Peer-to-Peer-Netzwerke

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Christian Schindelhauer

Sommersemester 2006

21. Vorlesung

19.07.2006

schindel@informatik.uni-freiburg.de

Inhalte

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Kurze Geschichte der Peer-to-Peer-Netzwerke**
- **Das Internet: Unter dem Overlay**
- **Die ersten Peer-to-Peer-Netzwerke**
  - Napster
  - Gnutella
- **CAN**
- **Chord**
- **Pastry und Tapestry**
- **Gradoptimierte Netzwerke**
  - Viceroy
  - Distance-Halving
  - Koorde
- **Netzwerke mit geordneter Speicherung**
  - P-Grid
  - Skip-Net und Skip-Graphs
- **Selbstorganisation**
  - Pareto-Netzwerke
  - Zufallsnetzwerke
  - Topologie-Management
- **Sicherheit in Peer-to-Peer-Netzwerken**
- **Anonymität**
- **Datenzugriff: Der schnellere Download**
- **Peer-to-Peer-Netzwerke in der Praxis**
  - eDonkey
  - FastTrack
  - Bittorrent
- **Juristische Situation**

Das Problem der byzantinischen Generäle

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **3 Armeen stehen bereit die gegnerische Burg zu besiegen**
- **Diese sind getrennt und kommunizieren über Boten**
- **Greift nur eine Armee an, so verliert diese.**
- **Greifen zwei an, so gewinnen diese**
- **Greift keine an, so wird die Burg ausgehungert**
- **Aber ein General ist übergelaufen**
  –man weiß nicht, wer...

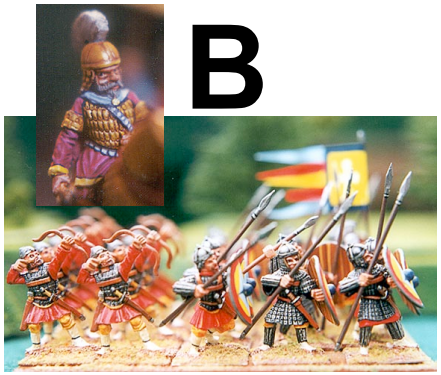
Das Problem der byzantinischen Generäle

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Der übergelaufene General X versucht nun**
  - –A zum Angriff zu überreden
  - –B zum Abwarten
- **A übermittelt den Befehl an B**
- **B übermittelt den Befehl an A**
  - –Widerspruch!

A

X



B

Das Problem der byzantinischen Generäle

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **A übermittelt den Befehl an B**
- **B übermittelt den Befehl an A**
  - –Widerspruch!
- **Weder B noch A können X als Betrüger überführen**
  - –da X A oder B als Überläufer darstellt

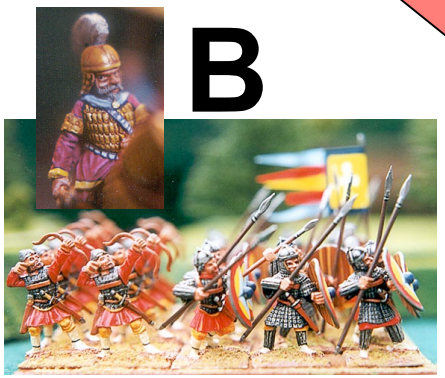
A

Attacke?

Abwarten?

