УДК 004.056.5

РАЗРАБОТКА АЛГОРИТМА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ С СОЗДАНИЕМ БЕЗОПАСНОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ В КОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ПРОТОКОЛА UDP

© 2020 *М. В. Бабичева, А. А. Поздняков*

Проанализированы распространённые методы аутентификации пользователя и создания безопасного канала передачи данных на прикладном уровне модели TCP/IP. Разработан алгоритм аутентификации с одновременным обменом ключом на основе протокола транспортного уровня UDP.

Ключевые слова: безопасная передача данных, мобильные коммуникационные системы, аутентификация, UDP, HTTPS.

Введение. Говоря о современных веб-технологиях в последние несколько лет, исследователи и эксперты всё чаще обращают взгляд на тему перехода пользователей от использования стационарных компьютеров и ноутбуков к использованию мобильных устройств. Так, за 10 лет, в период с 2009 по 2019 год, количество проданных по всему миру смартфонов увеличилось с 172.38 миллионов единиц в год, до 1524.84 миллионов. А количество пользователей смартфонов к 2020 году составило 3.5 миллиарда человек, или 44.81% от всего населения.

Кроме того, если в 2013 году только 16.2% всего интернет-трафика приходилось на смартфоны, то в 2019 году он составлял уже 53.3%. Важно отметить, что эти данные представляют только трафик через смартфоны, не включая другие мобильные устройства, такие как планшетные компьютеры, например, использование которых также выросло за этот период. Таким образом, большая часть пользователей всемирной сети уже перешла на использование мобильных устройств.

Учитывая эту тенденцию многие компании находят очень выгодным разработку мобильных решений для своего бизнеса. Это касается не только компаний, создающих веб-продукты, такие как интернет-магазины, социальные сети, сервисы развлечений и пр. Свою нишу на мобильном рынке сейчас также активно занимают автомобильные производители, производители бытовой техники, транспортные компании и многие другие. Такие компании, в отличие от производителей веб-продуктов, предпочитают строить коммуникацию своих систем на более простых в реализации протоколах транспортного уровня (TCP, UDP), нежели на протоколах прикладного уровня (HTTP).

Однако, в то время как для HTTP существует расширение, позволяющее создавать безопасные сессии с шифрование данных - HTTPS, для протоколов TCP и UDP нет подобных общепринятых расширений на транспортном уровне. В связи с этим компании вынуждены самостоятельно разрабатывать и реализовывать протоколы аутентификации пользователей, создание сессий и шифрование данных. Это, в свою очередь, раз за разом приводит к появлению небезопасных коммуникационных систем, подверженных атакам и утечкам данных в лучшем случае и к потенциально опасным для жизни и здоровья пользователей выходам оборудования из строя в худшем.

Постановка задачи. Целью данной работы является анализ известных протоколов аутентификации пользователя и создания безопасного канала передачи данных, а также разработка оптимального алгоритма для использования в системе с протоколом передачи UDP. Результаты предполагается использовать при построении коммуникационной системы с архитектурой клиент-сервер.

Схемы аутентификации HTTP. В первую очередь следует выбрать схему аутентификации пользователя. Во время аутентификации пользователя безопасный канал

передачи данных ещё может быть не организован. Поэтому будем считать, что все данные передаются в незашифрованном виде. Наиболее распространёнными схемами аутентификации в HTTP являются:

1) **Basic authentication**. Для аутентификации клиент отправляет серверу строку вида «логин:пароль», закодированную с помощью Base64 (рис. 1). Очевидным недостатком такого метода является то, что при перехвате пакета аутентификации, злоумышленник сможет легко получить логин и пароль пользователя. В таком случае злоумышленник сможет не только получить доступ к данному серверу, но и потенциально к другим сервисам, которыми пользуется данный пользователь, так как зачастую пользователи предпочитают использовать одинаковые или похожие логины и пароли для различных сервисов. Таким образом, чтобы использовать basic authentication необходимо сначала установить безопасный канал передачи, гарантирующий защиту от перехвата.

