

Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

Раздел 18 - SSH

Утилита SSH

SSH handshake

Цель: нужен доступ на удаленную машину по сети для выполнения команд или передачи файлов.

RSH, remote shell - 1983 г.

OSI L7 - приложение.

- Все данные, всегда, включая логин и пароль, передаются в открытом виде.
- Данные не верифицированы, поэтому “клиент” или “сервер” могут подменить свой IP адрес, имя хоста и получить доступ. Хосты сторон не аутентифицированы.

SSH v1, secure shell - 1995 г.

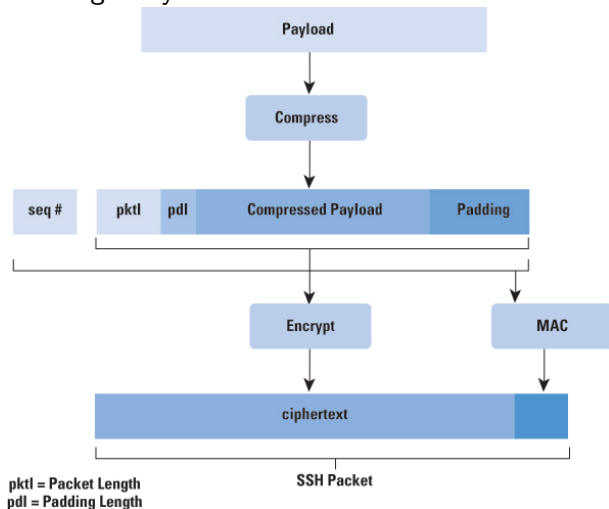
Шифрование. Контроль целостности: CRC32 (контрольная сумма). Выч. по данным. Зл-к может добавить в канал свои данные. И прочие ошибки в коде - возможна авторизация злоум-ка.

SSH v2 - первая версия спецификации в 1997, стандарт IETF с 2006.

- ssh - терминал и туннель
- scp, sftp - копирование файлов
- безопасный канал - ЕаМ - шифрование и MAC
- авторизация сервера по публичному ключу
(у клиента есть база данных соответствия IP \leftrightarrow п.к.) -
защита от подмены IP сервера
- авторизация клиента по паролю или публичному ключу
или сертификату - по защищенному каналу
- \Rightarrow защита от MitM
- MAC - защита от добавления и изменения сообщений
- номер сообщения - защита от атаки воспроизведения
- cookie - защита от DoS атаки

SSH сессия:

симметричные сессионные ключи для шифрования и MAC в одну сторону и в другую - всего 4, меняются по времени или объему данных.
Padding - случайный.



Раздел 18 - SSH

Утилита SSH

SSH handshake

1) Начало сессии, аутентификация сервера.

1. $C \rightarrow S: V_c$ - версия SSH

2. $S \rightarrow C: V_s$ - версия SSH

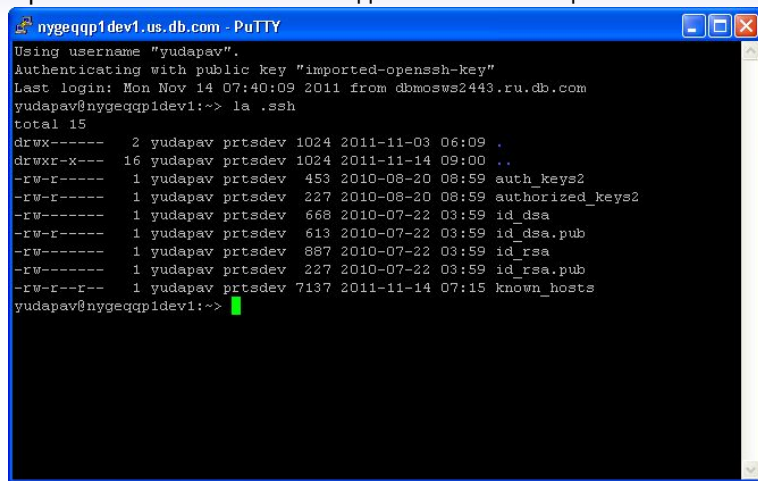
3. $C \rightarrow S: I_c$ - [алгоритм п.к. хоста клиента], список алгоритмов обмена ключами, список алгоритмов сессии

4. $S \rightarrow C: I_s$ - алгоритм п.к. сервера, список алгоритмов обмена ключами, список алгоритмов сессии

5. $S \rightarrow C: P_S, [CERT(P_S)], P_T$

Клиент проверяет P_S - публичный ключ хоста сервера, авторизует сервер.

