

# IRC/ICQ: Die dunkle Seite

Daniel Mahrenholz, MDLUG e.V.



Vortrag beim Themenabend: IRC und Instant Messaging  
06. August 2002

- IRC
  - ★ technische Aspekte
  - ★ Denial of Service Angriffe (*Flooding, Nukes*)
  - ★ Rückverfolgung
  - ★ Die feindliche Übernahme
  - ★ Schutzmaßnahmen
- ICQ
  - ★ Privatsphäre
  - ★ Angriffe
- Zusammenfassung und Vergleich

- Server-Ports 6666-6669 (Default: 6667)
- Channel-Kommunikation über den Server
- DCC (*Direct Client Communication*, Chat, Dateitransfer) direkt zwischen 2 Clients
  - ★ benötigt jeweils einen Port  $>1024$
  - ★ IP der Gegenseite sichtbar, wenn Verbindung aufgebaut
  - ★ IRC-Server übermittelt initialen Request

- Ziele:

- ★ Nutzer aus dem Channel werfen (↪ (Op-)Nutzer entfernen)
- ★ Channel unbrauchbar machen (↪ (Op-)Nutzer entfernen)
- ★ IRC-Clients abschiessen (↪ (Op-)Nutzer entfernen)
- ★ IRC-Server abschiessen oder überlasten (↪ *Netsplit*)

- Angriffe:

- ★ *Flooding*: Channel oder einzelne Nutzer mit legalen Nachrichten überfluten, um sie aus dem Channel zu werfen
  - \* z.B. einen Client durch mehrere Clone des Angreifers mit CCTP-Ping-Paketen zu einer Flut von Pong-Paketen provozieren ↪ *Flood-Protection* entfernt den Nutzer
- ★ *Nukes*: automatische Tools, um Channel, Nutzer und Clients mit gültigen und ungültigen Nachrichten und Pakete zu bombardieren

- IRC-Identität läßt sich leicht fälschen (*Identd*)
  - ★ registrierte Nicknames nur für (meist) 60 Sekunden
  - ★ eigene Domain meist nicht
- IRC-Server benutzen verschiedene Anti-Spoofing-Techniken ⇒ Angriffe auf den Channel oder Nutzer darin lassen sich zu einer realen IP zurückverfolgen
  - ★ benötigt Hilfe der IRC-Admins
  - ★ IP kann aber zu einer Firewall, IRC-Proxy bzw. -Relay gehören  
    ~> Rückverfolgung wenig sinnvoll
- Direkte Angriffe auf den Client können mit falschen IPs erfolgen
- **Aber:** kurzfristige Einwahl per Modem macht die Rückverfolgung eher einfacher (→ Zwang zur Speicherung von Verbindungsdaten)

- **Prinzip:** einzelner Nutzer im Channel wird automatisch Op
- **Methoden:**
  1. alle anderen Nutzer aus dem Channel werfen (Kick, Flooding)
  2. bei einem Netsplit in einem Segment alleine sein, Op in anderem Segment klonen, während der Resynchronisierung kurzzeitigen Op-Status zum Kicken (mind. aller anderen Ops) nutzen
- **Tools:**
  - ★ *Link Looker:* Wartet auf Netsplits und ermittelt abgetrennten Rechner
  - ★ *Multi Collide Bot (MCB):* Bot, der bei einem Netsplit beliebige Mengen von Nicknames versucht zu klonen und später aus dem Channel zu werfen

- Flooding, Nukes, . . .
  - ★ DCC vermeiden  $\Rightarrow$  eigene IP nicht preisgeben
  - ★ CTCP-Pings nur beantworten, wenn vom Server gefordert
- Channel-Übernahme
  - ★ Bots, die den Channel vor Übernahmen schützen (z.B. ChanServ)
  - ★ Veränderung des eigenen Nicknames während eines Netsplits  $\rightsquigarrow$  clonen im abgetrennten Segment sehr schwierig
- (persönliche) Firewalls sind **keine** Hilfe
  - ★ bei schnellen Leitungen ist Flooding sehr schwierig
  - ★ bei langsamen (Modem-)Leitungen ist die Firewall auf der falschen Seite der Leitung

- **Problem:** Hauptarbeit wird im Client erledigt, sehr viele Funktionen integriert
- Clients akzeptieren meist Nachrichten vom Server und anderen Clients
  - ★ notwendig für verschiedene Funktionen (Dateitransfer, Events, ...)
  - ★ Client anfällig für falsche Nachrichten (*Spoofing*)
  - ★ Absender kann auch seine IP fälschen
  - ★ Voraussetzung: IP des Opfers bekannt (Server ist behilflich)
- ICQ im Vergleich mit AIM und MSN-IM das sicherste System
- Alternative Clients mit weniger Funktionen meist wesentlich sicherer

- Flooding: Überfluten mit legalen Nachrichten
    - ★ Nachrichten direkt an den Client schicken
    - ★ EMail-Bomben über den EMail-Express-Dienst
  - Spoofing: Überfluten bzw. Verwirren mit gefälschten Nachrichten
    - ★ einfache Nachrichten
    - ★ Steuernachrichten (Hinzufügen zur Kontaktliste, z.B. den Nutzer selber)
  - DoS-Angriffe auf den ICQ-Webserver (ICQ-Homepage)
  - Aushebeln der *Invisible List*
    - ★ über die ICQ-Webseite (*web-aware*)
    - ★ durch geschicktes Clonen des eigenen Nutzers
- ⇒ **möglichst viele Zusatzdienste deaktivieren**

- **Hauptproblem:** UID müsste eigentlich geheim gehalten werden
- Anwesenheit im Netz läßt sich feststellen
- verschiedene Möglichkeiten für eine IP→UID Abbildung
- ICQ-Whitepages
- generell unverschlüsselte Kommunikation

- IRC:
  - ★ Hauptarbeit wird vom Server geleistet
  - ★ Angriffe hauptsächlich auf den Server und die Kommunikation mit den Clients
  - ★ Zusatzdienste durch Bots realisiert
- ICQ:
  - ★ Hauptarbeit wird vom Client geleistet
  - ★ Angriffe hauptsächlich gegen die Clients
  - ★ Zusatzdienste hauptsächlich in die Clients integriert

- <http://www.irchelp.org/irchelp/security/>
- <http://www.astalavista.com/library/irc/security/>
- <http://downloads.securityfocus.com/library/irc.txt>
- <http://www.livinginternet.com/?r/rs.htm>
- <http://onlinesecurity.virtualave.net/hacking/irc.htm>
- <http://blacksun.box.sk/icq.html>
- <http://www.reenigne.org/computer/icqpriv.html>