машин, имеющих доступ к сети, предпринимались только меры безопасности на физическом уровне. Под этим подразумевалась изоляция объектов от посторонних лиц, и данные меры являлись оправданными из-за, как указано выше, невысокого количества ЭВМ. Со временем, Интернет получил распространение в гражданской среде. В связи с этим в сети появилось множество различной информации, часть из которой является общедоступной, а другая часть доступна только для ограниченного числа людей. Следовательно, для защиты второй категории данных от несанкционированного доступа и необходимо обеспечивать безопасность передачи данных. В связи с этим разработка новых и совершенствование существующих методов защищенной передачи информации и аутентификации является актуальной научно-технической задачей.

Объекты исследования в данной работе – протокол с нулевым разглашением секрета Фиата-Шамира, предмет исследования – использование протокола с нулевым разглашением секрета в клиент-серверных приложениях для аутентификации.

Целью исследования является обзор и анализ методов аутентификации, реализуемого в клиент-серверных приложениях для защиты информации на примере протокола с нулевым разглашением секрета Фиата-Шамира.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор метода аутентификации;
2. Анализ метода;
3. Результаты исследования.

Обзор метода аутентификации. Аутентификация - это проверка соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации, в простейшем случае - с помощью имени входа и пароля.

В ходе исследования был рассмотрен следующий метод:

Протокол Фиата–Шамира. Основной идеей алгоритма является сложность извлечения квадратного корня по составному модулю, который включает не менее двух больших простых множителей[1]. При этом считается, что разложение этих множителей неизвестно. Доказывающим происходит выбор двух простых чисел (преимущественно больших) p и q и вычисляется модуль n = p * q. Затем в качестве своего личного секретного ключа выбирается случайное число s, такое, что $1 \leq s \leq n-1$, и вычисляется значение $y = s^2 \bmod n$.(Это делается для того, чтобы доказывать проверяющему, то что он знает квадратный корень из y.) Значение y, которое объявляется всем участникам протокола, играет роль открытого ключа в смысле его использования для проверки того, что доказывающий знает s.

Алгоритм протокола состоит из z-кратного повторения раундов, содержащих следующие шаги:

1. Доказывающим выбирается число k, которое удовлетворяет условию $1 \leq k \leq n-1$. Далее происходит вычисление значения $u = k^2 \bmod n$, называемое фиксатором, и это значение отправляется проверяющему. (Число k играет роль разового секретного ключа, это применяется для

обеспечения защиты и личного секретного ключа от разглашения при направлении ответа, зависящего от s.);

2. Проверяющий отправляет доказывающему равновероятный случайный бит r ($r = 1$ или $r = 0$);

3. Доказывающий производит вычисление значение $w = k*s^r \bmod n$ и отправляет его проверяющему.

При выполнении равенства $w^2 = u*y^r \bmod n$, проверяющий считает ответ верным.

Вероятность правильного прохождения раунда нарушителем равна 2^{-1}, следовательно, пройти проверку и выдать себя за пользователя, знающего секрет, возможно лишь с вероятностью 2^{-z}[3].

Анализ методов аутентификации. Для сравнительного анализа были выбранные следующие критерии:

Вычислительные затраты и предвычисления - число модульных умножений для обоих сторон.

Требования к памяти – необходимое количество памяти для записи ключей.

Гарантии безопасности – защита от злоумышленника, пытающегося получить доступ к секретной информации.

Кроме вышеупомянутого протокола Фиата-Шамира, для сравнения выбраны протоколы Гуилоу-Куйсквуатера и Шнорра[2]:

1.Вычислительные затраты. Менее требовательным к вычислительным затратам является протокол Фиата-Шамира, для него необходимо от 11 до 20 шагов. Далее идет протокол Шнорра, порядка 30 шагов. Заключает список протокол Гуилоу-Куйсквуатера с количеством шагов равным 60. Эти данные получены при kt=20 и размере n в 512 бит. Так же можно отметить, что неоптимизированный алгоритм RSA требует порядка 768 шагов;

2.Предвычисления. По совокупности вычислений проверяющей и доказывающей стороны данные протоколы приблизительно одинаковы. Протокол Шнорра имеет меньше вычислений у доказывающей стороны, из-за необходимости выполнения всего лишь одного модульного умножения (возвести в степень можно в ходе выполнения предвычислений), но у проверяющей стороны требуется большие вычисления, чем в протоколах Фиата-Шамира и Гуилоу-Куйсквуатера;

3.Требования к памяти и коммуникационные затраты. В протоколе Гуилоу-Куйсквуатера имеется возможность снизить требования к необходимой памяти и часть коммуникационных затрат. В других рассматриваемых протоколах данная возможность отсутствует;

4.Гарантии безопасности. Все вышеупомянутые протоколы способны обеспечить эффективное противодействие злоумышленнику, так как основываются на сложных математических операциях. Протокол Фиата-Шамира требует извлечения из числа корня по составному модулю, Гуилоу-Куйсквуатера основывается на невозможности получения из числа v корней по составному модулю, Шнорра требует вычисление дискретного логарифма по модулю простого числа.

В результате сравнения, протокол Фиата-Шамира является наилучшим вариантом, т.к. требованиями к памяти на текущий момент развития ЭВМ можно пренебречь.

Результаты исследования. В результате проведенного исследования было выяснено, что выбранный метод аутентификации, основанный на протоколе с нулевым разглашением секрета Фиата-Шамира является безопасным для защиты конфиденциальной информации. Так же, в ходе анализа были рассмотрены различные протоколы с нулевым разглашением секрета и выявлено, что выбранный протокол наиболее оптимальный для ряда основных критериев.

Литература

1. Протокол Фиата — Шамира [Электронный ресурс] // Википедия : свободная энцикл. URL: https://ru.wikipedia.org/wiki/Протокол_Фиата_—_Шамира (дата обращения: 05.03.2017).

2. Сравнение протоколов с нулевым разглашением [Электронный ресурс] // Cryptowiki : энциклопедия теоритической и прикладной криптографии URL: http://cryptowiki.net/index.php?title=Доказательства_с_нулевым_разглашением_знания (дата обращения: 06.03.2017).

3. Молдовян А.А., Молдовян Д.Н., Левина А.Б. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ СЕКРЕТА - Санкт-Петербург: СПб: Университет ИТМО, 2016. - 55 с. - экз.