Хранение локальной “базы данных” и вообще всего:



```
nygeqqp1 dev1.us.db.com - PuTTY
Using username "yudapav".
Authenticating with public key "imported-openssh-key"
Last login: Mon Nov 14 07:40:09 2011 from dbmosws2443.ru.db.com
yudapav@nygeqqp1dev1:~> ls -la .ssh
total 15
drwx-----  2 yudapav prtsdev 1024 2011-11-03 06:09 .
drwxr-x---- 16 yudapav prtsdev 1024 2011-11-14 09:00 ..
-rw-r-----  1 yudapav prtsdev  453 2010-08-20 08:59 auth_keys2
-rw-r-----  1 yudapav prtsdev  227 2010-08-20 08:59 authorized_keys2
-rw-----  1 yudapav prtsdev  668 2010-07-22 03:59 id_dsa
-rw-r-----  1 yudapav prtsdev  613 2010-07-22 03:59 id_dsa.pub
-rw-----  1 yudapav prtsdev  887 2010-07-22 03:59 id_rsa
-rw-----  1 yudapav prtsdev  227 2010-07-22 03:59 id_rsa.pub
-rw-r--r--  1 yudapav prtsdev 7137 2011-11-14 07:15 known_hosts
yudapav@nygeqqp1dev1:~>
```

Безопасность хранения ключей в UNIX достигается тем, что право на запись, чтение и исполнение дир-и `~/.ssh` и для всех файлов в ней имеет только сам пользователь.

known_hosts:

```
nygeqqpluat2,172.17.111.9 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA2KCpHhHTvsUTcjlzeMfqS+2dSfIqd
JxeeCZMQHTYr6cf4rhKSQRY83yecIq4jy4K41nBPJWqyv1q+57/Eh6aNWED9u8tYFbeleuTBopOzlRHQ8/nW0hbhNqY
2saY9aAPTuqEoSXeMF9hLPTM9eas9fG6w6opNbY05Oo8/fw772M=
```

```
yudapav@nygeqqp1dev1:~> rm .ssh/known_hosts
yudapav@nygeqqp1dev1:~> ssh nygeqqpluat2
The authenticity of host 'nygeqqpluat2 (172.17.111.9)' can't be established.
RSA key fingerprint is 4d:a3:98:08:d6:59:f2:15:ef:f7:e7:53:66:8a:8f:18.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'nygeqqpluat2,172.17.111.9' (RSA) to the list of known hosts.
Last login: Mon Nov 14 08:44:21 2011 from nygeqqp1dev1.us.db.com
```

fingerprint - 128-битный хэш ключа.

```

#####
@      WARNING: POSSIBLE DNS SPOOFING DETECTED!      @
#####
The RSA host key for arvo.suso.org has changed,
and the key for the according IP address 216.9.137.122
is unchanged. This could either mean that
DNS SPOOFING is happening or the IP address for the host
and its host key have changed at the same time.
Offending key for IP in /home/suso/.ssh/known_hosts:10
#####
@      WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @
#####
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
96:92:62:15:90:ec:40:12:47:08:00:b8:f8:4b:df:5b.
Please contact your system administrator.
Add correct host key in /home/suso/.ssh/known_hosts to get rid of this message.
Offending key in /home/suso/.ssh/known_hosts:53
RSA host key for arvo.suso.org has changed and you have requested strict
checking.
Host key verification failed.
```

2) Создание мастер ключа.

