УДК 004.05
doi:10.15217/issn1684-8853.2018.2.76

ФОРМАЛИЗОВАННЫЙ АНАЛИЗ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ

Д. В. Юркин[а], *канд. техн. наук, доцент, dvyurkin@yandex.ru*
А. А. Уткина[а], *магистрант, alena_utkina_95@mail.ru*
А. О. Первушин[б], *магистрант, aeksei94@gmail.com*
[а]*Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Большевиков пр., 22-1, Санкт-Петербург, 193232, РФ*
[б]*Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Кронверкский пр., 49, Санкт-Петербург, 197101, РФ*

Введение: *для уменьшения времени доступа к защищенному каналу связи разработчики телекоммуникационных систем всегда стремятся улучшить алгоритмическую реализацию протоколов аутентификации. При этом наряду с временными характеристиками всегда необходимо получать оценки защищенности, эффективности и надежности криптографических протоколов, что обеспечивается методами формализованного анализа.* ***Цель:*** *поиск типовых уязвимостей, наличие которых может скомпрометировать процесс аутентификации.* ***Методы:*** *на основе предикатов и постулатов формализованной логики проведен анализ протокола аутентификации Никитина — Юркина, использующего бесключевые хеш-функции.* ***Результаты:*** *по результатам анализа, проведенного с помощью механизмов BAN-логики, в исследуемом протоколе выявлены недостатки, которые накладывают ограничения на область его применения, а именно: отсутствие знания о свежести сообщения от центра распределения ключей у участников процесса аутентификации, а также невозможность использовать данный протокол для того, чтобы уникально идентифицировать трех и более участников. Приведена модификация исходного протокола аутентификации, в результате которой выявленные ограничения его применения были нивелированы. Сформулированы обоснованные выводы, что данные исследования являются эффективным и востребованным способом описания криптографических протоколов в силу того, что, пользуясь им, можно определить, какие действия выполняет тот или иной протокол, а также выявить его типовые недостатки.* ***Практическая значимость:*** *результаты исследований позволяют повысить безопасность существующих распределенных сетей радиодоступа.*

Ключевые слова *— аутентификация, уязвимости протоколов аутентификации, бесключевые хеш-функции, BAN-логика, логика аутентификации.*

Цитирование: Юркин Д. В., Уткина А. А., Первушин А. О. Формализованный анализ протоколов аутентификации// Информационно-управляющие системы. 2018. № 2. С. 76–83. doi:10.15217/issn1684-8853.2018.2.76
Citation: Yurkin D. V., Utkina A. A., Pervushin A. O. Formalized Analysis of Authentication Protocols. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 2, pp. 76–83 (In Russian). doi:10.15217/issn1684-8853.2018.2.76

Введение

В настоящее время в зависимости от различных требований к автоматизированным системам в защищенном исполнении средства защиты информации используют большое множество различных криптографических протоколов аутентификации [1, 2]. Высокой актуальностью обладает вопрос поиска уязвимостей в системах управления доступом к защищаемым информационным ресурсам, по причине чего возникает необходимость формализованного анализа самой модели работы криптографического протокола методами, инвариантными к его алгоритмической и программной реализации [3]. Нередко в области стандартизации и сертификации требуется формально изложить работу различных криптографических протоколов, чтобы понять и оценить, в какой степени они достигают нужных результатов, а также выявить их недостатки [4].

В данной статье рассмотрено применение аппарата логики формализованного анализа протоколов аутентификации — BAN-логики. С помощью механизмов формализованной логики проанализирован протокол аутентификации с использованием бесключевых хеш-функций с целью выявить в нем недостатки в различных схемах функционирования.

BAN-логика — это формализованный метод анализа криптографических протоколов, по результатам применения которого может быть получен резюмирующий ответ на ряд вопросов, например:

— какие фактические задачи выполняет этот протокол;

— присутствуют ли в этом протоколе избыточные действия, которые можно не выполнять без снижения защищенности;

— обеспечивает ли должную конфиденциальность передаваемых данных этот протокол, и могут ли скомпрометировать отправленные в открытом явном виде данные ход его работы [5–9].

Важнейшей целью разработки метода является объяснение основных концепций при провер-

ке подлинности, так как BAN-логика большей частью построена на парадигме доверия [10–12].

Основные предикаты и их обозначения

Протоколы аутентификации, как правило, описываются формализованным перечислением сообщений, передаваемых между участниками (корреспондентами), при этом указываются отправитель, получатель и содержимое каждого сообщения [10, 13–15]. Обычные неформально-описательные обозначения неудобны для операций в формализованной логике, так как на стадии описания требуется однозначное указание предопределенных значений полей каждой части каждого сообщения, и эти значения не всегда очевидно следуют из данных, содержащихся непосредственно в самих сообщениях. Для того чтобы ввести точное обозначение и обеспечить однозначное соответствие оригинальному описанию протокола, каждое сообщение преобразуется в логическую формулу, и эта логическая формула является модифицированной версией исходного описания сообщения. После чего логические формулы связываются утверждениями [15, 16].

