Secure Internet Live Conferencing

Frank Benkstein <frank@benkstein.net>

7. Juni 2008

Was ist SILC?

- Secure Internet Live Conferencing
- Chat-Protokoll
- IRC-ähnliche Benutzung
- Integrierte Verschlüsselung

Geschichte

1996	Idee und Entwurf durch Pekka Riikonen
1997	erster Code
1998	Rewrite in C++
1999	Rewrite in C
2000	erste Veröffentlichung der Quelltexte
	Einreichung der Spezifikationen bei der IETF
2003	SILC-Client 1.0
aktuell	SILC Client 1.1.4

Ziele

- Echtzeit-Textkommunikation
  - Viele-Zu-Viele (ähnlich IRC)
  - Eins-Zu-Eins (Instant Messaging)
- Multimediafähigkeit*
  - Video-Chat, Voice-Chat etc.
- Datei-Transfer
- Sicherheit
- Modularität

Protokoll-Eigenschaften

- Verschlüsselung
  - gesamte Kommunikation verschüsselt und authentifiziert
  - unverschlüsselte Kommunikation unmöglich*
- Signatur von Nachrichten
- Unicode (UTF-8) statt ASCII
  - Nicknames
  - Channel-Namen
  - Nachrichten
- Peer-to-Peer für Dateitransfer
- alles andere über Server

Clients

- Nicknamen
  - ausgewählt vom Nutzer
  - nicht eindeutig (!)
- Public-Key
  - generiert von der Software beim ersten Start
  - nicht eindeutig*

Nicknamen

- UTF-8-kodiert
- bestimmte Zeichen (z.B. Leerzeichen) verboten
- bis zu 128 Bytes (!) lang
- bis zu 256 Clients mit gleichem Nicknamen auf einem Server

Client-ID

- generiert vom Server bei Verbindungsaufbau
- nicht eindeutig
- zusammengesetzt aus:
  - IP-Adresse des Servers
  - (Zufalls)zahl (8 Bit)
  - Hash-Wert des Nicknamen

Channels

- eindeutiger Name (256 Bytes)
- Shared-Key
  - beim Betreten übermittelt
  - periodisch regeneriert oder vom Client ausgewählt
- Sicherung
  - Rechte-System (Operator, Founder)
  - (Zugangslisten, Bannlisten)
  - geheime Schlüssel
  - Unsichtbarkeit

Channel-Modi

privat:	wird nicht in der Channel-Liste eines Clients angezeigt
geheim:	wird nicht in der globalen Channel-Liste angezeigt
Founder:	bleibt erhalten, wenn leer
	Founder kann sich beim Betreten Op-Rechte wiederholen
Topic:	nur Ops können Topic ändern
...	

Software

- SILC-Client
  - irssi-fork
  - auch als irssi-Plugin
- Pidgin
- kopete