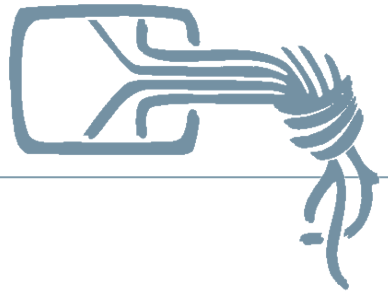


Privatsphäre und Sicherheit im Ubiquitous Computing

Stefan Schlott <stefan.schlott@ulm.ccc.de>

Übersicht

Vision „Ubiquitous Computing“
Privacy-Problem
Verschiedene Lösungsansätze
Einige Verfahren

Ubiquitous Computing

Geprägt von Mark Weiser („The computer for the 21st century“)

„Ubiquitous Computing enhances computer use by making computers available ***throughout the physical environment***, while making them effectively ***invisible*** to the user“

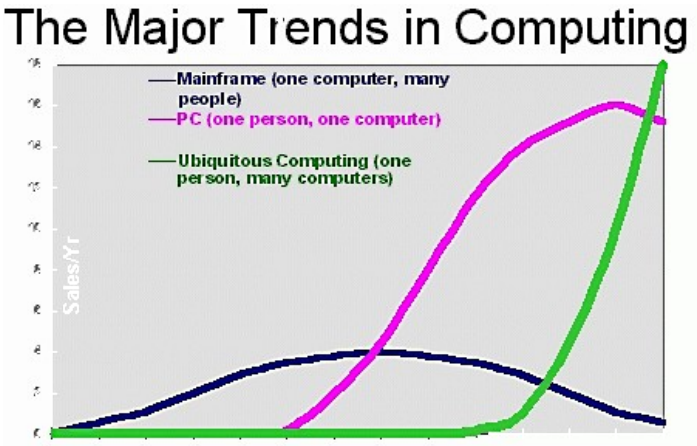
Übertragung vergangener technischer Trends auf heutige PCs:

- Spezialisierung
- Miniaturisierung
- vom technischen Gerät zum Alltagsgegenstand

Unsichtbar und allgegenwärtig

1943 - Thomas J. Watson –
"I think there is a world market for about five computers"

Bill Gates -
"Back when I was a teenager, I envisioned the impact that low-cost computers could have. 'A computer on every desk and in every home' became Microsoft's corporate mission, and we have worked to help make that possible"



1991 – Mark Weiser –
"*Hundreds of Devices per Person*"

Ubiquitous Computing

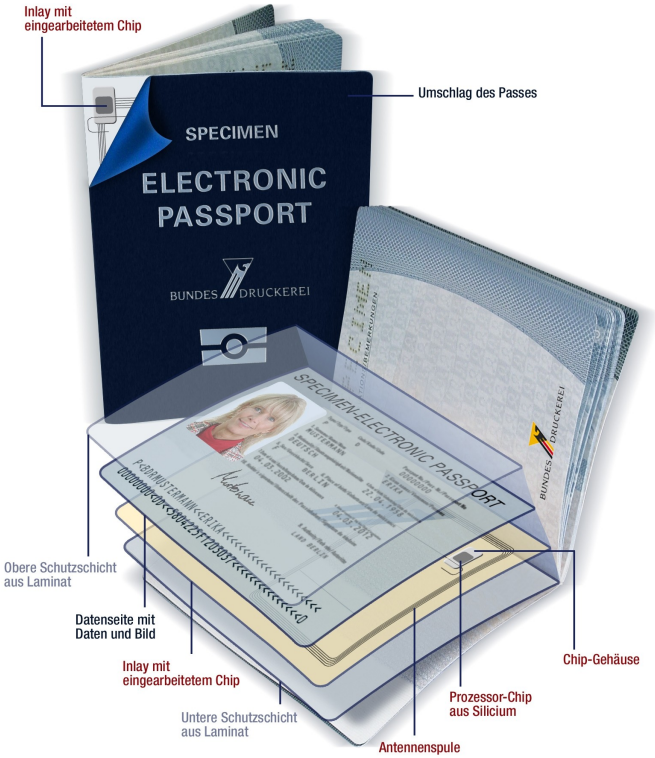
Verkleinerung und Spezialisierung von Computern

...Verkleinerung bis zum vollständigen Verschwinden
- Alltagsgegenstände um Funktionen anreichern
- Neue Funktionen generieren
- „Verschwinden“ Autonome Stromversorgung
- Miniaturisierung Portable Geräte