BAN-логика оперирует несколькими видами объектов, таких как участники (корреспонденты), ключи шифрования и формулы (утверждения). Сообщения протокола идентифицируются как утверждения. Идентификаторы A, B и S ассоциируются с участниками; идентификаторы K_{ab}, K_{as} и K_{bs} обозначают парные ключи для симметричных криптографических методов; K_a, K_b и K_s — открытые ключи; K_a^{-1}, K_b^{-1} и K_s^{-1} — секретные ключи для криптографических преобразований с открытым ключом, а N_a, N_b и N_c обозначают утверждения [11, 17, 18].

Единственной логической операцией, применяемой в данном математическом аппарате, является конъюнкция, которая обозначается запятой. Также применимы такие свойства конъюнкции, как ассоциативность и коммутативность. Аппаратом, помимо логической операции, используется следующая конструкция:

1) $A \mid\equiv X$ — корреспондент A верит в высказывание X;

2) $A \lhd X$ — корреспондент A видит высказывание X;

3) $A \mid\sim X$ — корреспондент A в определенное время отправил сообщение, содержащее X;

4) $A \mid\Rightarrow X$ — корреспондент A обладает юрисдикцией над X, т. е. участник A обладает авторитетом по высказыванию X;

5) $\#X$ — высказывание X является свежим, т. е. X не было отправлено в сообщении ранее до момента текущего выполнения итерации протокола;

6) $key(K, A \leftrightarrow B)$ — корреспонденты A и B могут использовать общий ключ K для взаимодействия, который никогда не может быть получен какими-либо другими корреспондентами, помимо A или B, или доверенными корреспондентами от A или B;

7) $\{X\}_K$ подразумевает, что данные X зашифрованы ключом K;

8) $Eq(h_1, h_2)$ — сравнение значений хеш-функций; истинно только тогда, когда h_1 полностью совпадает с h_2 [19].

Логические постулаты

Перед описанием логических постулатов необходимо отметить нижеприведенные положения BAN-логики.

В процессе аутентификации существует два условных временных интервала: прошлое и настоящее. Настоящий временной интервал начинается с момента выполнения рассматриваемого протокола. Все сообщения, отправленные до времени выполнения протокола, попадают в интервал прошлого [1, 20].

Все убеждения, принятые в настоящее время, являются действительными на протяжении всей работы протокола. Кроме того, предполагается, что когда участник A высказывает X, то он априори верит в истинность X.

Зашифрованное сообщение представляется как связанное логическое утверждение, зашифрованное ключом шифрования. Предполагается, что шифрование выполняется таким образом, что обрабатывается сразу все сообщение. Если в одно сообщение включены две части одного и того же исходного сообщения, зашифрованные отдельно, то считается, что обе части пришли в разных сообщениях.

Ниже приведено описание логических постулатов.

1. Правило назначения сообщения объясняет, как получить представление о происхождении сообщений.

Правило для общих ключей выглядит следующим образом:

$$\frac{A \mid\equiv key(K, A \leftrightarrow B), A \lhd \{X\}_K}{A \mid\equiv B \mid\sim X}. \qquad (1)$$

Если корреспондент A считает, что у него есть общий ключ K с корреспондентом B, и A видит сообщение X, зашифрованное на ключе K, то A верит в то, что B высказал X.

2. Правило проверки уникальности меток

$$\frac{A \mid\equiv \#X, A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid\equiv X}. \qquad (2)$$

То есть, если корреспондент A полагает, что сообщение X было высказано недавно и что корреспондент B однажды высказал X, то A считает, что B верит в X.

3. Правило юрисдикции

$$\frac{A \mid\equiv B \Rightarrow X,\ A \mid\equiv B \mid\equiv X}{A \mid\equiv X}. \qquad (3)$$

Правило говорит о том, что если корреспондент A считает, что корреспондент B имеет юрисдикцию над X, и A верит тому, что B верит в истину X, то A верит в истину X.

С учетом вышеописанных постулатов строится система доказательств. Формула X выводима из формулы Y, если существует последовательность формул Z_0; .. ; Z_n, где $Z_0 = Y$, $Z_n = X$ и каждая $Z_i + 1$ может быть получена из предыдущих путем применения вышеописанных правил [1].

Протокол аутентификации с использованием бесключевых хеш-функций

Рассмотрим в данной работе протокол аутентификации с использованием бесключевых хеш-функций, который был разработан В. Н. Никитиным и Д. В. Юркиным. Данный протокол предусматривает двухстороннюю аутентификацию корреспондентов путем передачи всего двух сообщений. Для однонаправленного преобразования информации используются бесключевые хеш-функции, а общий секрет используется в качестве входной переменной хеш-функции [21].

