Ubiquitous [juːˈbɪk.wɪ.təs]

Computing [kəmˈpjuːtɪŋ]

– Chancen und Risiken für Linux/OSS –

Dipl.-Ing. Klaus Knopper <knopper@knopper.net>

Klassisches Desktop-Computing (1)

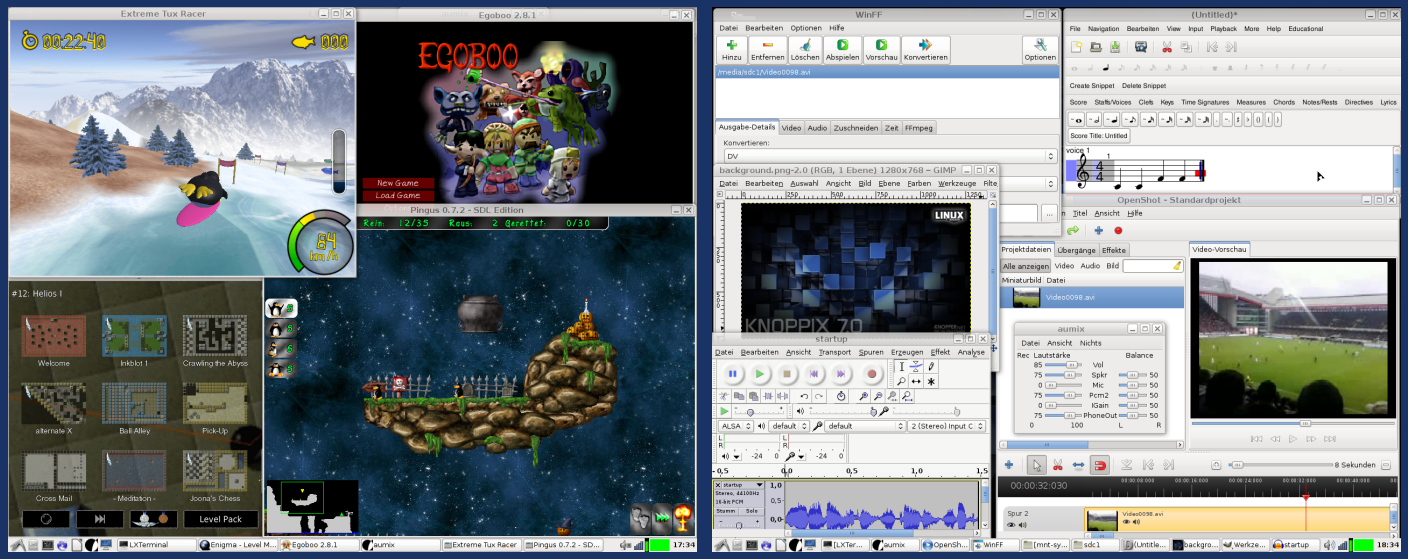
Ist Linux auf dem Desktop tot?*)

*) Wird immer wieder von einigen Interessensgruppen als widerlegbare These in den Raum gestellt.

Klassisches Desktop-Computing (2)

Ist Linux auf dem Desktop tot?

Wohl kaum, denn es gibt für kaum ein anderes Betriebssystem eine größere Menge an frei verfügbarer Desktop-Software, aber ...



Klassisches Desktop-Computing (3)

Ist Linux auf dem Desktop tot?

Wohl kaum, denn es gibt für kaum ein anderes Betriebssystem eine größere Menge an frei verfügbarer Desktop-Software, aber:

Vielleicht ist heimlich der Desktop-PC gestorben???