Attacke

X



B

Abwarten

Byzantinische Abstimmung

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

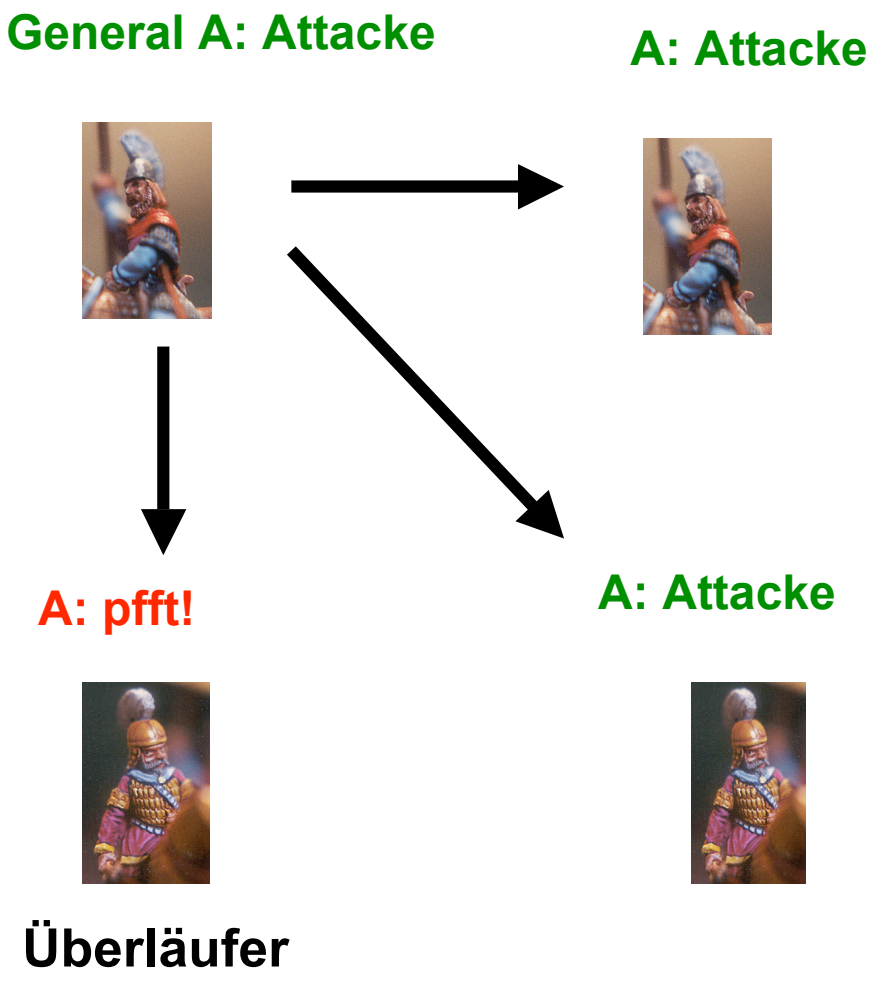
Theorem

Das Problem der drei byzantinischen Generäle kann nicht gelöst werden

Für vier Generäle ist das Problem lösbar:

1-General, 3 Offiziere-Problem

1. **Betrachte einen (loyalen) General und 3 Offiziere.**
2. **Verbreite Information des loyalen Generals an alle**



Byzantinische Abstimmung

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

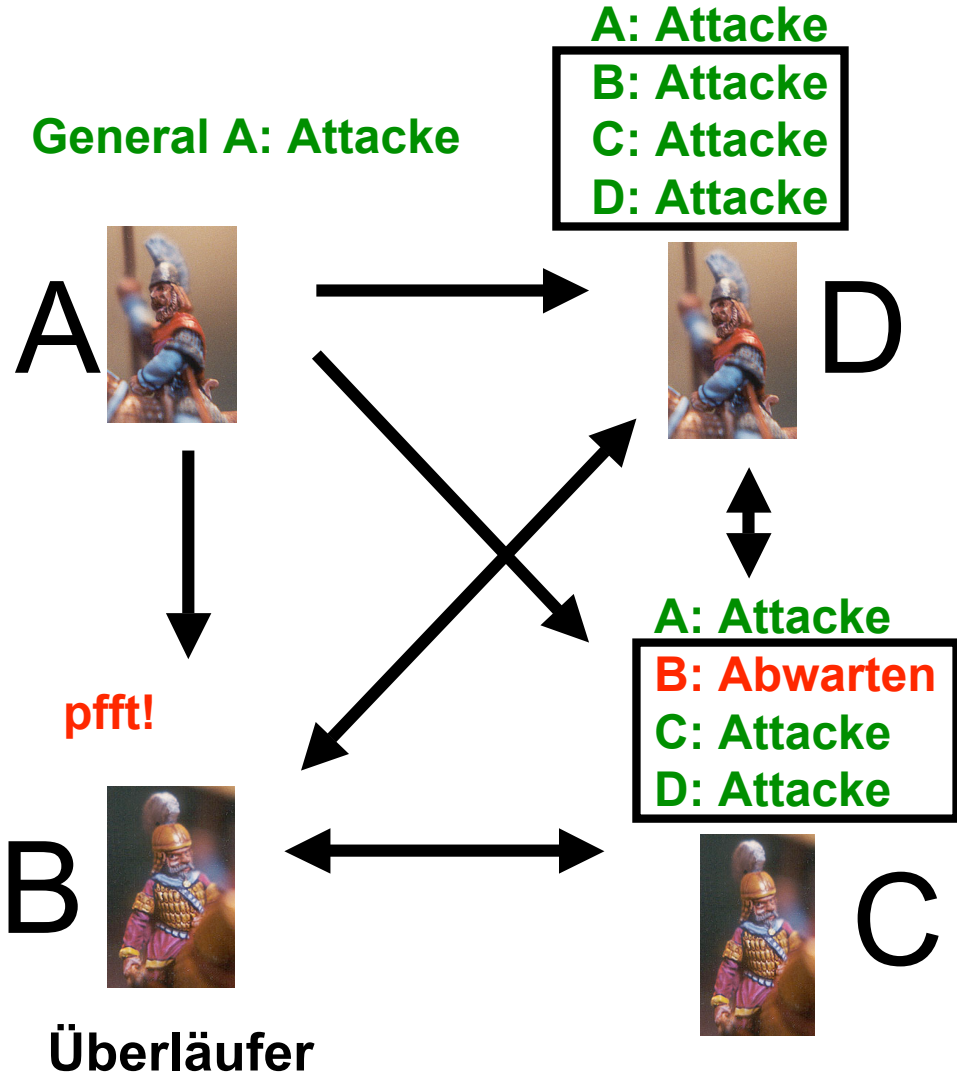
Für vier Generäle ist das Problem lösbar:

1-General, 3 Offiziere-Problem

1. **Betrachte einen (loyalen) General und 3 Offiziere.**
2. **Verbreite Information des loyalen Generals an alle Offizieren**

Algorithmus

1. **General A sendet seinen Befehl an alle anderen (A bleibt bei seinem Befehl)**
2. **Jeder andere General sendet diesen erhaltenen Befehl an alle anderen**
3. **Jeder berechnet die Mehrheitsentscheidung aus den Befehlen von B, .., D**



Byzantinische Abstimmung
Der Überläufer als General

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

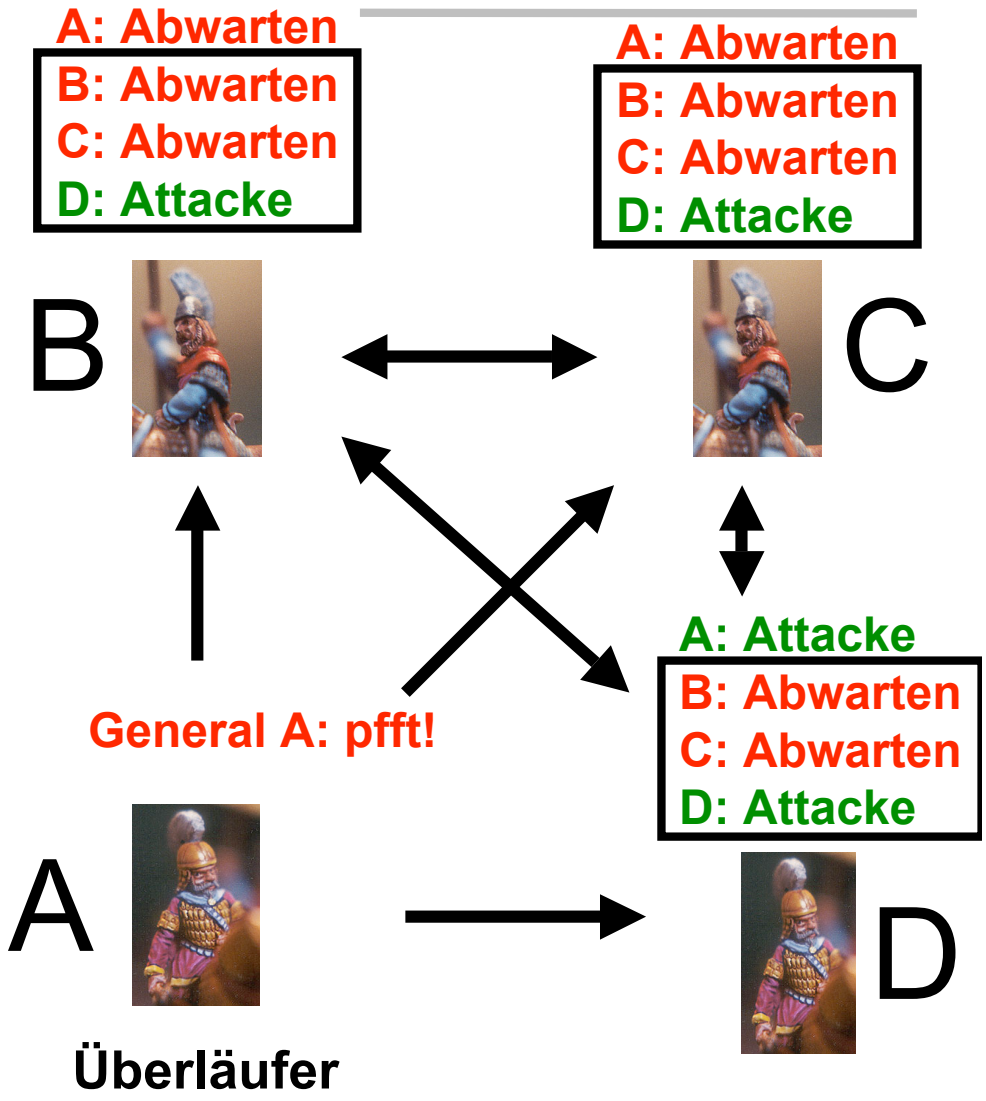
Für vier Generäle ist das Problem lösbar:

1-General, 3 Offiziere-Problem

1. **Betrachte einen (loyalen) General und 3 Offiziere.**
2. **Verbreite Information des loyalen Generals an alle Offizieren**

Algorithmus

1. **General A sendet seinen Befehl an alle anderen**
2. **Jeder andere General sendet diesen erhaltenen Befehl an alle anderen**
3. **Jeder berechnet die Mehrheitsentscheidung aus Befehl von B, .., D**



Lösung des Byzantinischen Generäle-Problems

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Theorem**
  - Falls m Generäle Überläufer sind, müssen mindestens 2m+1 Generäle ehrlich sein, damit das Problem der Byzantinischen Generäle lösbar ist.
- **Diese Schranke ist genau, wenn keine kryptographischen Annahmen gemacht werden**
  - D.h. wenn man genug Zeit hat jede Verschlüsselung zu brechen
- **Theorem**
  - Steht ein digitales Signaturschema zur Verfügung, dann kann eine beliebige Anzahl von falschen Generälen verkraftet werden
- **Lösung:**
  - Jeder General unterschreibt seinen Befehl
  - In jeder Runde gibt jeder General alle Befehle an alle anderen weiter
  - Jeder inkonsistenter Befehl oder jede falsche Weitergabe kann sofort aufgedeckt und bewiesen werden
  - Schweigt ein General, so kann das unter den ehrlichen Generälen festgestellt werden

Byzantinische Generäle und P2P-Netzwerke - Resumee

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Durch den Einsatz von digitalen Unterschriften reduziert sich das Problem auf den (bösartigen) Ausfall von Knoten in einem Netzwerk**
  - wenn die Nachbarn die Kommunikation rekonstruieren können
- **Problem**
  - dafür werden O(n) Nachrichten pro Peer verwendet

- **In „Scalable Byzantine Agreement“ von Clifford Scott Lewis und Jared Saja, 2003**
  - wurde ein skalierbares Verfahren auch ohne Signatur vorgestellt
  - verkraftet n/6 bösartige Generäle
  - verwendet nur O(log n) Nachrichten pro Knoten im Erwartungswert
  - und findet eine Übereinkunft mit hoher Wahrscheinlichkeit

