УДК 004.056(07)

ДОВЕРИЕ В КОНТЕКСТЕ АНАЛИЗА СТОЙКОСТИ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ

П.К. Шиверов, Т.Г. Новосад, М.Н. Осипов

В работе рассмотрены инструменты формального анализа стойкости протоколов аутентификации. Предложено формализованное понятие доверия, как основная мера анализа протоколов аутентификации. Данное представление рассматривается в рамках использования методов проверки стойкости протоколов аутентификации - BAN-логика и теоретико-автоматный метод Долева-Яо.

Ключевые слова: криптографические протоколы, аутентификация, BAN-анализ, метод Долева-Яо, доверие.

Актуальность

Большинство атак на протоколы аутентификации используют ошибки в дизайне протоколов. В случае прикладного использования уязвимого протокола, происходит потеря защищённости общения. Если же протокол с уязвимостью является основанием, на котором были созданы другие протоколы, то необнаруженные вовремя уязвимости могут передаться «потомкам» этого протокола.

Существует большое множество подходов и методов анализа стойкости протоколов. Однако, единственным показателем стойкости, к которому сводится любой метод проверки стойкости криптографического протокола, является понятие доверия. Само по себе доверие представляет из себя достаточно сложное, философское понятие. Но разработка модели доверия, а в дальнейшем, и теории доверия в контексте анализа криптографических протоколов необходима для уточнения общей технологии анализа стойкости.

В данной статье рассматривается формализованное понятие о доверии, как о мере стойкости протоколов аутентификации.

Понятие: аутентификация - доверие

Аутентификация - это проверка идентичности, заявленной участником или субъектом системы, в качестве которого (участника) может выступать одна из сторон коммуникации или источник некоторых данных [1].

Иными словами, аутентификация - это процесс подтверждения подлинности участника взаимодействия.

Понятие аутентификация - доверие в рамках представления криптографических протоколов, где каждому участнику отведена конкретная роль, можно определить следующим образом.

Аутентификация-доверие это логический процесс, при котором проверяющая сторона убеждается в соответствии намерений проверяемой стороны протокольным (ролевым) обязанностям.

Протокол аутентификации, как и любой криптографический протокол, предписывает каждому участнику строгую последовательность действий, которая приводит к выявлению истинности намерений – доверия одного (односторонняя аутентификация) или нескольких (взаимная аутентификация) участников.

Построение формализованной модели доверия в протоколах аутентификации

Формализованное описание математической модели доверия, позволит превратить процесс анализа стойкости протоколов в математическое доказательство. Такой подход повысит точность анализа и позволит в дальнейшем автоматизировать его. Иными словами, математическое описание доверия позволит анализировать результативность работы протоколов аутентификации по выявлению намерений их участников.

В работе [1] описывается доверие, как психологическое, философское или социальное понятие. Построение общей модели доверия - крайне сложный процесс, требующий детального и всестороннего рассмотрения. Однако модель криптографического доверия может быть описана в рамках механизма криптографических протоколов.

Криптографические протоколы - это формализованные логические алгоритмы, в которых все криптографические функции заменены идеальными, абсолютно стойкими объектами [2]. Если, описывая протокол, который необходимо анализировать, мы говорим, что некое сообщение было зашифровано и передано, то подразумевается, что злоумышленник ни при каких условиях не сможет провести успешный криптоанализ использованного шифралгоритма. Таким образом, запись криптографического протокола неизбеж-

но включает в себя ряд допущений. Такой вывод позволяет утверждать, что само понятие доверия идеально. Достигнуть абсолютного доверия (полностью доказать честность участника протокола) невозможно. К нему можно лишь приблизиться, используя некоторое число критериев доверия.

Доверие - это уверенность в намерениях участника протокола. Эта уверенность вырабатывается в процессе выполнения протокола и уже не подвергается сомнению после окончания его выполнения. Таким образом, доверие формируется из последовательности выполнения шагов конкретного протокола. Иными словами, доверие - это составное понятие, которое содержит в себе доверие или недоверие к каждому поступку участника протокола. Доверие дискретно и представляет собой набор утвердительных и отрицательных значений. Назовём такое доверие *характеристическим*:

$$D_{харак} = [d_1, d_2, \cdots d_n], \quad (1)$$

где $d_i \in \{0,1\}$.

В некоторых случаях доверие может быть рассмотрено как дискретный набор состояний *по времени*. Такое возможно в тех случаях, когда проводится многократная проверка стойкости.

$$D_{врем} = [d_1, d_2, \cdots d_t], \quad (2)$$

где $d_i \in \{0,1\}$.

Доверие так же может быть *комбинированным*.

$$D_{колб} = [D_1, D_2, \cdots D_t], \quad (3)$$

где $D_i = [d_1, d_2, \ldots d_n]$.

Из вышесказанного следует, что доверие может быть доказано в конкретный момент времени или с установленным набором критериев. Однако это не значит, что доверие доказано наверняка раз и навсегда. Иными словами, принимая доказанность характеристического или временного доверия за 1, можно записать следующее логическое выражение:

$$\lim \bigcup_{i=1}^{\infty} D_i = 1 \quad (4)$$

Доказанность доверия должна быть равна 1 на всех этапах проверки. В противном случае, доверие не будет доказано.

Представленное описание доверия идеально и описывает бесконечный ряд проверок, что неосуществимо на практике. Отсюда следует, что доверие может принимать нулевое значение, но никак не может принимать значение единицы. Значение доверия может лишь стремиться к 1, но никогда не может достигнуть его, поскольку невозможно добиться абсолютной уверенности в отсутствии уязвимостей.

Единственным инструментом выработки доверия является анализируемый протокол с его начальными предположениями (стойкость алгоритма шифрования, удачный выбор ключа, свежесть сертификата электронной цифровой подписи и т.д.).

В любой системе существует множество абонентов, доверие к которым равно единице. Задача протокола - доказательство принадлежности конкретного абонента к доверенному множеству.

$$\wp : (A \notin \aleph) \rightarrow (A \in \aleph), \quad (5)$$

где $\aleph = \{A,B,C,\ldots\}$ - множество доверенных абонентов.

Иными словами, протокол - это функция, которая позволяет выделить участника общения, принадлежащего ко множеству честных абонентов, из множества всех возможных абонентов (как честных, так и злоумышленников).

Любая функция задаётся конечным набором правил и множеством значений, описывающих её, что однозначно соответствует устройству протоколов и подтверждается тем, что все рассмотренные нами методы проверки стойкости протоколов аутентификации используют поэлементный анализ составляющих протокола.

Одним из самых распространённых инструментов проверки стойкости протоколов аутентификации являются методы, которые позволяют моделировать требования к протоколам с использованием логик, разработанных специально для анализа «знаний» и «доверия».

Одними из основных методов проверки стойкости протоколов аутентификации являются BAN-логика, с которой и началось развитие этого направления, и теоретико-автоматный метод Долева-Яо.

BAN-логика рассматривает подлинность, как функцию от целостности и новизны, используя логические правила для отслеживания состояния этих атрибутов на протяжении выполнения всего протокола [3]. BAN-логика позволяет составить схему взаимосвязей между отдельными участниками протокола,

секретными ключами и иными объектами на основе взаимного доверия. Далее, каждая связь проверяется на наличие доверия в ней. Иными словами, BAN-логика тестирует характеристическое доверие.

Метод Долева-Яо работает по принципу конечного автомата. В указанном методе рассматривается набор состояний нарушителя, имеющего доступ в среду функционирования протокола [4]. Путём перебора всех возможных преобразований состояний нарушителя даётся заключение, возможно ли злоумышленнику достичь состояния, в котором ему известны секреты подлинных участников протокола. Состояние нарушителя, как одного из участников общей системы общения, может быть переквалифицировано в общее состояние протокола аутентификации. Таким образом, метод Долева-Яо даёт возможность рассматривать состояние характеристического доверия внутри системы в различные моменты времени, т.е. анализировать комбинированное доверие.

В ходе проверки честности абонента, участник протокола аутентификации должен начать доверять собеседнику [5]. В случае успешных атак на протокол, доверие будет получено ошибочно. Выявление возможных ошибок в процессе выработки доверия является тем самым универсальным методом проверки стойкости любого протокола аутентификации.

Таким образом, учитывая специфику работы BAN-анализа, можно записать характеристическую модель доверия в виде булевой функции:

$$f(d_1, d_2 \cdots d_n) = d_1 \wedge d_2 \wedge \cdots \wedge d_n, \qquad (6)$$

где d_i - есть доверие на *i*-ом шаге между двумя принципалами (участником к участнику, участником к секретному ключу и т.д.). Если доверие на каждом отдельном *i*-ом участке получает подтверждение, то доверие внутри всей системы в целом можно считать доказанным. В случае если хотя бы на одном участке проверка не удалась, общее доверие останется без доказательства и дальнейшее использование системы окажется под вопросом.

В случае с комбинированным доверием метода Долева-Яо, мы получаем систему взаимосвязанных функций, которую можно изобразить, в свою очередь, как булеву функцию от булевых функций:

$$F(f_1, f_2, \ldots f_m) = f_1 \wedge f_2 \wedge \ldots \wedge f_m, \qquad (7)$$

где каждая функция f_i может быть представлена в виде (6). При рассмотрении полученной формулы, легко заметить, что взаимосвязь можно переписать, установив её между отдельными частными значениями d_i в разных состояниях системы. Такой подход позволит обобщить анализ системы, с помощью выделения одинаковых взаимосвязей в различных состояниях системы, и возможно позволит ускорить достаточно громоздкий метод перебора всех вариантов.

Как видно из этой статьи, предлагаемое формализованное понятие доверия - это универсальный показатель стойкости криптопротокола. Выбрав формализованное понятие доверия точкой отсчёта для анализа криптографической системы, можно свести анализ к булевой функции и в дальнейшем исследовать её, а не громоздкие системы логических связей.

Выводы

В данной работе рассмотрены различные представления о понятии доверия. Описана конкретизация требований к доверию в рамках криптографических протоколов. Сформулирована и представлена формализованная модель доверия в рамках протоколов аутентификации.

Развитие и дополнение представленной формализованной модели доверия позволит обобщить, систематизировать и уточнить механизм оценки стойкости протоколов аутентификации, то есть ввести понятие меры стойкости протоколов аутентификации.

СПИСОК ЛИТЕРАТУРЫ

1. Полянская, О.Ю. Инфраструктуры открытых ключей: учебное пособие / О.Ю. Полянская, В.С. Горбатов. – М.: Издательство «Открытые системы», 2007. – 370 с.
2. Алфёров, А.П. Основы криптографии: учебное пособие / А.П. Алфёров, [и др.]. - М.: Издательство «Гелиос АРВ», 2002 - 480 с.
3. Чмора, А.Л. Современная прикладная криптография: учебное пособие / А.Л. Чмора – М.: Издательство «Гелиос АРВ», 2001.– 244 с.
4. Сабанов, А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков. - Ползуновский Вестник №2/1 2012 – С. 61-67.
5. Черёмушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие – М.: Издательский центр «Академия», 2009. – 272 с.

*Аспирант **Шиверов П.К.**, shiverovpk@samregion.ru; студент **Новосад Т.Г.**,*