Instant Message Whispering via Covert Channels

Simon Bunten, Gruppe 35

TECHNISCHE UNIVERSITÄT DARMSTADT

Einführung

TECHNISCHE UNIVERSITÄT DARMSTADT

Verstecktes Instant Messaging

- Unentdecktes Senden von Nachrichten
- Umgehen von Sicherheitsvorkehrungen wie Firewalls

Einführung

TECHNISCHE UNIVERSITÄT DARMSTADT

Verstecktes Instant Messaging

- Unentdecktes Senden von Nachrichten
- Umgehen von Sicherheitsvorkehrungen wie Firewalls

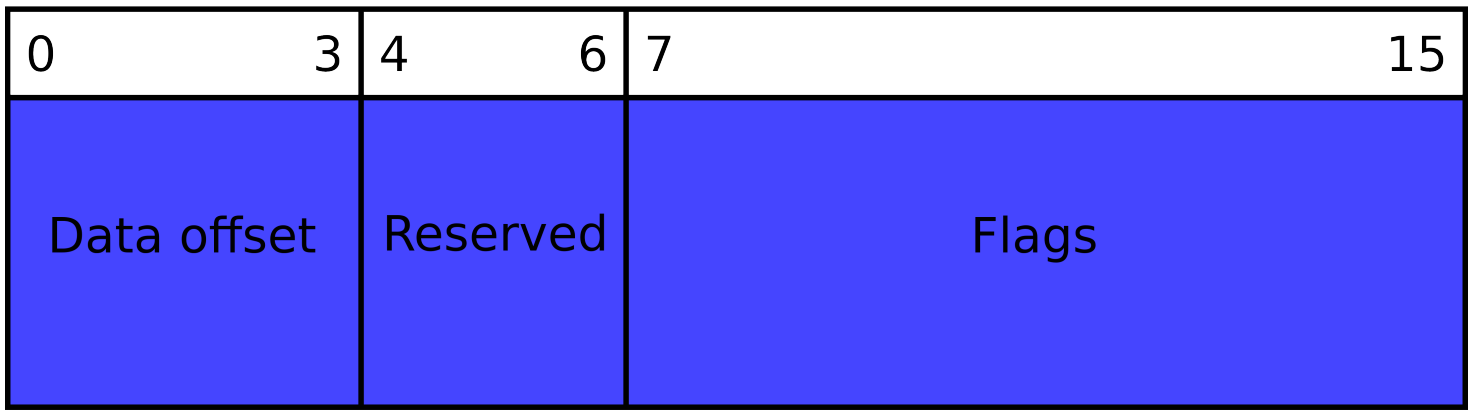
Kryptographie Verschlüsselt die Daten, Kanal bleibt sichtbar