Ein Zensor-Resistentes Peer-to-Peer-Netzwerk

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

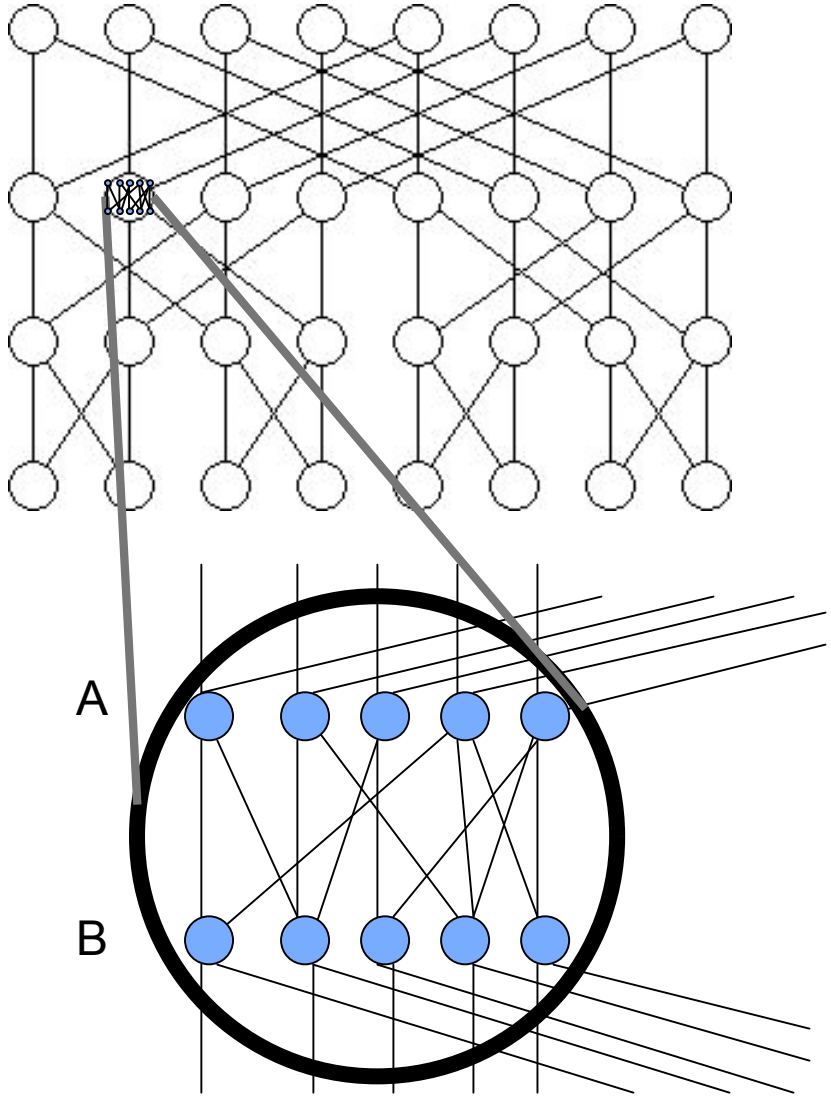
- **Amos Fiat, Jared Saia, 2002**
  - „Censorship Resistant Peer-to-Peer Content Addressable Networks“
- **Problemstellung**
  - Ein Angreifer schaltet 50% aller Peers durch einen Angriff aus
  - Gibt es ein Netzwerk, dass solche Angriffe verkraftet?
- **Annahme:**
  - Der Angreifer weiß nichts über die interne Netzwerk-Struktur
  - Verwendet man eine zufällige Zuweisung von Aufgaben,
  - fällt jeder Knoten mit W‘keit 1/2 aus

Das Netzwerk

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Besteht aus einer Butterfly-Struktur mit Clustern der Größe c log n**
- **Die Cluster sind bipartite Expander-Graphen**

- **Definition Bipartiter Graph**
  - Ein bipartiter Graph besteht aus zwei disjunkten Knotenmengen A und B, so dass jede Kante einen Knoten aus A und B besitzt
- **Definition Expander-Graph**
  - Ein bipartiter Graph ist ein Expander-Graph,
  - wenn für jede Teilmenge X von A, deren Größe A um höchstens einen (gewissen) konstanten erreicht,
  - die Menge der Nachbarknoten in B um einen (gewissen) konstanten Mindestfaktor größer ist



Diskussion

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Vorteile:**
  - Sehr effizientes, robustes und einfaches Verfahren
  - Das Funktionsprinzip lässt sich auf alle bisher diskutierten Verfahren verallgemeinern
- **Problem:**
  - Starke Annahme:
    - Der Angreifer weiß nichts/wenig über die interne Struktur
    - Funktioniert damit bei Systemen mit Zugangskontrolle
- **Falls der Angreifer die Struktur kennt:**
  - Dann kann er jedes System mit konstanten Grad mit einem Denial-of-Service-Angriff auf wenige Peers aushebeln