В данном протоколе A и B являются корреспондентами; S — центр распределения ключей; $H(X) = h$, где $H(X)$ — функция хеширования; X — некое высказывание; h — отображение высказывания X; $\|$ — операция конкатенации строк [20, 21].

До начала работы протокола доверенная сторона (центр распределения ключей) генерирует случайную секретную последовательность K_{ab}, на основании которой корреспонденты аутентифицируют друг друга. По защищенному каналу осуществляется передача секретной последовательности обеим сторонам:

1) $S \to A : \{K_{ab}\}_{K_{as}}$;

$S \to B : \{K_{ab}\}_{K_{bs}}$.

Корреспонденты A и B принимают общий секрет K_{ab} от центра распределения ключей.

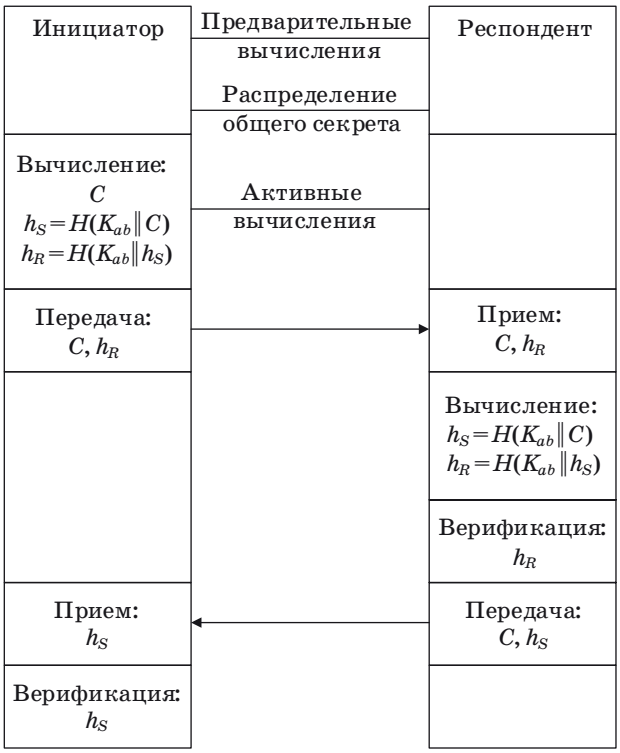
После предварительных вычислений и распределения общего секрета следует активная часть протокола. Сначала корреспондент A, который является инициатором, генерирует случайное число C. Далее корреспондент A вычисляет бесключевую хеш-функцию случайного числа C, конкатенированного с общим секретом: $h_S = h(K_{ab}\|C)$, а также хеш-функцию предыдущей хеш-функции $h(x)$ случайного числа и общего секрета $h_S = H(K_{ab}\|C)$, конкатенированной со значением общего секрета: $h_R = H(h_S\|K_{ab}) = H(K_{ab}\|h_S(K_{ab}\|C))$. После того как корреспондент A выполнил все вычисления, он отправляет корреспонденту B сообщение, содержащее случайное число C и значение бесключевой хеш-функции h_R:

2) $A \to B : C, h_R$.

Корреспондент B принимает сообщение (C, h_R) от корреспондента A и далее производит вычисление значения хеш-функции $\bar{h}_S$ от случайного числа C, принятого от инициатора, и общего секрета K_{ab}: $\bar{h}_S = H(K_{ab} \| C)$. На основе этого вычисленного значения он вычисляет h_R как значение бесключевой хеш-функции предыдущей хеш-функции случайного числа и общего секрета $\bar{h}_S = H(K_{ab} \| C)$, конкатенированной с общим секретом:

$$\bar{h}_R = H(K_{ab} \| \bar{h}_S) = H\left(K_{ab} \| H(K_{ab}) \| C\right).$$

После выполнения вычислений корреспондент B сравнивает полученное значение $\bar{h}_R$ и принятое от корреспондента A значение h_R. Если эти значения совпадают, то это значит, что A



■ Выполнение корреспондентами протокола двусторонней аутентификации

■ Execution of the protocol of reciprocal authentication by correspondents

успешно аутентифицирован, и корреспондент B отправляет корреспонденту A

3) $B \to A : \overline{h}_S$.

Далее корреспондент A принимает отправленное корреспондентом B значение $\overline{h}_S$ и сравнивает его со значением бесключевой хеш-функции, вычисленной им ранее: $h_S = \overline{h}_S$. Если значения этих хеш-функций совпадают, то протокол завершен успешно [21].

Схема работы протокола представлена на рисунке.

В результате после идеализации протокола шаги его работы выглядят следующим образом:

1) $S \to A : \{ key(K_{ab}, A \leftrightarrow B) \}_{K_{as}}$;

2) $S \to A : \{ key(K_{ab}, A \leftrightarrow B) \}_{K_{as}}$;

3) $A \to B : C, h_R = H(K_{ab} \| h_S(K_{ab} \| C))$;

4) $B \to A : \overline{h}_S = H(K_{ab} \| C)$.

На основании приведенного формального описания получен идеализированный протокол двусторонней аутентификации.

Анализ протокола аутентификации с использованием бесключевых хеш-функций

Запишем цели протокола аутентификации в терминах BAN-логики, т. е. укажем, какие логические утверждения должны быть выведены из предположений протокола с учетом последовательности шагов, выполняемых в данном протоколе [8, 15, 16]. Таким образом, аутентификация корреспондентов A и B считается выполненной, если существует такое K, что:

$$A \mid\equiv key(K, A \leftrightarrow B) = A \mid\equiv K_{ab};$$

$$B \mid\equiv key(K, A \leftrightarrow B) = B \mid\equiv K_{ab}.$$

Или, сказав иначе, оба корреспондента A и B должны поверить в то, что они используют для обмена сообщениями один и тот же секретный ключ K_{ab}. Однако для анализируемого протокола требуется большее:

$$A \mid\equiv B \mid\equiv key(K, A \leftrightarrow B) = A \mid\equiv B \mid\equiv K_{ab};$$

$$B \mid\equiv A \mid\equiv key(K, A \leftrightarrow B) = B \mid\equiv A \mid\equiv K_{ab}.$$

Таким образом, можно сказать, что каждый корреспондент должен верить в то, что другой корреспондент верит в то, что для обмена сообщениями они используют один и тот же секретный ключ K_{ab} [1].

Для того чтобы гарантировать успешное выполнение протокола, необходимо сделать начальные предположения:

1) $A \mid\equiv key(K_{as}, A \leftrightarrow S); B \mid\equiv key(K_{bs}, B \leftrightarrow S); S \mid\equiv \mid\equiv key(K_{as}, A \leftrightarrow S); S \mid\equiv key(K_{bs}, B \leftrightarrow S)$;

2) $S \mid\equiv key(K_{ab}, A \leftrightarrow B)$;

3) $A \mid\equiv (S \mid\Rightarrow key(K, A \leftrightarrow B)); B \mid\equiv (S \mid\Rightarrow key(K, A \leftrightarrow B))$;

4) $A \mid\equiv \#C$;

5) $A \mid\equiv \#key(K, A \leftrightarrow B); B \mid\equiv \#key(K, A \leftrightarrow B)$.

В первой группе выведены четыре формулы, обозначающие общие ключи для взаимодействия между клиентами A и B и сервером S. Формула $S \mid\equiv key(K_{ab}, A \leftrightarrow B)$ означает, что сервер изначально знает ключ, который должен стать общим секретом между A и B.

Третья группа из двух формул указывает на то, что корреспонденты A и B полагаются на S при генерации криптографического ключа.

Предположение $A \mid\equiv \#C$ указывает на то, что корреспондент A сгенерировал случайное число C и верит в его свежесть.

Последние два предположения в пятой группе кажутся необычными, но в дальнейшем анализе протокола будет показано, зачем они необходимы.

Перейдем непосредственно к анализу протокола аутентификации.

Предварительные вычисления.

1. Корреспондент A получает по защищенному каналу первое сообщение от центра распределения ключей S, на основе которого можно сделать следующий вывод:

$A \triangleleft \{K_{ab}\}_{K_{bs}}$ — A видит сообщение, зашифрованное ключом K_{as}, и делает вывод, что оно было послано S (1).

Однако A не может продолжать выполнять протокол, так как невозможно сделать вывод о том, что A поверил в полученный от S ключ по следующим причинам:

1) в тот момент, когда S отправляет сообщение A, то A не может знать, в какой момент времени это сообщение было отправлено. Так как вера в свежесть сообщения является необходимым условием в правиле проверки уникальности числовых вставок (2), следовательно, невозможно сделать вывод о том, что центр распределения ключей верит в отправленное им сообщение;

2) вследствие того, что невозможно точно утверждать, что S верит в посланное им сообщение, нельзя сделать вывод о том, что A поверил в принятый им ключ для обмена сообщениями с корреспондентом B от S на основе правила юрисдикции (3).

Поэтому A предполагает, что сообщение от S является новым.

Если делается необходимое предположение о том, что S является доверенным источником и канал связи с ним обладает гарантированной имитозащитой, то вся остальная активная

часть протокола формализуется. Получается $A \mid\equiv \mid\equiv key(K_{ab}, A \leftrightarrow B)$ с помощью (2) и (3).

2. Корреспондент B получает по защищенному каналу первое сообщение от центра распределения ключей S, на основе которого можно сделать следующий вывод:

$B \triangleleft \{K_{ab}\}_{K_{bs}}$ — B видит сообщение, зашифрованное ключом K_{bs}, и делает вывод, что оно было послано S (1).

