Vertrauen im und in Peer-to-Peer Netzen

Thomas Kollbach
kollbach@informatik.hu-berlin.de

- Was ist Vertrauen?
- Vertrauen innerhalb von p2p-Netzen
  - Was für arten von Vertrauen spielen eine Rolle, wie kann man sie Angreifen
- Vertrauen in p2p Technologie
  - Kurzer Ausblick in die Zukünftigen Anwendungen von p2p-Technologie

Vertrauen

Was ist Vertrauen?

Vertrauen ist die subjektive Überzeugung […] der Richtigkeit bzw. Wahrheit von Handlungen und Einsichten eines anderen […].

Quelle: Wikipedia

Vertrauen

- besteht zwischen zwei Personen
- beruht (meist) auf Gegenseitigkeit
- beruht auf einer Grundlage (Erfahrung, (Vor-)urteil, etc.)

Vertrauen

Vertrauen ist…

- subjektiv
- emotional
- nicht Messbar
- schwer technisch Abbildbar

Vertrauen innerhalb von p2p-Netzen

Vertrauen

Psychologischer Ansatz

Soziales Vertrauen

- Peer-to-Peer
  - Alle sind "gleich"
    - Gleiche Ziele
  - Gefühl kultureller Übereinstimmung mit anderen
  - Bildung einer "sozialen Vertrauensgruppe"

Technikvertrauen

- Vertrauen in ein komplexes System
- vom durchschnittlichen Teilnehmer nicht zu überblicken

Angriffsfläche

- Klagewellen
  - Ziel: Vertrauen zerstören
  - “Du bist nicht anonym!”
- Folge
  - Temporärer Rückgang der Nutzer zahlen
  - Nutzerwanderung zwischen Netzen
  - Technische Lösungsansätze

Vertrauen

Technischer Ansatz

Technisches “Vertrauen”

- Basierend auf Hash-Algorithmen (selten MD5,meist SHA-1)
- Gehascht werden
  - Dateien bzw. Chunks
  - evtl. Metainfos (Name, Autor, etc.)

Napster

- Schwachstellen
  - Nur MP3 Dateien
  - Keine Metadaten
  - Zentrale Index Server
- (Technische) Angriffsmethoden
  - Flasche Dateibenennung
  - (D)DoS gegen Indexserver

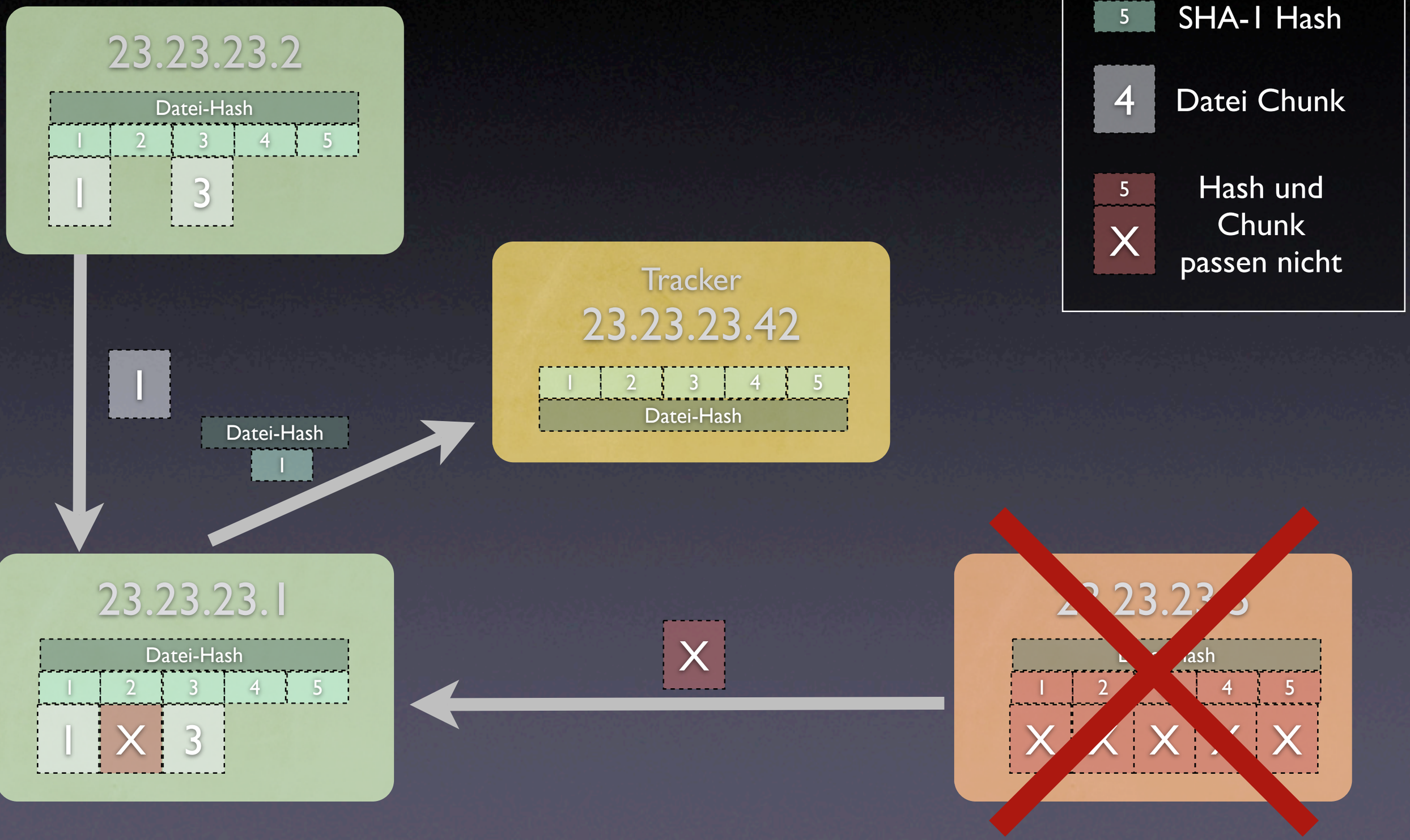
eDonkey

- Schwachstellen
  - Eindeutige ClientID (IP-basiert)
  - Datei zu Client Matching durch Server
  - MD4 (!) Datei-Hashing

Bittorrent

- Schwachstellen
  - Vertrauen in Clients
  - Nur ein Tracker
  - Keine Suche (bzw. kein unäres Netz)
  - Abhängigkeit von .torrent Verteilung
- Angriffsmethoden
  - “Gefälschte” Hashes bzw. Chunks
  - (D)DoS auf Tracker

Bittorrent Angriff



Fazit

- Alle Systeme sind angreifbar
- Gegen Inhaltsfälschung gibt es kein effektives Gegenmittel
- Angriffe auf p2p-Vernetzungsebene sind bei modernen System beinahe unmöglich

Vertrauen in p2p-Technologie

Ein Ausblick in die Zukunft von p2p-Technologie

Mehr als nur Filesharing

- Skype – Telefonie auf p2p-Basis
- JXTA – p2p Geräte Vernetzung
- Kolaboration – Groupware ohne Server
- Dauerhafte Datenarchivierung

Skype

- VoIP von den Machern des Kazaa (FastTrack) Filesharing Netzes
- Im Schnitt um 4 Mio. Aktive Nutzer
- Basiert auf Node/Supernode Struktur mit zentralem Logon
- Dazu gibt es noch eine Vortrag

JXTA

- Von Sun Microsystems initiert
- Offener Standard
- Vernetzen, entdecken, suchen, etc. von beliebigen Geräten
- Noch in Entwicklung – Referenzimplementation in Java und C

OceanStore Project

- Research Projekt der Berkley Universität
- Ziel: Dauerhaft, sichere Speicherung von Daten
- Archivierung von Kulturgut für lange Zeit
- Verwendet Chimera/Tapestry Projekt der University of California

Quellen

Bickson und Kulbak, "The eMule Protocol Specification", 2005, University of Jerusalem, http://www.cs.huji.ac.il/labs/danss/presentations/emule.pdf

Baset und Schulzrinne, "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol ", 2004, Columbia University, New York, http://arxiv.org/pdf/cs.NI/041201

Cohen, "Incentives Build Robustness in BitTorrent", 2003, http://www.bittorrent.com/bittorrentecon.pdf

"Vertrauen", Wikipedia, http://de.wikipedia.org/wiki/Vertrauen, 18.01.2006

"Soziales Vertrauen", Wikipedia, http://de.wikipedia.org/wiki/Soziales_Vertrauen, 18.01.2006

http://oceanstore.cs.berkeley.edu

http://www.jxta.org

Fin!

Folien online unter

http://bitfever.de/~toto/Folien/p2p_vertrauen.pdf