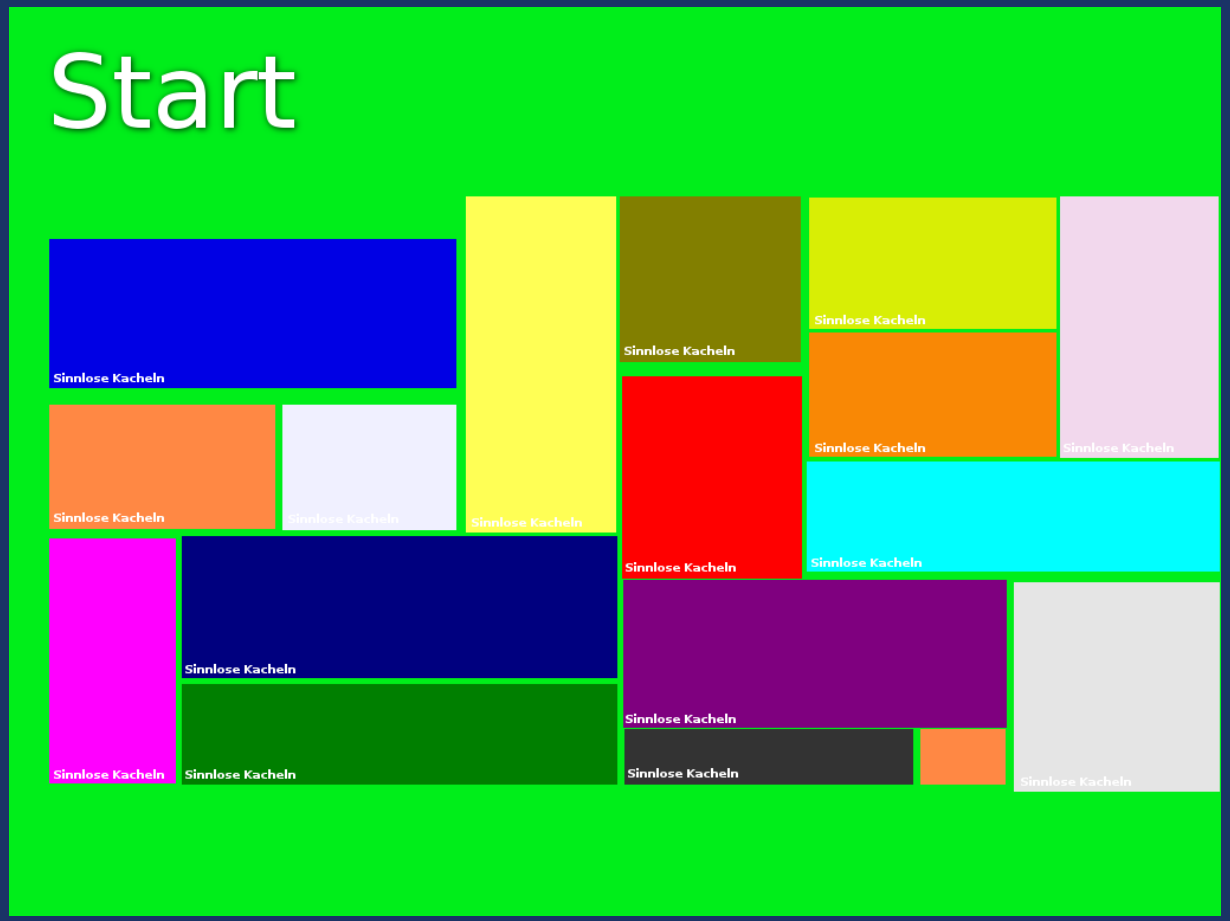
<UMFRAGE>

- In welchem Haushalt steht ein Computer, den die ganze Familie benutzt?
- Wer benutzt (ggf. neben dem „Hauptrechner“) noch ein Note-, Netbook, Tablet oder Smartphone?
- Wer hat täglich oder fast täglich mit mehreren Computern zu tun, oder mit mehreren Geräten, die als Computer gelten könnten?

</UMFRAGE>

Klassisches Desktop-Computing (4)

Ein weiteres Indiz für das Ende des Desktop? („DAS ist die Zukunft...“)



Etwas ist anders...

Die Art und Weise, Computertechnik einzusetzen und damit umzugehen, hat sich seit 2000 offenbar gewandelt.

Einen möglichen Erklärungsansatz liefert
Ubiquitous Computing.

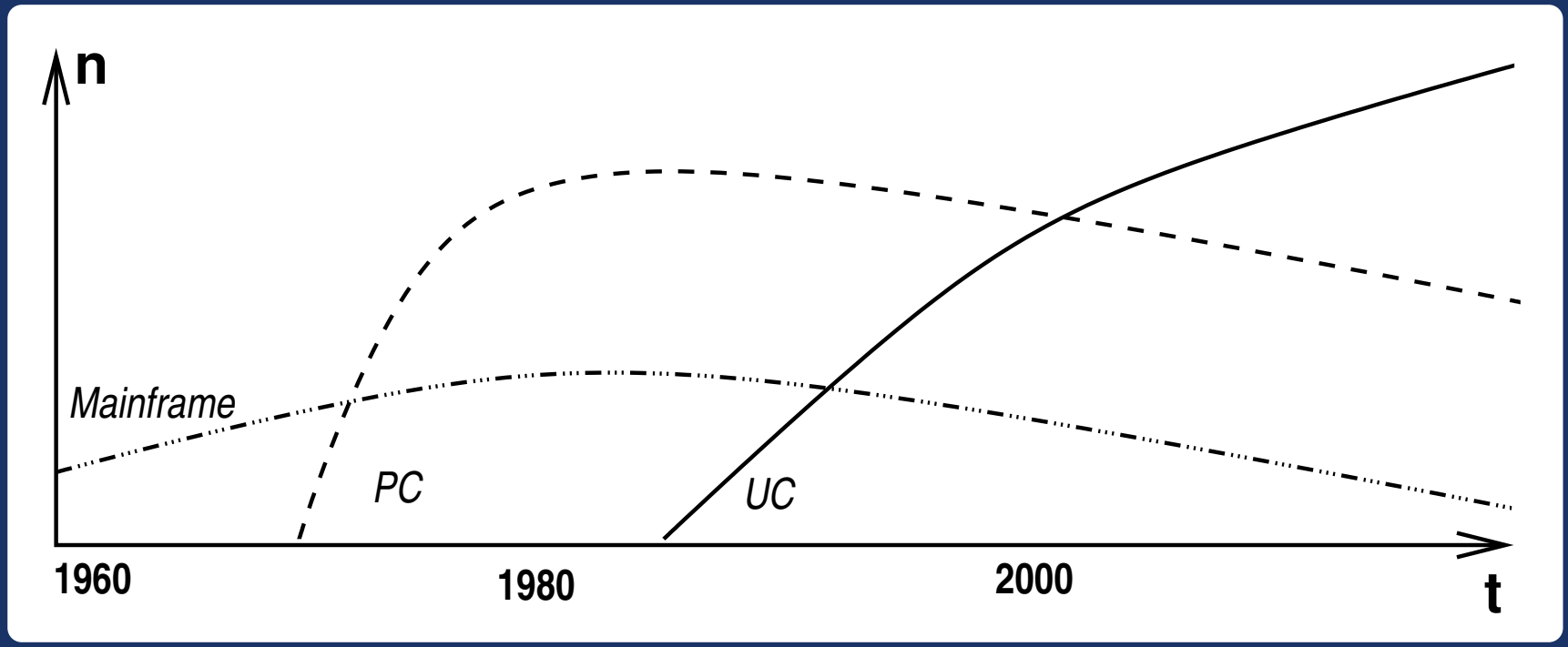
Ubiquitous*) Computing

*) "seeming to be in all places" (Cambridge Dictionary Online)

- Begriff UC wurde erstmals 1988/91 von Mark Weiser [3] verwendet, die Idee der „unsichtbaren Computer" reicht jedoch weiter zurück [2].
- Datenerfassung und Automatisierung von Abläufen mit (ggf. unsichtbar) in die Umgebung integrierter Sensorik, drahtloser Informationsübertragung und Auswertung in vernetzten Computersystemen, die nicht direkt von Menschen „bedient" werden müssen.
- Soll sowohl in Industrie und Handel, als auch in allen Lebensbereichen als Unterstützung dienen und Menschen von komplizierten Aufgaben entlasten. #)

Quantitative Sichtweise

1960-1980	Mainframe - Ein Computer, viele Computernutzer
1980-2000	Personal Computer - Ein Computer pro Nutzer
2000-	Ubiquitous Computing - Viele, auf bestimmte Aufgaben spezialisierte Computer pro Person



Verwandtschaft

Neben „Ubiquitous Computing“ werden in der Fachliteratur weitere Begriffe, teils alternativ und mit großen inhaltlichen Überschneidungen verwendet, jedoch mit unterschiedlichem Schwerpunkt.

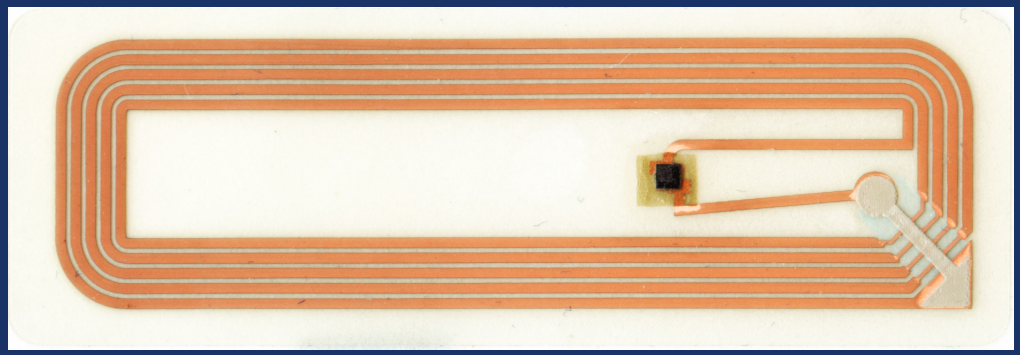
Internet der Dinge	Computergestützte Identifikation und Verwaltung von realen Objekten (z.B. RFID [10])
Pervasive Computing	„allesdurchdringende Vernetzung des Alltags“, kommerzielle Anwendung der automatisierten Datenerfassung und -auswertung (E-Commerce unterstützt durch u.a. RFID, Data Mining)
Ambient Intelligence*)	„Intelligente“ Technik soll v.a. den Menschen unterstützen, um dessen Leistungsfähigkeit und Lebensqualität zu erhöhen.
Organic Computing	„selbstorganisierende“ verteilte Rechnerstrukturen
Wearable Computing	Elektronische „Gadgets“ in Kleidung oder am Körper (Identifikation & Authentifizierung, Hilfsmittel, Entertainment)

Verwandtschaft

Zwei weitere Begriffe werden oft im Zusammenhang mit UC verwendet: ***„Smart Dust“*** (miniaturisierte Computer mit Sensoren, die zur Erkundung und Überwachung eingesetzt werden) und ***„Nomadic Computing“***, was eher die „Notebook- und Smartphone-Generation“ kennzeichnet, die immer und überall persönlich Internet-Dienste nutzt.

Next Generation Media ist ein Technologieprogramm des Bundesministerium für Wirtschaft und Technologie mit Fokus auf Konsumelektronik, Logistiknetze, Produktionsanlagen und Gesundheitsversorgung. [5]

Radio Frequency Identification



Seit 2000 werden passive 13,56 MHz RFID-Transponder in Form flexibler Etiketten zur Mediensicherung in Bibliotheken verwendet.

Je nach Einsatzzweck werden passive oder aktive Transponder, mit oder ohne Verschlüsselung, mit oder ohne (Wieder-)Beschreibbarkeit verwendet.

Der breiteste Einsatz findet sich derzeit in der Logistik. RFID-Chips sind außerdem in allen seit dem 1. November 2005 ausgestellten deutschen Reisepässen sowie ab dem 1. November 2010 in allen Personalausweisen enthalten. (Demo)

Einsatzgebiet Personenidentifikation

Reisepass oder ID-Karte mit RFID: für das Auslesen wird eine Applikation mit Basic Access Control (BAC) verwendet, die als Teil der Authentifizierung die optisch eingescannte maschinenlesbare Zone (MRZ) verwendet. Über eine Anwendung auf dem RFID-Chip ist es auch möglich, sich mittels Challenge-Response bei verschiedenen Diensten online anzumelden, ein geeignetes Lesegerät vorausgesetzt.

Chip-Implantate bei Menschen sind derzeit eine eher seltene Variante der Personenidentifizierung, bei Haus- und Nutztieren wird dieses Verfahren jedoch bereits angewendet.

In der Biometrie werden eindeutige Merkmale wie Fingerabdrücke, Konturen des Ohrs oder Retina-Signaturen verwendet. Über Ähnlichkeitskriterien wird der Bezug zur Identität hergestellt.

Einsatzgebiet Handel und Verleih

Aufklebbare Etiketten mit RFID-Chip werden häufig zur Warensicherung eingesetzt, können aber auch zur Inventarisierung oder automatischen Buchung verwendet werden. [10]

Einsatzgebiet Transport und Logistik

Die automatische oder halbautomatische Erfassung und Buchung von Waren mittels RFID oder optisch erfasstem Barcode (auch Matrix-Barcode, z.B. QR-Code) können die Effizienz in Warenwirtschaftssystemen und im Supply Chain Management steigern.

Die an allen Autobahnen in Deutschland vorhandenen Kontrollbrücken für die Mautgebühr von LKWs erfassen Fahrzeugnummern und Fahrzeugprofile (3D-Kontur) *aller* durchfahrenden Fahrzeuge. Bei LKWs mit On-Board-Unit werden zusätzlich Kenndaten per Infrarotsignal übermittelt.

UC im Unternehmen

- Zugangskontrolle, Facilitymanagement
  - ☞ Identifikation
- Supply-Chain-Management (Lagerverwaltung, Kühlkette, Qualitätsmanagement, Teileverfolgung, Wiederbeschaffung)
  - ☞ Ortsverfolgung
- Customer-Relationship-Management (Bestellungsverfolgung, Bezahlung, Kundenidentifikation, Kundenbetreuung, Vertriebskontrolle, Wartung)
  - ☞ Notifikation

s.a. Schoch/Strassner [4].

Einsatzgebiet Hausautomatisierung

Durch die Vernetzung von Geräten und Steueranlagen können die Bewohner unterstützt werden (Licht ein-/ausschalten, Fensterrollos helligkeitsbedingt öffen und schließen, Vorräte überwachen).

Beispiel: In einigen Hotels werden entnommene Waren aus der Minibar automatisch erkannt und nachbestellt.

Auch die Überwachung und Steuerung bei Abwesenheit ist möglich (vergessene Herdplatte ausschalten, Strom-/Wasserverbrauch überwachen, Videorecorder oder Staubsaugerroboter per Internet oder zeitgesteuert aktivieren).

Einsatzgebiet Gesundheitswesen und Pflege

Über drahtlos vernetzte, am Körper getragene Sensortechnik können pflegebedürftige oder hilflose Personen von einem Dienstleister betreut werden, und erhalten so mehr Selbstständigkeit und Sicherheit in ihrem eigenen Zuhause.

Durch „intelligente“ Sensortechnik kann ein Sturz oder außergewöhnliche Verhaltensweisen automatisch erkannt und an eine Zentrale gemeldet werden, so dass kein manueller Notruf ausgelöst werden muss.

Blinde Menschen können sich durch Geräte mit Sprachausgabe und Braille-Displays orientieren. Für motorisch eingeschränkte Personen ist Sprach- und Gestenerkennung eine Möglichkeit der direkten Mensch-Maschine-Kommunikation.

Risiken

„Informationstechnologie versagt in dem Moment, in dem man beginnt, sich darauf zu verlassen.“ [7]

UC ist heute in vielen Bereichen eine unverzichtbare Komponente. Studien zur Technikfolgen-Abschätzung [1] versuchen, die Risiken in aktuellen (an der jeweils aktuellen Technologie orientierten) Einsatzszenarien aufzuzeigen und abzuwägen.

„Der gläserne Bürger“

Obwohl in der für RFID & Co. verwendeten Near Field Communication nur wenige Zentimeter Abstand zwischen den Kommunikationspartnern liegen, ist es mit geeigneter Sende- und Empfangstechnik möglich, diesen „Minimalabstand“ auch auf mehrere Meter zu erweitern, so dass einige Datentypen „im Vorübergehen“ ausgelesen werden können.

Bei unsicher konfigurierten Handys oder anderen persönlichen Elektronischen Geräten ist es möglich, per WLAN oder Bluetooth sämtliche Daten auszulesen oder zu verändern. Unabhängig davon ist immer eine Ortung über die Funkzelle oder eine IP-Adresse möglich.

Über die Verknüfung gesammelter Daten ist die Erstellung eines Persönlichkeitsprofils möglich, das nicht nur zu Marketingzwecken, sondern schlimmstenfalls auch zum Identitätsdiebstahl verwendet werden kann. Die betroffene Person hat keine Kontrolle über die über sie gesammelten Daten.

☞ **Verlust der informationellen Selbstbestimmung**

Verlässlichkeit erkannter Daten

- Biometrische Merkmale wie Fingerabdrücke sind einfach zu fälschen [9], die Fehlerkennungsrate steigt z.B. bei alterungsbedingten Veränderungen.
- Unverschlüsselte RFID-Kommunikation lässt sich durch Replay-Attacken fälschen.
- Fehlerkorrekturmechanismen wie Checksummen sind nicht eindeutig. Zu einem geringen Prozentsatz kann es zu „zufälligen“ Treffern bzw. falsch erkannten Identifikationen kommen.
- Bei Hardwarefehlern in Sensor oder Transponder werden keine brauchbaren Daten geliefert und es muss auf Alternativinformation zugegriffen werden.
- Das Vertrauen die Verlässlichkeit elektronischer Information ist oft subjektiv zu hoch, wenn mögliche Fehlerquellen nicht berücksichtigt werden.

„99% Langeweile und 1% panische Angst“

(Feedback von Piloten und Operateuren, die mit neuen Bedien- und Automatisierungskonzepten konfrontiert wurden.). [8]

☞ Einschränkung von Arbeitsfeldern auf lediglich das, was nicht (oder noch nicht) automatisierbar ist.

☞ Kontrollverlust durch nicht beeinflussbare Automatismen. „Nicht wissen, was im Ausnahmefall zu tun ist.“

Folgen der Vernetzung disjunkter Information

Durch die Vernetzung von unabhängiger Information aus unterschiedlichen Quellen entsteht Potenzial für Fehlinterpretation aufgrund einer angenommenen, aber nicht tatsächlich vorhandenen Kausalität.
Beispiel:

- Der PKW einer Person wird von einer Verkehrskamera nahe Basel registriert. Der Führerschein des PKW-Besitzers wird zur gleichen Zeit in einer Verkehrskontrolle in Zweibrücken gescannt. Zur gleichen Zeit wird mit der Kreditkarte des PKW-Besitzers eine Restaurantrechnung in Berlin bezahlt.
  - Wurde das Auto gestohlen, der Führerschein, die Kreditkarte?

Da der Computer bei einer automatischen Auswertung einem Ereignis keine *Relevanz in der realen Welt* zuordnen kann, können auch Fehlentscheidungen unterschiedlichen Ausmaßes getroffen werden.

Datenschutz und Datensicherheit

Die beim UC anfallenden Daten sind oft personenbezogener Natur, und bedürfen besonderem Schutz vor unberechtigtem Zugriff, der bei der Übertragung und Speicherung nicht immer gewährleistet ist. Das Einholen einer Einverständniserklärung der betroffenen Personen ist problematisch, da für diese meist wegen der „Unsichtbarkeit“ der Sensoren gar nicht ersichtlich ist, dass und welche Daten erfasst werden.

Die gesammelten Daten, z.B. durch die zur Maut-Kontrolle aufgestellten Kontrollbrücken, können prinzipiell verwendet werden, um Bewegungsprofile von Fahrzeugen und Personen zu erstellen. Derzeit dürfen die Daten nur stichprobenweise für die Kontrolle der bezahlten LKW-Maut verwendet werden, und die Kontrollbrücken sind nur zu bestimmten Tageszeiten in Betrieb.

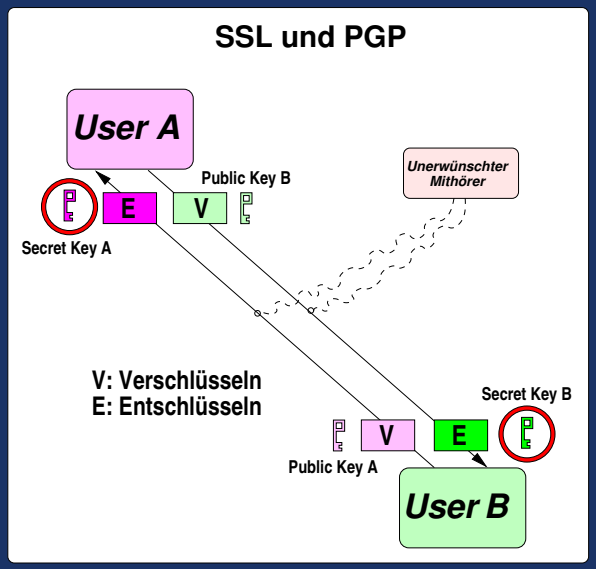
UC und die Cloud (Technik)

- Oft ist der Wirkungsbereich im UC lokal begrenzt, und eine dauerhafte Speicherung der Daten findet nicht statt.
- Wenn die beim Ubuquitous Computing anfallenden Daten jedoch zentral ausgewertet und gespeichert werden sollen, liegt es nahe, die notwendige Rechenleistung und Datenspeicher aus einer ebenfalls vernetzten Struktur zu beziehen (v.a. private clouds [6]).
- Um den sicheren Transfer und die Weiterverarbeitbarkeit der Information zu gewährleisten, werden standardisierte Protokolle verwendet (XML, http(s), ISO/IEC 15961/15962, SSL).

UC und die Cloud (Sicherheit)

Die Technologie der sicheren Datenübertragung und Datenhaltung mit kryptographischen Verfahren ist heute in der Theorie ausgereift und mathematisch verifizierbar.

Bei Public Key Verfahren, die heute auch für Online-Banking u.ä. eingesetzt werden, wird ein Schlüsselpaar verwendet, mit dem nur der jeweils komplementäre Schlüssel in der Lage ist, die Information zuvor mit dem Primärschlüssel gesicherten Daten wieder zugänglich zu machen. Da die Schlüssel selbst bei der Kommunikation nicht übertragen werden, ist das „Knacken“ der verschlüsselten Übertragung mit üblichen Computersystemen nicht möglich.



Trotzdem ist es Angreifern in manchen Fällen möglich, unautorisierten Zugriff auf Daten zu erhalten, und diese auch zu manipulieren (Industriespionage, Zerstörung von IT-Infrastruktur, Identitätsdiebstahl). Frage: Wie?

(☞ Lösung: siehe Skript)

Die Rolle von Linux und Open Source im UC (1)

GNU/Linux als Systemsoftware

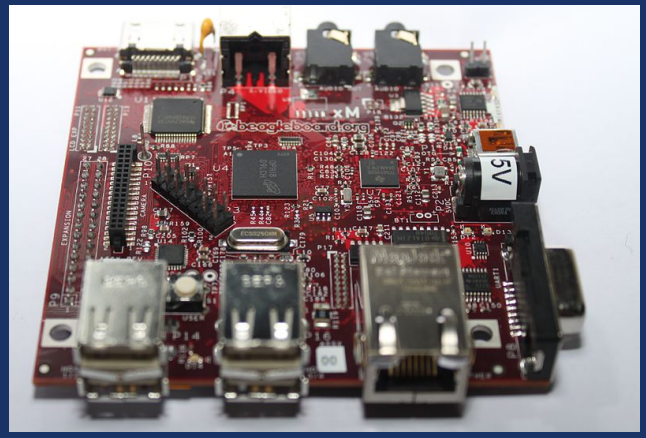
Nur wenige Hersteller spezialisierter Geräte sprechen gerne über „interne Angelegenheiten“ wie die auf ihren Geräten laufende Firmware, technische Analysten können aber oft aufgrund verfügbarer Information und Spezifikationen Rückschlüsse ziehen (z.B. bei Haushaltsrobotern).

Eine Ausnahme von diesem „Informationsdefizit“ stellen Smartphones dar, bei denen die Systemsoftware und die damit verbundene Verfügbarkeit von Anwendungen ein publiziertes Verkaufsmerkmal ist, hier erfährt das Linux-basierte *Android* derzeit messbar die höchste Verbreitung (Marktanteil 53% im 3. Quartal 2011 lt. Garnter-Analyse vom November 2011).

Die Rolle von Linux und Open Source im UC (2)

Linux Embedded

In einem Großteil der komplexeren im Ubiquitous Computing auftauchenden „intelligenten Geräte“ kommen Mini-Computerboards zum Einsatz, auf denen z.B. ein Linux-Kernel mit einem sehr spartanischen System (oft *busybox*) und auf die Hardware angepassten Modulen die Steuerungsaufgaben übernimmt.
☞ Embedded GNU/Linux



Ein Mini-Linux wird z.B. in vielen Multimedia-Geräten (Fernseher, Receiver, digitale Videorecorder) und Netzwerkkomponenten als „Firmware“ eingesetzt.

Die Rolle von Linux und Open Source im UC (3)

„Geschäftsgeheimnis“ vs. Open Source? (1)

Der Einsatz von Open Source Software als Basis für ihre Anwendungen erspart den Herstellern einerseits Aufwand für die Neuentwicklung der Plattform und stellt eine solide und flexibel anpassbare Entwicklungsbasis dar, andererseits bleiben lizenzrechtliche Fragen genausowenig aus wie bei proprietärer Software:

- Bedeutet das Mitliefern der Software auf dem Gerät eine „Verbreitung der Software“ im Sinne der GNU GENERAL PUBLIC LICENSE, oder handelt es sich um eine hardwaregebundene „Firmware“, die gar nicht von einem Anwender direkt „genutzt“ wird? Muss man dementsprechend jedem Käufer Zugang zum Quelltext gewähren, und der Konkurrenz damit auch selbst entwickelte Algorithmen offenlegen? ☞ Für einige Geräte, bei denen der Anwender sehr wohl direkt mit der Software arbeiten kann (z.B. Accesspoints) gibt es bereits einschlägige Streitfälle und gerichtliche Auseinandersetzungen, die die Offenlegung der auf GPL-Code basierenden Quelltexte fordern und auch Bearbeitungen durch Dritte erlauben. [11]

Die Rolle von Linux und Open Source im UC (3)

„Geschäftsgeheimnis“ vs. Open Source? (2)

- Saubere Trennung von proprietären und freien Programmteilen der Systemsoftware? ☞ Lösbar durch Anbieten des Source Code nur für die Freien Bestandteile, allerdings dürfen die proprietären Teile nicht so untrennbar mit dem System verbunden sein, dass ohne sie gar nichts mehr funktioniert.
- Lassen sich gemischt proprietäre/Open Source Systeme in kritischen Bereichen einsetzen, bei denen es um hohe Betriebssicherheit, z.B. in medizinischen Bereich geht, wenn eine vollständige Analyse auf Quelltextbasis durch die proprietären Teile nicht möglich ist?
- Wie können zertifizierte Systeme aktualisiert werden (z.B. dringende Fehlerbehebungen, neuer Kernel), ohne dass jedesmal neu zertifiziert werden muss?

§§§

Zusammenfassung

- UC: Datenerfassung und Automatisierung von Abläufen mit (ggf. unsichtbar) in die Umgebung integrierter Sensorik, drahtloser Informationsübertragung und Auswertung in vernetzten Computersystemen,
- verdrängt zunehmend den klassischen „Desktop“-Universalcomputer,
- kann in fast allen Lebensbereichen Assistenz bieten und Abläufe vereinfachen und beschleunigen.
- Datenschutz und Datensicherheit sind technisch realisierbar, jedoch wg. Interessenskonflikten oft eingeschränkt oder fehlerhaft implementiert.
- Relationsbildung gesammelter und vernetzter Daten erlaubt die Erstellung von Persönlichkeitsprofilen und Protokollierung der Aufenthaltsorte von Personen.
- Automatische Aus- und Bewertung von Daten kann zu Fehlinterpretationen und Fehlentscheidungen führen, die schwer korrigierbar sind (Kontrollverlust).
- GNU/Linux und Open Source bieten über offene Schnittstellen und öffentliche Verfügbarkeit des Quelltextes Nachhaltigkeit und Transparenz und fördern unter günstigen Voraussetzungen Vertrauen in die Zuverlässigkeit und Erweiterbarkeit der vernetzten Systeme.

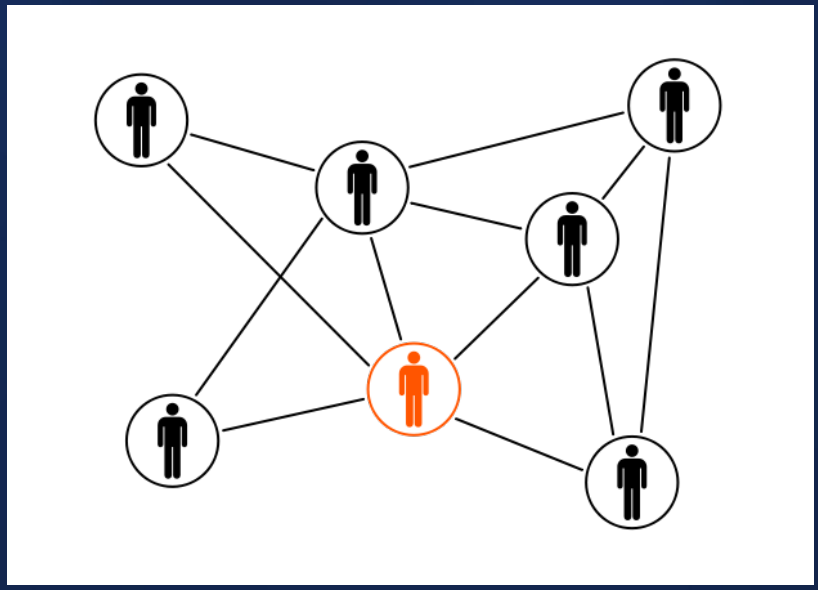
Fragen & Diskussion

Ubiquitous [juː'bɪk.wɪ.təs]

Computing [kəm'pjuːtɪŋ]

– Chancen und Risiken für Linux/OSS für Linux/OSS –

Klaus Knopper <uc@knopper.net>



[12] *Cliparts* aus dem Public Domain Repertoire von www.openclipart.or