Kommunikation mit anderen Geräten
- Unauffällig Funktechnologie

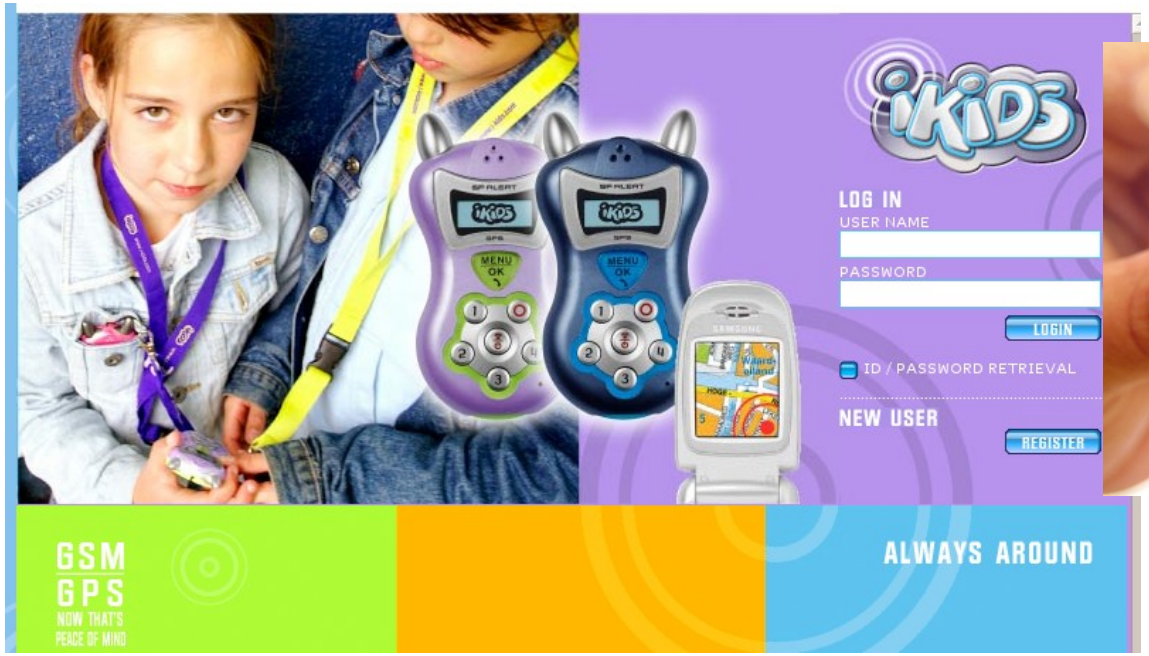
...schon heute?

Ubiquitous Computing - heute



Quelle: Bundesdruckerei GmbH

▶ Der Chip kann entweder in die Datenseite oder in den Umschlag des Reisepasses integriert werden.


iKIDS
LOG IN
USER NAME
PASSWORD
LOGIN
ID / PASSWORD RETRIEVAL
NEW USER
REGISTER
GSM
GPS
NOW THAT'S
PEACE OF MIND
ALWAYS AROUND


PHILADELPHIA


2006 FIFA World Cup Germany™
WINNER GROUP A - RUNNER-UP GROUP B
Round of 16 - FIFA WM-Stadion München - 24 June 2006
Kick-off: 17:00 hrs
Hans M
- BLUE SECTOR -
Nordtribüne
Block: 243 Row: 14 Seat: 1
Round of 16
49
GERMANY 2006
FIFA
Price: € 75.00

Ubiquitous Computing - Visionen

Ubiquitous Computing - Visionen

Bekommt von Patrick noch 20 €

Dezentraler Service: Pollenflug-Vorhersage

Bestellung aufgeben Angebote

Info-Stele: Temperatur, Ozon-Wert, etc.

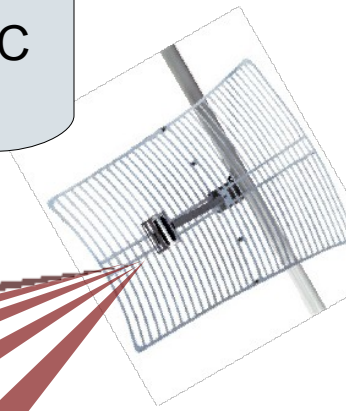
Bob hat morgen Geburtstag

Termin mit Patrick zum Squashen vereinbaren

Bild: „eine momentaufnah… …se / minimalism

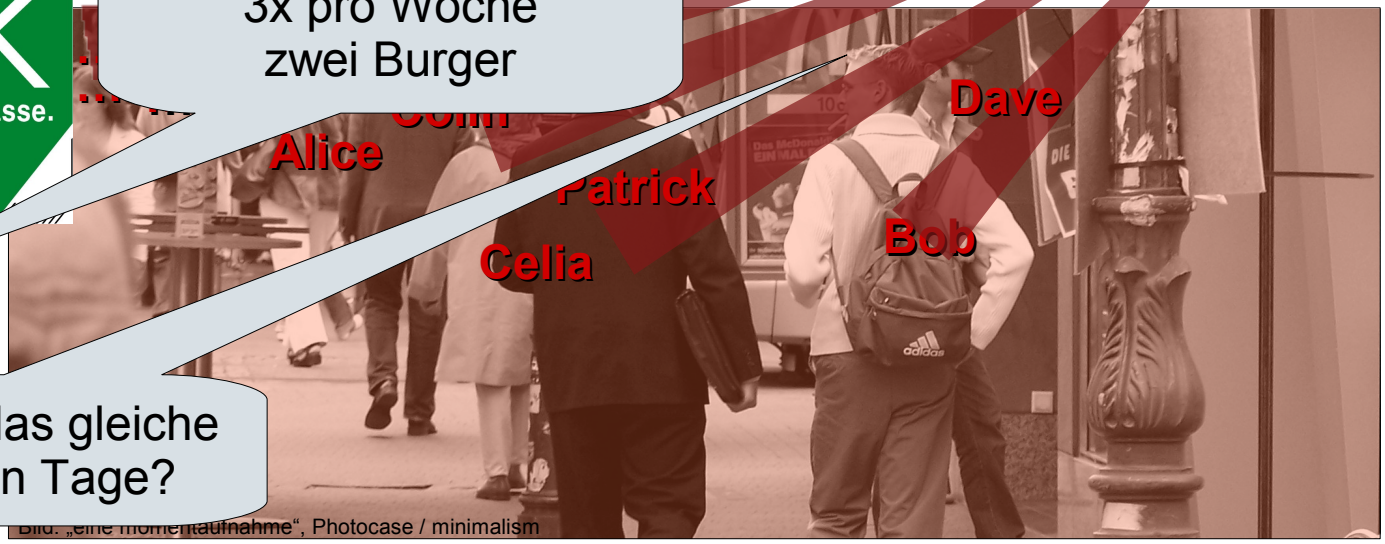
Personen im Raum? -- Nein!

