Peer-to-Peer-Netzwerke

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

Christian Schindelhauer

Sommersemester 2006

20. Vorlesung

13.07.2006

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**

Verschlüsselungs-methoden

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

Symmetrische Verschlüsselungsverfahren

- z.B. Cäsars Code, DES, AES
- Es gibt Funktion f,g, so dass
  - f(schlüssel,text) = code
  - g(schlüssel,code) = text
- Der Schlüssel
  - muss geheim bleiben
  - dem Sender und Empfänger zur Verfügung stehen

Asymmetrische Verschlüsselungsverfahren

- z.B. RSA, Ronald Rivest, Adi Shamir, Lenard Adleman, 1977
  - Diffie-Hellman, PGP
- Geheimer Schlüssel `privat`
  - kennt nur der Empfänger der Nachricht
- Öffentlichen Schlüssel `offen`
  - Ist allen Teilnehmern bekannt
  - Wird erzeugt durch Funktion
    - keygen(`privat`) = `offen`
- Verschlüsselungsfunktion f und Entschlüsselungsfunktion g
  - sind auch allen bekannt
- Verschlüsselung
  - f(offen,text) = code
  - kann jeder berechnen
- Entschlüsselung
  - g(privat,code) = code
  - nur vom Empfänger

Digitale Unterschriften (Signaturen)

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

- **Beruhen auf asymmetrischen Verschlüsselungsverfahren, z.B. RSA**
  - Der Unterzeichner erzeugt geheimen Schlüssel (`privat`)
  - und öffentlichen Schlüssel (`offen`)
  - Komprimat des Texts, z.B. durch kryptographische Hash-Funktion h
    - `txt` = h(`text`)
  - Unterzeichner berechnet g(`privat`,h(`text`)) = `signature`
  - Empfänger kennen
    - `offen`, `text` und `signature`
    - verifizieren f(`offen`,h(`text`)) = `signature`
- **Problem:**
  - Veröffentlichte Berechnung mittels geheimen Schlüssel kann die Sicherheit des Schemas gefährden (chosen-message-attack)
- **Lösung:**
  - Nachweisbar sicheres Signaturschem von Shafi Goldwasser, Silvio Micali, und Ronald Rivest, 1988

Sicherheit in Peer-to-Peer-Netzwerken

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

- **P2P-Netzwerke sind offen und autonom**
  - Scheinbarer Widerspruch zu Sicherheit?
- **P2P-Netzwerk arbeitet in feindlicher Umgebung**
  - Internet
- **Anforderungen**
  - Verfügbarkeit
  - Dokumentauthentifizierung
  - Anonymität
  - Zugangskontrolle
- **Maßnahmen gegen Attacken**
  - Verhinderung
  - Entdeckung
  - Handhabung
  - Systemwiederherstellung nach einer Attacke

Verfügbarkeit

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

- **Denial-of-Service Attack**
  - Dienstverweigerungsangriff, z.B.
  - Viele Peers fragen ein Dokument nach
  - Viele Peers bombardieren Knoten mit zentralen Aufgaben, z.b. Super-Nodes in Gnutella
- **Chosen-Victim Angriff in Gnutella II**
  - Ein bösartiger Peer lässt sich zum Super-Node erklären
  - Dann erzeugt er eine Menge von Scheinanfragen für einen seiner Peers
- **Typische Angriffe**
  - Ausnutzung von Protokoll-Schwächen
    - kann nachgebessert werden
  - Infiltration durch bösartigen Peers
    - siehe byzantinische Generäle

Dokumentauthentifizierung

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

- **Problemstellung:**
  - Welches Dokument ist authentisch?
  - Welches ist gefälscht, nachgemacht oder verfälscht?
- **Lösung:**
  - Digitale Unterschriften
- **Das Problem des Alters:**
  - Welches Dokument war zu erst da?
  - Das Independent-Label oder der Markentitel

- **Wie kann man nachweisen, dass eine Datei älter ist als ein anders?**
  - C14-Methode, Vergilbung etc. funktioniert nicht
  - Man kann mit herkömlichen Methoden höchstens nachweisen, dass ein Dokument jung ist (aber nicht, dass es alt ist)
    - z.B. durch Referenz auf aktuelle nicht vorhersehbare Ereignisse
      - (Europa-Meisterschaft)

Anonymität

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?
- **FreeNet, GnuNet,...**
  - bieten eine Palette verschiedener Grade der Anonymität

Zugangskontrolle

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

- **Motivation:**
  - Anwendung von Peer-to-Peer-Netzwerken in Unternehmen, Militär, etc. über das Internet
  - Bezahl-Peer-to-Peer-Netzwerke
    - siehe aktuelles Napster
- **Lösung:**
  - Zentrale Authorisierung
  - Virtual Money (ebenfalls zentral authentifiziert?)

- **Verteilte Lösungen hängen mit dem Problem der Identifizierung zusammen**
  - Kollision mit Anonymität
  - Beispiel
    - „Jeder darf sich eine Datei herunterladen“
    - Wie erkennt man, dass er nicht schon dran war?

Die Sybil Attacke

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

- **Wer war Sybil?**
  - Flora Rheta Schreiber schrieb 1973 ein Buch „Sybil“
  - Es handelte von einer Frau mit 16 separaten Persönlichkeiten:
    - Sybil: Aushilfslehrerin mit „Zeit-Aussetzern“
    - Peggy: 9 Jahre altes wütendes, verängstigtes Mädchen
    - Vicki: spricht fließend französisch, weiss alles
    - Vanessa: spielt Klavier und ist befreundet mit dem Nachbarn
    - Marsha: dunkle Persönlichkeit mit Selbstmordabsichten
    - ...
  - Das Buch (und der darauf folgende Film 1976) geht auf einen tatsächlichen Fall zurück von
  - Multipler Persönichkeitsstörung, mehrfacher Schizophrenie
- **Bis heute ist umstritten, in wie weit diese Krankheit bei Menschen wirklich existiert**
- **Bei Peer-to-Peer-Netzwerken ist eine absichtliche Persönlichkeitsstörung ein probates Mittel um die Strukturen zu unterlaufen**

Was kann eine Sybil-Attacke bewirken?

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

- **Ein Netzwerk kann dadurch den Zusammenhalt verlieren**
  - betrifft CAN, Chord, Viceroy, Pastry, Tapestry
  - aber nicht Napster (nicht verteilt)
  - nicht zwingend Gnutella
- **Mehrheitsabstimmungen über den Zustand des Netzwerks können gestört werden**
  - Mehrheitsfrage: „Verhält sich ein Peer korrekt“
  - Entscheidend für die Lösung des Problems der byzantinischen Generäle
- **Anfragen im Netzwerk**
  - können dadurch weitestgehend observiert werden
  - können verlangsamt werden
  - durch Zerstörung der Netzwerkstruktur
- **DoS-Angriffe können gestartet werden**

- **Sybil-Attacken greifen Peer-to-peer-Netzwerke wirkungsvoll an**

Wie kann man Sybil-Attacken abwehren?

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

- **Durch zentrale Authorisierung der teilnehmenden Peers**
  - Eine zentrale Instanz authentifiziert die Existenz eines Teilnehmers und die Gültigkeit seiner öffentlicher Schlüssel durch eine digitale Unterschrift
  - Jeder Peer kann sich dadurch von der Existenz des Peers überzeugen
- **Problem: Dezentrale Authorisierung**
  - Erlaubt man einem Peer auch nur eine kleine Menge von anderen Peers zu authorisieren, dann
  - Authorisiert Peer 1 den Peer 2
  - Peer 2 authorisiert Peer 3
  - Peer 3 authorisiert Peer 4
  - ...
  - Damit steht einer Sybil-Attacke nichts mehr im Wege

Der Sybil-Abwehransatz John Douceur

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

- **Annahmen:**
  - Peers sind einzelne Rechner, die einer Person unterstehen
  - Einzelpersonen besitzen nicht unbeschränkte Rechenresourcen
- **Alle Teilnehmer des Peer-to-Peer-Netzwerks**
  - müssen ein bestimmtes mathematisches Problem (**Challenge**) lösen.
  - Zum Beispiel müssen sie für verschiedene Werte y, das x finden mit h(x)=y,
    - h ist eine kryptographisch sichere Hash-Funktion
    - y= h(x) wurde von einem herausfordenden Peer (**Challenger**) gewählt
    - Die Größe der Aufgabe kann durch die teilweise Bekanntgabe der Bits von x bestimmt werden
- **Innerhalb einer gewissen Zeit kann jeder virtuelle Peer nur eine bestimmte Anzahl von solchen „Challenges“ lösen**
- **Vorteil:**
  - Liefert einen Ansatz mit Sybil-Attacken fertig zu werden
- **Nachteile: ...**

Nachteile

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

- **Riesige Verschwendung von Rechenresourcen**
- **Durch „Ein-Hacken“ in fremde Rechner stehen Angreifer durch enorme Rechenkapazitäten zur Verfügung**

- **Heterogenität des Netzwerks**
  - Studenten an Universitäten können über Pool-Recher große Rechenkapazitäten verfügen
  - Staatliche Einrichtung verfügen über noch größere Resourcen (siehe Motivation)
  - Wenig leistungsfähige Peers können durch den Challenge überfordert werden
    - ältere PCs, Pocket-PCs, etc.

- **Der Challenge selbst ist ein institutionalisierte Form des Denial-of-Service-Attacks**

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

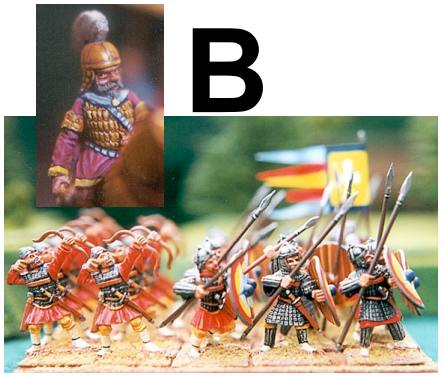
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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

Attacke

X



B

Abwarten

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

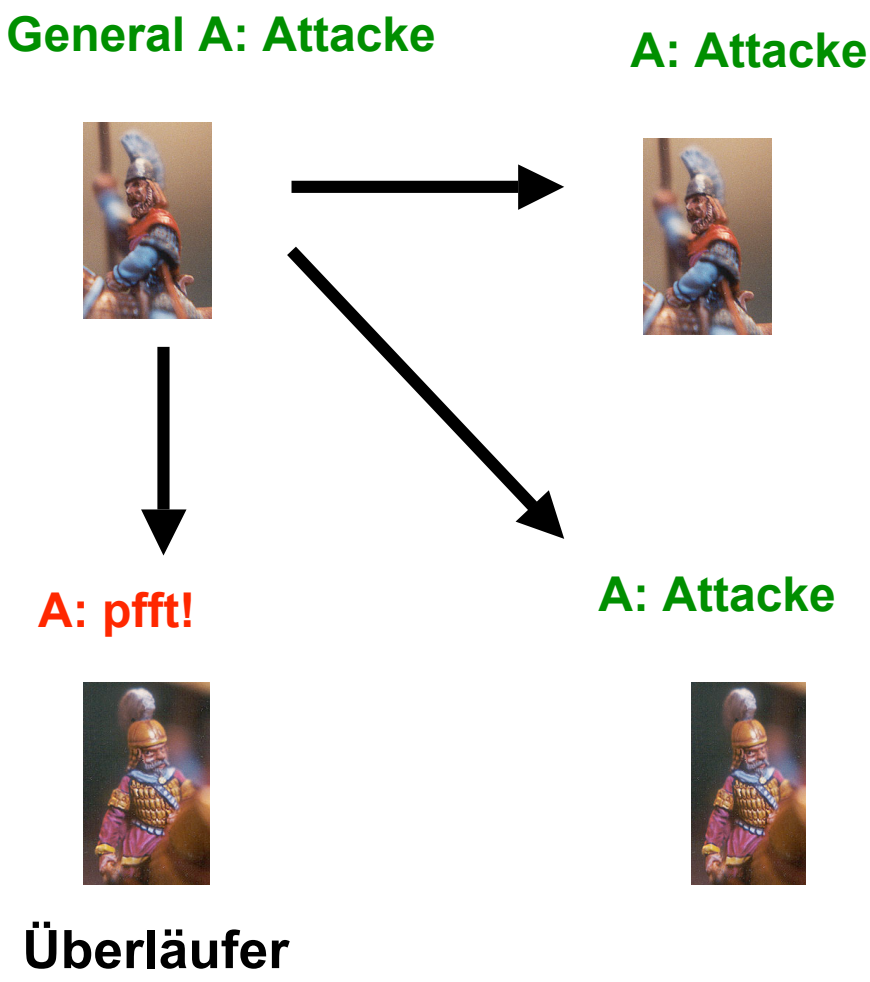
Theorem

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**



Ende der 20. Vorlesung

Peer-to-Peer-Netzwerke

Christian Schindelhauer

schindel@informatik.uni-freiburg.de

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