Так же, как и в случае с корреспондентом A, невозможно сделать вывод о том, что B поверил в полученный от S ключ по аналогичным причинам. Следовательно, B просто предполагает, что сообщение от S является новым. Сразу получается, что $B \mid\equiv key(K_{ab}, A \leftrightarrow B)$ с помощью (2) и (3).

Активные вычисления.

1. $A \mid\equiv \#C$.

Корреспондент A генерирует случайное число C, следовательно, он верит в его свежесть.

$$2.\ \frac{A \mid\equiv K_{ab},\ A \triangleleft C,\ h_S = H(K_{ab} \| C)}{A \mid\equiv h_S}.$$

Корреспондент A верит в общий ключ для обмена сообщениями с B и видит сгенерированное им случайное число C. На основе этих значений он генерирует хеш $h_S = H(K_{ab}\|C)$, в который он верит.

$$3.\ \frac{A \mid\equiv K_{ab},\ A \triangleleft h_S,\ h_R = H(K_{ab} \| h_S)}{A \mid\equiv h_R}.$$

A верит в общий с B секрет и видит сгенерированный им хеш h_S. На основе этих значений он вычисляет новый хеш $h_R = H(K_{ab}\|h_S)$, в который он верит.

4. $A \to B : \{C, h_R\}$.

Корреспондент A отправляет B сообщение, которое содержит в себе сгенерированное им случайное число C и вычисленный им хеш h_R.

5. $B \triangleleft \{C, h_R\}$.

Корреспондент B видит полученное от корреспондента A сообщение, содержащее случайное число C и хеш h_R.

$$6.\ \frac{B \mid\equiv K_{ab},\ B \triangleleft C,\ \bar{h}_S = H(K_{ab} \| C)}{B \mid\equiv \bar{h}_S}.$$

B верит в общий с корреспондентом A секрет и видит случайное число C. На основе этих значений он вычисляет хеш $\bar{h}_S$, в который он верит.

$$7.\ \frac{B \mid\equiv K_{ab},\ B \triangleleft \bar{h}_S,\ \bar{h}_R = H(K_{ab} \| \bar{h}_S)}{B \mid\equiv \bar{h}_R}.$$

Корреспондент B верит в общий с A секрет, видит сгенерированный хеш $\bar{h}_S$. На основе этих значений он вычисляет хеш $\bar{h}_R$, в который он верит.

$$8.\ \frac{B \triangleleft Eq(h_R, \bar{h}_R)}{B \mid\equiv A \mid\sim h_R}.$$

Корреспондент B сравнивает хеш h_R, полученный от A, и хеш $\bar{h}_R$, сгенерированный им самим. Если они равны, то B может сделать вывод о том, что A когда-то мог сгенерировать такой хеш.

$$9.\ \frac{B \mid\equiv A \mid\sim h_R,\ B \mid\equiv \#(C)}{B \mid\equiv A \mid\equiv h_R}.$$

Если B не получал прежде числовую метку C, то он верит, что метка свежая. А это значит, что хеш h_R не мог быть передан повторно и никто, кроме корреспондента A, не мог сгенерировать такой хеш. Следовательно, основываясь на том, что B верит в то, что A когда-то послал значение h_R, и том, что B верит в свежесть числовой метки C, можно сделать вывод о том, что B верит в то, что A верит в сгенерированный им хеш h_R (2).

$$10.\ \frac{B \mid\equiv A \mid\equiv h_R}{B \mid\equiv A \mid\equiv K_{ab}}.$$

Поскольку хеш h_R является отображением секрета K_{ab}, следует считать K_{ab} и h_R эквивалентными. Следовательно, B верит, что A верит в то, что для обмена сообщениями они используют один и тот же секретный ключ K_{ab}.

11. $B \to A : \{\bar{h}_S\}$.

Корреспондент B отправляет A сообщение, содержащее вычисленный B хеш $\bar{h}_S = H(K_{ab} \| C)$.

12. $A \triangleleft \{\bar{h}_S\}$.

Корреспондент A видит полученное от B сообщение, содержащее вычисленный B хеш $\bar{h}_S$.

$$13.\ \frac{A \triangleleft Eq(h_S, \bar{h}_S)}{A \mid\equiv B \mid\sim \bar{h}_S}.$$

Корреспондент A сравнивает хеш $\bar{h}_S$, полученный от B, и h_S, сгенерированный им самим. Если они равны, то A делает вывод, что B когда-то мог сгенерировать такой хеш.

$$14.\ \frac{A \mid\equiv B \mid\sim \bar{h}_S,\ A \mid\equiv (C)}{A \mid\equiv B \mid\sim \bar{h}_S}.$$

Корреспондент A верит, что числовая метка является свежей. А это значит, что хеш $\bar{h}_S$ не мог быть сгенерирован ранее и никто, кроме B, не мог сгенерировать такой хеш. Следовательно, основываясь на том, что A верит в то, что B когда-то послал значение $\bar{h}_S$, и том, что A верит в свежесть числовой метки C, можно сделать вывод о том, что A верит в то, что B верит в сгенерированный им хеш $\bar{h}_S$ (2).

$$15.\ \frac{A \mid\equiv B \mid\equiv \bar{h}_S}{A \mid\equiv B \mid\equiv K_{ab}}.$$

Поскольку хеш $\bar{h}_S$ является отображением секрета K_{ab}, следует считать K_{ab} и $\bar{h}_S$ эквивалентными. Следовательно, A верит, что B верит, что для обмена сообщениями они используют один и тот же секретный ключ K_{ab}.

