Московский физико-технический институт

Эсее по защите информации

Криптрографические протокол Girault

Выполнила студентка Б01-907

Юлия Прохорова

Долгопрудный, 2022

Содержание

Кто владеет информацией, тот владеет и миром.

Натан Майер Ротшильд

1. Введение

Криптографию назвают наукой или даже искусством безопасных сообщений называется. Криптография встречается и в повседневной жизни, например, суметь помешать прочитать ваш личный дневник, зашифровав его особым образом. Но здесь мы поговорим о криптографии, которая защищает важные файлы, документы или банковские счета от любого, кто попытается их прочесть.

> Брюс Шнайер пишет: "Если я беру письмо, кладу его в сейф где-нибудь в Нью-Йорке, затем велю Вам прочитать это письмо, то это не безопасность. Это непонятно что. С другой стороны, если я беру письмо и кладу его в сейф, затем передаю этот сейф Вам вместе с детальным описанием, передаю также сотню подобных сейфов с их комбинациями, чтобы Вы и лучшие "медвежатники мира"могли изучить систему замков, а вы все равно не сможете открыть сейф и прочитать письмо - вот это и есть безопасноть."

Современная криптография - общирная область знаний, сложившаяся в результате серьезных исследований на протяжении последних десятков лет.

Данная работа направлена на то, чтобы познакомить читателя с криптографическими протоколами,а именно с протоколом Girault. Но не обо всем сразу. Начнем с сновных понятий и терминов.

2. Общая теория

Обычная ситуации при изучении криптографии - две стороны: отправитель и получатель, и первый хочет послать сообщение второму. При этом отправлять сообщение необходимо безопасным образом - чтобы перехвативший не мог его прочесть.

В данном случае само сообщение будет называться **открытым текстом**. Изменение сообщения так, чтобы не была понятна его суть - это **шифрование**, полученный текст - **шифротекст**. **Дешифрованием** же называется процесс преобразования шифротекста в открытый текст.

Шифр(или криптографический алгоритм) представляет собой математическую функцию, используемая для шифрования и дешифрования.

2.1. Протоколы

Протокол - порядок действий, предпринемаемых сторонами, чтобы решить поставленную задачу. Каждое действие должно выполняться в свою очередь и только после окончания предыдущего.

Каждый протокол должен обладать следующими характеристиками:

- Известность - каждый участник протокола должен знать протокол и последовательность составляющих его действий;
- Согласованность - каждый участник протокола должен согласиться следовать ему;
- Отсутствие противоречий (прозрачность) - каждое действие должно быть определено так, чтобы не было возможности непонимания;
- Полнота - каждой ситуации соответствует определенное заранее действие.

Криптографический протокол выходит за рамки одной лишь безопасности, участники протокола могут:

- Поделится секретом друг с другом;
- Случайно сгенерировать случайную последовательность;
- Подтвердить свою подлинность или подписать контракт одновременно.

Для демонстрации работы протоколов обычно обозначают его участников: Alice - начинает протокол, Bob - отвечает, также при необходимости третьих сторон появляются Carol и Dave.

Далее рассмотрим основные виды протоколов:

Протокол с посредником

Посредник - незаинтересованная 3я сторона, которая завершает протокол. При этом все участники протокола принимают за истину все, что скажет посредник. Все его действия - правильные, и все стороны протокола уверены в том, что посредник выполнит свою часть протокола.

такой вид протоколов предназначен для взаимодействия недоверяющих друг другу сторон.

У данного протокола, как и любого другого существуют недостатки:

- Сложно доверять безликому посреднику
- Компьютерная сеть должна обеспечить поддержку посредника
- Задержка
- Посредник должен принимать участие в каждой транзакции, являясь узким местом ы крупномасштабных реализациях протокола.
- Так как каждый участник протокола должен доверять посреднику, то посредник может стать слабым местом сети при попытке ее взлома.

Арбитражные протоколы

Арбитражный протокол делится на два подпротокола: один представляет из себя протокол без посредника - он выполняется, если стороны смогл самостоятельно договориться, второй - протокол с посредником, которого приглашают в случае разногласия между сторонами (здесь посредника называют арбитром).

Арбитр - это незаинтересованное лицо, участвующее в протоколе, которому доверяют обе стороны. Его приглашают для проверки честности выполнения протокола между сторонами. Хороший арбитражный протокол может не только определить факт мошенничества, но также и определить сторону, которой были совершены злодеяния. Такой протокол лишь обнаруживает мошенничество, но не предсказывает и не предотвращает его.

Самодостаточные протоколы

Такие протоколы называются лучшими, так как они обеспечивают полную честность сторон. Здесь не требуется посредники, даже в критические моменты, как в арбитражных протоколах. Протокол построен так, что при попытке смошенничать одной стороны - другая сразу узнает об этом, а протокол прекращает выполняться. Главный минус такого протокола состоит в том, что не сущетсвует такого самодостаточного протокола, который подходил бы под все ситуации.

Попытки вскрытия протоколов

Существует много способов взломать протокол. Можно просто подслушивать протокол, пробуя добыть информацию - это **пассивное вскрытие**, так как взломщик никак не воздействует на сам протокол. Такой тип взлома относится к взлому с использованием шифротекста. Такой вид взлома сложно обнаружить, поэтому протоколы стараются предотвратить их.

Другой способ - **активное вскрытие** , по сути - просто изменение протокола. Например, можно попробовать подменить сообщение, повторное оправить старое или внести новое. Пассивные взломщики занимаются сбором информации и криптоанализом сообщений. Активные взломщики стараются получить доступ к ресурсам или ухудшить работу системы. Взломщиком может оказаться, кто угодно - даже участник протокола. Он может обманывать, выполняя протокол или наоборот не следовать протоколу вовсе. Такой взломщик - мошенник. Пассивные мошенники выполняют правила протокола, но стараютсяполучить больше информации, чем предусмотренно протоколом. Активные нарушают работу протокола.

2.2. Распространение ключей

Для того чтобы создать и настроить надежную сеть необходимо безопасно распределять ключ - так, чтобы два конечных пользователя могли в одновременно получить секретный сессионный ключ шифрования.
Вот параметры, по которым определяют качество качество протокола распространения ключей:

- Результатом работы протокола является - секретный сессионный ключ.
- Окончание протокола подразумевает под собой - успешную взаимную аунтефикацию абонентов.
- Внешний пользователь не должен иметь возможность получить общий сессионный ключ с кем-то из внутренних пользователей.
- Добавление и удаление участников из сети производится без уведомления всех участников сети.

Сети бывают с выделенным доверенным центром и без. Второй вариант плох тем, что с ростом количества участников сети, количество пар мастер-ключей растет с квадратичной скоростью.

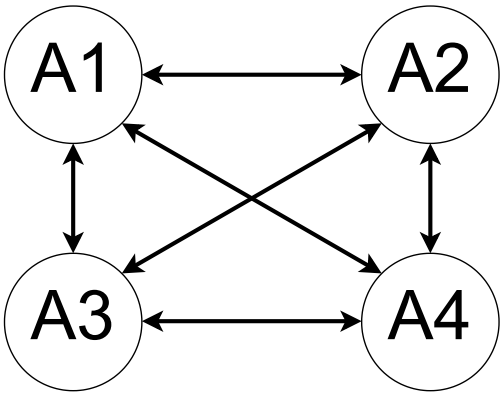

Рис. 1: Сеть без выделенного доверенного центра.

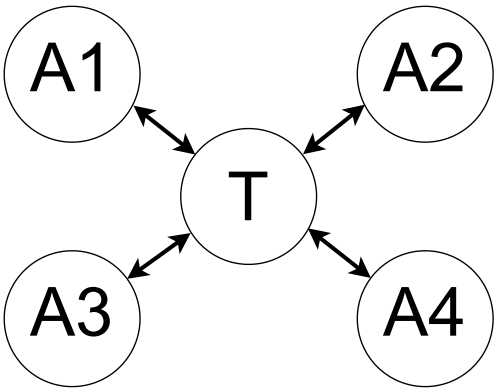

Рис. 2: Сеть с выделенным доверенным центром.

Протокол распространения ключей должен реализовывать следующие цели:

- Аунтефикация сторон протокола;
- Защита от повтора;
- Аунтефикация ключа;
- Подтверждение владения ключом;
- Совершенная секретность;
- Формирование новых ключей;
- Ограниченная ащита от атак каза в обсуживании.

Изучим более подробно схемы распределения ключей с доверенным центром на примере протокола Жиро. Но для начала рассмотрим этапы:

1) Доверенный центр создает секрет, известный только ему.
2) Для каждого нового участника сети доверенный центр, используя секрет, вырабатывает сертификат, который позволяет новому участнику вырабатывать сеансовые ключи с другими участниками.
3) Начинается общение участников. Они предъявляют друг другу идентификаторы от доверенного центра. Далее используя эту информацию они могут сгенерировать секретный сеансовый ключ для общения мужду собой.

Протокол Girault

Протокол Жиро (фр. Marc Girault) — криптографический протокол, позволяющий двум сторонам получить общий секретный ключ, не используя явную сертификацию (схема распределения ключей с доверенным центром). Полученный ключ используется для шифрования дальнейшей обмениваемой информации с помощью симметричного шифрования.

Схема распределения ключей, предложенная Жиро в 1991, решает проблему ранних протоколов, основанных на удостоверении личности, в которых стороны выбирают свои секретные ключи заключалась в том, что пользователи используют свои личные данные для формирования новых скрытых сертификатов. Так как верификатор и пользователь могут образовывать противоречивые свидетельства, то не возможно определить, кто из них может быть злоумышленником, когда появляются два сертификата.

Жиро решил эту проблему путём определения ключа, который сам себя сертифицирует. Схема Жиро предполагает участие доверенного Трента, с которым пользователи могут обмениваться информацией по надёжному защищённому каналу. Только доверенный Трент может генерировать скрытую сертификацию для этих ключей.

В схеме Жиро пользователь может сам выбрать свой закрытый ключ. Надёжность схемы Жиро строится на стойкости криптосистемы RSA (сложности факторизации больших чисел и вычисления дискретного корня). Опишем общий алгоритм:

1) Доверенный центр T:
   а) выбирает оббщий модуль $n = p \cdot q$, где p и q - большие простые числа;
   б) выбирает пару из закрытого (d, n) и открытого (e, n) ключей;
   в) выбирает элемент g поля $Z_n^\times$ максимального порядка;
   г) публикует в открытом доступе для участников параметры: n, e, g.
2) Участники:
   а) выбирают себе закрытый ключ s (каждый свой) и идентификатор;
   б) вычисляет и отправляет доверенному центру $v = g^{-s} mod n$;
   в) используя протокол аунтефикации сторон участник доказывает доверенному центу T, что владеет закрытым ключом, не раскрывая его значение;
   г) получает от доверенного центра свой открытый ключ $P = (v - I)^d = (g^{-s} - I)^d mod n$;
3) в результате для каждого участника будет выполняться $P^e + I = g^{-sA} mod n$

Как проходит аунтефикация пользователей между собой?
Пусть есть две стороды обычно их называют Alice и Bob, тогда процесс аунтефикации между ними выглядит так:

1) Alice выбирает случайное R_A и передает B
$$A \to \{I_A, P_A, t = g^{R_A} \ mod \ n\} \to B$$
2) Bob также выбирает случайное R_B
$$B \to \{R_B\} \to A$$
3)
$$A \to \{y = R_A + s_A \cdot R_B \ mod \ n\} \to B$$
4) Bob вычисляет $v_A = P_A^e + I_A \ mod \ n$
5) Bob проверяет, что $t = g^y \cdot v_A^{R_B} \ mod \ n$

Схема Жиро

Протокол генерации сессионного ключа, наываемый схемой Жиро состоит из проходов обмена открытой информацией и вычисления ключа.

1) $Alice \ \to \{P_A, I_A\} \to Bob$
2) Bob вычисляет $K = (P_A^e + I_A)^{S_B} \ mod \ n$
$$Bob \ \to \{P_B, I_B\} \to Alice$$
3) Alice вычисляет $K = (P_B^e + I_B)^{s_A} \ mod \ n$.

В результате работы схемы стороны сгенерировали одинаковый общий сеансовый ключ.

$$K_A B = (P_A^e + I_A)_B^s = (g^{-s_A})_B^s = g^{-s_A s_B} \ mod \ n;$$
$$K_B A = (P_B^e + I_B)_A^s = (g^{-s_B})_A^s = g^{-s_A s_B} \ mod \ n;$$
$$K = K_{AB} = K_{BA} \ mod \ n;$$

Данная схема обеспечивает аунтефикацию ключа - только легальные пользователи могут вычислить корректное значение общего сессионного ключа.

3. Литература

Список литературы

[1] Брюс Шнайер - "Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С."

[2] Венбо Мао - "Современная криптография. Теория и практика."