1. Протоколы идентификации

*Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования. Протоколы интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением (протокол Фейга-Фиата-Шамира). Протокол цифровых денег Чаума. Протокол идентификации Окамото. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов*

Идентификация (identification) ‑ установление тождественности неизвестного объекта известному на основании совпадения признаков; опознание. В информационных системах идентификация ‑ это присвоение субъектам и объектам идентификатора и/или сравнение идентификатора с перечнем присвоенных идентификаторов (логины, штрихкод, паттерн биометрической идентификации).

Аутентификация (authentication) - проверка (подтверждение) соответствия (подлинности) объекта или субъекта предъявленному им идентификатору.

Авторизация (authorization) ‑ предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.[1][2][3] Часто можно услышать выражение, что какой-то человек «авторизован» для выполнения данной операции — это значит, что он имеет на неё право.

Авторизацию не следует путать с аутентификацией — процедурой проверки легальности пользователя или данных, например, проверки соответствия введённого пользователем пароля к учётной записи паролю в базе данных, или проверка цифровой подписи письма по ключу шифрования, или проверка контрольной суммы файла на соответствие заявленной автором этого файла. Авторизация же производит контроль доступа к различным ресурсам системы в процессе работы легальных пользователей после успешного прохождения или аутентификации.

Идентификация и аутентификация – это первая линия обороны, «входная дверь» в информационное пространство организации.

В любой информационной системе должны быть определены все субъекты, участвующие в информационном обмене. Часть из них может быть сгруппирована, если они наделены одинаковыми (схожими) правами и обладают одинаковыми (схожими) характеристиками. Каждый субъект (группа субъектов) должен обладать уникальным именем (обозначением).

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.

В том случае, если в ходе процедуры аутентификации клиент должен предъявить сразу несколько аутентификаторов, аутентификация называется многофакторной. Например, в ходе двухфакторной аутентификации клиент должен знать пароль и воспользоваться смарт-картой.

В протоколе аутентификации участвуют две стороны: претендент (claimant - Р), или доказывающий, и проверяющий (verifier -V). Последний уже предполагает некоторую ожидаемую идентичность претендента, т. е. Р не является для V совсем незнакомым лицом - его только нужно правильно выбрать из списка известных лиц. Цель V заключается в том, чтобы подтвердить предполагаемую идентичность претендента, т. е. что он в самом деле является Р, а не кем-то иным. Проверяющий на выходе протокола аутентификации должен либо принять претендента как аутентичного, либо отвергнуть его как не соответствующего заявленной идентичности. Более строго, требования к протоколу аутентификации состоят в следующем:

1. если Р и V являются честными, V завершит протокол, приняв идентичность Р;
2. V не может повторно использовать протокол, совершенный с Р, для того, чтобы успешно деперсонифицировать Р в протоколе с третьей стороной М\
3. вероятность того, что любая сторона М, отличная от Р, проведя протокол и играя роль Р, может заставить V завершить протокол с принятием идентичности Р, пренебрежимо мала;
4. предыдущие свойства остаются справедливыми, даже если между Р и V совершено большое, но полиномиально ограниченное число сеансов протокола аутентификации, противник М участвовал в предыдущих сеансах выполнения протокола и несколько сеансов могли выполняться одновременно.

Известны четыре принципиально разных способа аутентификации:

1. «Субъект знает» - претендент обладает некоторой информацией, которой нет у других субъектов компьютерной системы (паролями, цифровыми кодами, секретными ключами) и знание которой он демонстрирует в протоколах аутентификации.
2. «Субъект обладает» - претендент имеет некоторый физический предмет (магнитную карту, интеллектуальную карту, генератор паролей), который необходим для его участия в протоколе аутентификации и который выполняет для него криптографические преобразования информации.
3. «Субъект есть» - в протоколе проверяются некоторые признаки, характеризующие человеческую индивидуальность субъекта (иными словами, биометрические признаки: отпечатки пальцев, голос, рисунок радужной оболочки глаза и др.);
4. «Субъект находится в определенном месте» ‑ выходит в сеть с конкретного статического IP-адреса, находится в зоне действия радиочастотной идентификации и т.п.