Alle im Urlaub, Heizung auf 16°C absenken



Patrick ißt mindestens 3x pro Woche zwei Burger

AOK Die Gesundheitskasse.



Hallo Patrick, das gleiche wie die letzten Tage?

Bild: „eine Momentaufnahme“, Photocase / minimalism

„Hacker“-Meinungen zum Thema Daten...

„Information möchte frei sein“
-- Steward Brand, 1985

„Alle Information soll frei
und unbeschränkt sein.“
-- „Hackerethik“,
Chaos Computer Buch, 1988

„Öffentliche Daten nützen,
persönliche Daten schützen“
-- „Hackerethik“,
CCC-Webseite 1998

Identity Management – eine Lösung?

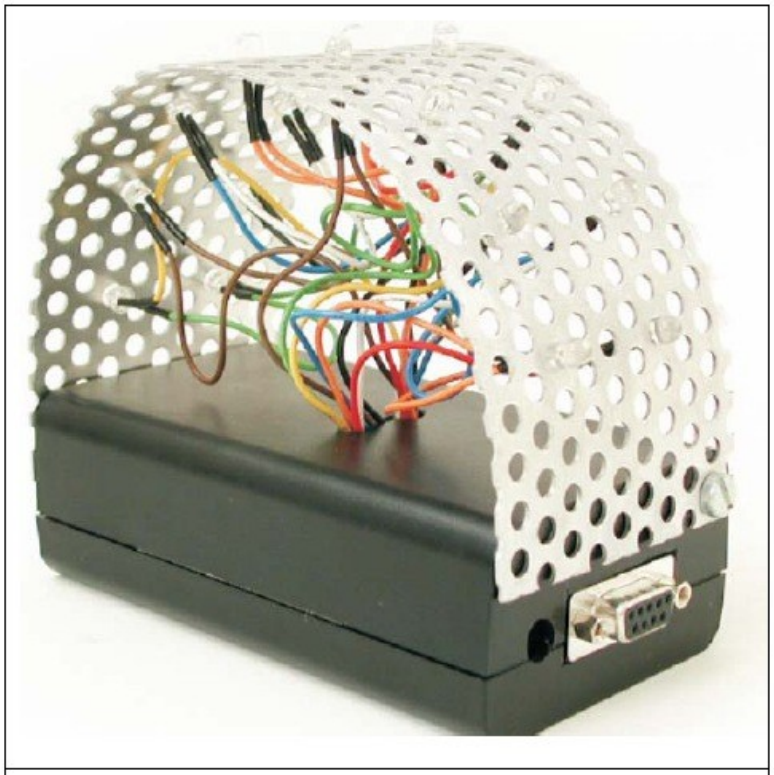
Identity Management: Spezielle Identitäten (Pseudonyme) für verschiedene Einsatzzwecke

- Je generischer, desto größer die Gefahr des Datenabgleichs
- Je spezieller, desto unübersichtlicher

Probleme:

- Definition einer Identität: Was darf sie, was darf sie nicht
- Wahl der passenden Identität
- Kontrolle des Datenflusses

Privacy-Assistant Prototyp



Privacy-Beacon Prototyp (IRREAL)

Bild: Marc Langheinrich

Selbstschutz meiner Daten

Sind Daten einmal unterwegs,
hat man keine weitere Kontrolle über sie!

Datenweitergabe und -auswertung geschieht
vollkommen unspürbar für den Betroffenen!

Gesetzlicher, gesellschaftlicher, moralischer Schutz weiterhin wichtig – reicht aber im Zweifelsfall nicht aus

Selbstschutz meiner Daten

Verhindern der Verlinkung von Daten
- ...bei der Nutzung zentraler Dienste
- ...im lokalen Fall

Verhindern der Datenerhebung
- Wähle Deine Kommunikationspartner mit Bedacht
- Lasse niemanden mithören

Datensparsamkeit
- ...als Rückversicherung für den Worst Case
  (Weitergabe, Diebstahl, Begehrlichkeiten durch Behörden, ...)
- ...Datenmenge in Abhängigkeit vom Vertrauen

Sorge zunächst für Anonymität
Gebe diese dann bewußt und selektiv auf

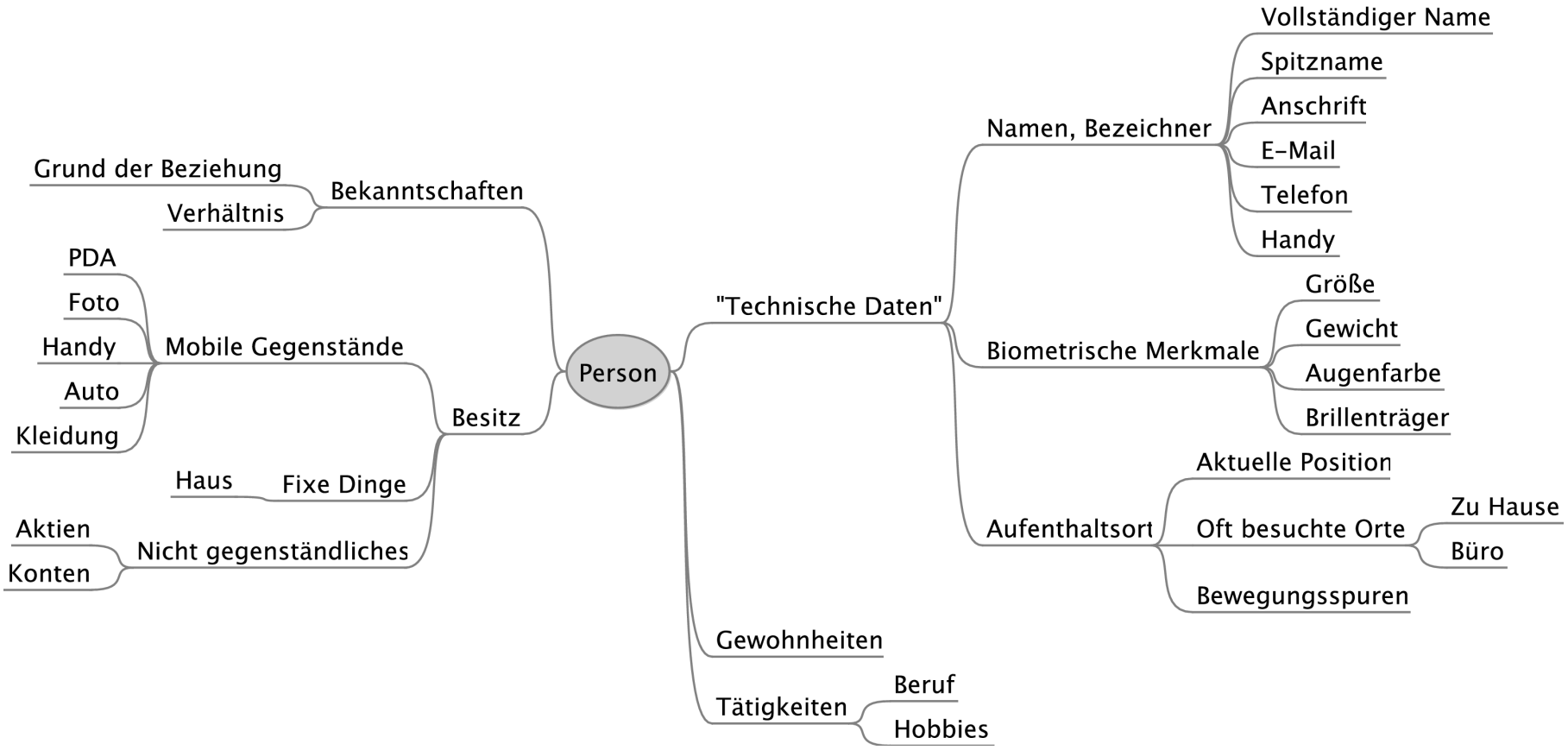
Definition Privatsphäre

Wikipedia: „Die Privatsphäre einer Person bezeichnet den Bereich, der nicht öffentlich ist, in dem nicht im Auftrag eines Unternehmens, Behörde o.ä. gehandelt wird, sondern der nur die eigene Person angeht.“

Daten, die direkt mit einer Person verbunden sind („personenbezogene Daten“)
...oder über Zwischenschritte eindeutig ihr zuzuordnen sind
    z.B. Hundehalsband – Hundemarkennummer – Besitzer

Umgekehrt können solche Daten
    eine Person eindeutig identifizieren
    den Suchraum nach einer Person einschränken

Privatsphäre einer Person



Anonymisierung mit Infrastruktur

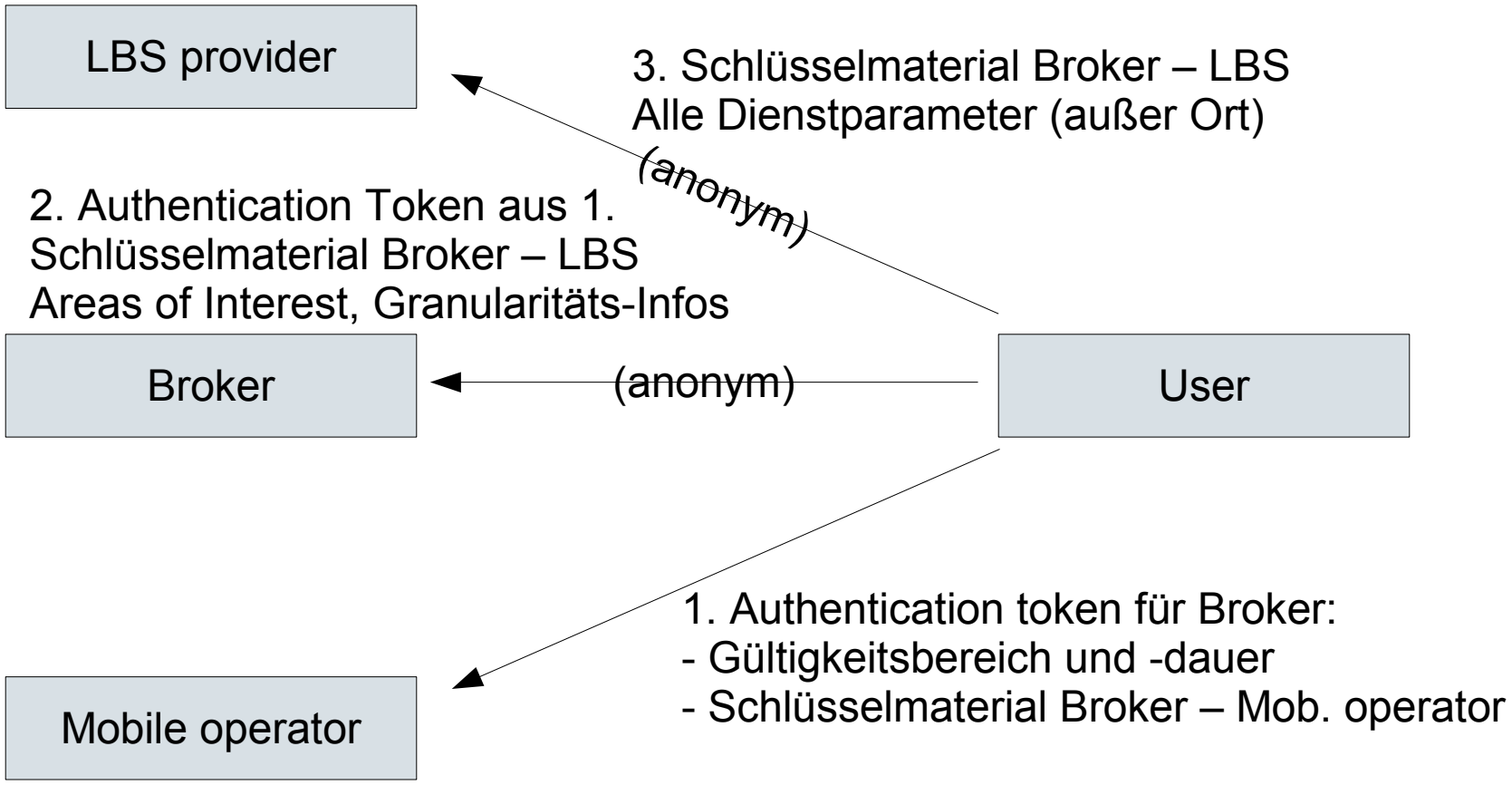
Benutzung von zentralen Diensten: Kommunikation über gegebene (Multihop)-Infrastruktur

- GPRS – Internet
- Mist/Gaia ubiquitous infrastructure

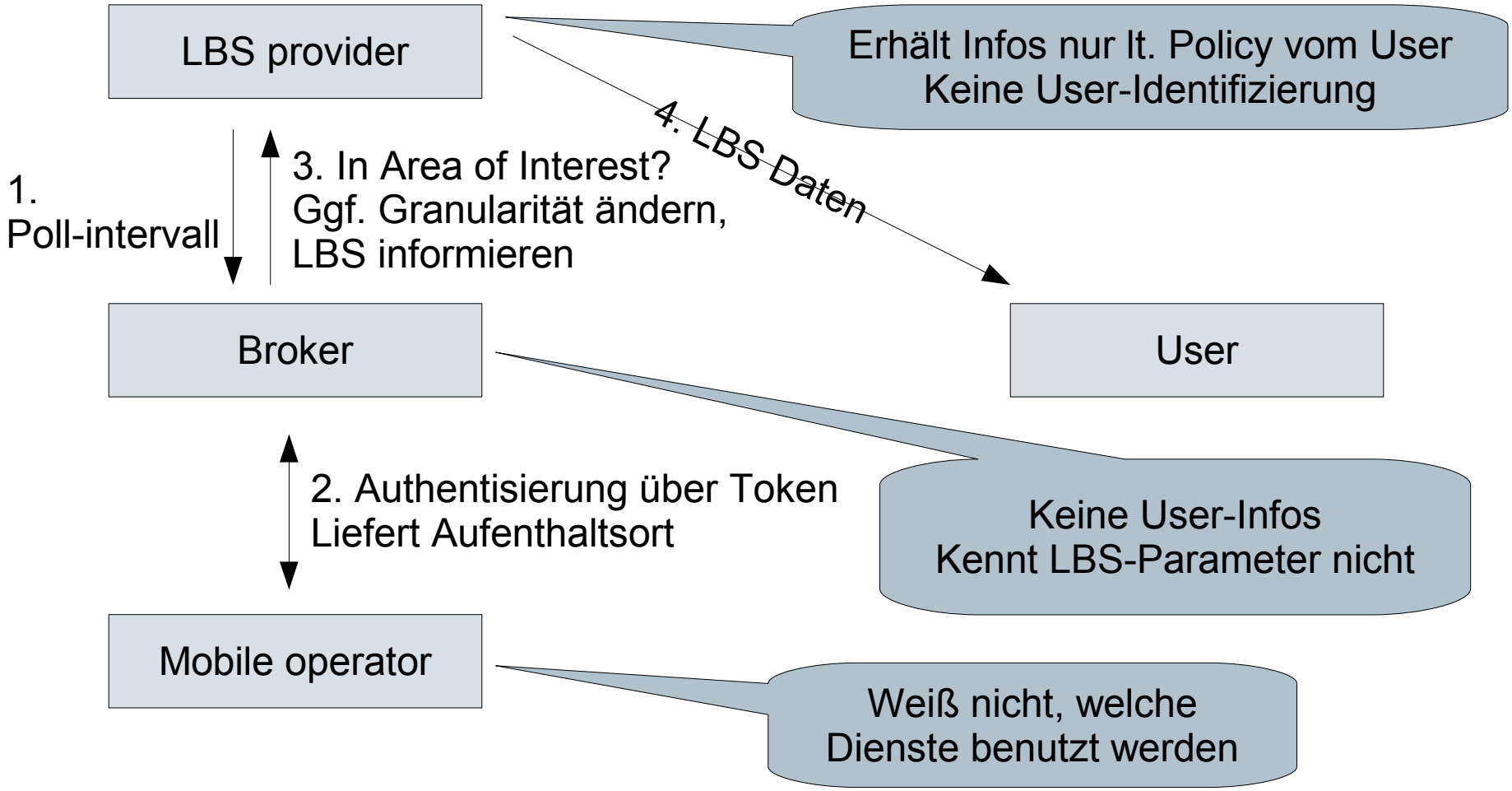
Mix-Netze

Broker (vertraute Zwischeninstanz)

Location Privacy – LBS mit Broker



Location Privacy – LBS mit Broker



Datenminimalisierung

„Blend with the crowd“: Je weniger herausstechende Merkmale, desto geringer die Trackingchance

Verfälschung der Daten

- „GPS-Problem“ :-) Jitter kann man u.U. herausmitteln

Vergröberung der Daten

Reduzieren der Anfragefrequenz

Anonymisierung ohne Infrastruktur

„Mit Infrastruktur“ ≈ Anonymisierung auf Routingschicht
Was passiert im „lokalen Fall“, ohne dazwischenliegende Schritte?

Mögliche Szenarien:

- Zufälliger Beobachter: Ohne spezielle technische Vorkehrungen (z.B. Access Point)
- Tracker: Technische Möglichkeit, einzelne Quelle zu verfolgen (z.B. Richtantennen, Kreuzpeilung)
- „Vogelperspektive“: Lokalisierung aller Sender

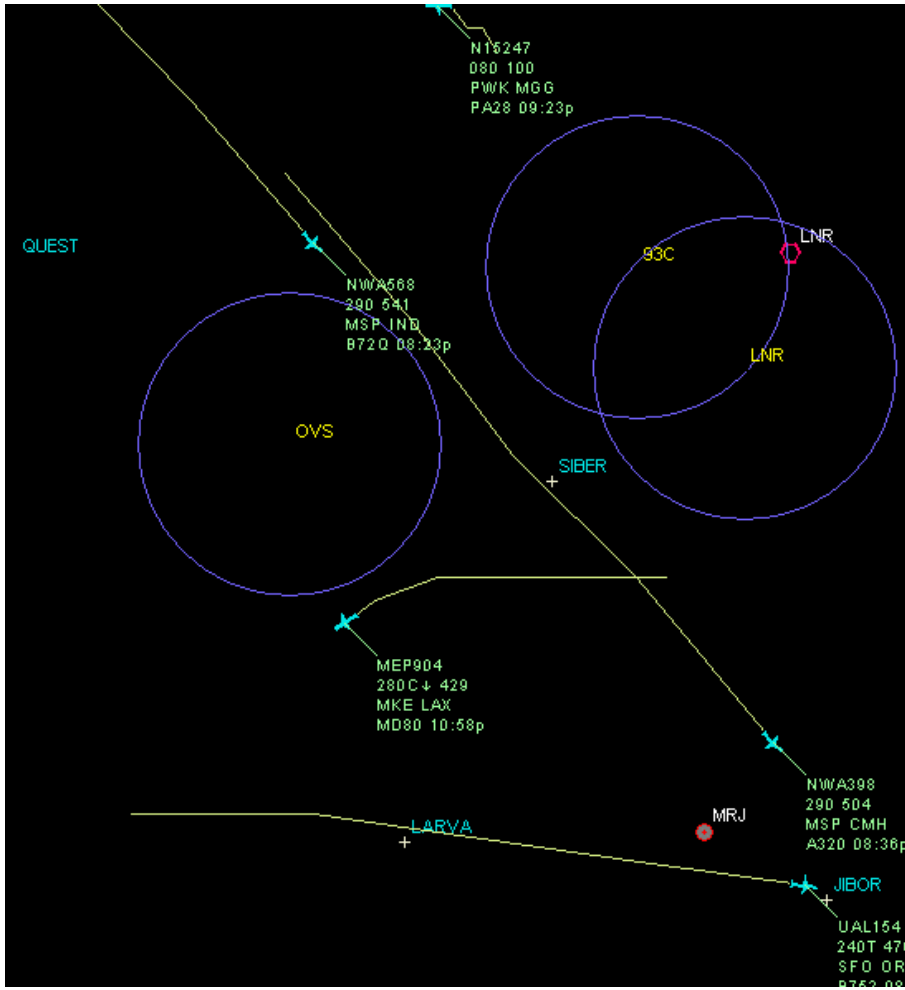
Side channels, z.B.

- Randbedingungen (z.B. Autos auf Straße, ...)
- Bevorzugte Aufenthaltsorte (Büro, ...)

Verfeinerungen für Tracking-Angriffe

Ausnutzen zusätzlicher Infos

- Bewegungsverhalten von Fußgängern
  - Keine aprupten Richtungsänderungen
  - Kalman-Filter...
  - ...oder Reid's MHT
- Typischer Verkehr
  - Spitzkehre im Gang
  - Mittags: Die meisten auf dem Weg zur Mensa
  - Beresford: Mix Zone



Anonymisierung ohne Infrastruktur

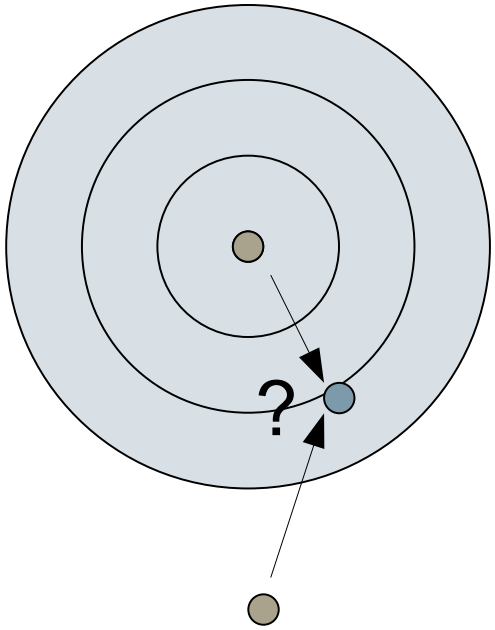
Aufteilen der Kommunikation in „Sessions“
- Möglichst kurz halten

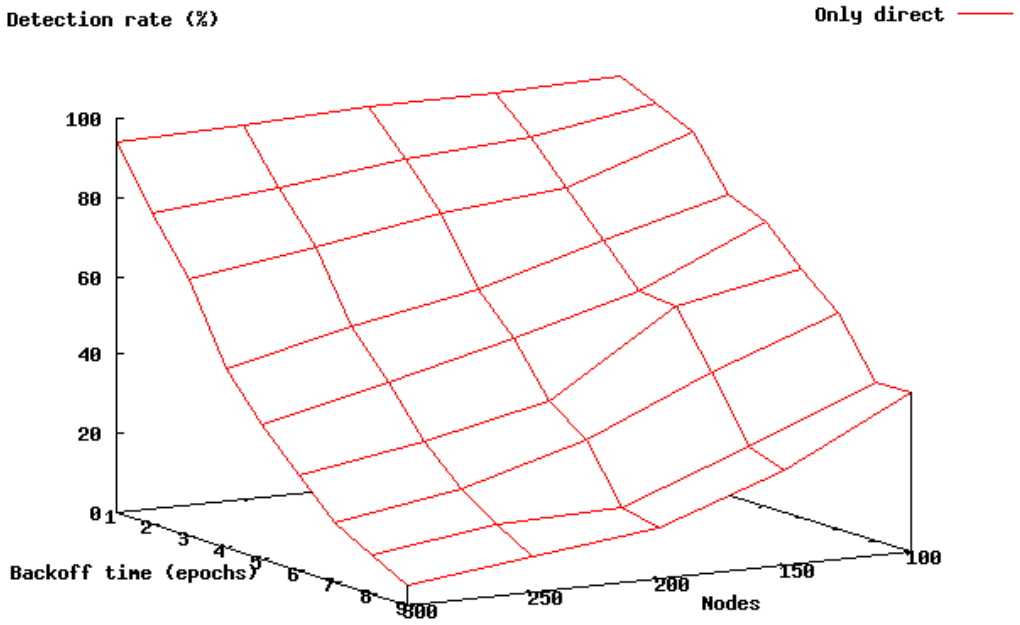
Nach Session: Kommunikationspause

Effizienz abhängig von
- Knotendichte
- Länge der Pause
- Knotengeschwindigkeit
- Randinfos des Angreifers

Viele Zusatzinfos für spezielle Angriffe müssen aufwendig erhoben werden!

Anonymisierung ohne Infrastruktur





Anonymität und Schlüsselaustausch

Schwierig! Fallabhängig!

