ВУЗ: МГТУ им. Баумана

Группа: ИУ5-61Б

Студент: Белоусов Евгений

1. This text is about safe data transfer.
2. Security is very important for data transmission.
3. We want to bad guys can not read our messages, or communicate with our partners instead us.
4. Public-key cryptography is very popular safe data transfer technology for data transmission.
5. MAC is used for message tamper proof.
6. Digit certificates are used widely in Web for user`s authenticates.
7. To sum up, standards of secure transactions will change, but tenets of secure transaction will remain the same.

Безопасная Передача Данных

Безопасные транзакции через Интернет преследуют три цели. Во-первых, две стороны, участвующие в транзакции (скажем, электронная почта или покупка бизнеса), не хотят, чтобы третья сторона могла прочитать их передачу. Для предотвращения этого необходима определенная форма шифрования данных. Во-вторых, получатель сообщения должен быть в состоянии определить, не вмешался ли кто-то в его передачу. Это требует схемы целостности сообщения, наконец, обе стороны должны знать, что они общаются друг с другом, а не с самозванцем. Это делается с помощью аутентификации пользователя.

Современные методы шифрования данных опираются на метод, называемый криптографией с открытым ключом. Каждый, кто использует систему с открытым ключом, имеет открытый ключ и закрытый ключ. Сообщения шифруются и расшифровываются с помощью этих ключей. Сообщение, зашифрованное вашим открытым ключом, может быть расшифровано только системой, которая знает ваш закрытый ключ.

Чтобы система работала, две стороны, участвующие в безопасной транзакции, должны знать открытые ключи друг друга. Однако секретные ключи-это тщательно охраняемые секреты, известные только их владельцам. Когда я хочу отправить вам зашифрованное сообщение соедините ваш открытый ключ, чтобы превратить мое сообщение в тарабарщину. Я знаю, что только вы можете превратить эту тарабарщину обратно в исходное сообщение, потому что только вы знаете свой секретный ключ. Криптография с открытым ключом также работает в обратном направлении - то есть только ваш открытый ключ может расшифровать шифрование вашего закрытого ключа.

Чтобы сделать сообщение защищенным от несанкционированного доступа (обеспечивая целостность сообщения), отправитель запускает каждое сообщение через функцию дайджеста сообщений. Эта функция в приложении создает число, называемое кодом аутентификации сообщений (MAC). Система работает потому, что почти невозможно, чтобы измененное сообщение имело тот же MAC, что и другое сообщение. Кроме того, вы не можете взять MAC и превратить его обратно в исходное сообщение.

Программное обеспечение, используемое для данного обмена, создает MAC для сообщения, прежде чем оно будет зашифровано. Затем он шифрует MAC с помощью закрытого ключа отправителя. Затем он шифрует как сообщение, так и зашифрованный MAC с открытым ключом получателя и отправляет сообщение.

Когда получатель получает сообщение и расшифровывает его, он также получает зашифрованный MAC. Программное обеспечение принимает сообщение и запускает его через ту же функцию дайджеста сообщений, что и отправитель, и создает свой собственный MAC. Затем он расшифровывает MAC отправителя. Если это одно и то же, то сообщение не было подделано.

Динамика Интернета диктует необходимость существования системы аутентификации пользователей. Это можно сделать с помощью цифровых сертификатов.

Сервер аутентифицирует себя клиенту, отправляя незашифрованный цифровой сертификат на основе ASCII. Цифровой сертификат содержит информацию о компании, управляющей сервером, включая открытый ключ сервера. Цифровой сертификат "подписывается" доверенным эмитентом цифрового сертификата, что означает, что эмитент

исследовал компанию, эксплуатирующую сервер, и считает его законным. Если клиент доверяет эмитенту, то он может доверять и серверу. Эмитент "подписывает" сертификат, генерируя для него MAC, а затем шифрует MAC с помощью закрытого ключа эмитента. Если клиент доверяет эмитенту, то он уже знает открытый ключ эмитента.

Динамика и стандарты защищенных транзакций изменятся, но три основных принципа защищенных транзакций останутся прежними. Если вы понимаете основы, то вы уже на три шага впереди всех остальных.

a.

1. a
2. c
3. public-key cryptography
4. decrypt
5. a
6. information about the company operating the server including the server`s public-key

b

1.

a - 4

b - 3

c - 1

d – 2

2.

a - 3

b - 4

c - 6

d - 1

e - 2

f – 5

3.

a - false

b - true

c - false

d - false

e - false

f - false

g - true

h – true

4. c, d, b, a

desiper – десайпер

1. Jump instruction is used for program navigation.

2. The main parts of the virus code are misdirection, reproduction, trigger and payload.

1c

2b

3d

4c