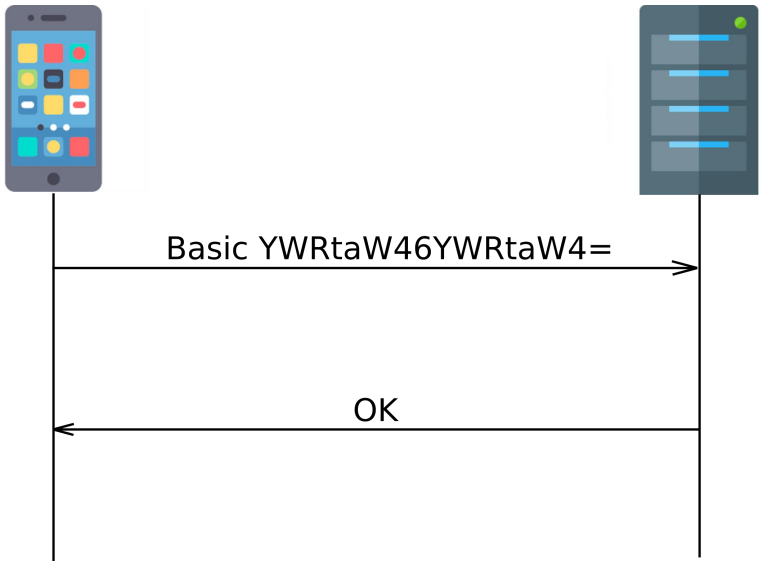

Рисунок 1. Basic authentication

2) **Bearer authentication.** В данной схеме, клиент не передаёт свои логин и пароль для аутентификации. Вместо этого он отправляет серверу заранее выданный ему токен аутентификации. Эта схема также уязвима для перехвата. Получив токен, злоумышленник сможет аутентифицироваться на сервере под видом клиента. Однако такая схема не ставит под удар другие сервисы, так как токен аутентификации уникален для данного сервера и не будет принят другими сервисами.

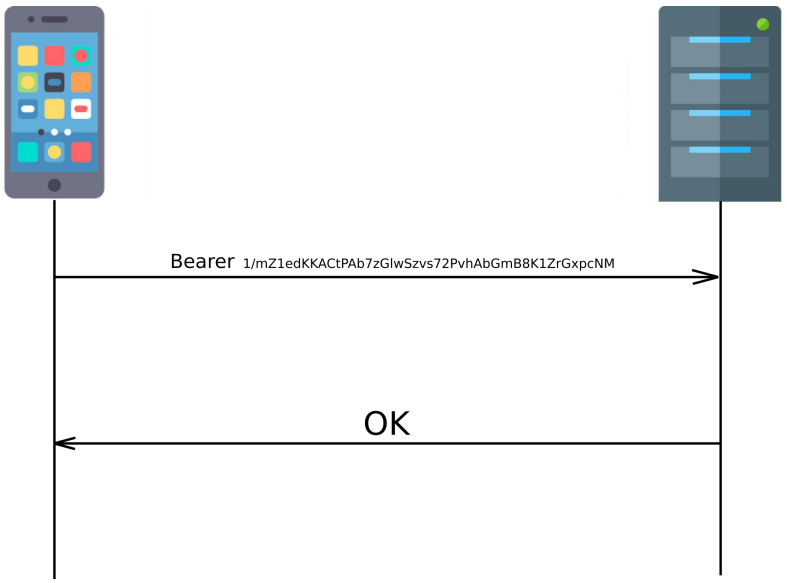

Рисунок 2. Bearer authentication

3) **Digest authentication.** В схеме digest authentication клиент отправляет серверу запрос на аутентификацию. Сервер в ответ присылает случайное число (nonce). Далее клиент вычисляет MD5 хеш от конкатенации логина, пароля и nonce и отправляет его на сервер. Сервер вычисляет такой же хеш и сравнивает его с полученным от клиента, если данные ссовпадают, то пользователь проходит аутентификацию. Графически схема представлена на рисунке 3. Несмотря на то, что данная схема требует больше шагов, она же является и саомй надёжной из рассмотренных. Digest authentication гарантирует, что даже при перехвате данных злоумышленник не имеет возможности обратить хеш-функцию и получить необходимые для аутентификации данные.

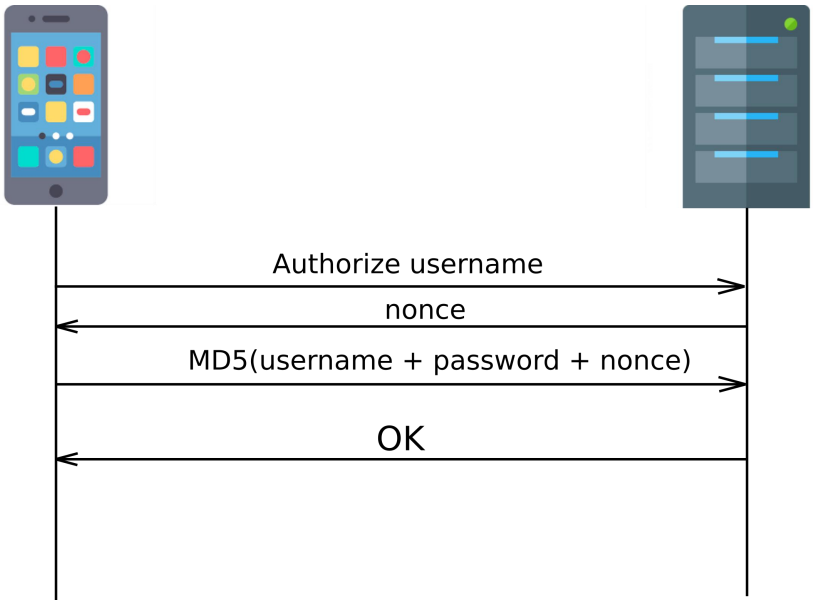

Рисунок 3. Digest authentication

Создание безопасного канала передачи данных в HTTPS. Как уже было сказано, протокол HTTP имеет расширение HTTPS, позволяющее создавать безопасный канал передачи между клиентом и сервером. В HTTPS клиент и сервер в начале сеанса связи договариваются о ключе шифрования при помощи ассиметричного алгоритма (RSA, Diffie-Hellman), а затем шифруют данные с помощью симметричного алгоритма (AES, DES, RC4,

RC2, 3-DES) используя этот ключ. Наиболее существенной и наиболее уязвимой частью данного протокола является обмен ключом. Рассмотрим оба алгоритма.

1) **RSA.** Алгоритм RSA был разработан в конце 1970-х тремя учёными: Ривестом, Шамиром и Адлеманом, по первым буквам фамилий которых и назвали алгоритм. Обмен ключом по этому алгоритму осуществляется следующим образом. Алиса отправляет Бобу свой открытый ключ RSA (e, n). Далее Боб создаёт ключ шифрования для симметричного алгоритма, шифрует его открытым ключом Алисы и возвращает Алисе зашифрованный ключ. Алиса, используя свой приватный ключ (d, n), расшифровывает сообщение и получает ключ шифрование. Таким образом и у Алисы, и у Боба есть одинаковый ключ, которым они теперь могут шифровать данные и передавать по незащищенному каналу. Графически алгоритм представлен на рисунке 4.

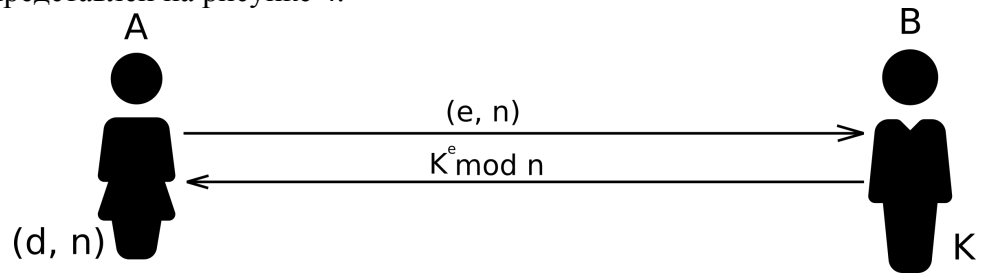

Рисунок 4. Обмен ключом по RSA

2) **Diffie-Hellman.** Алгоритм опубликован Диффи и Хеллманом в 1976, на год раньше RSA. По этому алгоритму Алиса и Боб заранее договариваются о публичном ключе (g, n). Когда им нужно договорится о ключе, Алиса и Боб выбирают секретные числа (a и b). После этого они обмениваются значениями $A = g^a \bmod n$ и $B = g^b \bmod n$. Дальше Алиса вычисляет $K = B^a \bmod n$, а Боб $K = A^b \bmod n$. Таким образом теперь они оба имеют ключ для дальнейшего шифрования данных (рис. 5).