Covert Channels Versteckt den Kanal

Covert Channel im TCP Header

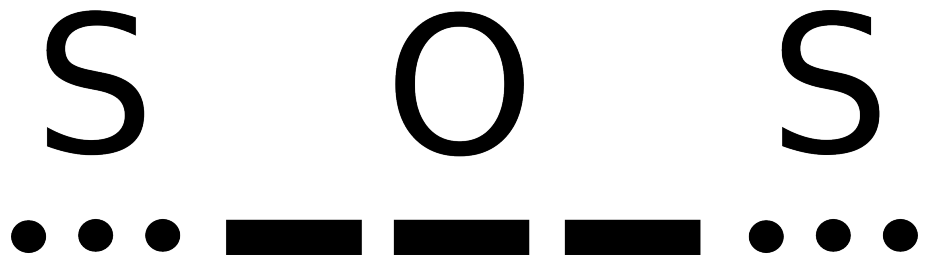
TECHNISCHE UNIVERSITÄT DARMSTADT

Tcp Header Bits 96-111



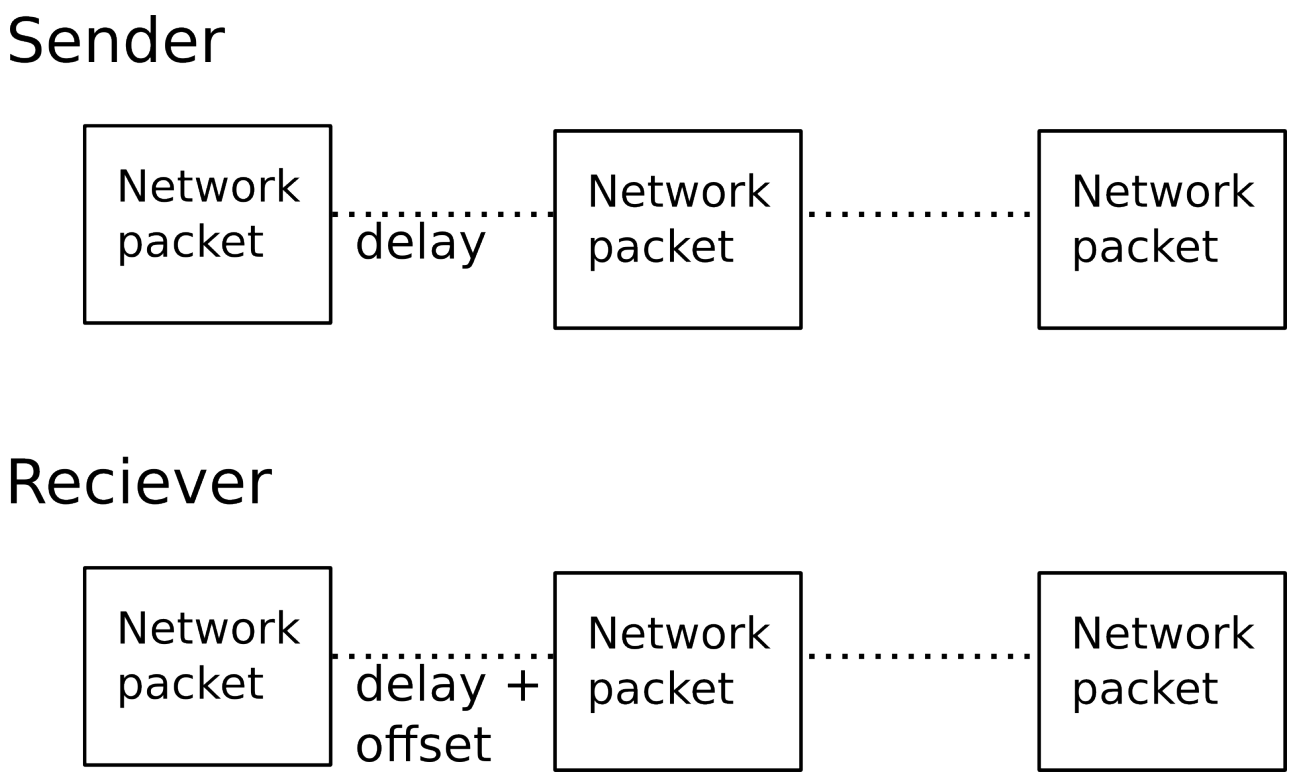
Covert Channel im Inter Packet Delay

TECHNISCHE UNIVERSITÄT DARMSTADT



Covert Channel im Inter Packet Delay

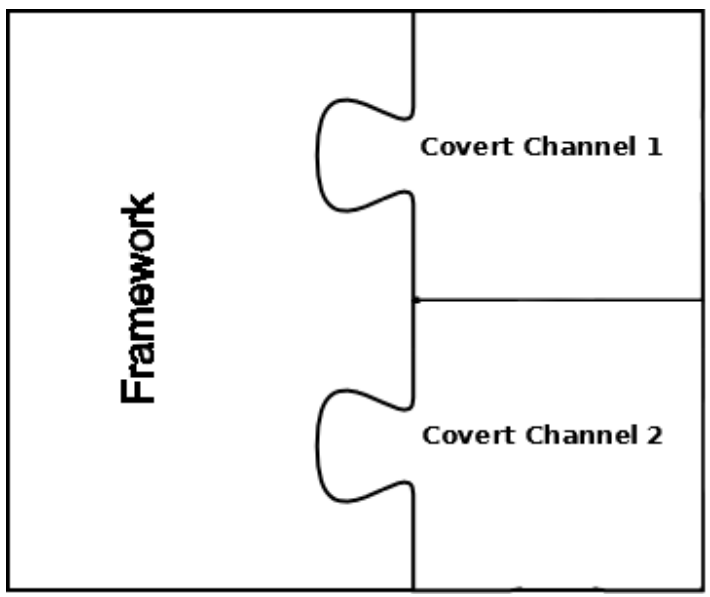
TECHNISCHE UNIVERSITÄT DARMSTADT



Projektbeschreibung

TECHNISCHE UNIVERSITÄT DARMSTADT

Programmieren einer Bibliothek für Covert Channels

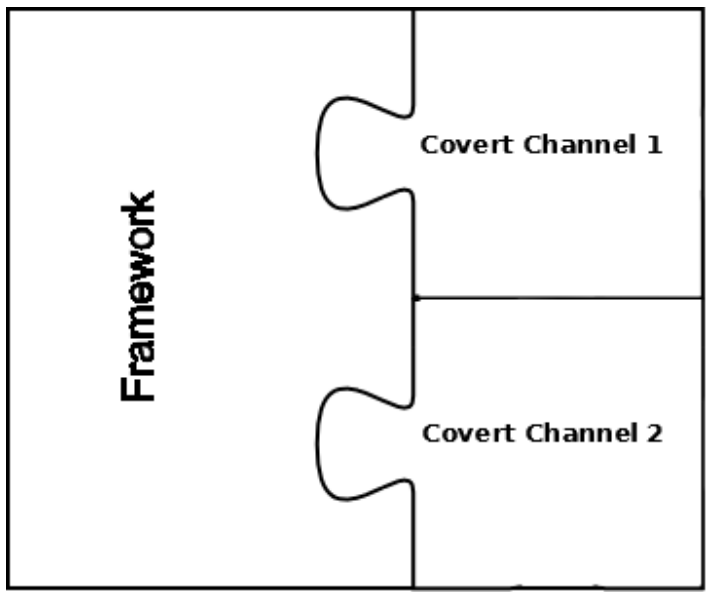


Projektbeschreibung

TECHNISCHE UNIVERSITÄT DARMSTADT

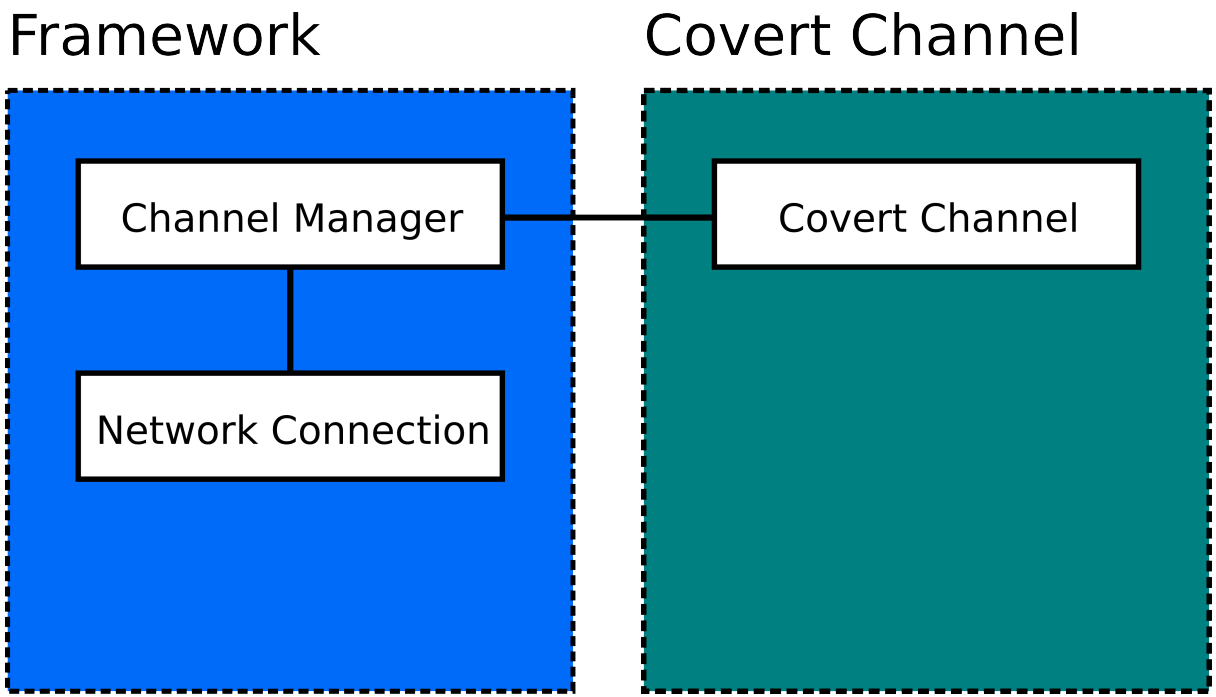
Programmieren einer Bibliothek für Covert Channels

- öffnet und verwendet Covert Channels
- Hilft Nutzern bei der Erstellung eigener Covert Channels
- Veröffentlichung als Open Source



Top-Level Design

TECHNISCHE UNIVERSITÄT DARMSTADT



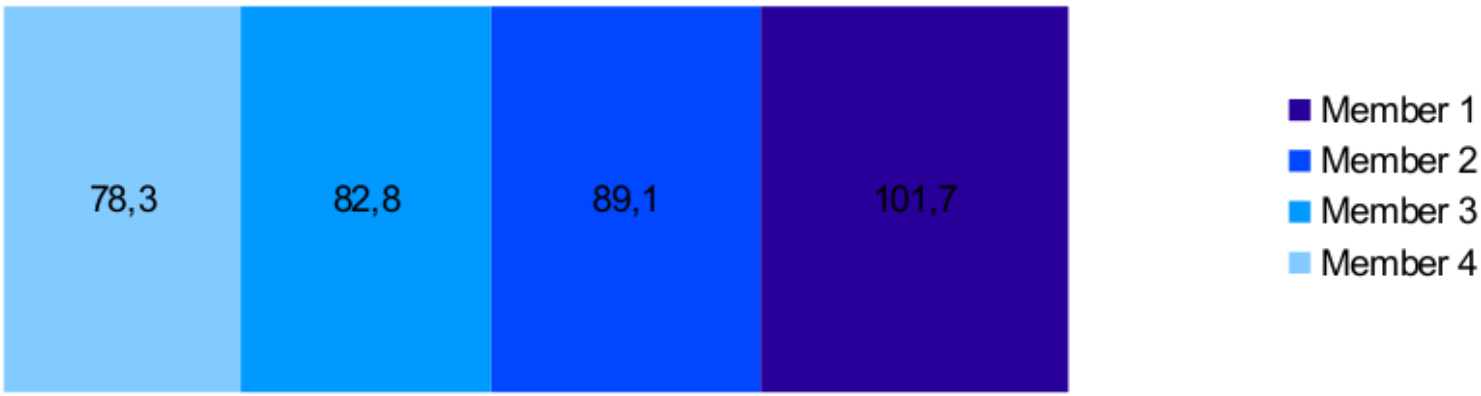
QS-Ziele und ihre Sichherstellung

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Zuverlässigkeit**
  - automatisierte Tests mit Boost.Test
  - Ticket-System im SCM-Server
  - Code Reviews
- **Testbarkeit**
  - Zuteilung der Aufgaben an Module
  - eigene Tests schreiben
  - Architektur bei Problemen anpassen