Inhalte

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Kurze Geschichte der Peer-to-Peer-Netzwerke**
- **Das Internet: Unter dem Overlay**
- **Die ersten Peer-to-Peer-Netzwerke**
  - Napster
  - Gnutella
- **CAN**
- **Chord**
- **Pastry und Tapestry**
- **Gradoptimierte Netzwerke**
  - Viceroy
  - Distance-Halving
  - Koorde
- **Netzwerke mit geordneter Speicherung**
  - P-Grid
  - Skip-Net und Skip-Graphs
- **Selbstorganisation**
  - Pareto-Netzwerke
  - Zufallsnetzwerke
  - Topologie-Management
- **Sicherheit in Peer-to-Peer-Netzwerken**
- **Anonymität**
- **Datenzugriff: Der schnellere Download**
- **Peer-to-Peer-Netzwerke in der Praxis**
  - eDonkey
  - FastTrack
  - Bittorrent
- **Juristische Situation**

Problembeschreibung

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Motivation**
  - nicht nur die Verhinderung des berechtigten Zugriffs staatlicher Verfolgungsbehörden gegen die gesetzeswidrige Verletzung von Urheberschutzgesetzen
  - Zensur und Verfolgung in Diktaturen
- **Grade der Anonymität**
  - Autor
    - Wer hat das erzeugt?
  - Server
    - Wo wird das gespeichert?
  - Leser
    - Wer hat sich das geholt?
  - Dokument
    - Welche Dokumente werden auf einen bestimmten Peer gespeichtert?

Methoden der Anonymisierung

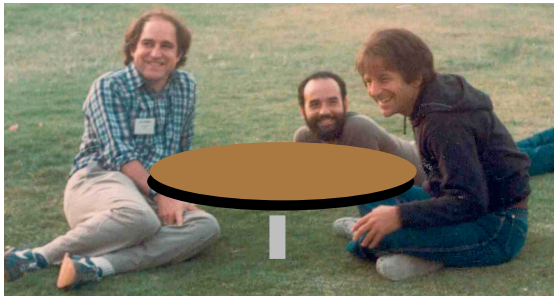
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Dining Cryptographers**
  - Wer hat's geschickt?
- **Onion Routing**
  - Verwickelte Umwege...
- **F2F-P2P**
  - Friend-to-Friend
- **Dark-Net**
  - War das was?
- **Steganographie**
  - nichts zu sehen...
- **Verschlüsselte Inhalte**
  - Denn sie wissen nicht, was sie speichern...
- **Verschlüsselte, unterschriebene Index-Einträge**
  - gezeichnet: Zorro

Dining Cryptographers

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Methode zur anonymen Kommunikation ohne Rückverfolgung der Nachricht zum Sender**
- **$n \geq 3$ Kryptographen sitzen um einen kreisförmigen Tisch**
- **Zwei benachbarte Kryptographen**
  - können sich unbemerkt unterhalten (hinter den Menus)
- **Jeder i wählt eine (für die anderen) geheime Zahl x_i und teilt sie den rechten Tischnachbar i+1 mod n mit**



- **Falls i eine Nachricht m senden möchte:**
  - Veröffentlicht er $s_i = x_i - x_{i-1} + m$
- **Ansonsten:**
  - $s_i = x_i - x_{i-1}$
- **Dann veröffentlichen alle $s_1,..,s_n$**
- **Falls die Summe 0 ist:**
  - Keine Nachricht
- **Sonst**
  - Summe der Nachrichten

Onion Routing

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Von David Goldschlag, Michael Reed, and Paul Syverson**
- **Ziel**
  - Schutz der Privatsphäre von Sender und Empfänger einer Nachricht
  - Schutz der übermittelten Nachricht
- **Annahme**
  - Spezielle Infrastruktur (Onion Routers), die bis auf wenige Ausnahmen kooperieren
- **Methode:**
  - Basierend auf Mix Cascades (D. Chaum)
  - Nachricht wird von der Quelle zum Ziel über Zwischenstationen geleitet (Proxies - Onion Routers)
  - Onion Routers wählen unvorhersehbar andere Onion Routers als Zwischenstationen
  - Zwischen Sender, Onion Routers und Empfängern ist die Nachricht jeweils symmetrisch verschlüsselt
  - Jeder Onion Router kennt nur die nächste Zwischenstation
  - Die Nachricht ist wie eine Zwiebel mehrfach für die Zwischenstationen verschlüsselt
- **Onion Routers sind eine frewillige Infrastrukturerweiterung des Internets**
  - Verstehen sich nicht als Peer-to-Peer-Netzwerk