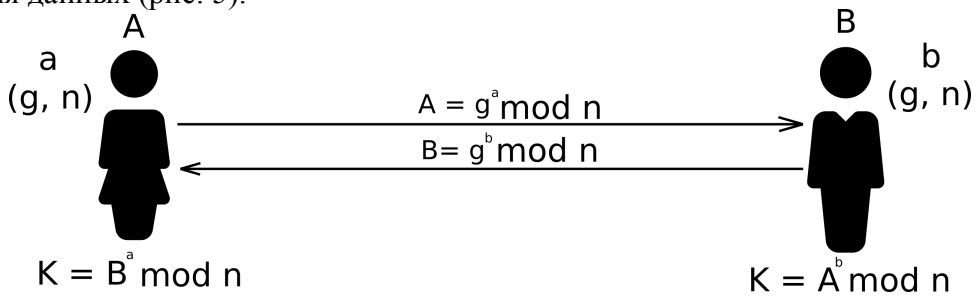

Рисунок 5. Обмен ключом по Diffie-Hellman

Создание собственного алгоритма. Вначале разработки, была предложена схема с базовой аутентификацией и обменом ключом по алгоритму RSA. Рассмотрим эту схему.

В первую очередь клиент инициирует процесс аутентификации, отправляя серверу логин пользователя. Сервер присылает клиенту публичный ключ для шифрования пароля. Клиент шифрует пароль пользователя и отправляет шифротекст серверу. Сервер расшифровывает сообщение и проверяет пароль пользователя. Если пароли совпадают, то пароль используется как ключ шифрования для алгоритма AES в дальнейшей передаче данных. Графически алгоритм представлен на рисунке 6.

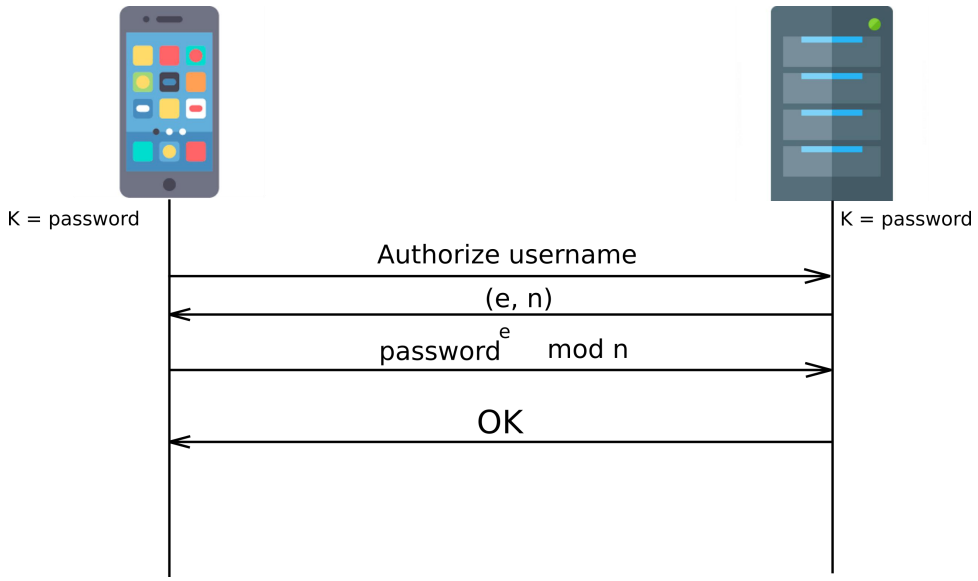

Рисунок 6. Аутентификация RSA

В данной схеме перехвативший трафик злоумышленник не сможет получить пароль пользователя, так как данные не передаются в открытом виде. Однако при дальнейшем анализе системы выявилось, что злоумышленник потенциально может не только перехватывать трафик, но и подменять его. В таком случае предложенная схема является уязвимой к атаке Man-In-The-Middle (MITM).

Для разрешения этой проблемы был разработан модифицированный алгоритм, основанный на digest authentication (рис. 7). Первый шаг алгоритма не изменился - клиент отправляет серверу логин, под которым он хочет аутентифицироваться. Сервер отвечает клиенту случайным числом. Далее клиент вычисляет SHA256 от конкатенации пароля пользователя и этого случайного числа и отправляет хеш-сумму серверу. Сервер проводит те же вычисления и сравнивает результат с ответом клиента. Если они совпадают, то аутентификация считается успешной и пароль пользователя можно использовать как ключ шифрования для дальнейшего обмена данными.

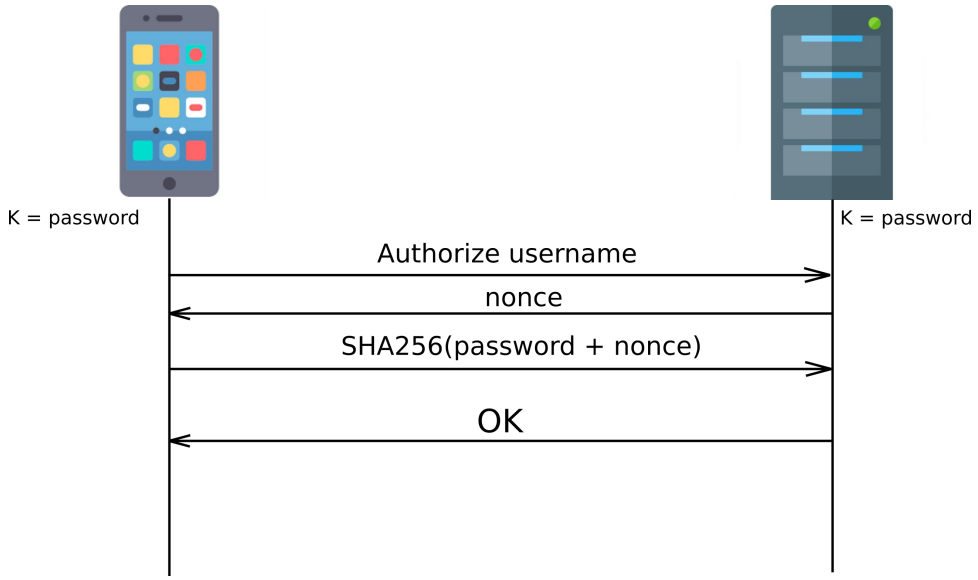

Рисунок 7. SHA256 аутентификация

Выводы. Проведенный анализ алгоритмов аутентификации пользователя и создания безопасного канала передачи данных, позволил разработать алгоритм аутентификации с одновременным обменом ключом в клиент-серверной коммуникационной системе, основанной на протоколе UDP. Алгоритм был улучшен для устранения уязвимости MITM,

что также значительно ускорило скорость работы системы, за счёт устранения сложных вычислений в рамках алгоритмов RSA или Диффи-Хеллмана.

СПИСОК ЛИТЕРАТУРЫ

1. Diffie W. New Directions In Cryptography / W. Diffie, M. E. Hellman // IEEE Transactions on Information Theory. - 1976. - № 6. - P. 644 – 654.
2. Gardner M. A New Kind of Cipher that Would Take Millions of Years to Break / M. Gardner, M. Gardner // Scientific American. - NYC.- 1977. - Vol. 237. - P. 120 – 124.
3. Rescola E. SSL and TLS: Designing and Building Secure Systems / E. Rescola // Addison-Wesley Professional. - 2000. - 386 p.
4. Hypertext Transfer Protocol – HTTP/1.1 / The Internet Society. - Текст : электронный. - URL: https://tools.ietf.org/html/rfc2616 (дата обращения: 11.10.2020).

DESIGNING AN ALGORITHM OF AUTHENTICATION WITH SECURE TRANSMISSION CHANNEL CREATION WITHIN COMMUNICATION SYSTEMS BASED ON UDP PROTOCOL

M. V. Babicheva, A. A. Pozdniakov

Analysed most common methods of user authentication and creation secure data transmission channel on the application level of TCP/IP network model. Designed authentication algorithm with secure data transmission channel creation based on UDP protocol.

Keywords: secure data exchange, mobile communication systems, authentication, UDP, HTTPS.

Бабичева Маргарита Вадимовна
ст. преподаватель кафедры радиофизики и инфокоммуникационных технологий ГОУ ВПО "Донецкий национальный университет", ДНР, Донецк.
E-mail: m.v.babicheva60@gmail.com

Babicheva Margarita Vadimovna
Senior Lecturer at Department of Radiophysics and
Infocommunication Technologies
of Donetsk
National University,
DPR, Donetsk.

Поздняков Александр Андреевич
студент кафедры радиофизики и инфокоммуникационных технологий ГОУ ВПО "Донецкий национальный университет", ДНР, Донецк.
E-mail: mail.0awawa0@gmail.com

Pozdniakov Alexander Andreyevich
Student at Department of Radiophysics and Infocommunication Technologies of Donetsk National University, DPR, Donetsk.