The Passive Ex 9

1. Is Latin taught at this school?
2. -\\-
3. He was hit with the tennis racquet
4. Preparations has been made.
5. Whom the is cleaned by?
6. Whom the Pyramids were built by?
7. We are going to receive a pay rise
8. My car is going to be delivered
9. The suspects are questioned by police
10. Were thieves detected by your neighbors?
11. Paul has been asked to star in school play
12. Computers are used by children
13. Whom the kitchen window had been smashed
14. The work hadn’t been completed by the end of this month.
15. Letters are going to be posted.
16. Pancakes are made from flour, eggs and milk
17. Had the window been closed?
18. The work hasn’t had done yet
19. The parcel won’t been delivered.

Translation

Безопасные транзакции во всём пространстве интернета подразумевают 3 цели. Первое, две стороны заинтересованные в транзакции (скажем, email или бизнес покупка), не желают, что б 3-я сторона могла прочитать их отправки. Некоторые шифровщики данных призваны предотвратить данное действо. Вторая —получатель должен иметь возможность отследить вмешался ли кто-либо в процессе получения или отправки. Это называется: схема целостности сообщения. И наконец, две стороны должны быть уверены, что они общаются друг-с-другом, а не с 3-м лицом. Данное действо реализуемо с помощью пользовательской аутентификации.

На сегодняшний день, методы шифрования данных основаны на технике, называемой шифрование с открытым ключом. Каждый, кто пользуется данным методом, имеет приватный и публичный ключ. Сообщения шифруются и дешифруются этими ключами. Сообщения шифруются и дешифруются этими ключами. Сообщение зашифрованное именно вашим публичным ключом может быть расшифровано системой, которая знает только ваш приватный ключ.

Что б система заработала, две стороны, вовлечённые в подобную транзакцию должны знать публичные ключи друг друга. Приватные же, шифруются исключительно для одного пользователя— владельца. Когда я хочу отправить зашифрованное сообщение, я использую ваш публичный ключ, что б преобразовать моё сообщение в бессмыслицу и я знаю о том, что только вы можете преобразовать обратно из набора бреда в первоначальное сообщение , поскольку только вы знаете приватный ключ. Шифрование с открытым ключом может работать и в обратном направлении, только ваш публичный ключ может расшифровать ваши приватные ключи шифрования.

Что б сделать сообщение защищённым от внедрения (обеспечивающаяся целостью сообщения),отправитель пропускает каждое сообщение через функцию дайджеста сообщения. Эта функция в приложении генерирует номер, называемым кодом аутентификации сообщения(MAC). Эта система работает по причине того, что практически невозможно, что у изменённого сообщения будет такой же код, как и у другого. Также, система обеспечивает невозможность преобразования из кода в первоначальное сообщение.

Софт, используемый для данного обмена, порождает MAC для сообщения перед тем, как оно будет зашифровано. Далее, он шифрует MAC приватным ключом отправителя. После, оно шифрует оба сообщения и шифрует MAC публичным ключом получателя и отправляет сообщение.

Когда получатель получает сообщение и расшифрует его , он так же получают зашифрованный MAC. Софтина принимает сообщение и пускает его через всё ту же функцию дайджеста сообщения, которую использует отправитель а так же генерирует свой MAC. Если же они одинаковые, то сообщение не было подделано либо изменено.

Динамика интеренета всё более сводится к тому, что система пользовательской аутентификации обязана существовать. Такое может быть осуществлено путём использования цифровых сертификатов.

Сервер аутентифицирует себя к клиенту, используя незашифрованные, основанные на ASCII цифровые сертификаты. Цифровые сертификаты содержат информацию про компанию, обслуживающую сервер, включая публичный ключ сервера. Цифровая сертификация «подписана» доверенным издателем, что предполагает что издатель уже исследовал и дал добро компании, держащая сервера и подтверждает что компания законна. Если клиент доверяет издателю, то тогда и идёт доверие серверу. Издатель подписывает сертификат путём генерации MAC для него, потом шифрует MAC приватным ключом издателя. Если клиент доверяет издателю, тогда уже становится известным публичный ключ издателя.

Динамика и стандарты безопасности операций будет изменена, но три базовые понятия безопасности проводки операций останется неизменной. Если вы понимаете базис, тогда вы на 3 шага впереди всех остальных.

EX A

1 a

2 c

3 public-key cryptography

4 decipher or decryption

5 b

6 company’s public key, information of server holder

EX B

1

1 a

2 d

3 b

4 c

2

1 d

2 e

3 a

4 b

5 f

6 c