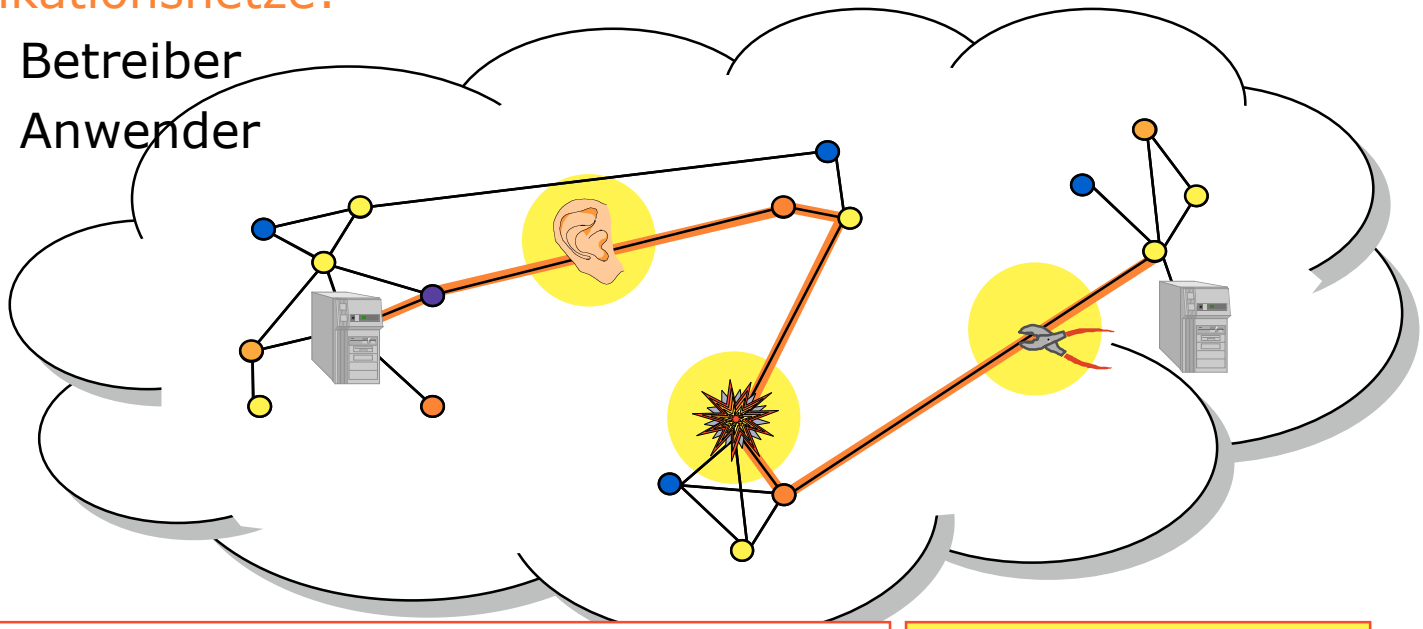
Sicherheit und Schutz im Internet

Hannes Federrath

http://www.inf.fu-berlin.de/~feder/

Sicherheit in Rechnernetzen

- Telekommunikationsnetze:
  - sehr viele Betreiber
  - sehr viele Anwender



Bedrohungen

- unbefugter Informationsgewinn
- unbefugte Modifikation
- unbefugte Beeinträchtigung der Funktionalität

Schutz der

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Maximal berücksichtigte Stärke eines Angreifers

Angreifermodell

- Schutz vor einem allmächtigen Angreifer ist unmöglich.
  - Rollen des Angreifers (Außenstehender, Benutzer, Betreiber, Wartungsdienst, Produzent, Entwerfer …), auch kombiniert
  - Verbreitung des Angreifers
  - Verhalten des Angreifers
    - passiv / aktiv
    - beobachtend / verändernd (bzgl. seiner erlaubten Handlungen)
  - dumm / intelligent
  - Rechenkapazität:
    - unbeschränkt: informationstheoretisch
    - beschränkt: komplexitätstheoretisch

Geld

Zeit

Sicherheit: Abgrenzung von Security & Safety

SECURITY
Schutz gegen beabsichtigte Angriffe

Vertraulichkeit
- Abhörsicherheit
- Sicherheit gegen unbefugten Gerätezugriff
- Anonymität
- Unbeobachtbarkeit

Integrität
- Übertragungsintegrität
- Zurechenbarkeit
- Abrechnungsintegrität

Verfügbarkeit
- Ermöglichen von Kommunikation

SAFETY
Schutz vor unbeabsichtigten Ereignissen

Fehlertoleranz

Verfügbarkeit
- Funktionssicherheit
- Technische Sicherheit
- Schutz vor Überspannung, Überschwemmung, Temeraturschwankungen
- Schutz vor Spannungsausfall

Sonstige Schutzziele
- Maßnahmen gegen hohe Gesundheitsbelastung
- …

Schutzziele: Einordnung

	WAS?	WANN?, WO?, WER?
	Kommunikations-gegenstand	**Kommunikations-umstände**
Un-erwünschtes verhindern	**Vertraulichkeit** **Verdecktheit** **Inhalte**	**Anonymität** **Unbeobachtbarkeit** **Sender** **Empfänger** **Ort**
Erwünschtes leisten	**Integrität** **Inhalte**	**Zurechenbarkeit** **Senden** **Empfangen**
	Verfügbarkeit **Inhalte**	**Erreichbarkeit** **Rechtsverbindlichkeit** **Bezahlung**

Vertraulichkeit

Vertraulichkeit

Verdecktheit

Integrität

Zurechenbarkeit

Anonymität

Unbeobachtbarkeit

Verfügbarkeit

Erreichbarkeit

Rechtsverbindlichkeit

Verschlüsselungsverfahren

- **Symmetrische Verschlüsselung, z.B. DES, AES**
  - Kommunikationspartner teilen ein gemeinsames Geheimnis (symmetrischer Schlüssel)
  - Sicherheit basiert meist auf Chaos
  - Schlüssellänge ≥ 128 Bits
- **Asymmetrische Verschlüsselung, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Verschlüsselungsschlüssel
    - *Privaten* Entschlüsselungsschlüssel
  - Sicherheit basiert auf zahlentheoretischen Annahmen
  - Schlüssellänge ≥ 1024 Bit
  - Neuerdings: Elliptische Kurven: ca. 160 Bit
- **Bekannte Verschlüsselungssoftware**
  - Pretty Good Privacy
  - http://www.pgp.com

Vertraulichkeit

Verdecktheit

Integrität
Zurechenbarkeit

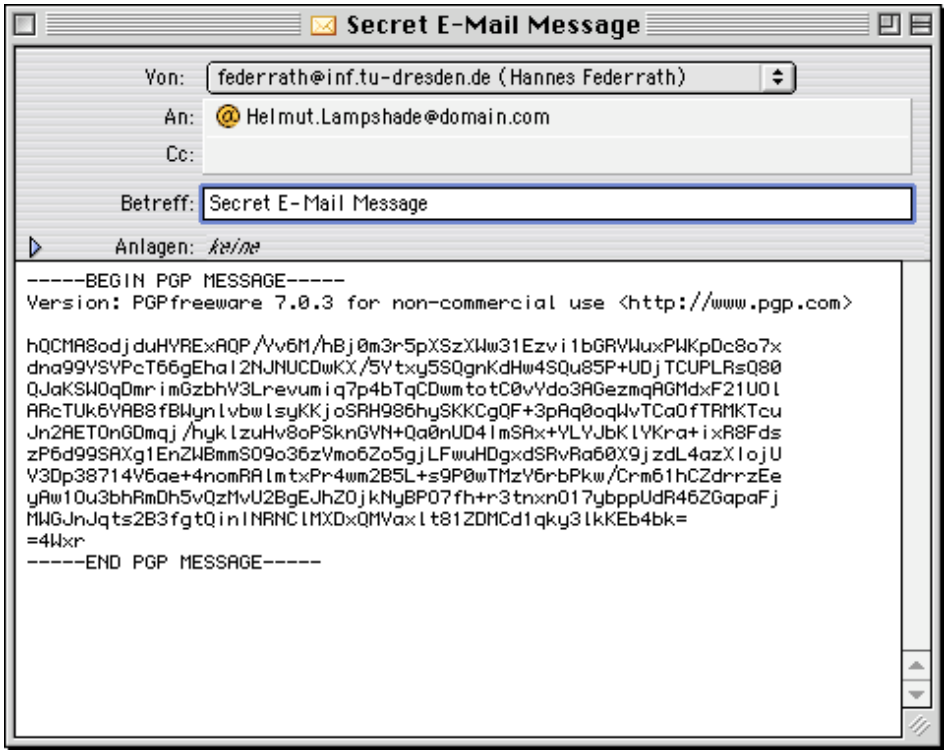
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Verschlüsselungssoftware

- Pretty Good Privacy
  - http://www.pgp.com
- Gnu Privacy Guard
  - http://www.gnupg.org



Verdecktheit: Steganographie

Vertraulichkeit

Verdecktheit

Integrität
Zurechenbarkeit

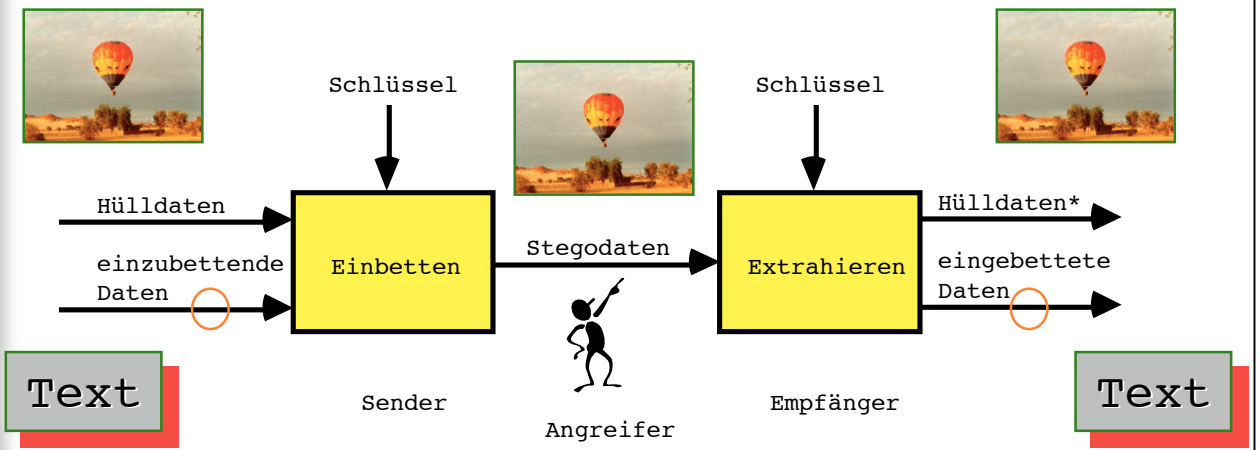
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Steganographie

- **Verbergen der Existenz einer geheimen Nachricht**
  - geheimzuhaltende Nachricht wird in eine Hülle eingebettet
  - minimale Veränderungen kaum bzw. nicht erkennbar
  - Veränderungen nicht mit Messmethoden nachweisbar



Integrität und Zurechenbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Message Authentication Codes

- **Symmetrisches Verfahren**
  - Kommunikationspartner teilen ein gemeinsame Geheimnis (symmetrischer Schlüssel)
- **Gehört heute zum Grundschutz**
  - Verfälschungen von Nachrichten (böswillige und zufällige) sind erkennbar
- **Keine Nachweisbarkeit gegenüber Dritten**

Digitale Signatur

- **Asymmetrisches Verfahren, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Testschlüssel
    - *Privaten* Sigierschlüssel
- **Nachweisbarkeit gegenüber Dritten**
- **Ebenfalls einsetzbar:**
  - Pretty Good Privacy
  - http://www.pgp.com

Anonymität und Unbeobachtbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Verfahren zum Schutz von Verkehrdaten

- **Adressierungsinformationen können nicht verschlüsselt werden**
  - Problem Verkehrsdaten:
    - Wer mit wem, wann, wie lange, wo, wieviel Information?
  - Problem Interessensdaten:
    - Wer interessiert sich für was?
- **Spezielle Verfahren:**
  - Proxies
  - Mix-Netz
  - DC-Netz
  - Dummy traffic
  - …

> Empfehlungen für sicheres Surfen

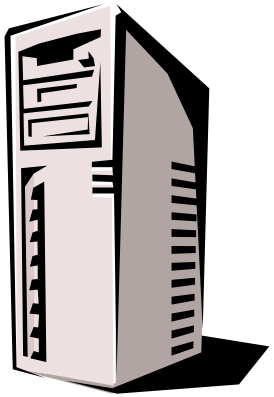
- Cookies und andere Verkettungsmerkmale deaktivieren
  - Web Server kann alle Benutzeraktivitäten verketten
  - Zusätzlicher Filter nützlich (WebWasher, JunkBuster, CookieCooker)
  - Ebenfalls filtern: »Web Bugs« (transparente 1x1-Grafiken)
- Java und JavaScript im Browser deaktivieren
  - IP-Adresse kann abgefragt und übermittelt werden
    - Teilnehmer u.U. identifizierbar durch Server
- ActiveX und andere aktive Inhalte deaktivieren
  - Unberechtigter Zugriff auf Systemressourcen (Festplatte etc.) möglich
- Profil der Dienstnutzung kann zur Beobachtung führen
  - Online-/Offline-Phasen
  - Gleicher Nutzer besucht gleiche Webseite häufiger
    - Aktionen verkettbar

Funktionsweise von Cookies

Erster Besuch:

1. GET www.amazon.de

2. Set Cookie: id=12241235564



3. ggf. Warnung

4. Speichern auf Festplatte

Folgende Besuche:

GET www.amazon.de
Cookie: id=12241235564

- wird nur an zugehörigen Server zurückgesendet
- hat ein vom Server definiertes Verfallsdatum
- wird auch bei Abruf eingebetteter Objekte gesendet (z.B. Bilder)

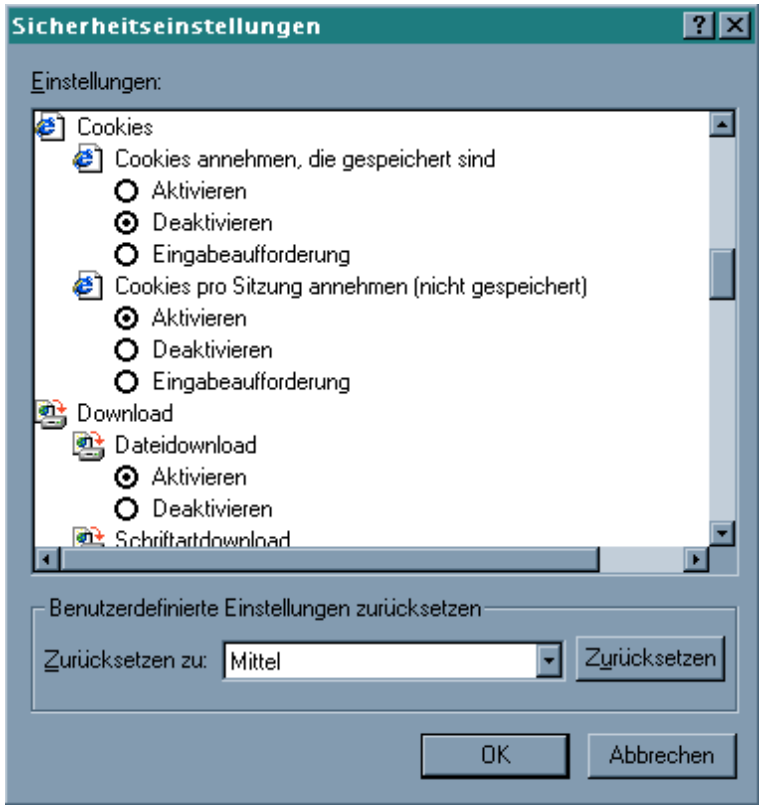
Ungefährliche Kekse ?

- Löschen nicht die Festplatte
- Übertragen keinen Viren
- Verraten keine lokal gespeicherten Daten
  - Passwörter, geheime Schlüssel usw.
- Webserver erkennt Nutzer bei jedem Besuchen seiner Seite wieder
  - Positiv:
    - personalisierte Webseiten
  - Negativ:
    - Erstellung von Nutzerprofilen

Gefährliche Kekse !

- Werberinge (z.B. Doubleclick.com):
  - Plazieren Banner auf Seiten vieler Anbieter
  - Alle Banner werden von zentralem Server geladen, Cookie wird gesendet
  - Werbeserver erhält globales Nutzungsprofil
  - Alle Server könnten Informationen erfahren, die man an einen gesendet hat.

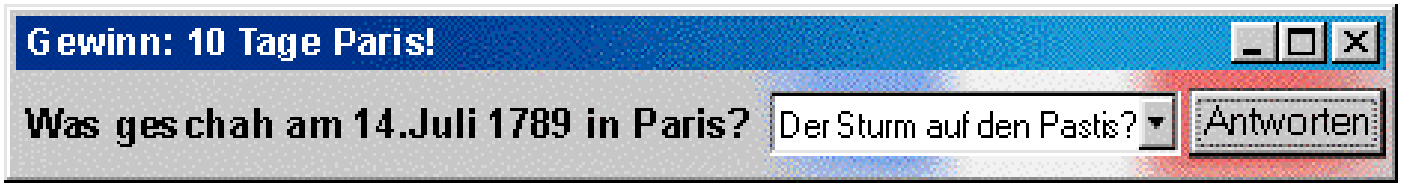
- Gegenmaßnahmen
  - Cookies deaktivieren
  - Problem:
    - Viele Angebote nur mit Cookies verfügbar
    - nützliche Anwendungen für Cookies



Third-Party Cookies

- Laden eines eingebetteten Bildes (z.B. Werbebanner) von einem fremden Server (z.B. Werbering)
  - Werbering setzt Cookie
  - Referer verrät Herkunft des Requests

- Verschiedene Shops arbeiten mit demselben Werbering zusammen:
  - Website A (z.B. Bookshop)
  - Website B (z.B. Lebensversicherung)
  - Website C (z.B. Gesundheitsberatung)



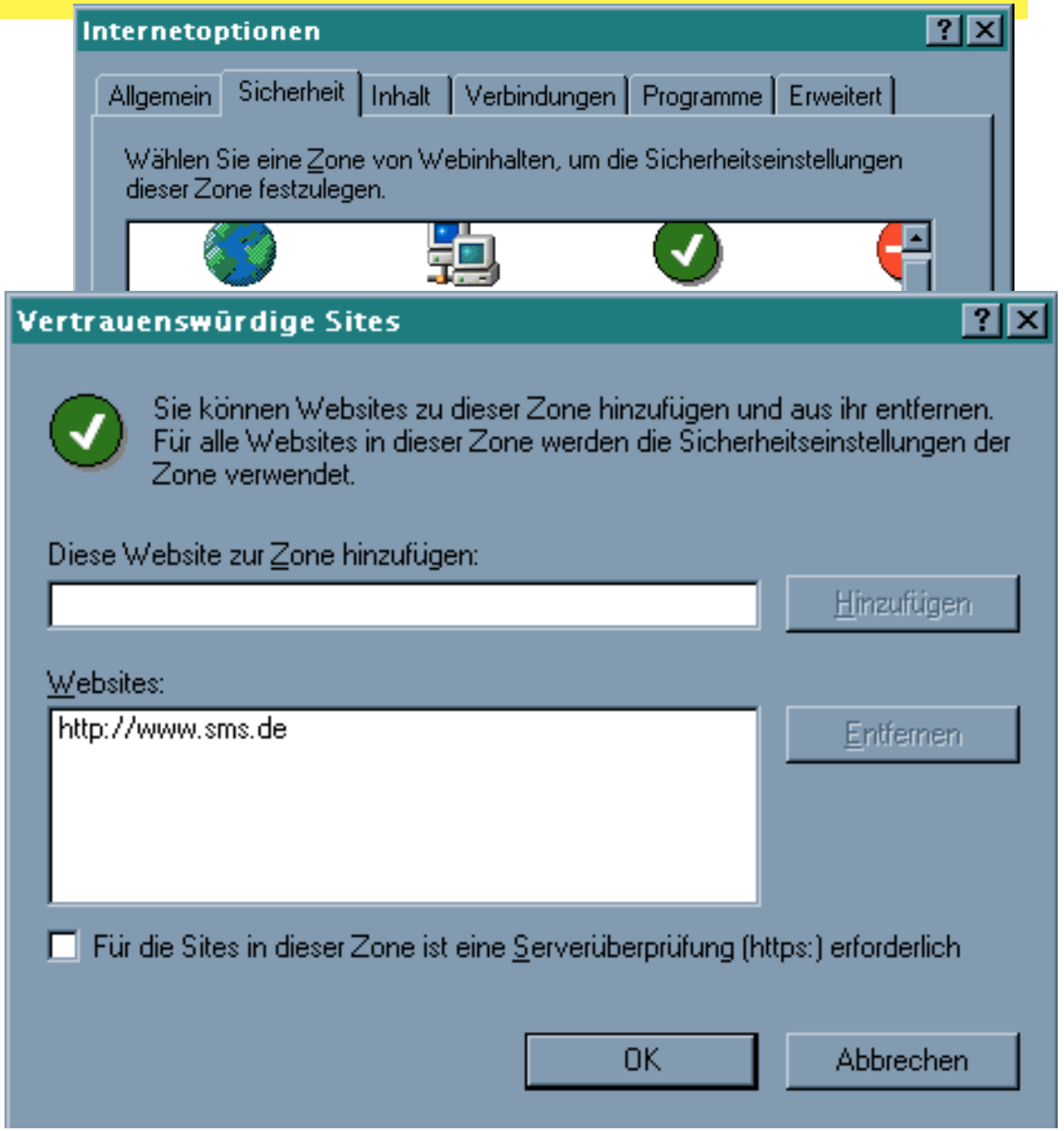
Third-Party Cookies

Gläserner Bürger? Legal?

Gegenmaßnahmen

Cookies

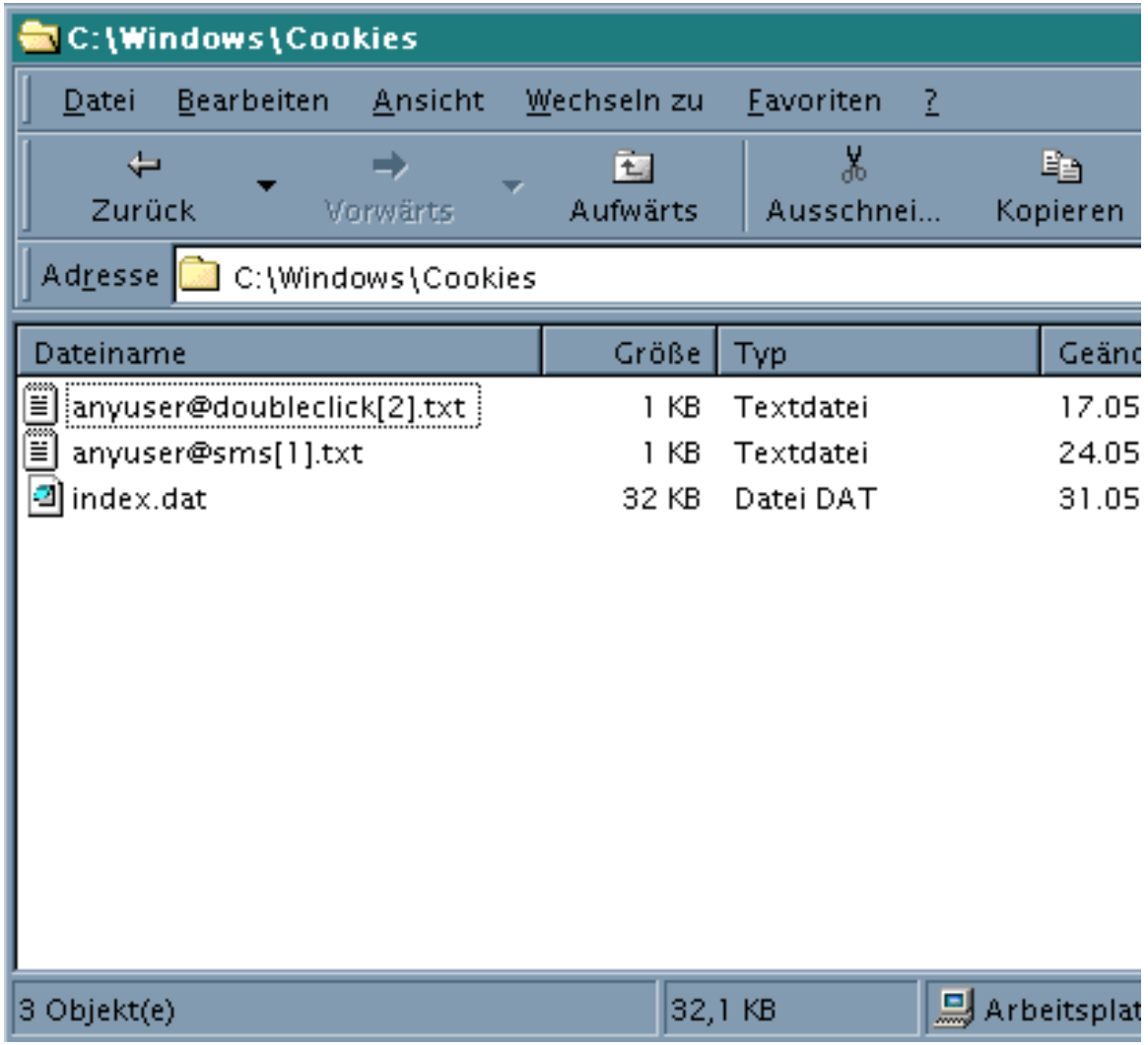
- ⌘ nur bei ausgewählten Seiten speichern
- ⌘ regelmäßig löschen
- ⌘ filtern
- ⌘ regelmäßig weltweit austauschen



Gegenmaßnahmen

Cookies

- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen



Gegenmaßnahmen

Cookies

- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen

http://www.junkbusters.com/

http://www.guidescope.com/

http://www.webwasher.com

Gegenmaßnahmen

Cookies

- ⌘ nur bei ausgewählten Seiten speichern
- ⌘ regelmäßig löschen
- ⌘ filtern
- ⌘ regelmäßig weltweit austauschen

CookieCooker
cookie.inf.tu-dresden.de

CookieCooker

cookie.inf.tu-dresden.de

- Filter software für Cookies
  - ähnlich JunkBuster und WebWasher

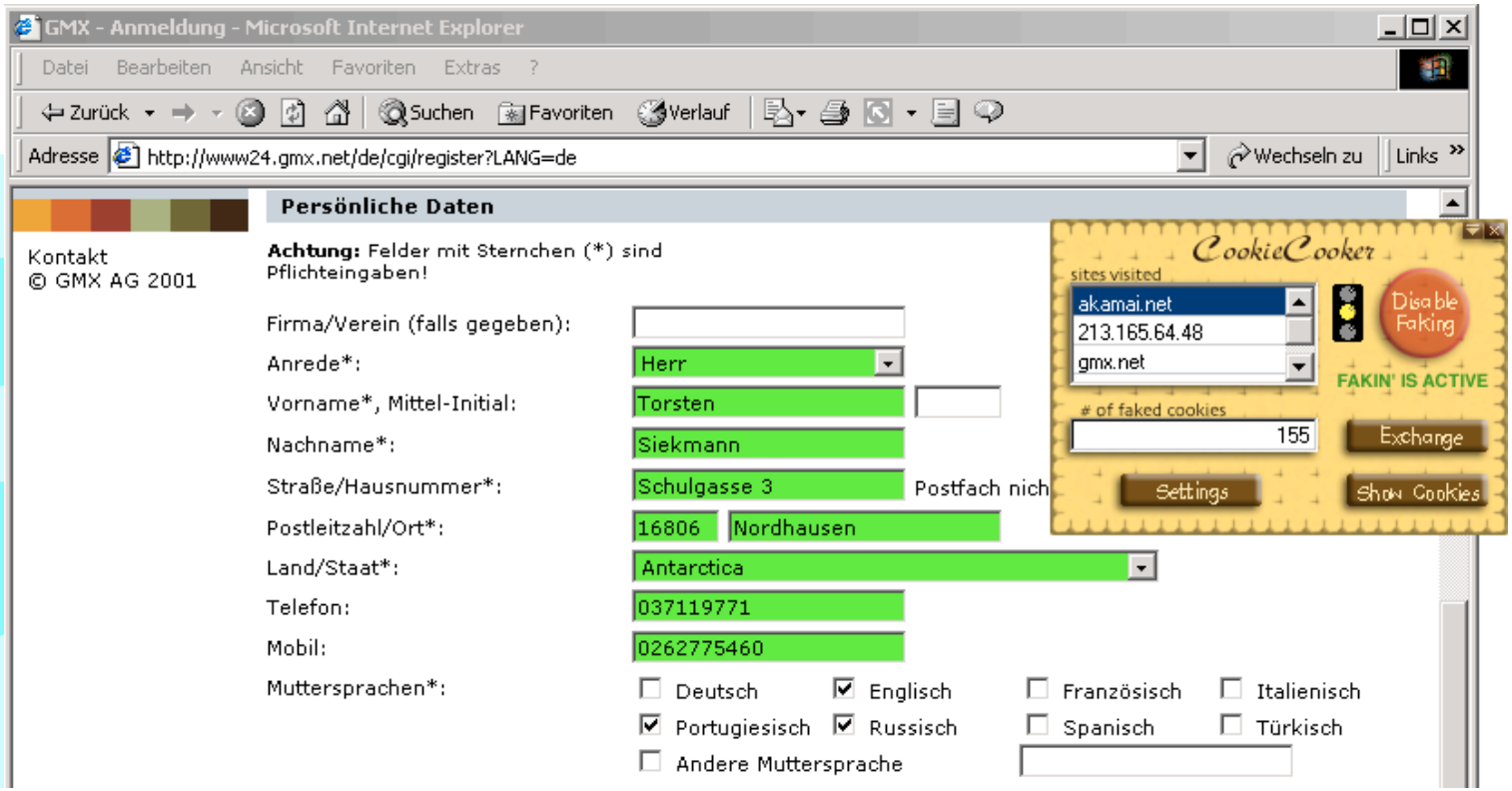
- Aktiver Schutz durch Cookie-Austausch

CookieCooker

cookie.inf.tu-dresden.de

- Idee:
  - Aktiver Schutz durch Cookie-Austausch zwischen Nutzern
  - Andere Personen surfen unter dem fremden Cookie
  - Verfälschung der Nutzerprofile
- Unterscheidung nötig zwischen nützlichen und ungewollten Cookies
- Cookie-Austausch über Peer-to-Peer-Service

- Zusätzliche Funktionen:
  - Automatisiertes Ausfüllen von Web-Formularen
    - sehr schnelles Anlegen von Free-Mail-Accounts
  - Identitätsmanagement
    - Cookie Cooker merkt sich (pseudonyme) Zugangsdaten (Name/Passwort etc.)



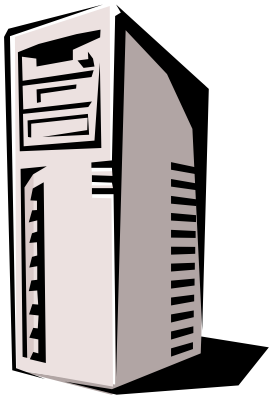
Überwachung auch ohne Cookies

- IP-Nummern

Adresse:
123.86.9.5

GET www.amazon.de
To: 195.66.15.4
From: 123.86.9.5

HTTP ...
To: 123.86.9.5
From: 195.66.15.4



Adresse:
195.66.15.4

Einschränkung:

Zuweisung dynamischer IP-Nummern bei Einwahlzugang

Überwachung auch ohne Cookies

- Überwachung durch Internet Service Provider

Beispiel:

http://www.predictivenetworks.com/

Anonymität und Unbeobachtbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

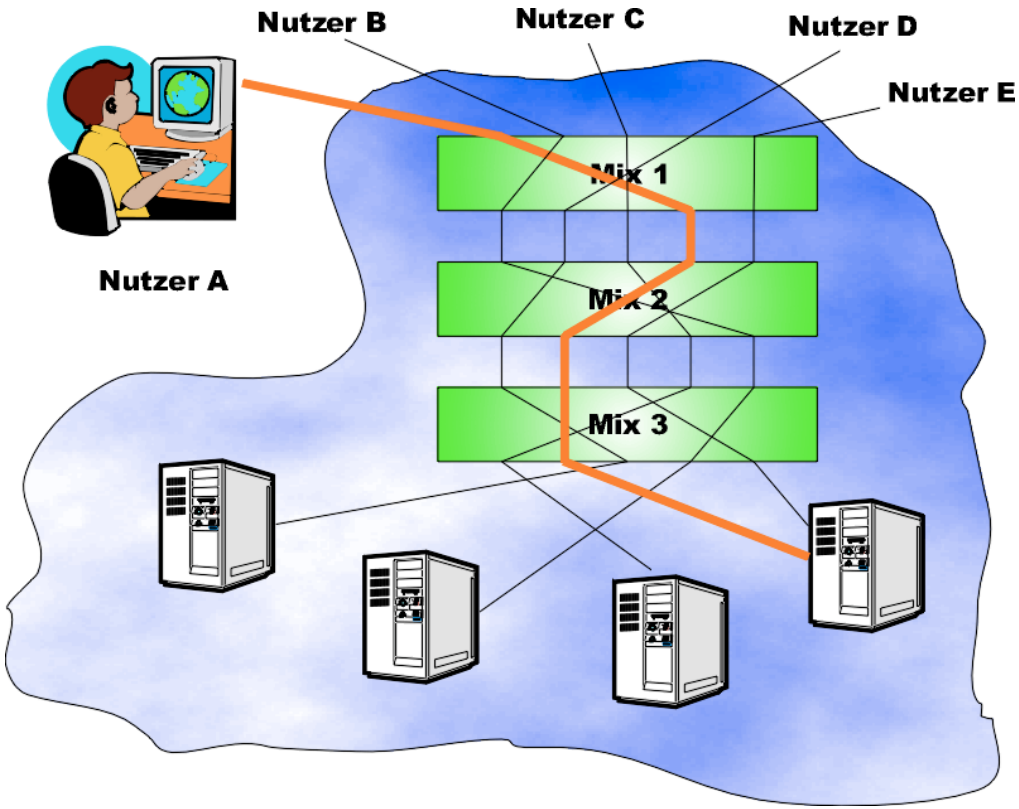
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Verfahren zum Schutz von Verkehrdaten

- **Anonymisierung von Web-Zugriffen**
  - JAP-Software
  - http://jap.inf.tu-dresden.de



Verfügbarkeit und Erreichbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

- **Verfügbarkeit**
  - Nutzbarkeit von Diensten und Ressourcen, wenn ein Teilnehmer sie benutzen will.
- **Erreichbarkeit**
  - Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht.
- **»Mechanismen«**
  - Mehrfach redundante Leitungsführung
  - Diversitärer Entwurf der Komponenten
  - Starke Vermaschung der Kommunikationsverbindungen
- **Techniken zur Verteilung von Kontrolle**
  - Offenlegung von Designkriterien und Algorithmen
  - Open Source Software
  - Sichere Betriebssysteme

Verfügbarkeit und Erreichbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

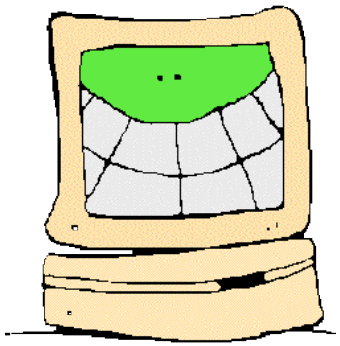
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Denial-of-Service-Angriffe

- **DoS-Angriffe auf Schwachstellen im System**
  - Mail-Bombing – Spamming
  - Broadcast-Storm
  - SYN-Flooding
  - Angriffe auf einen Switch
- **DoS-Angriffe auf Implementationsfehler**
  - Ping of Death
  - WinNuke
  - Teardrop und Nachfahren



Vorher

Nachher

Verfügbarkeit und Erreichbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Denial-of-Service-Angriffe

- **Smurf IP Denial-of-Service Attack (CERT Advisory CA-1998-01)**
  - basiert auf Fooding-Angriff mit Ping-Paketen
  - Ping: Management-Service zur Überprüfung der Empfangsbereitschaft eines Rechners
  - Ping-Pakete werden mit gefälschter Absender-Adresse an eine schlecht administriertes LAN/Intranet geschickt.
  - Konfigurationsfehler in LANs vervielfachte Ping:
    - Weiterleitung an alle Rechner des LAN hinter dem Gateway
    - Jeder Rechner des LAN antwortet mit Pong

Verfügbarkeit und Erreichbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

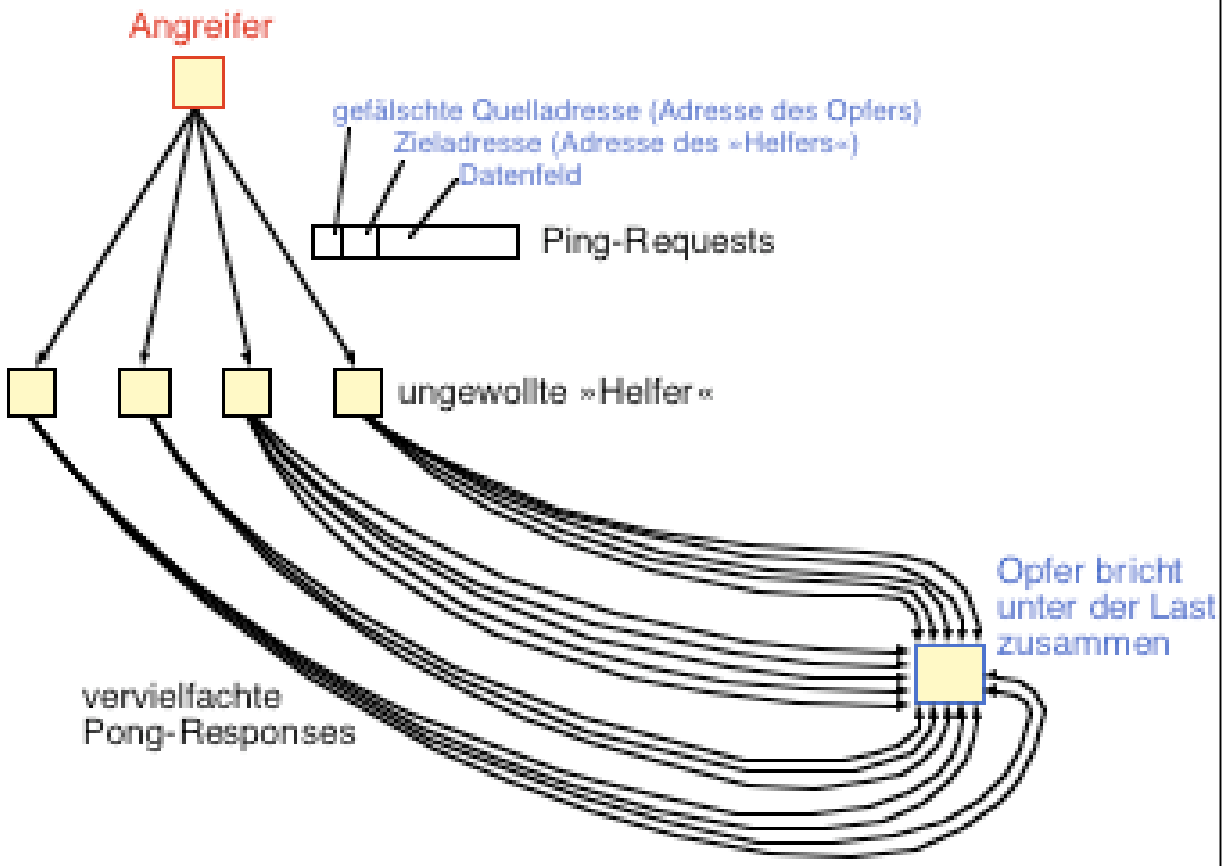
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Denial-of-Service-Angriffe

- **Smurf IP Denial-of-Service Attack (CERT Advisory CA-1998-01)**



Rechtsverbindlichkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

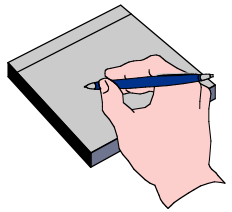
Rechtsverbindlichkeit

- **Rechtsverbindlichkeit**
  - Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.
  - Kann nicht technisch geschaffen werden
- **Rechtsverbindlichkeit der Digitalen Signatur**
  - Klare Regeln bzgl. Beweiswert
  - Zertifizierung von Schlüssel (Public Key Infrastructure PKI)
- **Sicherheit der Netzkomponenten**
  - Zertifizierung von Netzkomponenten
  - Physische Sicherheit, immer dann, wenn Vertrauen in fremde Netzkomponente aufgebracht werden muss.

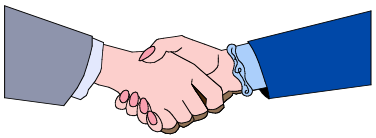
Mehrseitige Sicherheit

- Jeder Beteiligte hat **Sicherheitsinteressen**.

- Jeder Beteiligte kann seine Interessen **formulieren**.



- Konflikte werden erkannt und Lösungen **ausgehandelt**.



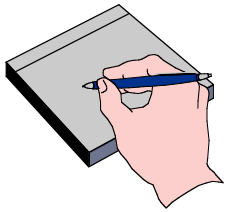
- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen **durchsetzen**.

Sicherheit mit minimalen Annahmen über andere.
So wenig wie möglich Vertrauen in andere setzen müssen.

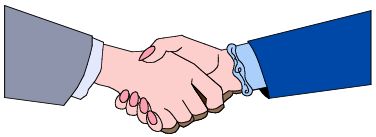
Mehrseitige Sicherheit: Wie?

- Jeder Beteiligte hat **Sicherheitsinteressen**.
  - Schutzziele

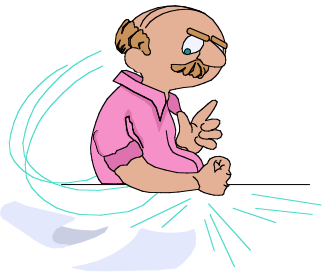
- Jeder Beteiligte kann seine Interessen **formulieren**.
  - Setzt Verständnis des Benutzers voraus
  - Gute Bedienoberflächen sind nötig



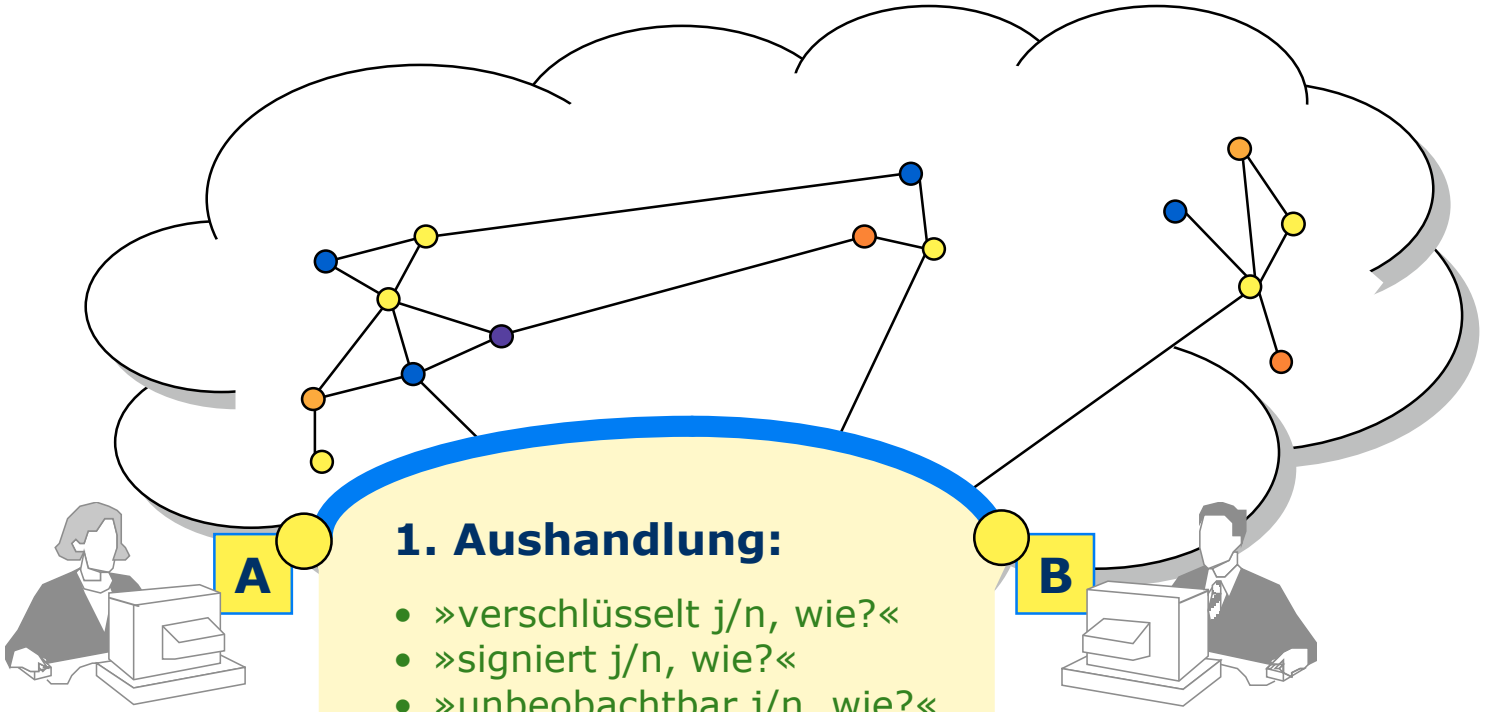
- Konflikte werden erkannt und Lösungen **ausgehandelt**.
  - Setzt entsprechende Tools und
  - Technische Protokolle voraus



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen **durchsetzen**.
  - Anwender brauchen Werkzeuge zum Selbstschutz



Formulierung und Aushandlung



Die Anwendung von mehrseitiger Sicherheit setzt die explizite Formulierung der Sicherheitsinteressen und die Notwendigkeit voraus, aufeinander einzugehen.

Selbstschutz-Tools: Beispiele

- Verschlüsselung, Signatur
  - PGP, GPG
- Filter
  - Webwasher, JunkBuster, CookieCooker
- Personal Firewall
  - Norton Personal Firewall, Zone Alarm
- Anonymisierer
  - Anonymizer, JAP
- Sichere Dienste anstelle ihrer unsicheren Vorläufer verwenden
  - telnet ssh, ftp scp, http https
- Betriebssysteme mit Zugriffskontrolle/Rechtevergabe/OpenSource
  - Linux, BSD

Mehrseitige Sicherheit: Umfassendes Schutzkonzept

- Spannungsfeld Privatheit — Verbindlichkeit
  - Datenvermeidung:
    - Erfassungsmöglichkeit und Speicherung personenbezogener Daten vermeiden.
  - Datensparsamkeit:
    - Jeder behält seine personenbezogenen Daten auf seinem PC.
- Wechselwirkung Datenschutz — Datensicherheit
  - Datenschutz: Schutz der Menschen
  - Datensicherheit: Schutz der Daten
  - Mehrseitige Sicherheit verbindet beides.

Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen *aller* Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.