Secure Internet Live Conferencing

Frank Benkstein <frank@benkstein.net>

26.10.2007, 19:12:23h

Übersicht

- Einführung
- SILC vs. IRC vs. XMPP
- Architektur
- Protokoll

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

Ziele

- Echtzeit-Text-Kommunikation
  - Viele-Zu-Viele (ähnlich IRC)
  - Eins-Zu-Eins (Instant Messaging)
- Multimedia-Fähigkeit
- 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

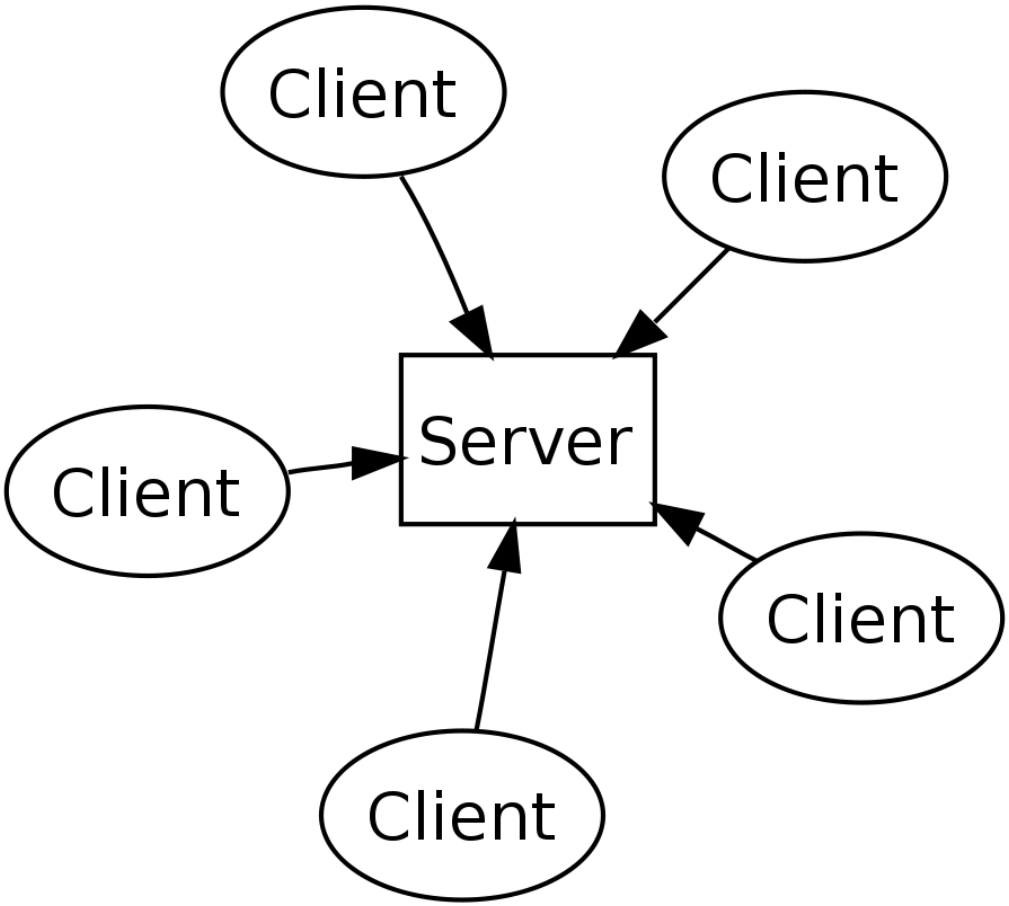
Clients

- eindeutige Client-ID
- Nicknamen
  - nicht eindeutig*
  - UTF-8
  - bis zu 128 Bytes (!) lang
- gleicher Public-Key möglich

