Эссе
по курсу «защита информации»
студента 916 группы
Залесова Александра Ивановича

Использование схемы шифрования «All-or-Nothing»[1] для организации совместного доступа к информации

(An All-or-Nothing Encryption Scheme for Secure Multi-user Information Distribution)

Введение

Несмотря на относительно большой возраст, проблема безопасного использования информации группой организаций или коллективом из нескольких человек, а также организации совместного доступа к информации по-прежнему остается актуальной. И этому есть причина: задачи, требующие не только распределения прав доступа для отдельных лиц, но и особых конфигураций уровней секретности для групп и подгрупп пользователей встречаются на практике сплошь и рядом.

Сегодня, когда успех или провал любого дела, любой миссии зависит от владения информацией, как нельзя более важной становится проблема ее защиты. Каждое современное государство накапливает огромные массивы информации о его гражданах. Делается это не обязательно с целью ущемления прав своих граждан – в руках разумного, ориентированного на великие идеалы гуманизма правительства, эта информация способствует улучшению благосостояния населения, снижению уровня преступности, а в сочетании с бурно развивающимися информационными технологиями в медицине позволяет спасти и сохранить миллионы жизней, тысячи будущих талантов и десятки гениев. Однако в руках преступников вся эта жизненно важная для нормального функционирования общества информация может стать реальной угрозой. Сложно даже оценить масштабы катастрофы, которая может наступить оттого, что информация попадет в нечестные руки.

Конечно, любое государство, любая крупная организация тратит массу усилий для защиты своей информации. К сожалению, злоумышленники становятся все более и более изощренными. Многие помнят недавний скандал, когда база абонентов оператора сотовой связи «Мобильные ТелеСистемы» была украдена и стала доступной каждому за небольшую плату. Каждое подобное происшествие вызывает новый всплеск интереса к вопросам защиты информации, потому что неизвестно, кто станет следующей жертвой мошенников.

На всех уровнях, где люди сообща работают с важной информацией, необходимы четко определенные и хорошо защищенные протоколы обмена информацией и доступа к данным. Но требования к этим протоколам постоянно растут. Во-первых, в связи с развитием вычислительных мощностей современных компьютеров требуется все большая стойкость алгоритмов шифрования. Во-вторых, постоянно отыскиваются уязвимости применяемых алгоритмов, и порой приходится сильно усложнять протоколы доступа, чтобы сделать их неподверженными атакам, использующим эти уязвимости. В третьих, в

[1] Дословный перевод термина «All-or-Nothing» означает «бескомпромиссный». Использование данного термина показалось автору не отражающим суть дела, поэтому, за неимением адекватного русского перевода, он решил оставить оригинальное наименование.

связи с распространением информационных технологий, ими приходится овладевать людям, далеким от техники, что требует от механизмов работы с защищенной информацией большей простоты, наглядности и защищенности от неправильных действий пользователя.

В нашей работе мы коснемся некоторых аспектов защиты информации в случае ее использования группами людей или организаций. Основное внимание будет уделено постановкам практических проблем, а также достоинствам и недостаткам конкретных схем их решения.

Схема шифрования «All-or-Nothing»

Рассмотрим схему шифрования «All-or-Nothing», обладающую очень важным с точки зрения криптографии свойством. Это свойство заключается в том, что не расшифровав *всю* зашифрованную с помощью данной схемы информацию невозможно расшифровать ни одного ее отдельного блока, что, безусловно, сильно увеличивает общую криптоустойчивость шифра. В дальнейшем мы покажем, как такое свойство позволяет строить системы общего доступа к информации. А пока остановимся на том, как работает схема «All-or-Nothing».

Проанализируем алгоритм работы широко применяемого на практике режима шифрования с зацеплением CBC (cipher-block chaining), одним из преимуществ которого является сильно случайная в статистическом смысле выходная информация. Для шифрования выбирается некоторое начальное значение

$$c_0=IV,$$

а далее необходимое для полной зашифровки количество раз вычисляются значения блоков

$$c_{i+1}=E\,(K,c_i \oplus m_i).$$

Недостаток приведенного алгоритма состоит в том, что любой блок зашифрованной таким образом информации может быть получен, если расшифрован хотя бы один блок шифра (термин «расшифрован» означает здесь, что криптоаналитику становится известен открытый текст и ключ, с помощью которого производится шифрование):

$$m_i=c_i \oplus D\,(K,c_{i+1}).$$

Чтобы ликвидировать этот недостаток, специалистами Массачусетского Технологического Института было предложено элегантное решение. Они стали предварять этап кодирования с помощью режима CBC (и с помощью других методов, обладающими сходными недостатками) специальным перемешиванием блоков шифруемых данных.

Идея ученых заключалась в том, чтобы произвести над исходными блоками информации специальное преобразование, названное «All-or-Nothing Transfrom», обладающее следующими характеристиками:

- преобразование обратимо;
- преобразование легко вычисляется;

- вычислительно трудно подсчитать какую-либо функцию любого блока данных, если неизвестны все полученные в результате преобразования блоки.

Еще раз отметим, что преобразование «All-or-Nothing Transfrom» является предварительным и не является непосредственно шифрованием. Шифрование осуществляется уже после выполнения преобразования.

