Sichere Verbindungen mit IRC

IRC mit SSL und SASL

Emanuel Duss

2014-05-07

IRC - Internet Relay Chat (RFC 1495)

Luxeria @ IRC

- Server: `irc.freenode.net`
- Channel: `#luxeria`

Client

- IRC-Client: `irssi`, `weechat`, Pidgin, XChat, ...
- Webmail: `https://webchat.freenode.net/?channels=#luxeria`

Beispielsitzung

```
$ telnet chat.luxeria.ch 6667
NICK luxerianer
USER luxerianer 8 * : luxerianer
PING :kornbluth.freenode.net
JOIN #luxeria
PRIVMSG #luxeria :Hoi zäme!
QUIT
```

Nickname reservieren/registrieren

Nickname registrieren:

```
/nick foo
/msg NickServ REGISTER password mail@example.net
```

Mailadresse verbergen (auf `freenode` Default):

```
/msg NickServ SET HIDEMAIL ON
```

Alternative Nicknames:

```
/nick foo_
/msg NickServ IDENTIFY foo bar23
/msg NickServ GROUP
```

Anmeldung am Server

Nach dem Verbinden authentifizieren:

```
/connect chat.freenode.net 6667
/nick foo
/msg NickServ IDENTIFY foo bar23
```

Direkt mit `irssi`:

```
/connect chat.freenode.net 6667 foo:bar23
```

SSL

- Datenübertragung zwischen IRC-Client und IRC-Server ist verschlüsselt
- Keine Ende-zu-Ende Verschlüsselung
- Freenode bietet SSL/TLS auf Port 6697, 7000 oder 7070 an
- Usermode +Z
- `/whois username: is using a secure connection`

Beispiel `irssi`

```
/connect -ssl_verify -ssl_capath /etc/ssl/certs chat.freenode.net 6697
```

Beispiel `weechat`

```
/server add -auto -ssl -ssl_verify -ssl_capath  /etc/ssl/certs \
  -network Freenode irc.freenode.net 707
```

SASL (Simple Authentication and Security Layer)

- Framework zur Authentifizierung an Diensten (SMTP, IMAP, XMPP, IRC, . . .)
- Definiert im RFC 4422
- Aushandung von Kommunikationsparametern
- Transparent für die Applikation (Entwickler muss nur SASL Implementierung nutzen)
- Unterstützen viele IRC-Clients
- Bevor etwas anderes passiert, authentifiziert man sich am Server
- Erst danach wird IRC gesprochen (vs. zuerst IRC und dann authentifizieren)

Beispiel `weechat`

```
/set irc.server_default.sasl_mechanism dh-blowfish
freenode.sasl_username = "fnordbar"
freenode.sasl_password = "bar23"
```

Weitere Schritte

- Freenode unterstützt mit `CertFP` auch Client Zertifikate
- Ende-zu-Ende Verschlüsselung mit OTR[1]

[1] Ein anderes Mal

Referenzen

- RFC 1459 (IRC): `http://www.faqs.org/rfcs/rfc1459.html`
- Freenode: `https://freenode.net/`
- Freenode SASL: `https://freenode.net/sasl/`
- Freenode SSL: `https://freenode.net/irc_servers.shtml#ssl`
- Freenode CertFP: `https://freenode.net/certfp/`
- O'Reilly. IRC Hacks. 2004. Paul Mutton. ISBN: 978-0-596-00687-7
- WP SASL: `https://en.wikipedia.org/wiki/Simple_Authentication_and_Security_Layer`
- Beschreibung von SASL: `https://github.com/atheme/charybdis/blob/master/doc/sasl.txt`

Fragen

?