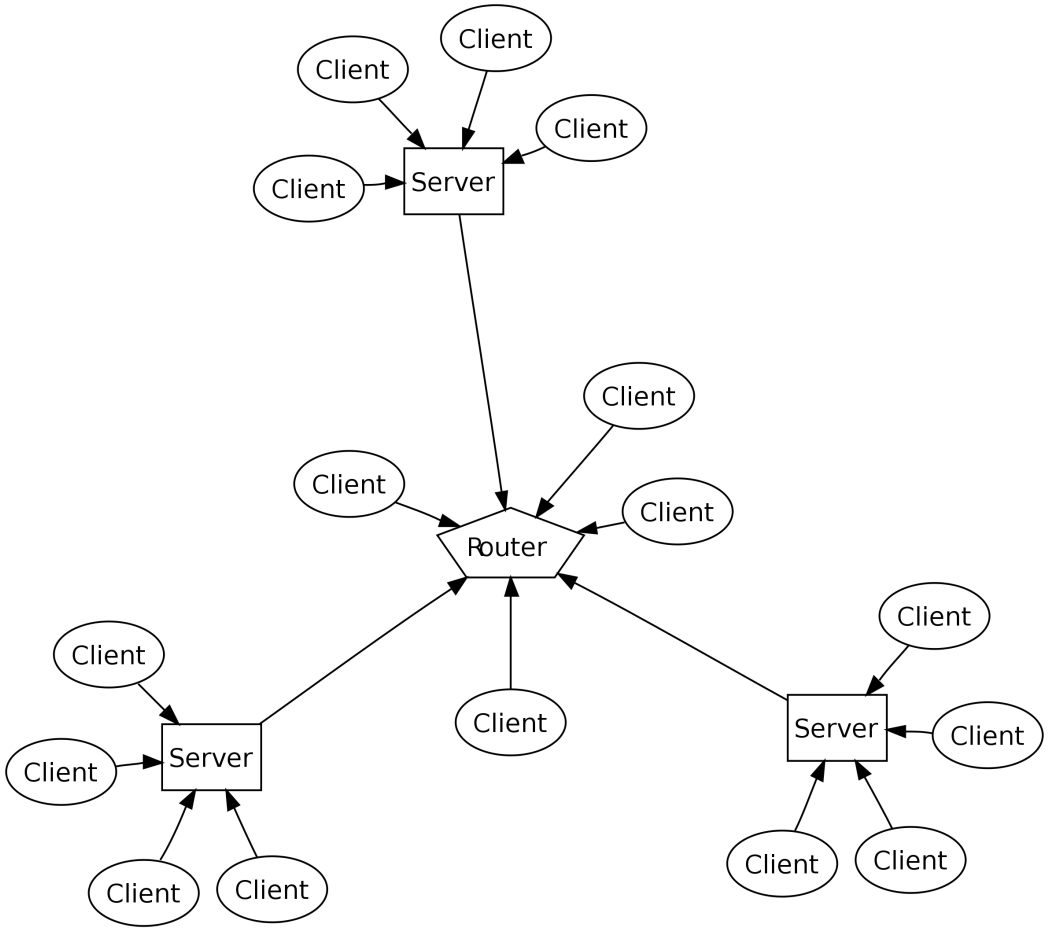
Channels

- eindeutiger Name (256 Bytes)
- Shared-Key
- Sicherung
  - Rechte-System (Operator, Founder)
  - Zugangslisten, Banlisten
  - geheime Schlüssel
  - Unsichtbarkeit

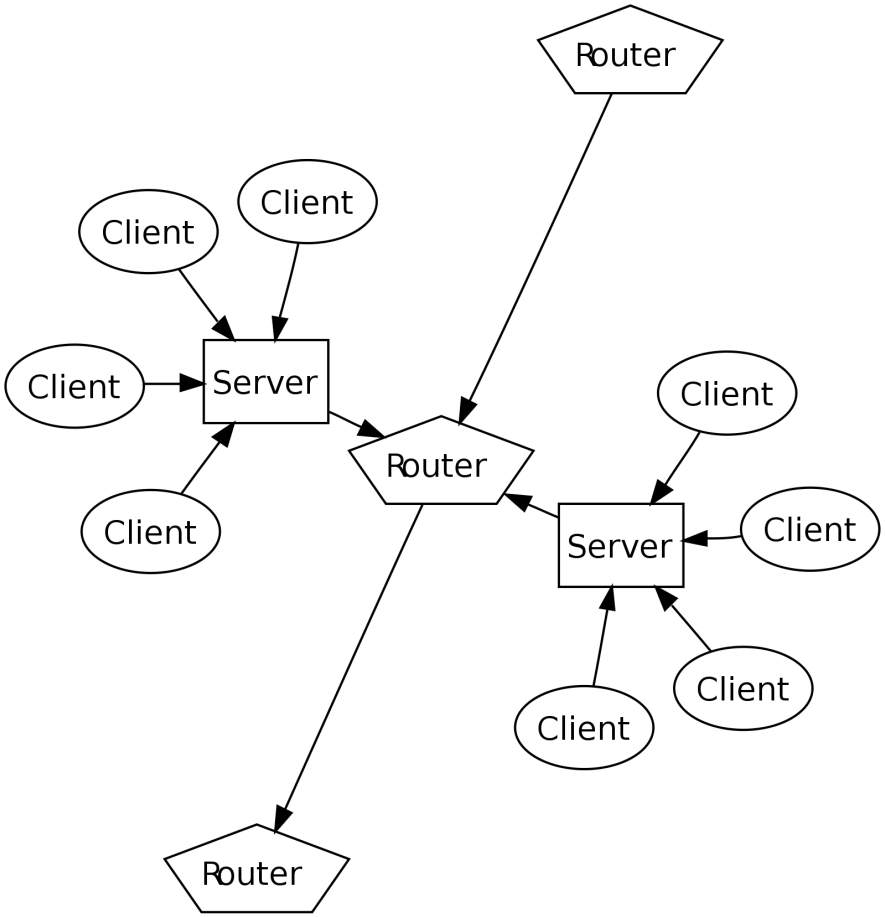
Server



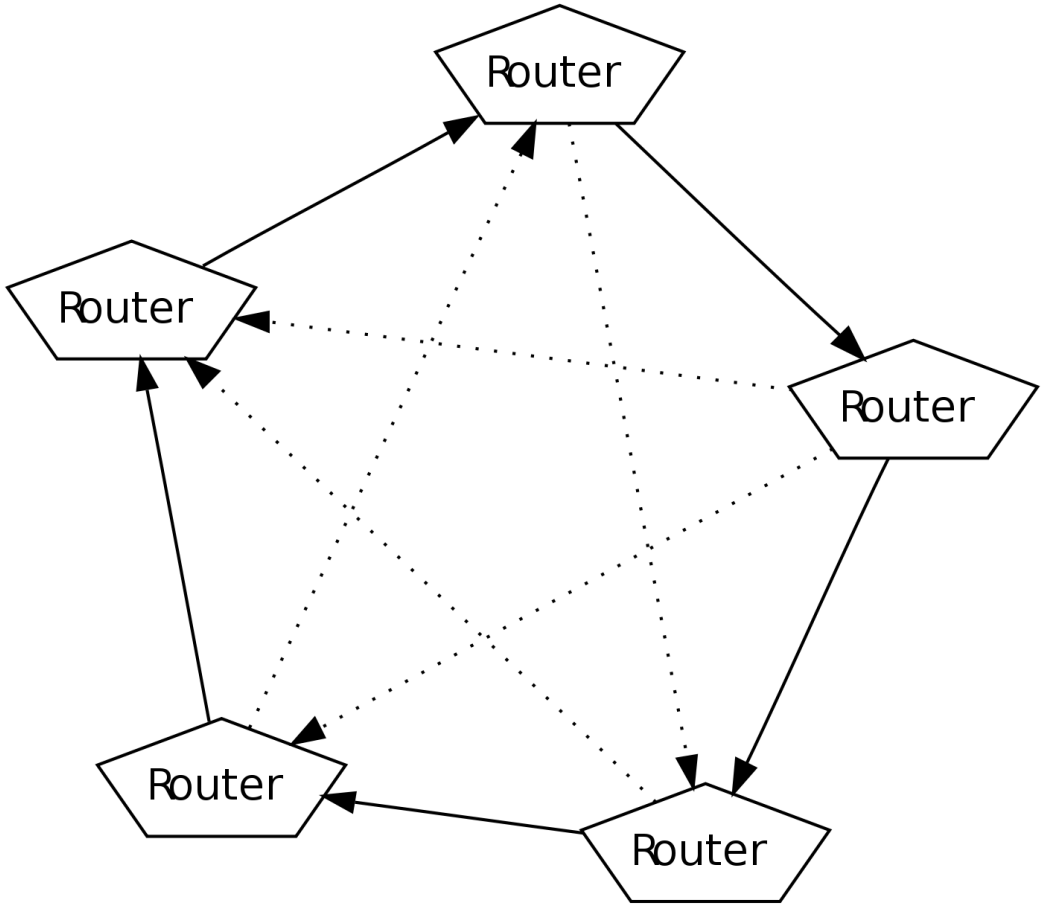
Zelle


Client
Client
Client
Client
Server
Client
Client
Client
Router
Client
Client
Client
Server
Client
Client
Client
Server
Client
Client
Client

Router zu Router



Ring-Mesh



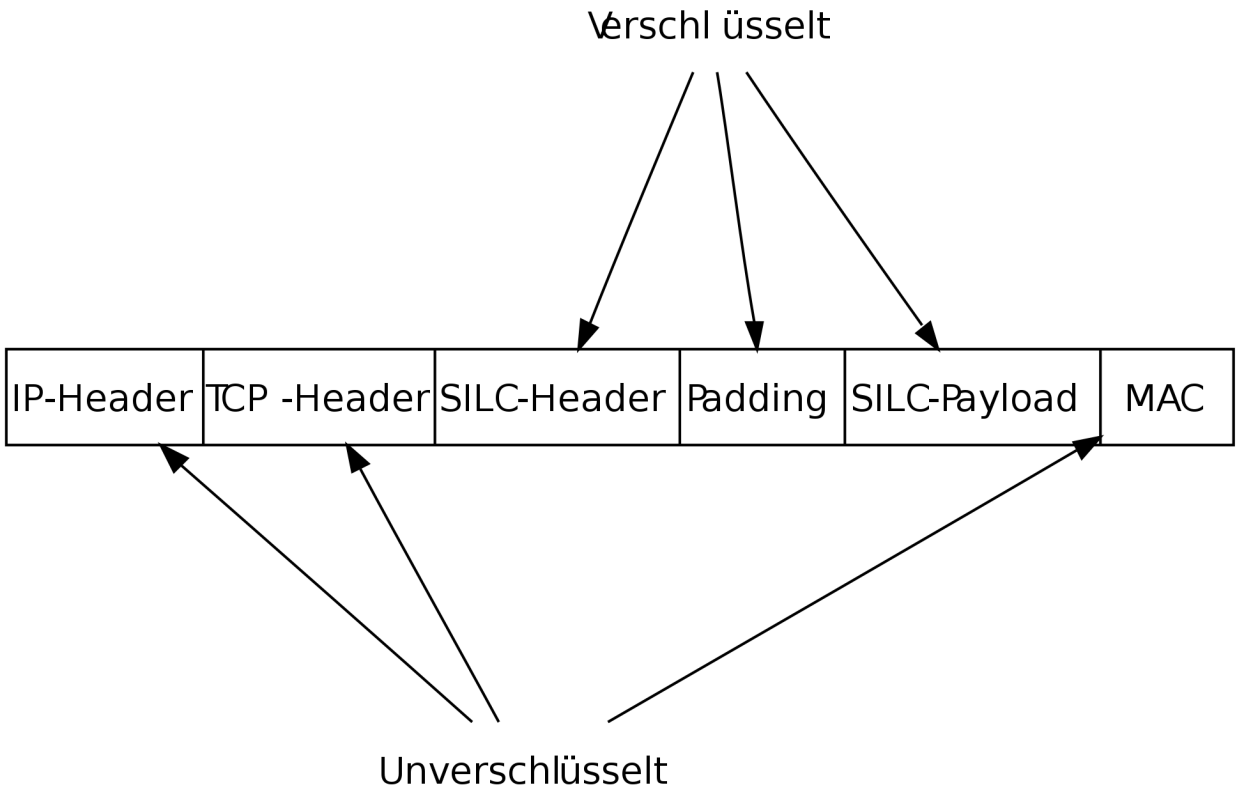
Channel-Nachrichten

- Schlüssel
  - regelmäßige Regenerierung
  - Zellen-lokal
- zwischen Routern mit Session-Key verschlüsselt
- Signierung möglich

private Nachrichten

- verschiedene Verschlüsselungsmethoden
  - Session-Key
  - separater Key-Exchange
  - Public-Key
- Signierung möglich

SILC-Paket


Verschlüsselt
IP-Header
TCP -Header
SILC-Header
Padding
SILC-Payload
MAC
Unverschlüsselt

SILC-Paket-Header

Payload-L		Flags	Typ
Padding-L	Reserviert	Quell-ID-L	Ziel-ID-L
Quell-ID-Typ		Quell-ID-Daten	
Ziel-ID-Typ		Ziel-ID-Daten	

SILC-Key-Exchange

- Rollenverteilung
  - Initiator (bietet an)
  - Responder (wählt aus)
- Vereinbarung
  - Protokoll-Version
  - DH-Gruppen
  - PKCS-Algorithmus
  - Verschlüsselung
  - Hashes
  - HMAC
  - Kompression

SILC-Authentication

- einseitige oder beidseitige Authentifizierung
- Public-Key-basiert
- Passphrase

andere Paket-Typen

- 29 verschiedene Typen durch Protokoll definiert
- 54 Typen zur freien Verfügung

SILC-Command-Pakete

- wichtigster Paket-Typ
- 27 verschiedene Typen durch Protokoll definiert
- 54 Typen zur freien Verfügung
- komplex zu erzeugen
- komplex zu parsen

Fazit

- komplexes Problem
- komplexes Protokoll
- bessere Alternativen nicht vorhanden
- aktuelle Implementation nur wenig besser als IRC oder Jabber