Diffie-Hellman
- u.U. zu rechenintensiv
- Man in the Middle

PKI mit Zertifikaten
- Gibt eindeutige Identität preis

Ephemereal pairing
- Lösung für kurze, spontane Verbindungen
- Benötigt entweder einen sicheren oder einen authentischen Kanal geringer Bandbreite

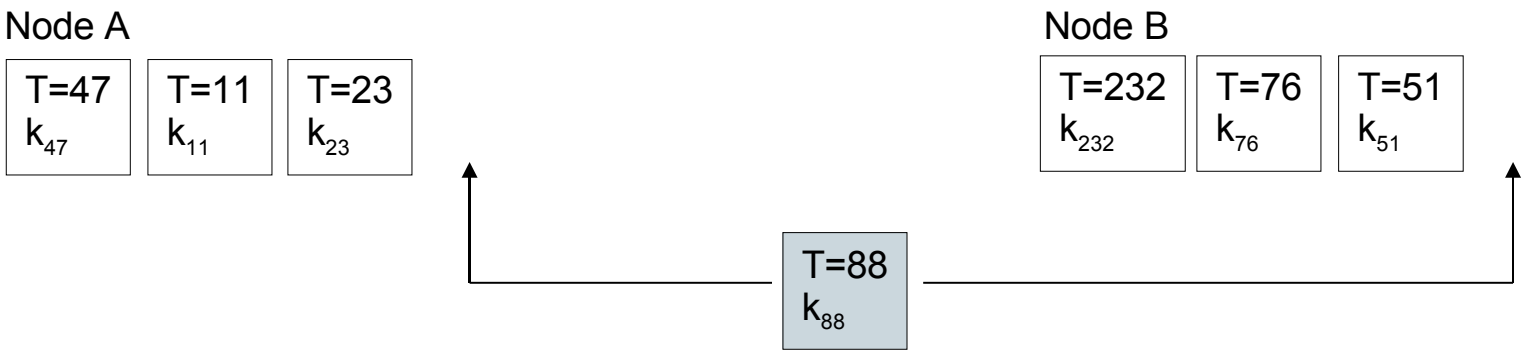
Wiedererkennung von Knoten

Problem: Wie erkenne ich „befreundete“ Knoten?

- Diensteanbieter: An Anonymität kein Interesse
- ...aber: PDAs und andere Kleingeräte!
- Keiner der Partner will seine Anonymität zunächst aufgeben

Voraussetzung: Initiales Treffen mit sicherem Kanal

- Session key für die Zukunft: $k_{A,B}$
- Gemeinsames Token: $T_{A,B}$
  - Zufallszahl, welche das Pairing identifiziert



Wiedererkennung von Knoten

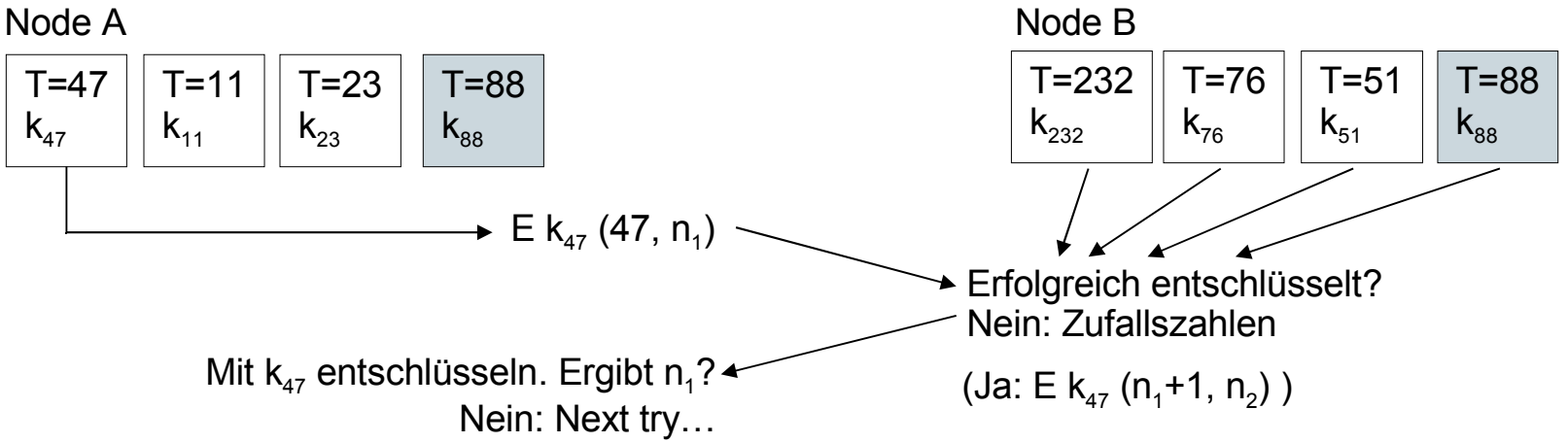
On re-encounter:

A wählt nonce n_1 (Zufallszahl)

Probiert beim Gegenüber alle gespeicherten Sitzungen

B versucht, Paket mit allen gespeicherten Sitzungen zu entschlüsseln

Funktioniert, aber hoher Aufwand. Verbesserungen vorhanden :-)



Fazit

- Privacy und Kontrolle über die eigenen Daten machbar
- Privacy ist mehr als „nur Pseudonyme“
  - Untere Schichten im Netzwerk-Stack: Pseudonymwechsel
  - Anwendungsschicht: Individuelle Behandlung
    - Datensparsamkeit
    - Sessionlänge
- Softwaredesign-Prozeß:
  - Früher: Erst Securitykonzept, dann Anwendung
  - Zukünftig(?): Erst Privacyanforderungen, dann Security, dann Anwendungsdesign