В ходе анализа не было выявлено избыточных шагов, после исключения которых корреспонденты все равно смогли бы однозначно аутентифицировать друг друга. В работе протокола было выявлено два недостатка:

1) при получении общего ключа от центра распределения ключей оба корреспондента не могут точно знать, в какое время было отправлено сообщение, содержащее ключ; знание о свежести сообщения является необходимым условием для дальнейшей работы протокола аутентификации;

2) данный протокол аутентификации не может быть использован для того, чтобы уникально идентифицировать трех и более корреспондентов, среди которых распределен общий секрет, так как невозможно однозначно определить, кем именно был послан сгенерированный хеш, поскольку каждый из участников мог его сгенерировать.

Для исключения первого недостатка было принято решение дополнить первое сообщение от центра распределения ключей, в котором содержится общий ключ для корреспондентов A и B, временной меткой. В результате шаги протокола будут выглядеть следующим образом:

1) $S \to A : \{T_S, L, K_{ab}\}_{K_{as}}$; $S \to B : \{K_{ab}\}_{K_{bs}}$;

2) $A \to B : C, h_R$;

3) $B \to A : \bar{h}_S$,

где T_S — временная метка, а L — время жизни.

Благодаря наличию временной метки оба корреспондента, принимая первое сообщение от центра распределения ключей, могут убедиться в его свежести [15, 19]. На основе правила проверки уникальности числовых вставок оба корреспондента могут поверить в то, что центр распределения ключей верит в отправленное им сообщение. Далее все действия протокола будут происходить без каких-либо проблем.

Заключение

Исследования криптографических протоколов с использованием BAN-логики являются надежным доказательным способом анализа и описания. При использовании формализованного анализа можно определить, какие действия выполняет тот или иной протокол, а также выявить его типовые недостатки. Необходимо отметить, что по причине работы изложенных методов на заданном уровне абстракции не рассматриваются такие аспекты специфики реализации протоколов, как, например, стойкость используемых криптосистем.

Также было отмечено, что, несмотря на допущение возможности существования злоумышленников, данный метод концентрируется исключительно на доверии надежных сторон, которые участвуют в процессе аутентификации.

В работе был произведен анализ протокола аутентификации с использованием бесключевых хеш-функций с помощью BAN-логики. При анализе не выявлено избыточных шагов, без которых процесс аутентификации выполнялся бы успешно. Однако определено два существенных недостатка, один из которых был успешно устранен путем добавления временной метки в первое сообщение от центра распределения ключей.

Протокол предоставляет достаточно быструю и надежную аутентификацию субъектов, поскольку в нем выполняется передача только двух сообщений, а также используются бесключевые хеш-функции для преобразования информации, что не требует дополнительных операций генерации и смены сеансового ключа, как в случае использования ключевой хеш-функции. Однако данный способ аутентификации требует некоторой доработки для возможности аутентификации трех и более корреспондентов.

Литература

1. **Burrows M., Abadi M., Needham R. M.** A Logic of Authentication // Proc. of the Royal Society A: Mathematical, Physical and Engineering Sciences. 1989. Vol. 426. Iss. 1871. P. 233–271. doi:10.1098/rspa. 1989.0125
2. **Chatzieleftheriou G., Bonakdarpour B., Katsaros P., Smolka S.** Abstract Model Repair// Logical Methods in Computer Science. 2015. Vol. 11. P. 1–43.
3. **Марков А. С., Рауткин Ю. В., Фадин А. А.** Состояние и перспективы анализа защищенности Wi-Fi сетей // Тр. Научно-исследовательского института радио. 2012. № 1. С. 85–90.
4. **Hongda Yin, Guanling Chen, Jie Wang.** Detecting Protected Layer-3 Rogue APs. Broadband Communications // Networks Broadband Communications: Networks and Systems, Raleigh. 2007. P. 449–458.
5. **Watkins L., Robinson W. H., Beyah R. A.** A Passive Approach to Rogue Access Point Detection // Global Telecommunications Conf., Washington. 2007. P. 355–360.
6. **Chong E., Loo M., Christopher L., Marimuthu P.** Intrusion Detection for Routing Attacks in Sensor Networks // International Journal of Distributed Sensor Networks. 2006. Vol. 2. N 1. P. 313–332.
7. **Chung-Hsin L., Po-Cheng T., Chun-Lin L., Kuo-Hao L.** The Study of the Wireless Network Dos Attack // Information Technology, Culture and Human: Proc. of the 2nd Intern. Conf. on Interaction Sciences. N. Y., 2009. P. 418–421.
8. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1 // Common Criteria Portal. 2006. http://www.commoncriteriaportal.org/files/