Криптографические протоколы аутентификаци реализуют первый подход - опознавание по логическому признаку. Очень часто при использовании технических средств становится возможной комбинация двух, а то и всех трех методов сразу. Одно из основных применений протоколов аутентификации - содействие контролю доступа к ресурсам компьютерных систем. Привилегия доступа к ресурсам обычно связывается с определенной идентичностью субъекта, что делает неизбежным предварительное выполнение протоколов аутентификации. Другие важные применения протоколов аутентификации - учет использования ресурсов компьютерной системы, распределение ключей криптографических систем и средств защиты информации.

Идея, лежащая в основе метода парольной аутентификации, чрезвычайно проста. Каждый субъект компьютерной системы имеет пароль - секрет, который он разделяет с системой. Демонстрация знания этого секрета (чаще всего путем разглашения самого пароля) принимается системой как подтверждение идентичности субъекта. В качестве пароля обычно выбирается буквенная и(или) цифровая последовательность, которую пользователь при необходимости должен ввести по запросу системы. Различные парольные протоколы различаются по средствам, которыми хранится парольная информация внутри системы, и по методам ее проверки.

Можно выделить три основные угрозы протоколам парольной аутентификации: разглашение, прослушивание и угадывание пароля. Угрозы могут проявиться при осуществлении трех характерных видов атак на парольные протоколы: при повторе паролей легальных пользователей злоумышленниками, полном переборе паролей и при словарной атаке на протокол.

Идея, заложенная в основе протоколов аутентификации типа «запрос — ответ» (challenge - response), заключается в том, что одна сторона (претендент) доказывает свою идентичность другой стороне (проверяющему) посредством демонстрации знания секрета проверяющему (в некоторых протоколах секрет известен проверяющему и используется для проверки ответа, в других - вообще нет необходимости, чтобы секрет был известен проверяющему). Претендент должен ответить на запрос, меняющийся во времени, причем ответ должен зависеть и от его секрета и от запроса. Запрос - это обычно число, выбираемое одной стороной в начале протокола. Если линия связи между участниками протокола прослушивается противником, ответ претендента не должен снабжать противника полезной информацией, которая могла бы быть использована в последующих сеансах протокола, так как последующие запросы проверяющего изменятся.

Протоколы «запрос — ответ» с использованием симметричных криптосхем. В этих протоколах претендент и проверяющий имеют симметричный секретный ключ либо ключи парновыборочной связи.

Общая идея асимметричных протоколов аутентификации, основанных на доказательствах с нулевым разглашением знания, состоит в том, что законный пользователь Р, имеющий открытый и секретный ключи, и проверяющий V выполняют совместный криптографический протокол интерактивного доказательства, в процессе которого Р должен доказать свою подлинность, продемонстрировав знание секретного ключа законного пользователя, но не разгласив его для проверяющего V (т. е. из информации, полученной V, ему вычислительно невозможно получить секретный ключ Р).

Все протоколы имеют два этапа: предварительный и рабочий. На предварительном, который выполняется однократно, специфицируются некоторые параметры и вырабатываются величины, участвующие в рабочем этапе протокола (в частности, открытые и секретные ключи Р). На рабочем этапе собственно выполняется доказательство аутентичности Р.

Протокол Фейга — Фиата — Шамира — протокол идентификации с нулевым разглашением, обобщение более раннего протокола Фиата — Шамира, разработанный У. Фейге, А. Фиатом и А. Шамиром в 1986 г.

Протокол позволяет одному участнику (доказывающему A) доказать в течении t раундов другому участнику (проверяющему B), что он обладает секретной информацией, не раскрывая ни единого бита этой информации.

Безопасность протокола основана на сложности извлечения квадратного корня по модулю достаточно большого составного числа n, факторизация которого неизвестна.

Существуют некоторые улучшения основной версии протокола, позволяющие уменьшить сложность взаимодействий между участниками или встроить в схему идентификационные данные.

Кроме того, схему идентификации Фейга-Фиата-Шамира можно легко преобразовать в схему подписи.

Схема идентификации:

1. Доверенный центр T публикует большое число n = pq, где p и q — простые числа, которые держатся в секрете. Также выбираются целые числа k и t - параметры безопасности.

2. Каждый участник выбирает k случайных целых чисел s1, s2, ..., sk, 1 ≤ si ≤ n-1 и k случайных бит b1, b2, ..., bk.

3. Каждый участник vi=(-1)bi ⋅ (s2i)-1 mod n, 1 ≤ i ≤ k.

4. Участник идентифицирует себя остальным участникам с помощью значений (v1, v2, …, vk; n), которые выступают в качестве его открытого ключа, в то время как секретный ключ s = (s1, s2, ..., sk) известен только самому участнику.

Последовательность действий протокола в рамках одного раунда:

1. A выбирает случайное целое число r, 1 ≤ r ≤ n-1} r и случайный бит b; вычисляет: x = (-1)b ⋅ r2 mod n и отправляет x стороне B.

2. B отправляет A случайный k-битный вектор (e1, e2, ... ,ek), где ei = 0 или ei = 1.

3. A вычисляет и отправляет B: .

4. B вычисляет: и проверяет, что z = ±x и z ≠ 0, что является доказательством для аутентификации.

Слепая подпись ‑ технология, позволяющая идентифицировать полученную информацию, то есть убедиться, что она пришла от конкретного отправителя в неизмененном виде, и удостоверить (подписать) ее, не зная ее содержания. Понятие слепой подписи придумано Дэвидом Чаумом в 1982 г., им же предложена первая реализация через алгоритм RSA.

Основная идея схемы идентификации Чаума заключается в следующем:

1. Отправитель А шифрует документ и посылает его стороне В.

2. Сторона В, не видя содержимое документа, подписывает его и возвращает обратно стороне А.

3. Сторона А снимает свой шифр, оставляя на документе только подпись стороны В.

4. По завершении этого протокола сторона В ничего не знает ни о сообщении t, ни о подписи под этим сообщением.

Данная схема характеризуется следующими свойствами – нулевое разглашение, непрослеживаемость, неподложность.

Ниже приведена реализация схемы Чаума:

1. Изначально у Боба есть открытый ключ (p,e) , где p ‑ это модуль, а e ‑ публичная экспонента ключа.

2. Алиса выбирает случайный маскирующий множитель r , взаимно простой с p, и вычисляет m' = mre mod p.

3. Алиса посылает m' по открытому каналу Бобу.

4. Боб вычисляет s' ≡ (m')d mod p, используя свой закрытый ключ (p,d).

5. Боб отсылает s' обратно Алисе.

6.Алиса убирает свою изначальную маскировку и получает подписанное Бобом исходное сообщение m следующим образом: s ≡ s' ⋅ r-1 mod p ≡ md mod p.

Д. Чаум придумал целое семейство более сложных алгоритмов слепой подписи под общим названием неожиданные слепые подписи. Схема Д.Чаума нашла применение в системах электронных платежей, позволяя клиентам осуществлять авторизированные банком платежи при неотслеживаемости банком назначения платежа.

Протокол идентификации Окамото. Параметрами системы, выбираемыми центром доверия и известными всем участникам, являются:

*p*, *q* – простые числа, такие что *q*/(*p—*1);

α1, α2 Z*p*\*, оба порядка *q*;

*t* *N* – параметр безопасности, *q*>2*t*.

Кроме того, центр доверия имеет свои собственные секретный и открытый ключи.

Параметры участника P:

*s*1, *s*2 Z*q* – секретный ключ;

*v=*α1-s1 α2*-s*2 mod *p* – открытый ключ.

Регистрация пользователя в центре доверия состоит в генерации для него некоторой идентификационной строки I, после чего центр подписывает пару (I,*v*).

Протокол аутентификации P перед V состоит в выполнении следующих шагов:

1. P→V: *x=*α1*r*1 α2*r*2 mod *p*, где *r*1, *r*2Z*q*\* - случайные числа;

2. V→P: случайное число 1≤*e*≤2*t*;

3. P→V: *y*1*=*(*r*1*+s*1*e*) mod *q*, *y*2*=*(*r*2*+s*2*e*) mod *q*;

4. V: проверяет сравнение *x*≡α1*y*1α2*y*2*ve* (mod *p*) и, если оно выполняется, то принимает доказательство.

Полнота проверяется непосредственно подстановкой в сравнение на шаге 4 значений *y*1, *y*2, *v*. Корректность доказывается аналогично корректности протокола идентификации Шнорра.

Протокол Окамото имеет немного различий с протоколом Шнорра, однако в отличие от последнего, обладает условной стойкостью к попыткам имперсонификации (успешной подмены подлинного P подставным) при условии невычислимости  за полиномиальное время с близкой к 1 вероятностью.