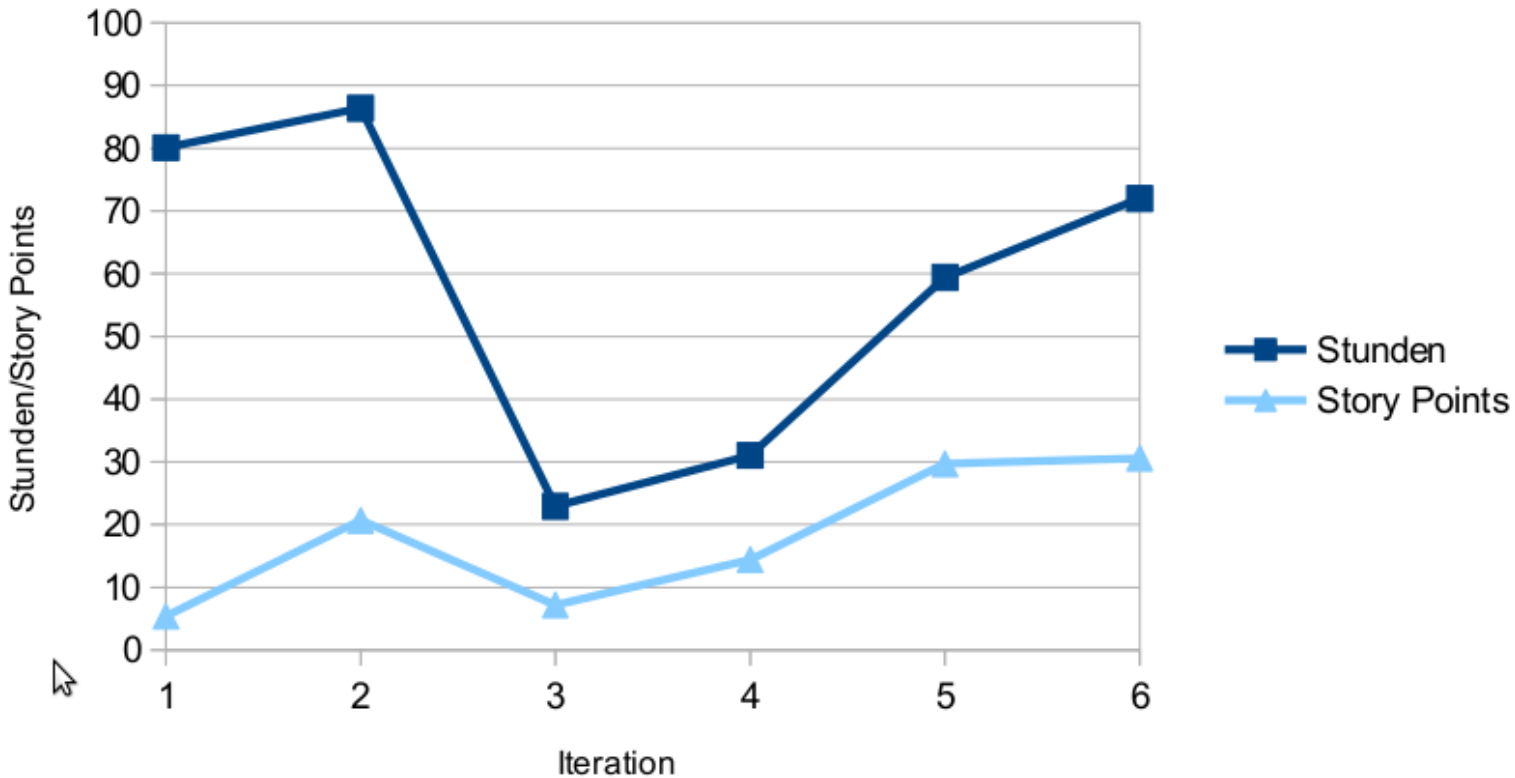
Zeitaufwand

TECHNISCHE UNIVERSITÄT DARMSTADT



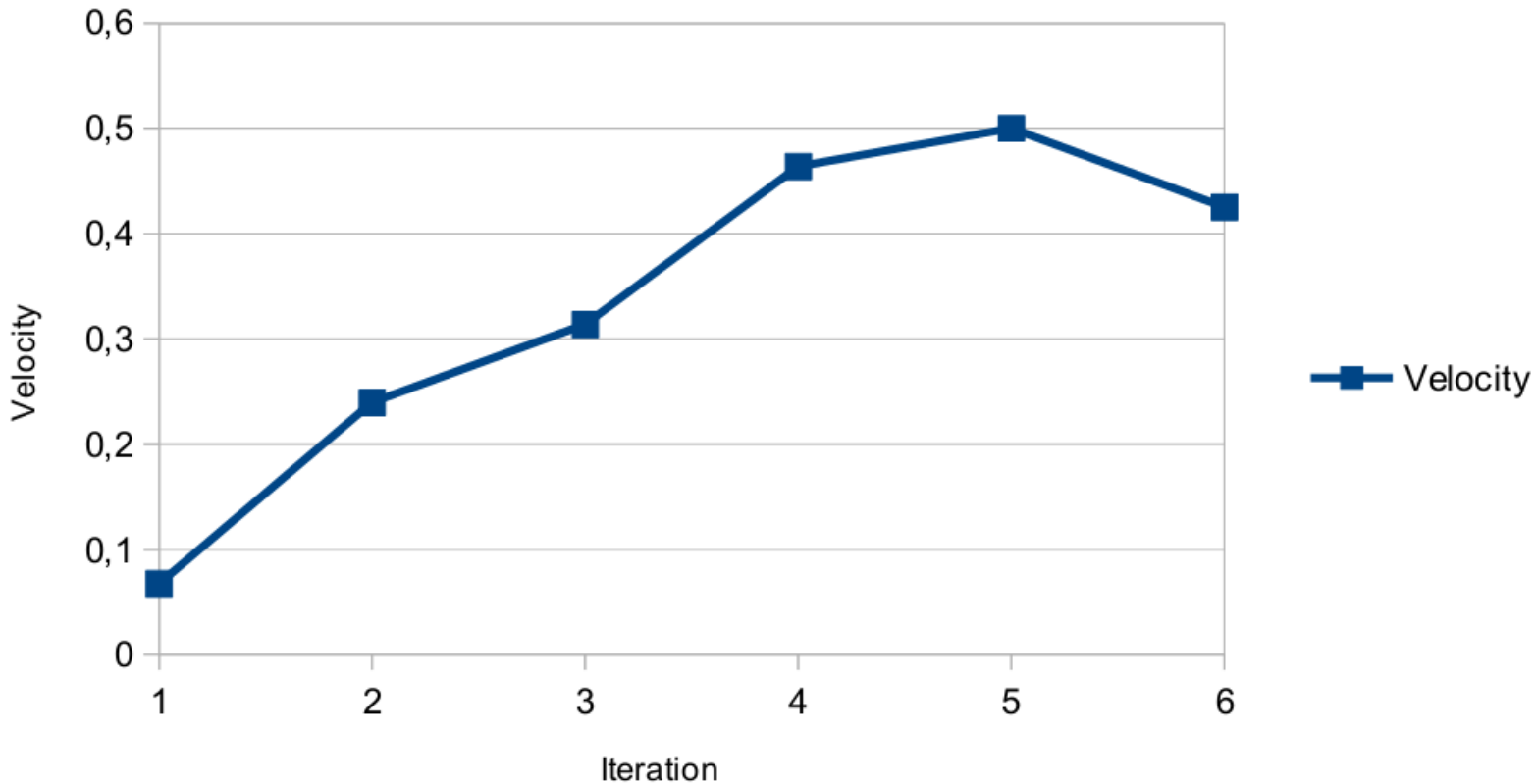
Zeitmanagement

TECHNISCHE UNIVERSITÄT DARMSTADT



Zeitmanagement

TECHNISCHE UNIVERSITÄT DARMSTADT



Zusammenfassung

TECHNISCHE UNIVERSITÄT DARMSTADT

- Entwicklung einer modularen Bibliothek
- Implementierung von Covert Channels zur versteckten Kommunikation
- Nutzbar für möglichst viele Covert Channels
- Veröffentlichung als Open Source unter GPL Lizenz
- Nutzbar für verschiedene Anwender