Friend-to-Friend

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **von Dan Bricklin (2000)**
- **Peer-to-Peer-Netzwerk mit Verbindungen nur zwischen Personen, die sich gegenseitig vertrauen**
  - weitere Verbindungen werden nicht aufgebaut
- **Kommunikation läuft über lange Pfade im Netzwerk**
  - ist jeweils verschlüsselt
  - Nachricht für den Router nicht erkennbar
  - Statt IP-Adresse wird eine Identifikation weitergeleitet
- **Vorteil**
  - IP-Adresse wird niemals veröffentlicht
  - Absolute Sicherheit

Dark-Net

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Dark-Net ist ein privates Peer-to-Peer-Netzwerk**
  - Teilnehmer vertrauen allen anderen Teilnehmer
  - Beispiel:
    - Freundeskreis
    - Sport-Club
- **nicht zu Verwechseln mit dem gleinamigen Nachfolger von Free-Net**

- **Dark-Nets regeln den Zugang über**
  - geheimgehaltene Zugangsadressen und Software
  - oder über Authorisierung über Password
  - oder über zentrale Authentifikation

Steganographie

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Die Steganographie ist die Kunst und Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen.**
- **Ziele**
  - Verstecken von Botschaften
  - Prüfung des Ursprungs von Dokumenten (durch versteckte Botschaften)
- **Beispiele**
  - Kleine unmerkliche Veränderungen von Audio-Dateien, Bildern, Videos
  - durch Veränderung des kleinsten signifikanten Bits
- **Vorteile**
  - Übertragung von Daten lässt sich vollkommen verschleiern
- **Nachteile**
  - Erheblicher Overhead, z.B. unter 0,5% Datendichte bei Manipulation des kleinsten signifikanten Bits bei Audio-Übertragungen

Verschlüsselte Daten

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Peer speichern nur verschlüsselte Daten**
  - Dem Speichernden ist es nicht möglich die Daten zu lesen
  - Die Daten werden vom Veröffentlicher verschlüsselt
- **Zusätzlich können diese Daten vom Veröffentlicher auch unterschrieben werden, so dass**
  - dieser die Daten ändern oder löschen kann
  - kein anderer die Daten unbefugt löscht
- **Diese können gelesen werden, wenn**
  - Der Veröffentlicher den Schlüssel über einem anderen Weg den Abfrager mitteilt oder
  - Der Abfrager einen Indexeintrag gefunden hat auf einem anderen Peer, der zum Entschlüsseln genügt
    - Dadurch wird der Veröffentlicher nicht offenbart
- **Vorteil**
  - Der Speichernde kann für die Inhalte nicht belangt werden
- **Nachteil**
  - Der Speichernde kann die Wichtigkeit der Inhalte nicht beurteilen
    - Löschen oder nicht Löschen

Verschlüsselte, unterschriebene Indexeinträge

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Methode**
  - Der Suchbegriff wird durch eine kryptographische Hash-Funktion bearbeitet und abgelegt
  - Dieser verschlüsselte Index wird kombiniert mit der Identifikation des Speichers
  - Der Index enthält den Schlüssel zur Entschlüsselung des Datums
  - Beides wird unterschrieben durch den Veröffentlicher
- **Vorteil:**
  - Die Suche kann ohne den Veröffentlicher durchgeführt werden
  - Alleine mit diesem Index kann die Datei entschlüsselt werden
  - Nur durch das Suchen nach dem Index können die Dateien gelesen werden
  - Nur der Veröffentlicher kann den Such-Index verändern oder löschen (wegen digitaler Unterschrift)
- **Nachteil:**
  - Anfällig für eine Wörterbuch-Attacke
  - Keine Suche nach ähnlichen Begriffen möglich

Ende der 21. Vorlesung

Peer-to-Peer-Netzwerke

Christian Schindelhauer

schindel@informatik.uni-freiburg.de

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer