На основе анализа зашифрованных текстов мы можем сделать вывод, что частотности символов в них равномерно распределены в отличии от частотности исходного текста.

Скорость шифрования по алгоритму RSAявляется большей, чем скорость шифрования в других алгоритмах.

После изменения одного символа в файле «Opentext.txt» и после проверки истинности ЭЦП система не смогла распознать изменения.

В качестве организации криптографического обмена между двумя абонентами в симметричных и асимметричных криптосистемах были проделаны нижеперечисленные операции в нашей программе.

a. Зашифровали некоторый файл по симметричному алгоритму DES и вместе с ключом шифрования передали зашифрованный файл соседу.

b. Получили от соседа файл, зашифрованный по алгоритму DES, а также ключ шифрования, и попытались расшифровать данный файл.

c. Зашифровали для соседа некоторый файл по асимметричному алгоритму RSA и передали зашифрованный файл соседу.

d. Получили от соседа файл, зашифрованный по алгоритму RSA на Нашем открытом ключе, и попытались расшифровать данный файл.

Так как все операции прошли успешно, можно сказать, что получилось реализовать организацию криптографического обмена между двумя абонентами в симметричных и асимметричных криптосистемах.

Литература

1. Теоретические основы компьютерной безопасности. Уч. Пособие для вузов по спец. "Компьютерная безопасность", "Компьютерное обеспечение информационной безопасности автоматизированных систем"/ П.Н. Девытин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербатов. – М.: Радио и связь.2000 – 190 с.

2. Основы информационной безопасности. Учебное пособие для вузов/Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов – М.: Горячая линия – Телеком, 2006-544 с.

3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001 – 368 с.

П.К. Шиверов, В.М. Пахомов

ИСТОЧНИКИ ДОВЕРИЯ В КОНТЕКСТЕ СТОЙКОСТИ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ

(Самарский государственный университет)

Введение

Анализ стойкости протоколов аутентификации, во многом, зависит от возможности установить наличие доверия между двумя или более общающимися абонентами сети.

Если, в процессе выполнения протокола аутентификации, каждая сторона общения убеждается в истинности намерений собеседника, то стойкость протокола может быть полностью доказана.

Модель доверия

Существует ряд трудов, описывающих доверие, как психологическое, философское или социальное понятие [1]. Построение общей модели доверия - крайне сложный процесс, требующий детального и всестороннего рассмотрения. Однако, модель криптографического доверия опирается на конкретный механизм криптографических протоколов.

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:

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

где D_i– есть доверие, доказанное на некотором участке выполнения протокола в некоторый момент времени.

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.)[2].

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. Так доказуемость простоты больших чисел определяется применением некоторого набора критериев на простоту. Аналогично, необходимо использовать критерии доверия.

Критерии доверия

В философском понимании доверия существует несколько его источников: этика, репутация, угроза расправы (риск), закон [3].

Понятие доверия, в контексте анализа стойкости протоколов аутентификации с одной стороны включает в себя все эти источники, но с другой стороны, преобразует их в некие новые понятия-критерии.

Далее, будет рассмотрен каждый источник и связанный с ним критерий доверия.

Этика - система моральных и нравственных норм. В контексте протоколов аутентификации, этика представляет собой требования к выполнению непосредственно протокольных обязанностей каждого участника общения. В случае, если в процессе проверки выясняется, что один из абонентов имеет возможность нарушить свои обязанности, доверие, определяемое протоколом,становится нулевым.

Репутация - мнение субъектов о человеке, группе людей или организации на основе определенного критерия. В протоколах аутентификации репутация неизбежно присутствует на уровне прикладного использования. Если один из пользователей протокола (например, интернет-магазин) заботится о своей репутации, то такой подход позволяет выработать доверие каждого пользователя этого протокола по отношению к конкретному участнику – интернет-магазину [4]. Этот критерий очень хорошо подходит для оценки среды использования протокола, а также позволяет углубить представление о доверии в контексте протоколов аутентификации. Отсюда можно выделить понятие *относительного доверия*– доверия, имеющего направление. *A* может доверять*B*, но *B* может не доверять *A*.

Угроза расправы, в протоколах аутентификации может быть определена как риск. В случае пассивных атак на криптографические протоколы, злоумышленник практически ничем не рискует, поскольку, по умолчанию, невидим для участников общения. Такие механизмы проверки стойкости протоколов аутентификации, как метод Долева-Яо, вообще предполагают, что злоумышленник всегда прослушивает каналы связи абонентов [5]. При этом, активные атаки, такие как попытка взять на себя чужую роль или атака отражением, влекут за собой неизбежные риски, связанные, в лучшем случае, с ограничением доступа. Иными словами, при анализе протокола необходимо рассматривать, какими ограничениями рискует злоумышленник. В случае пассивных атак, он не рискует ничем, а потому считается, что такие атаки ведутся постоянно. В случае активных атак, протокол должен иметь встроенные средства защиты и средства выявления злоумышленника с последующей его ликвидацией. Если протокол содержит такие средства защиты, доверие может получить некую количественную оценку.

Закон - свод обязательных норм и правил, регулирующих общественные отношения. Закон включает в себя этические требования, однако, подразумевает обеспечение этих требований путём угрозы расправы. Фактически, закон – это критерий доверия, подразумевающий выполнение сразу всех указанных выше критериев.

Выводы и следствия

Обобщая перечисленные критерии, можно сформировать представление о доверии в контексте понятия стойкости протоколов аутентификации.

Доверие может быть относительным и безотносительным. Безотносительное доверие обязательно включает в себя относительное, поскольку не может быть доверия без объекта и субъекта.

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

где $d_i \in \{0,1\}$ – есть относительное доверие.

Доверие обязательно может быть оценено путём постановки криптографического протокола в различные условия: присвоение участникам ролей, предположение о возможных видах атак и т.д.

Доверие всегда зависит от наличия в протоколах средств выявления злоумышленников с возможностью последующей их изоляции. Стоимость атаки на протокол определяется стоимостью ответных мер в случае раскрытия вторжения.

Но самое важное следствие, которое необходимо указать, это представление о протоколе, как о функции выработки доверия. В любой системе существует множество абонентов, доверие к которым равно единице. Задача протокола –путём выполнения предустановленных правил, получить доказательство принадлежности конкретного абонента к доверенному множеству.

$$\wp : (A \notin \aleph) \rightarrow (A \in \aleph), \qquad (3)$$

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

Полученное представление о доверии, как о факторе стойкости протоколов аутентификации, позволит систематизировать представление о методах анализа стойкости протоколов аутентификации и ввести совершенно новые механизмы анализа криптографических протоколов.

Литература

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, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. - 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.