SSH-protokollet

Niels Möller

2018-03-21

Historia

1993 Kerberos version 5 (RFC 1510)

1995 Första SSH släpps av Tatu Ylonen, för att ersätta telnet, rsh,. . .

1995 SSL-2.0 (trasigt) släpps av Netscape.

1996 SSL-3.0 släpps av Netscape.

1997 Första Internet-Draft för SSH-2, IETF secsh wg.

1998 Första incheckning i LSH.

1999 TLS 1.0, RFC 2246.

2000 OpenSSH för stöd för SSH-2.

2001 Nettle-1.0 släpps (spin-off från LSH).

2006 RFC 4250-4254 publiceras.

Flera protokoll

- Transportprotokoll, RFC 4253.
- Användarautenticering, RFC 4252.
- Multiplexade kanaler, RFC 4254.
- SFTP (ingen RFC, fastnade i feature creep).

Transportprotokollet

- En rad klartext:

  ```
  SSH-2.0-softwareversion SP comments CR LF
  ```

- Binärt paketprotokoll:

  ```
  uint32    packet_length
  byte      padding_length
  byte[n1]  payload
  byte[n2]  random padding
  byte[m]   mac
  ```

- Ordning: Komprimering, mac, kryptering.

Protokollmeddelanden

Första byten i payload är meddelandetyp:

1	SSH_MSG_DISCONNECT
2	SSH_MSG_IGNORE
3	SSH_MSG_UNIMPLEMENTED
4	SSH_MSG_DEBUG
5	SSH_MSG_SERVICE_REQUEST
6	SSH_MSG_SERVICE_ACCEPT
20	SSH_MSG_KEXINIT
21	SSH_MSG_NEWKEYS

Handskakning

```
byte          SSH_MSG_KEXINIT
byte[16]      cookie (random bytes)
name-list     kex_algs
name-list     server_host_key_algs
name-list     encryption_algs_client_to_server
name-list     encryption_algs_server_to_client
name-list     mac_algs_client_to_server
name-list     mac_algs_server_to_client
name-list     compression_algs_client_to_server
name-list     compression_algs_server_to_client
name-list     languages_client_to_server
name-list     languages_server_to_client
boolean       first_kex_packet_follows
uint32        0 (reserved)
```

Nyckelutbyte med `diffie-hellman-group14-sha1`

- Diffie-Hellman nyckelutbyte.
- Sessionsid är en hash av

```
string    V_C, the client's identification
string    V_S, the server's identification
string    I_C, the client's SSH_MSG_KEXINIT
string    I_S, the server's SSH_MSG_KEXINIT
string    K_S, the host key
mpint     e, exchange value sent by the client
mpint     f, exchange value sent by the server
mpint     K, the shared secret
```

- Servern signerar sessionsid, för serverautenticering.
- Ger nya nycklar används efter `SSH_MSG_NEWKEYS`.
- Bör göras om efter en timme eller 1 GB data.

Autenticering, SERVICE_REQUEST ssh-userauth

Använder följande meddelanden:

- 50 SSH_MSG_USERAUTH_REQUEST
- 51 SSH_MSG_USERAUTH_FAILURE
- 52 SSH_MSG_USERAUTH_SUCCESS
- 53 SSH_MSG_USERAUTH_BANNER

Vanliga metoder:

- publickey Nyckelpar.
- keyboard-interactive Passar med PAM.
- password Lösenord.
- gssapi Kerberos.

Begäran om autenticering

- Begär service `ssh-connection`

```
byte      SSH_MSG_USERAUTH_REQUEST
string    user name in UTF-8
string    service name in US-ASCII
string    method name in US-ASCII
....      method specific fields
```

- För metoden `publickey`:

```
boolean   TRUE
string    public key algorithm name
string    public key to be used
string    signature
```

- Signatur på sessionsid + meddelandet ovan.

Svar på autenticering

- Efter `USERAUTH_SUCCESS` startas begärd service.
- Misslyckad begäran ger

```
byte          SSH_MSG_USERAUTH_FAILURE
name-list     authentications that can continue
boolean       partial success
```

Service ssh-connection

```
90 SSH_MSG_CHANNEL_OPEN
     byte      SSH_MSG_CHANNEL_OPEN
     string    channel type
     uint32    sender channel
     uint32    initial window size
     uint32    maximum packet size
     ...
91 SSH_MSG_CHANNEL_OPEN_CONFIRMATION
     byte      SSH_MSG_CHANNEL_OPEN_CONFIRMATION
     uint32    recipient channel
     uint32    sender channel
     uint32    initial window size
     uint32    maximum packet size
92 SSH_MSG_CHANNEL_OPEN_FAILURE
97 SSH_MSG_CHANNEL_CLOSE
     byte      SSH_MSG_CHANNEL_CLOSE
     uint32    recipient channel
```

Att skicka data

```
93 SSH_MSG_CHANNEL_WINDOW_ADJUST
     byte      SSH_MSG_CHANNEL_WINDOW_ADJUST
     uint32    recipient channel
     uint32    bytes to add
94 SSH_MSG_CHANNEL_DATA
     byte      SSH_MSG_CHANNEL_DATA
     uint32    recipient channel
     string    data
95 SSH_MSG_CHANNEL_EXTENDED_DATA
     byte      SSH_MSG_CHANNEL_EXTENDED_DATA
     uint32    recipient channel
     uint32    data_type_code
     string    data
96 SSH_MSG_CHANNEL_EOF
     byte      SSH_MSG_CHANNEL_EOF
     uint32    recipient channel
```

Andra operationer

80 SSH_MSG_GLOBAL_REQUEST

```
byte      SSH_MSG_GLOBAL_REQUEST
string    request name
boolean   want reply
....      request-specific data follows
```

81 SSH_MSG_REQUEST_SUCCESS

82 SSH_MSG_REQUEST_FAILURE

98 SSH_MSG_CHANNEL_REQUEST

```
byte      SSH_MSG_CHANNEL_REQUEST
uint32    recipient channel
string    request type
boolean   want reply
....      type-specific data follows
```

99 SSH_MSG_CHANNEL_SUCCESS

100 SSH_MSG_CHANNEL_FAILURE

Skal, CHANNEL_OPEN session

Operationer för CHANNEL_REQUEST:

pty-req	Allokera pty, sätter storlek, $TERM, termios-flaggor.
window-change	Signalerar ny storlek på klientens terminal.
x11-req	Begär X11-forwarding, cookie, skärmnummer.
env	Sätt omgivningsvariabel.
shell	Starta interaktivt skal.
exec	Kör kommando, /bin/sh -c.
subsystem	Används för att starta sftp.
signal	Skicka signal till processen.
exit-status, exit-signal	Rapportera exit-kod.

X11 forward

- Begärs med `x11-req`, med fejk-cookie.
- Servern skapar socket under `/tmp.X11-unix` och xauth-fil.
- Och sätter `$DISPLAY` och `$XAUTH` i skalets omgivning.
- Accept på socket ger en `CHANNEL_OPEN x11` över SSH.
- SSH-klienten verifierar cookie, byter mot sin riktiga cookie, och forwardar till lokal X-server.
- Kanalen lever vidare oberoende av `session`-kanalen som begärde forwarding.

TCP-forward med `ssh -L`

```
byte      SSH_MSG_CHANNEL_OPEN
string    "direct-tcpip"
uint32    sender channel
uint32    initial window size
uint32    maximum packet size
string    host to connect
uint32    port to connect
string    originator IP address
uint32    originator port
```

TCP-forward med `ssh -R`

- Begärs med

```
byte      SSH_MSG_GLOBAL_REQUEST
string    "tcpip-forward"
boolean   want reply
string    address to bind (e.g., "0.0.0.0")
uint32    port number to bind
```

- Servern binder porten. Accept ger en

```
byte      SSH_MSG_CHANNEL_OPEN
string    "forwarded-tcpip"
uint32    sender channel
uint32    initial window size
uint32    maximum packet size
string    address that was connected
uint32    port that was connected
string    originator IP address
uint32    originator port
```

Exempel

```
ssh remote.example.org /bin/foo < in > out
```