ccfiles/CCPART1V3.1R3.pdf (дата обращения: 20.10.2013).
9. Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Requirements, Version 3.1 // Common Criteria Portal. 2006. http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf (дата обращения: 20.10.2013).
10. **Wagatsuma K., Harada T., Anze S., Goto Y.** Formalization for Formal Analysis of Cryptographic Protocols with Reasoning Approach // Advanced Multimedia and Ubiquitous Engineering: Future Information Technology. Springer, 2015. P. 25–32.
11. **Косачев А. С., Пономаренко В. Н.** Анализ подходов к верификации функций безопасности и мобильности. — М.: Триумф, 2004. — 101 с.
12. **Могилевская Н. С., Новиков А. М.** Формализация и анализ протоколов аутентификации // Информационное противодействие угрозам терроризма. 2009. № 12. С. 99–102.
13. **Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.** Основы криптографии. — М.: Гелиос АРВ, 2002. — 480 с.
14. **Зегжда Д. П., Коваленко С. Л.** Проблемы безопасности беспроводных сетей семейства IEEE 802.11a/b/g // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 45–49.
15. **Смарт Н.** Криптография. — М.: Техносфера, 2005. С. 168–179.
16. **Романец Ю. М., Тимофеев П. А., Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 2001. — 376 с.
17. **Cohn-Gordon K., Cremers C., Dowling B., Garratt L., Stebila D.** A Formal Security Analysis of the Signal Messaging Protocol// 2nd IEEE European Symp. on Security and Privacy (EuroS&P 2017). 2017. P. 451–466.
18. **Bauer R. K., Berson T. A., Feiertag R. J.** A Key Distribution Protocol using Event Markers // ACM Transactions on Computer Systems. 1983. Vol. 1. N 3. P. 249–255.
19. Современная криптография: теория и практика: пер. с англ. — М.: Вильямс, 2005. — С. 633–640, 656–658.
20. **Никитин В. Н., Юркин Д. В.** Анализ протоколов шифрования// Журнал радиоэлектроники. 2009. № 4. http://jre.cplire.ru/jre/apr09/5/text.html (дата обращения: 14.10.2013).
21. **Никитин В. Н., Юркин Д. В.** Улучшение способов аутентификации для каналов связи с ошибками // Информационно-управляющие системы. 2010. № 6. С. 42–46.

UDC 004.05
doi:10.15217/issn1684-8853.2018.2.76

Formalized Analysis of Authentication Protocols

Yurkin D. V.[a], PhD, Tech., Associate Professor, dvyurkin@yandex.ru
Utkina A. A.[a], Master Student, alena_utkina_95@mail.ru
Pervushin A. O.[b], Master Student, aeksei94@gmail.com
[a]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 22-1, Bolshevikov Pr., 193232, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, 49, Kronverkskii Pr., 197101, Saint-Petersburg, Russian Federation

Introduction: Telecommunication system developers always try to reduce the time of authentication protocol execution using algorithmic implementation of authentication protocols. However, along with the temporal characteristics, it is always important to estimate the security, efficiency and reliability of cryptographic protocols. This can be provided by formalized analysis methods. **Purpose:** Search for typical vulnerabilities whose presence can undermine the authentication. **Methods:** On the base of predicates and postulates of formalized logic, Nikitin-Yurkin authentication protocol with keyless hash functions was analyzed. **Results:** BAN logic analysis revealed certain shortcomings in the studied protocol, which impose limitations on its application scope; namely: the lack of knowledge about how fresh a message for the authentication participants from the key distribution center is, and also the impossibility to use this protocol to uniquely identify three or more participants. The paper presents a modification of the initial authentication protocol which removed the limitations of its application. Well-founded conclusions are formulated that these studies are an effective and much-needed way of describing cryptographic protocols because they can help you determine what actions are performed by a certain protocol, and also to identify its typical shortcomings. **Practical relevance:** The results of this research allow you to improve the security of distributed radio access networks.

Keywords — Authentication, Authentication Protocol Vulnerabilities, Keyless Hash Function, BAN Logic, Authentication Logic.

Citation: Yurkin D. V., Utkina A. A., Pervushin A. O. Formalized Analysis of Authentication Protocols. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 2, pp. 76–83 (In Russian). doi:10.15217/issn1684-8853.2018.2.76

References

1. Burrows M., Abadi M., Needham R. M. A Logic of Authentication. *Proc. of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 1989, vol. 426, iss. 1871, pp. 233–271. doi:10.1098/rspa. 1989.0125
2. Chatzieleftheriou G., Bonakdarpour B., Katsaros P., Smolka S. Abstract Model Repair. *Logical Methods in Computer Science*, 2015, vol. 11, pp. 1–43.
3. Markov A. S., Rautkin Y. V., Fadin A. A. The State and Prospects of Wi-Fi Network Security Analysis. *Trudy Nauchno-issledovatel'skogo instituta radio*, 2012, no. 1, pp. 85–90 (In Russian).
4. Hongda Yin, Guanling Chen, Jie Wang. Detecting Protected Layer-3 Rogue APs. Broadband Communications. *Networks Broadband Communications: Networks and Systems*, Raleigh, 2007, pp. 449–458.
5. Watkins L., Robinson W. H., Beyah R. A. A Passive Approach to Rogue Access Point Detection. *Global Telecommunications Conference*, Washington, 2007, pp. 355–360.
6. Chong E., Loo M., Christopher L., Marimuthu P. Intrusion Detection for Routing Attacks in Sensor Networks. *International Journal of Distributed Sensor Networks*, 2006, vol. 2, no. 1, pp. 313–332.
7. Chung-Hsin L., Po-Cheng T., Chun-Lin L., Kuo-Hao L. The Study of the Wireless Network Dos Attack. *Proc. of the 2nd Intern. Conf. on Interaction Sciences "Information Technology, Culture and Human"*, New York, 2009, pp. 418–421.
8. *Common Criteria for Information Technology Security Evaluation*. Part 1. *Introduction and General Model, Version 3.1*. Common Criteria Portal, 2006. Available at: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf (accessed 20 October 2013).
9. *Common Criteria for Information Technology Security Evaluation*. Part 2. *Security Functional Requirements, Version 3.1*. Common Criteria Portal, 2006. Available at: http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf (accessed 20 October 2013).
10. Wagatsuma K., Harada T., Anze S., Goto Y. Formalization for Formal Analysis of Cryptographic Protocols with Reasoning Approach. *Advanced Multimedia and Ubiquitous Engineering: Future Information Technology*, Springer, 2015, pp. 25–32.
11. Kosachev A. S., Ponomarenko V. N. *Analiz podkhodov k verifikatsii funktsii bezopasnosti i mobil'nosti* [Analysis of Approaches to Verification of Safety Functions and Mobility]. Moscow, Triumph Publ., 2004. 101 p. (In Russian).
12. Mogilevskaya N. S., Novikov A. M. Formalization and Analysis of Authentication Protocols. *Informatsionnoe protivodeistvie ugrozam terrorizma*, 2009, no. 12, pp. 99–102 (In Russian).
13. Alferov A. P., Zubov A. Y., Kuzmin A. S., Cheremushkin A. V. *Osnovy kriptografii* [Fundamentals of Cryptography]. Moscow, Helios ARV Publ., 2002. 480 p. (In Russian).
14. Zegzhda D. P., Kovalenko S. L. Security Problems of Wireless Networks of the IEEE 802.11a / b / g family. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2006, no. 2, pp. 45–49 (In Russian).
15. Smart N. *Kriptografiia* [Cryptography]. Moscow, Tekhnosfera Publ., 2005. Pp. 168–179 pp. (In Russian).
16. Romanets Y. M., Timofeev P. A., Shanguin V. F. *Zashchita informatsii v komp'iuternykh sistemakh i setiakh* [Protection of Information in Computer Systems and Networks]. Moscow, Radio i svyaz' Publ., 2001. 376 p. (In Russian).
17. Cohn-Gordon K., Cremers C., Dowling B., Garratt L., Stebila D. A Formal Security Analysis of the Signal Messaging Protocol. *IEEE European Symp. on Security and Privacy (EuroS&P)*, 2017, pp. 451–466.
18. Bauer R. K., Berson T. A., Feiertag R. J. A Key Distribution Protocol using Event Markers. *ACM Transactions on Computer Systems*, 1983, vol. 1, no. 3, pp. 249–255.
19. *Sovremennaia kriptografiia: teoriia i praktika* [Modern Cryptography: Theory and Practice]. Moscow, Williams Publ., 2005. Pp. 633–640, 656–658 (In Russian).
20. Nikitin V. N., Yurkin D. V. Analysis of Encryption Protocols. *Zhurnal radioelektroniki*, 2009, no. 4 (In Russian). Available at: http://jre.cplire.ru/jre/apr09/5/text.html (accessed 14 October 2013).
21. Nikitin V. N., Yurkin D. V. Modification of Authentification Technics for Errorprone Channels. *Informatsionno-upravlyayushchiye sistemy* [Information and Control Systems], 2010, no. 6, pp. 42–46 (In Russian).