Каким же образом устроено преобразование «All-or-Nothing Transfrom»? Вариант, предложенный учеными из ведущего американского технического ВУЗа, так называемый «Package Transfrom» выглядит следующим образом:

- Назовем исходные блоки данных $m_1,m_2,\ldots,m_s$.
- Выберем случайным образом ключ K'.
- Вычислим итоговую последовательность длины s'=s+1 как:
  - $m_i' = m_i \oplus E(K',i)$ для i=1,2,..,s.
  - $m'_{s'} = K' \oplus h_1 \oplus h_2 \oplus \ldots \oplus h_s$; где $h_i = E(K_0, m_i' + i)$ для i=1,2,…,s; а K_0 – фиксированный, общеизвестный ключ для шифрования.

Очевидно, что приведенное преобразование легко обратимо:

$$K' = m'_{s'} \oplus h_1 \oplus h_2 \oplus \ldots \oplus h_s;$$

$$m_{i=} m_i' \oplus E(K',i).$$

В то же время, если хотя бы один блок последовательности m_i' неизвестен, невозможно будет вычислить K', а, значит, и не один из блоков m_i. Таким образом, преобразование «Package Transfrom» удовлетворяет выдвинутым требованиям.

После того, как мы преобразовали исходную последовательность m_i в последовательность m_i', мы должны ее зашифровать одним из общепринятых алгоритмов. При этом мы получает такие выходные данные, что никакая их часть не может быть расшифрована, если не известен весь шифротекст.

Задачи, решаемые с помощью метода «All-or-Nothing»

Самая простая и распространенная задача при совместном доступе к информации – сделать так, чтобы доступ к данным могли получить только члены определенной группы. Простейшее решение этой задачи – применение общего пароля, ненадежно в том смысле, что пароль может попасть к человеку, не принадлежащему этой группе, что даст ему доступ ко всей закрытой информации.

Решением этой проблемы может стать модификация процедуры доступа, предусматривающая, что каждый пользователь хранит свою часть общего ключа, а получить доступ к системе каждый из них может, только когда они все соберутся вместе. Такая процедура хороша еще тем, что в одиночку никто из членов группы не сможет получить доступа к хранимой информации.

Указанная процедура доступа может быть легко реализована с помощью схемы «All-or-Nothing». Действительно, если вся информация кодируется с общедоступным

ключом K_0, и у каждого из членов группы хранится только один блок кодированных данных, то получить доступ к секретным данным они могут только все сразу.

Дальнейшее развитие этого подхода заключается в том, что иногда необходимо начать работу с закрытой информацией без одного-двух человек из группы, хотя бы в целях удобства и гарантий того, что информация не станет навсегда недоступной, если с одним членом группы что-нибудь произойдет.

Чтобы добиться такой устойчивости, необходимо привнести некоторую избыточность. Пусть теперь у каждого члена группы хранится не один блок, а два подряд идущих блока, как показано на рисунке 1. Теперь в случае отсутствия одного члена группы остальные смогут получить доступ к защищенной информации, но сам он опять же не может получить доступ к системе в одиночку.

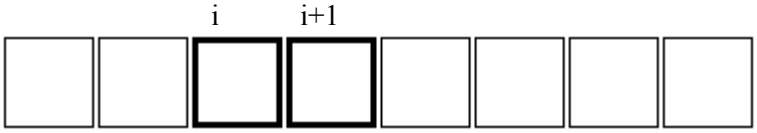

Рисунок 1
Блоки, известные i-му пользователю

Эту схему легко распространить на случай, когда необходимо допустить отсутствие двух или больше пользователей. Для этого нужно просто увеличить количество известных блоков до значения n+1, где n – количество отсутствующих членов группы.

Когда необходимо, чтобы доступ к защищенной информации имели любые два члена группы, необходимо раздать пользователям все блоки, кроме одного. При этом, благодаря замечательным свойствам схемы «All-or-Nothing», никто из них не сможет расшифровать даже части информации, несмотря на то, что будет иметь почти все данные.

Достоинства схемы «All-or-Nothing» позволяют также использовать открытый канал, который, как правило, мощнее закрытого, для передачи большого объема кодированных данных. По закрытому каналу можно передать один лишь блок, в то время как по открытому можно пересылать все оставшиеся блоки. При этом мы можем быть практически на сто процентов уверенны, что у «перехватчика» практически нет шансов понять хотя бы часть информации, поскольку для него задача расшифровки многократно усложняется.

Наконец, остановимся на недостатках описанной схемы. Главным и самым принципиальным недостатком является то, что при частичном или даже очень незначительном искажении кодированных данных становится невозможно их восстановление. Это может привести к усложнению алгоритма путем введения дополнительной избыточности с целью увеличения надежности передачи.

Второй не менее важный недостаток заключается в том, что для шифрования-дешифрования необходимы все блоки сразу, то есть схема «All-or-Nothing» не может применятся для кодирования поточной информации или информации неопределенной длины. Это, безусловно, ограничивает возможности применения данной схемы в практических приложениях.

Литература

1. Ronald R. Rivest. All-or-Nothing Encryption and the Package Transfrom. MIT Laboratory for computer science.
2. *Hugo Krawczyk*. Secret Sharing made short. CRYPTO 93
3. *Matt Blaze*. "Key Management in an Encrypting File System". AT&T Bell Laboratories.