Аутентификация

2. Взаимная аутентификация

Рассмотрим простой протокол взаимной аутентификации с использованием криптосистемы с открытым ключом. Допустим, Алиса и Боб хотят проверить подлинность друг друга. У каждого из них есть пароль, известный другому, которыми они обменялись предварительно по защищённому каналу связи: у Алисы P_A; у Боба P_A.

1. Алиса и Боб обмениваются открытыми ключами;
2. $A \rightarrow B$: $\{E_B(P_A)\}$, Алиса шифрует P_A открытым ключом Боба и отправляет Бобу;
3. $B \rightarrow A$:$\{E_A(P_B)\}$, Боб шифрует P_B открытым ключом Алисы и отправляет Алисе;
4. Боб расшифровывает P_A, полученный на этапе 2, и проверяет корректность пароля. Алиса расшифровывает P_B, полученный на этапе 3, и проверяет корректность пароля.

Аутентификация

2. Взаимная аутентификация

Однако этот протокол не устойчив против атаки «человек посередине», которую Мэллори может провести следующим образом:

1. Алиса и Боб обмениваются открытыми ключами. Мэллори перехватывает оба сообщения. Затем она подменяет ключи и отсылает обоим корреспондентам собственный открытый ключ.
2. Алиса шифрует P_A открытым ключом «Боба» и отсылает пароль Бобу. Мэллори перехватывает сообщение, расшифровывает P_A своим закрытым ключом, опять шифрует P_A открытым ключом Боба и посылает пароль Бобу.
3. Боб шифрует P_B открытым ключом «Алисы» и отсылает пароль Алисе. Мэллори перехватывает сообщение, расшифровывает P_B своим закрытым ключом, опять шифрует P_B открытым ключом Алисы и посылает пароль Алисе.
4. Боб расшифровывает P_A, полученный на этапе 2, и проверяет корректность пароля. Алиса расшифровывает P_B, полученный на этапе 3, и проверяет корректность пароля.

Алиса и Боб не заметят никаких отличий, однако теперь Мэллори знает и P_A и P_B.

Аутентификация

2. Взаимная аутентификация

Для противостояния этой атаке Ро́нальд Риве́ст и Ади Шамир пре дложили протокол «взаимоблокировки» или «Держась за руки» (Interlock Protocol).

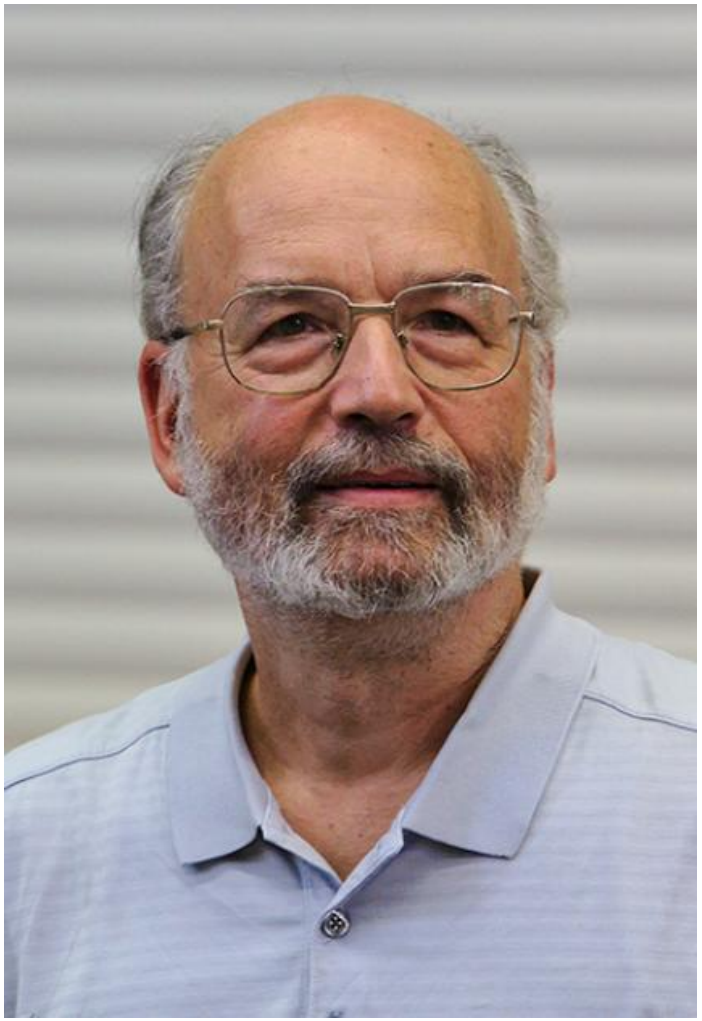
Ро́нальд Линн Риве́ст (англ. *Ronald Linn Rivest*; род. 1947, Скенектади, Нью-Йорк) — американский специалист по криптографии. Имеет звание «профессора имени Эндрю и Эрны Витерби по компьютерным наукам» на «факультете электротехники и компьютерных наук» MIT (EECS) и состоит в штате кафедры CSAIL в MIT. С 2015 года Институтский профессор MIT. Также является членом лаборатории «Теория вычислений» и лидером группы «Криптография и информационная безопасность».

Аутентификация

2. Взаимная аутентификация

Для противостояния этой атаке Ро́нальд Риве́ст и Ади Шамир пре дложили протокол «взаимоблокировки» или «Держась за руки» (Interlock Protocol).

Ади Шамир (6 июля 1952 года, Тель-Авив, Израиль) — известный израильский криптоаналитик, учёный в области теории вычислительных систем, профессор информатики и прикладной математики в институте Вейцмана, лауреат премии Тьюринга. Член НАН Израиля (1998), иностранный член НАН США (2005), Французской академии наук (2015), Лондонского королевского общества (2018) и Американского философского общества (2019).



Аутентификация

2. Взаимная аутентификация

Протокол «Держась за руки» (Interlock Protocol):

1. Алиса и Боб обмениваются открытыми ключами;
2. $A \rightarrow B$: $\{E_B(P_A)_1/2\}$, Алиса шифрует P_A открытым ключом Боба и отправляет первую половину зашифрованного сообщения Бобу.
3. $B \rightarrow A$:$\{E_A(P_B)_1/2\}$, Боб шифрует P_B открытым ключом Алисы и отправляет первую половину зашифрованного сообщения Алисе.
4. $A \rightarrow B$: $\{E_B(P_A)_2/2\}$, Алиса отправляет вторую половину Бобу.
5. $B \rightarrow A$:$\{E_A(P_B)_2/2\}$, Боб отправляет вторую половину Алисе.
6. Боб конкатенирует $E_B(P_A)_1/2$ и $E_B(P_A)_2/2$, полученные на этапах 2 и 4, расшифровывает P_A и проверяет корректность пароля. Алиса, выполняет аналогичные действия от этапов 3 и 5, расшифровывает P_B и подтверждает корректность пароля.

Суть метода заключается в том, что половина зашифрованного сообщения не может быть дешифрована без второй половины. Боб не сможет прочитать ни одной части сообщения Алисы до этапа 6, так же как и Алиса. Но и Мэллори, перехватив половину сообщения Алисы на этапе 2, не сможет расшифровать её своим закрытым ключом и снова зашифровать открытым ключом Боба.

Аутентификация

2. Взаимная аутентификация

Протоколы SKID

Для проекта RACE RIPE были разработаны симметричные криптографические протоколы аутентификации SKID2 и SKID3. Для обеспечения секретности в протоколах используется код MAC (ХЭШ-функция с добавлением закрытого ключа, т.е. хэш-значение зависит от функции и от ключа). Кроме того, предполагается, что Алиса и Боб пользуются общим секретным ключом K.

Протокол SKID2 (Боб доказывает свою подлинность Алисе):

1. $A \rightarrow B$: $\{R_A\}$, Алиса отправляет своё случайное число (спецификация RIPE предписывает использование 64-битового числа).
2. $B \rightarrow A$:$\{R_B, H_K(R_A, R_B, B)\}$, где B — имя Боба, R_B, — случайное число Боба (спецификация RIPE предписывает использование 64-битового числа), H_K — это код MAC.
3. A: вычисляет $H_K(R_A, R_B, B)$ и сравнивает результат со значением, полученным от Боба. Если результаты совпадают, Алиса убеждается в том, что она связалась именно с Бобом.

Аутентификация

2. Взаимная аутентификация

Протоколы SKID

Для проекта RACE RIPE были разработаны симметричные криптографические протоколы аутентификации SKID2 и SKID3. Для обеспечения секретности в протоколах используется код MAC (ХЭШ-функция с добавлением закрытого ключа, т.е. хэш-значение зависит от функции и от ключа). Кроме того, предполагается, что Алиса и Боб пользуются общим секретным ключом K.

Протокол SKID3 (Алиса доказывает свою подлинность Бобу):

4. $A \rightarrow B$: $\{H_K(R_B, A)\}$, где A — это имя Алисы.
5. B: вычисляет $H_K(R_B, A)$ и сравнивает результат со значением, полученным от Алисы. Если результаты совпадают, Боб убеждается в том, что он связался именно с Алисой.

Аутентификация

3. Аутентификация сообщений

Для подтверждения подлинности сообщения могут быть использованы следующие три подхода.

1. Цифровая подпись. Чтобы подтвердить кому угодно подлинность сообщения Алисы, совершенно достаточна ее цифровая подпись.

2. Симметричные алгоритмы тоже обеспечивают некоторую аутентификацию. Когда Боб получает от Алисы сообщение, зашифрованное их общим ключом, он знает, что это сообщение поступило от Алисы, поскольку он надеется, что этот ключ не знает никто посторонний. Однако у Боба нет никакой возможности убедить в этом какую-либо третью сторону. Трента можно убедить, что сообщение отправлено или Алисой, или Бобом, но у него нет способа установить конкретного автора сообщения.

3. Если сообщение не шифровано, Алиса может также использовать код MAC. Это тоже убедит Боба в подлинности сообщения, но возникнут те же проблемы, что и при симметричной криптографии. По сути, код MAC в этом случае выступает в роли электронной подписи, но общей для Алисы и Боба.