По RFC 4432:

6. Клиент создает случайный мастер ключ K .

$C \rightarrow S$: $\text{RSA}(P_T, K)$ - для PFS.

7. Сервер расшифровывает K , вычисляет

$H = \text{hash}(V_c \mid V_s \mid I_c \mid I_s \mid P_S \mid P_T \mid \text{RSA}(P_T, K), K)$

$S \rightarrow C$: $\text{sign}(S_S, H)$. H - секретное!

Алгоритмы создания мастер ключа:

- RFC 4253 (2006): Диффи-Хеллман. Нагружает ЦП обеих сторон.
- RFC 4432 (2006): RSA. Меньше грузит ЦП клиента (RFC 4432).
- RFC 5656 (2009): ECRSA. Еще меньше грузит ЦП обеих сторон.

3) Создание сессионных ключей

по RFC 4253:

Если это была первичная иниц-я сессии, то $SID := H$.

Сессионные ключи и IV для первого сообщения:

$$IV_CS = \text{hash}(K \mid H \mid "A" \mid SID)$$
$$IV_SC = \text{hash}(K \mid H \mid "B" \mid SID)$$
$$ke_CS = \text{hash}(K \mid H \mid "C" \mid SID)$$
$$ke_SC = \text{hash}(K \mid H \mid "D" \mid SID)$$
$$ki_CS = \text{hash}(K \mid H \mid "E" \mid SID)$$
$$ki_SC = \text{hash}(K \mid H \mid "F" \mid SID)$$

По истечении срока действия сессионных ключей, повторить их создание с пункта 6.

4) Авторизация клиента.

Методы авторизации клиента:

- публичный ключ P_C
- пароль
- сертификат (RFC 6187, 2011 год)

User Authentication Protocol

Все данные шифруются и заверяются сессионными ключами.

8. Заранее на сервере сохраняется P_C
или сейчас передается P_C , заверенный сертификатом.

$C \rightarrow S$: username

9. Сервер создает случайное число r

$S \rightarrow C$: $E(P_C, r)$

10. $C \rightarrow S$: r

11. $S \rightarrow C$: Ack/Rej, [список других способов авторизации]

Файл `authorized_keys2` на сервере:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAsYUpSGRtTc4whpWt8n/92OEvyo5SsacUG3TYbDgfYoE5iNRVoI3vDEeDU22kqVyf4+
sB5h6TBuyI2insG/qXfGbpvfvILpgdcraFECq19HFe2TK52+ek93/92WviiNUcpXGBTnCNu6wbdJvMywFjONjTo49nhEpDJmtN8kl
WUu6M= yudapav@sydeqws33
.ssh/authorized_keys2 lines 1-1/1 (END)
```

Возможности утилиты SSH (рассказать на семинаре)

- ssh-keygen (puttygen)
- ssh терминал
- первый логин на сервер, изменение IP сервера или ключа в known_hosts на клиенте
- ssh исполнение команды
- scp
- ssh port forwarding (туннель, все соедин. к локальному порту форв. на удал. сервер)

SSH port forwarding: [https:](https://help.ubuntu.com/community/SSH/OpenSSH/PortForwarding)

[//help.ubuntu.com/community/SSH/OpenSSH/PortForwarding](https://help.ubuntu.com/community/SSH/OpenSSH/PortForwarding)

и http://support.suso.com/supki/SSH_Tutorial_for_Linux

Литература к лекции

1. W. Stallings, *Protocol Basics: Secure Shell Protocol*.

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_12-4/124_ssh.html

2. J. Purser, *SSHv1 or SSHv2? What's the big deal?* <https://learningnetwork.cisco.com/blogs/network-sheriff/2008/09/22/sshv1-or-sshv2-whats-the-big-deal>

3. RFC 4432 - *SSH Key Exchange*.

<http://tools.ietf.org/html/rfc4432>,
а также RFC 4251, RFC 4253.

4*. S. Williams, *Analysis of the SSH Key Exchange Protocol*.

<https://eprint.iacr.org/2011/276.pdf>