Allgegenwärtige Rechner: eine neue Dimension der IT-Sicherheitsproblematik

Dipl.-Inform. Andreas Heinemann, Prof. Dr. Max Mühlhäuser,
BSc. Wesley W. Terpstra, Dipl.-Ing. Erwin Aitenbichler

Hintergrund

Das einundzwanzigste Jahrhundert markiert den Übergang vom PC-Zeitalter, wo jeder IT-Nutzer i.w. mit einem Computer – seinem *persönlichen* Computer (PC) – interagierte, ins Post-PC-Zeitalter der allgegenwärtigen oder ubiquitären Computer (engl.: *ubiquitous computing*). IT-Nutzer sind künftig von vielen – in wenigen Jahren oft Hunderten – Computern umgeben. Das sind dann allerdings spezialisierte Rechner, die teilweise in Alltagsgegenstände eingebettet sind, teilweise in der Umgebung (Büro- und Arbeitsräume, öffentliche Plätze etc.) installiert sind und teilweise *mobil* mitgeführt werden (heutige Vorboten: PDAs und Mobiltelefone). Im Unterschied zu heutigen – z.B. in Waschmaschinen und Videorekordern – eingebetteten Systemen sind die allgegenwärtigen Rechner vernetzt – ein Mehrwert, der oft mit dem Unterschied zwischen der Leistungsfähigkeit einer einzelnen Nervenzelle und derjenigen des Gehirns verglichen wird. Ein zweiter großer Mehrwert soll durch *Kontextwissen* erreicht werden: spezielle Sensoren verleihen den allgegenwärtigen Rechnern Kenntnisse über ihre Lokation (und damit den Aufenthaltsort des Nutzers bzw. Gegenstandes) und andere Umgebungsdaten wie Temperatur und Lage, aber auch über Reisepläne oder Aufgaben des Nutzers u.v.a.

Offensichtlich kann das beschriebene neue IT-Zeitalter viele wünschenswerte Verbesserungen unseres Alltags und Berufslebens mit sich bringen. Es kann aber auch zum Alptraum werden, falls nicht in mehreren Problembereichen weitreichende Fortschritte erzielt werden. So muss die Interaktion mit den allgegenwärtigen Computern und dabei auch ihre *Bedienung radikal vereinfacht werden:* Diese muss großteils unmerklich oder „nebenbei" erfolgen; die Organisation verteilter DV-Systeme (heute hauptsächlich nach dem Client-Server-Prinzip) muss noch stärker dezentralisiert und für um Größenordnungen mehr Rechnernetzknoten *skalierbar* gemacht werden; spontane Vernetzung *zufällig zusammentreffender Rechner* (vgl. [8]) über variable Netztechnologien ohne menschlichen Eingriff muss beherrscht werden;

Security in Ubiquitous Computing

Ubiquitous devices continue to evolve; the future will soon see many small and wirelessly connected devices. Due to their near invisibility and pervasiveness, many existing security issues will gain heightened relevance alongside some entirely new problems. The SICARI project was launched in October 2003 to research these issues. Therein, the Telecooperation Group and ITO have identified physical security, trust establishment, spontaneous authentication, and privacy of context as important open research topics. Our approach is the introduction of a small device, called a minimal entity (ME). The ME operates as the owner's digital delegate and assumes responsibility for his security needs.

Softwaretechnik muss so weiterentwickelt werden, dass mit vertretbarem Aufwand Anwendungen gebaut werden können, die das Potenzial der Kontextanpassung und der Anpassung an ihre Nutzer und deren aktuelle Bedürfnisse auch tatsächlich nutzen; und *last but not least* muss eine ganz neue Qualität von IT-Sicherheit erreicht werden. Auf diesen letztgenannten Aspekt konzentrieren wir uns nachfolgend unter dem Stichwort *Sicherheit im ubiquitous computing.*

Als wichtigste *enabling technology* für allgegenwärtiges Rechnen muss die Mobilkommunikation in die nachfolgenden Betrachtungen einbezogen werden. Sie ermöglicht insbesondere *mobile computing* im Sinne der drahtlosen Versorgung von mobilen Nutzern mit Informationen und Diensten über autonome Endgeräte. Kommunikationstechnologien für Kurzstrecken (Bluetooth, Irda etc.) werden künftig parallel zu Netzzugangs-Technologien (vgl. wireless LAN) und öffentlichem Mobilfunk (GSM, GPRS, UMTS) verwendet. Details, Auswahl und laufender Wechsel der Technologien und Anbieter sowie Optimierungen (Wahl der günstigsten Technologie, verzögerte Synchronisation u.a.) sollten die Nutzer im Alltag nicht „belästigen"; stattdessen muss komfortable Systemsoftware diese Entscheidungen im Nutzersinne treffen und schlicht *ständigen drahtlosen Internetzugang* als einheitliche Schnittstelle anbieten.

Forschungsumfeld

Während viele populärwissenschaftliche Beiträge angesichts der Vielfalt und Allgegenwart künftiger Rechner unüberlegt das Ende jedweglichen persönlichen Computers vorhersagen, weisen bei genauer Betrachtung viele Argumente darauf hin, dass einem besonders ausgezeichneten persönlichen Endgerät künftig mehr statt weniger Bedeutung zukommt! Dazu sind nachfolgende Vorüberlegungen notwendig.

In einer Welt allgegenwärtiger Rechner wird schrittweise, aber unaufhaltsam auch der potentiell rechtsverbindliche Charakter fast aller Verrichtungen unseres Berufslebens und Alltags rechnergestützt behandelt. Dazu kann man sehr stark vereinfacht drei Stufen betrachten:

1. Rechtsverbindlichen Charakter hat zunächst das, *wofür wir unmittelbar bezahlen sollen,* also Einkäufe, Kaufvertragsabschlüsse, Inanspruchnahme von Diensten im Internet und in der realen Welt etc.

2. Insbesondere im beruflichen Umfeld ermöglicht die fälschungssichere automatisierte Erfassung von Verrichtungen eine neue Qualität von Abrechnungen und von deren Vertrauenswürdigkeit, man denke nur z.B. an die Stundensätze von Wartungstechnikern oder gar Beratern als Grundlage von Umsätzen in Milliardenhöhe in der westlichen Industriegesellschaft. Gleichzeitig ergeben sich aus detaillierten zuverlässigen Arbeitsprotokollen neue Ansätze zur Optimierung von Prozessabläufen, worin wiederum ein enormes Einsparungspotenzial liegt – und damit ein enormes Potenzial für Wirtschaftswachstum. Längst haben beispielsweise die Krankenkassen unter ihrem enormen Kostensenkungsdruck erkannt, dass im Gesundheitswesen eine zigfach detailliertere Abrechnung des Behandlungsablaufs jedes Patienten deutliches Kostensenkungspotenzial birgt – und sie haben ebenfalls erkannt, dass manuelle Erfassung dieses Ablaufs, wie er heute üblich ist, das Einsparpotenzial zunichte machen würde. Der Einsatz von *ubiquitous computing* im Gesundheitswesen gerade zu Zwecken der detaillierten Abrechnung wird daher schon heute in umfangreichen Projekten gefördert.

3. Langfristig wird alles, was der Rechtsprechung unterliegt, potenziell auf die Kommunikation und Arbeitsweise der allgegenwärtigen Rechner übergreifen. Ob wir uns in einem Gebäude(teil) zu einem bestimmten Zeitpunkt aufhalten, ob wir ein Fahrzeug oder öffentliches Transportmittel benutzen, was wir auch tun: Wenn es zum Rechtsstreit kommt, wenn Kosten-, Schuld- oder Regressfragen zu klären sind, wird man sich mit Computerhilfe absichern oder verteidigen wollen oder andererseits Verursacher auffinden wollen.

Selbstverständlich beschreibt das Vorstehende im schlimmsten Fall den „gläsernen Menschen" und stellt folglich ein äußerst sensibles und schwieriges Thema dar. Unter den *schutzwürdigen* Daten im Sinne der IT-Sicherheit versteht man also im Zeitalter und Umfeld des *ubiquitous computing* insbesondere Daten über Verrichtungen mit potentiell rechtsverbindlichem Charakter. Darüber hinaus sind natürlich alle Arten schutzwürdiger Daten zu beachten, vom digitalen Urlaubsfoto über persönliche Kommunikation bis zu hoch sicherheitskritischen Unternehmensdaten. Dabei wird physischer Schutz (vgl. „meine Festplatte") weit schwieriger, weil sich einerseits physische Spei-

cherorte immer mehr im *Cyberspace* auflösen (das INTERNET wird als Speicherort gerade deshalb immer interessanter, weil *logische* Speicherorte darin mobilen Nutzern „hinterher reisen können", wobei Anteil und Bewegungsfrequenz der beweglichen Daten von Systemsoftware im Netz optimiert werden kann), andererseits miniaturisierte Speicherorte (bspw. USB-Memory-Sticks) leichter denn je verloren oder gestohlen werden können.

Das ungeheure Potenzial ubiquitären Rechnens bedeutet also aus der Sicht der Nutzer, dass Vertrauen und Selbstbestimmung mehr denn je elementare Forderungen sind, wenn Daten mit potenziell rechtsverbindlichem Charakter erzeugt, gespeichert und ausgetauscht werden. Nach umfangreichen Untersuchungen sind die Autoren des vorliegenden Beitrags zur Überzeugung gelangt, dass der Ausgangspunkt für brauchbare Lösungen nur in einem vertrauenswürdigen Endgerät liegen kann, welches als *Stellvertreter des Nutzers* und in Abstimmung mit diesem über Erzeugung, Speicherung, Transport und Verwertung von schutzwürdigen Daten bestimmt. Dies impliziert auch, dass dieses Gerät die *digitale Identität* des Nutzers verwaltet.

Wie erläutert nimmt die Zahl der Situationen und Verrichtungen, die durch ein solches Endgerät in Alltag und Berufsleben unterstützt werden (müssen), in den nächsten Jahren immer weiter zu. Das Endgerät sollte also das Potenzial eines *ständigen Begleiters* seiner Nutzer und Besitzer haben, vergleichbar dem Personalausweis oder der Kreditkarte (genauer: beidem zusammen).

Man muss sich nur den Mangel an IT-Sicherheit bewusst machen, auf den man sich an der Tankstelle einlässt, wenn man Magnetstreifen *und* PIN seiner EC-Karte einem wenig vertrauenswürdigen Gerät überlässt, dann wird unmittelbar einsichtig, dass die Bündelung von digitaler Identität und Computer- und Kommunikationsfunktionalität in einem persönlichen Gerät vorteilhaft ist. So genannte SmartCards sind für die weiter oben aufgezeigten Szenarien nicht hinreichend, weil sie nur vorbestimmte *minimale* Sicherheitsfunktionen auf der Karte selbst realisieren.

Die Forschung der Autoren widmet sich daher einem so genannten *minimalen Endgerät* (ME), das ein Nutzer ständig mit sich führt und das digitale Identität und Grundlagen für ubiquitäre Sicherheit sowie Funktionen eines allgemein verwendbaren allgegenwärtigen Rechners in sich vereint.

Den GSM-Mobiltelefonen wurde in der Vergangenheit ein großes Potenzial als allgemein verwendbares, sicheres Endgerät zugeschrieben, sie können insofern als erste Vorboten eines MEs angesehen werden. Ihre Nutzung z.B. als digitale Identität für Telebanking, unter Nutzung der GSM-SIMcard zur zuverlässigen Authentifizierung und Verschlüsselung, blieb aber unter anderem aus zwei Gründen sehr beschränkt: erstens hatten die meisten Mobilfunk-Netzbetreiber große Sorge, mit der Öffnung ihrer Sicherheitsinfrastruktur für beliebige Software die Verbreitung von Handy-Viren heraufzubeschwören mit der Gefahr, das Vertrauen der Nutzer zu verlieren und dem missbräuchlichen Telefonieren in großem Stil die Tür zu öffnen; zweitens waren die Tarife für derlei Anwendungen noch prohibitiv. Weitere Gründe, vor allem marktwirtschaftlicher und politischer Art, kamen hinzu. Im Gegensatz zu dieser Entwicklung arbeiten die Autoren an einem ME, welches seine Bewährungsprobe in nicht-öffentlichen Einsatzgebieten des beruflichen Umfeldes bestehen und dort großes wirtschaftliches Potenzial nachweisen kann.

Talking Assistant

Ein ME beinhaltet insbesondere folgende funktionalen Komponenten:

- digitale Identität und Grundfunktionen ubiquitärer Sicherheit
- Sprache als Ein- und Ausgabemedium als Grundlage für fast beliebige Miniaturisierung (die Verwendung von Displays und manueller Eingabe, z.B. Stift, beschränkt bei heutigen Endgeräten das Miniaturisierungspotenzial; diese Ein-Ausgabekanäle können bei MEs über assoziierte Endgeräte realisiert werden, welche nicht ständig mitgeführt werden müssen)
- eingebaute feingranulare Ortsbestimmung (als wichtigste Art von sensorgestütztem *Kontextwissen*)
- spontane Vernetzung sowohl zwischen Endgeräten als auch mit Festnetzzugängen.

Mit Hilfe einer offenen Plattform können MEs sowohl soft- als auch hardwareseitig erweitert werden. Die ersten Prototypen von MEs wurden unter dem Namen Talking Assistant [1] entwickelt. Dabei handelt es sich um sprachgestützte Headsets, die über Prozessor und Speicher, drahtlose Netzwerkanbindung sowie eine Kombination von Sensoren bzw. Aktuatoren zur Handhabung von Kontextinformation verfügen. Letztere umfasst u.a. Identität und Standort des mobilen Benutzers sowie die ungefähre Blickrichtung (Abbildung 1 zeigt eine Aufnahme eines Talking Assistant).

Ubiquitäre Sicherheit mit Minimalen Endgeräten

Wie in den vorausgegangenen Abschnitten erläutert, erhalten im Zusammenhang mit allgegenwärtigem Rechnen viele Fragen der IT-Sicherheit eine neue Qualität und Dimension, wobei alle klassischen Aspekte wie Authentifizierung, Autorisierung und Abrechnung [9] betroffen sind.

Die Fragestellungen, mit denen sich die Autoren in diesem Zusammenhang beschäftigen, betreffen derzeit insbesondere folgende Gebiete ubiquitärer Sicherheit:

1. Physikalische Sicherheit

MEs vertreten ihre Benutzer (=Besitzer) im Sinne einer digitalen Identität, mit der diese Benutzer sich in der digitalen Welt ausweisen, Dienste in Anspruch nehmen, Vertrauen aufbauen (siehe nächster Punkt) etc. Dies bedeutet aber für Verlust oder Diebstahl: 1. MEs sollten nur in Gegenwart des *wahren* Benutzers als digitale ID fungieren; 2. MEs sollten für andere als den Besitzer in keinem Fall kopierbar sein; 3. MEs sollten aber andererseits für den Besitzer selbst nach Verlust sehr leicht reproduzierbar sein.

Heutige Ansätze beinhalten den Einsatz von SmartCARD-Technologie. Diese konnte jedoch das Ziel einer manipulations- und fälschungssicheren Hardware noch nicht befriedigend verwirklichen (vgl. [2,13]). Darüber hinaus ist das o.g. Duplikat-Dilemma (unmöglich für Dritte, sehr einfach für *legitime* Besitzer) noch nicht hinreichend gelöst.

2. Etablierung von Vertrauen

Vertrauen basiert bei heutiger öffentlicher Mobilkommunikation auf der engen Bindung von Nutzer und Betreiber. Beispielsweise sind die wenigen Betreiber im System „fest verdrahtet" (exklusiv zugeteilte Frequenzbereiche etc.) und die Betreiber identifizieren ihre Nutzer ebenfalls über „fest verdrahtete" Kennzeichen (SIM-card, IMAI). Diese Infrastruktur unterscheidet sich substantiell von einer offenen Welt des drahtlosen Internet und der ad hoc Vernetzung [7,15], in der Dienste und Netzzugänge von beliebigen Anbietern geleistet werden können (vgl. kabellose Internet-Zugangspunkte in *Starbucks Coffee Houses*). Gewünscht ist eine Technologie, die wie die Kreditkarten im realen *business-to-consumer*-Geschäft Millionen von Anbietern und Milliarden von Nutzern zu koppeln gestattet; die bekannten substantiellen Verluste aller Kreditkartenfirmen durch betrügerischen Karten(-nummern-)einsatz wären allerdings für ubiquitäre Sicherheit untragbar, da solche Betrügereien durch die im *Cyberspace* gegebene Automatisierbarkeit und Rechengeschwindigkeit ruinös würden. Außerdem ist für bestimmte Abläufe die Verwendung von Pseudonymen ausreichend und nutzerseitig (teilweise sogar anbieterseitig) dringend erwünscht, für andere strikt verboten. Eine universelle Lösung muss anders als die Kreditkarte beide Fälle abdecken.

3. Spontane Authentifizierung und spontane Vernetzung

Eine weitere Eigenschaft des MEs ist seine Fähigkeit zur spontanen Vernetzung mit potenziell unbekannten Endgeräten. Eine solche Vernetzung muss sicher realisiert werden, komfortabel sein und vor Missbrauch geschützt werden. Die Existenz bzw. Verfügbarkeit einer zentralen Zertifizierungsinstanz kann nicht vorausgesetzt werden. Fragen der spontanen Authentifizierung werden in etlichen Forschungsprojekten weltweit angegangen (bspw. [3,6,10]). Ein verbreiteter Ansatz besteht darin, physische Nähe für die *Assoziation* zwischen Geräten vorauszusetzen und das Einverständnis von Benutzern zu verlangen, wie dies in *Bluetooth* [4] unterstützt wird (physische Nähe ist dort durch die Reichweite gegeben, pairing kann z.B. über PINs erfolgen, die auf beiden Geräten

identisch gewählt werden müssen). Im drahtlosen Internet ist *Nähe* nicht mehr einfach durch *Erreichbarkeit* zu ersetzen und Benutzerinteraktion im Umfang des Bluetooth-Pairing-Vorgangs als Voraussetzung für Assoziation nicht mehr tolerabel – Benutzerzustimmung andererseits unverzichtbar.

Als Beispiel für die „Leichtigkeit", mit der Assoziation zu erfolgen hat, soll folgendes Szenario dienen: ein ME-Träger bittet einen anderen ME-Träger, dessen Digitalkamera für einen Moment borgen zu dürfen. Im Augenblick des *In-die-Hand-Nehmens* sollten die gespeicherten Bilder des ursprünglichen Besitzers der Digitalkamera unzugänglich werden, neu aufgenommene Bilder sollten im virtuellen Speicher des aktuellen Benutzers gespeichert werden und bei Rückgabe für den ursprünglichen Besitzer der Digitalkamera unzugreifbar werden. Charakteristisch für dieses Szenario ist einerseits, dass die Assoziation von Geräten (ME-Kamera) über den Vorgang *In-die-Hand-Nehmen* ausgelöst und genehmigt wird – offensichtlich verlangen andere Geräte andere Arten von Auslösern und Genehmigungen. Charakteristisch ist weiterhin, dass die Assoziation nur Teile der Daten und Funktionen umfasst (z.B. nicht: fremde Bilder, Kamera initialisieren), andererseits für diese Teile *sicher* sein soll in dem Sinn, dass erwartete und durchgeführte Funktionen fälschungssicher übereinstimmen; diese Fähigkeiten sollten allgemein Bestandteil einer Assoziation sein können.

Ein weiterer Assoziationsaspekt ist Gedächtnis: Geräte, die sich einmal „kennen", sollen diese Beziehung ggf. erhalten können und *spontan*, d.h. ohne Genehmigung oder gar mit weniger restriktiven Auslösern, Nutzerinteraktion wieder etablieren können. Vergleichbar mit zwei Menschen, die sich einmal vorgestellt wurden und kennen gelernt haben, werden diese sich anhand Aussehen, Sprache, Stimme und Erinnerung bei einem neuen Treffen wieder erkennen und sich „vernetzen".

Alle genannten Aspekte der *spontanen Authentifizierung* werden für MEs erforscht.

4. Schutz der Privatsphäre, Schutz von Verrichtungs- und Kontextinformation

Wie in den vorausgegangenen Unterkapiteln erläutert, erhält ubiquitäres Rechnen einen wesentlichen Mehrwert durch Kontextinformation wie insbesondere Ortskontext; auch die Bedeutung der Aufzeichnung und Auswertung von Tätigkeiten mit potentiell rechtsverbindlichem Charakter wurde diskutiert. In diesem Zusammenhang muss dem Schutz der Privatsphäre ein hoher Stellenwert eingeräumt werden [11,12].

Um die Schimäre des „gläsernen" Menschen zu bekämpfen, wird allgemein von den gängigen Schutzmechanismen wie Rechtevergabe und Verschlüsselung abgeraten, da das „Knacken" oder versehentliche Öffnen dieser Mechanismen zu weitreichende Folgen haben kann, als dass darüber das notwendige Vertrauen in Systeme und Anwendungen zu erreichen wäre. Stattdessen wird an Verfahren gearbeitet, bei denen grundsätzlich nur so viel Information *erreichbar* gespeichert wird, dass deren Auswertung ohne Hinzunahme weiterer Daten systeminhärent unmöglich ist: die erreichbaren Daten erscheinen jedem Auswerteversuch gegenüber als *statistisches Rauschen*. Die erforderlichen Zusatzdaten (z.B. Anfangswerte von Zufallszahlengeneratoren) können dann mit unvergleichbar höherem Aufwand geschützt werden, z.B. physisch im – vertrauenswürdigen – ME, so dass in jedem Fall die Anwesenheit und Zustimmung des Nutzers erforderlich ist, wenn Kontext- oder Verrichtungsinformation ausgewertet werden soll.

Es zeigt sich also, dass die Visionen des *ubiquitous* und *mobile computing* neue Herausforderungen und Fragen an die Sicherheit stellen. Einige der genannten Fragestellungen bilden einen von einer Reihe von Schwerpunkten im Projekt *SICARI – Eine Sicherheitsarchitektur und deren Werkzeuge für die ubiquitäre Internetnutzung* [14]. SICARI ist ein Verbundprojekt von 11 wissenschaftlichen und 6 industriellen Partnern. Das übergeordnete Forschungsziel des Projekts besteht in der Entwicklung einer Sicherheitsarchitektur mit den entsprechenden Werkzeugen, um Informationstechnik im allgegenwärtigen Umgang sicher nutzen zu können. Zur Realisierung der Infrastruktur wird ein modularer Baukasten mit zugehörigen Handlungsanweisungen entwickelt. SICARI wird im Rahmen des Programms *futur: Der deutsche Foschungsdialog* [5] vom Bundesministerium für Bildung und Forschung gefördert.

Zusammenfassung:

Die Umsetzung der Vision des *ubiquitous computing* wird die Art und Weise, wie wir im alltäglichen Leben mit Computern umgehen und wie wir sie wahrnehmen, entscheidend verändern. Der Erfolg hängt hierbei in grossen Teilen davon ab, die neuen Sicherheitsanforderungen zu erkennen, zu verstehen und passende Antworten darauf zu geben. Dieser Beitrag hat an einigen Beispielen aufgezeigt, welche

Das Fachgebiet Telekooperation und das ITO an der TU Darmstadt

Das Fachgebiet Telekooperation erforscht, wie Menschen mit und mittels Netzen (bspw. dem INTERNET) zusammenarbeiten können. Global oder lokal, drahtlos oder via Breitbandkabel, explosionsartig wachsend, ist das Netz Infrastruktur für die Konvergenz von Informationstechnik, Telekommunikation und *Medien*, allgegenwärtig (engl.: ubiquitous) und hoffentlich unauffälliger Bestandteil unserer Umwelt (engl.: invisible, ambient). Leitlinie der Forschung sind innovative Anwendungen, für deren effiziente Herstellung Werkzeuge, Plattformen und Methoden, programmiersprachliche und Hypertext-Konzepte, sogar Hardware-Prototypen entwickelt werden. Der Forschungsbereich *uBiz* betrachtet *ubiquitous computing* für eCommerce, für das INTERNET als viertes Massenmedium und für vernetzte multimediale Softwaresysteme, insbesondere bei heterogenen Netzen und Betriebsmodellen (UMTS, wireless LAN-Hotspots etc.). Weitere Arbeiten betreffen innovative Endgeräte, mobile commerce, bioanaloge Handhabung von Multimediadaten, Durchstöbern und Editieren riesiger Digitalvideo-Datenbestände, innovatives Musizieren im INTERNET und mehr. Der zweite Forschungsbereich *ubiquitous learning* unterstützt mobile Nutzer, die Vollzeit oder lebenslang lernen bzw. mit Wissenserwerb verknüpfte Aufgaben lösen. Klassenzimmer und Hörsäle werden aber nicht nur *virtualisiert*, sondern wirken – aufgerüstet mit *learning appliances* und Softwarewerkzeugen – als Katalysator und bilden als Ort der Begegnung die Wurzel innovativen Lernens.

Das Information Technology Transfer Office (ITO) ist ein am Fachbereich Informatik der TU Darmstadt angesiedeltes Zentrum für angewandte Forschung auf den Gebieten IT Sicherheit, Middleware und *ubiquitous computing*. Seit seiner Gründung wird das ITO zu 100% aus Drittmitteln finanziert. Diese setzen sich aus Kooperationen mit führenden IT und Software-Unternehmen sowie aus öffentlichen Fördermitteln zusammen. Die Stärke des ITO ist der breite Forschungshorizont, in den die Themen und Forschungsgruppen der assoziierten TU Professoren einfließen.

Zu den Autoren: Prof. Dr. Max Mühlhäuser ist Leiter des Fachgebietes Telekooperation und Mitglied im Leitungsgremium des ITO, Andreas Heinemann, Erwin Aitenbichler sind Mitarbeiter des Fachgebietes Telekooperation und Wesley W. Terpstra ist Mitarbeiter des ITO.

Ansprechpartner:
Prof. Dr. M. Mühlhäuser
TU Darmstadt, FB20 Telekooperation
Alexanderstraße 6
D-64283 Darmstadt
max@informatik.tu-darmstadt.de

neuen Anforderungen zu erwarten sind und kurz das Projekt SICARI vorgestellt, das sich mit diesen Fragen befasst.

Literatur:

[1] Aitenbichler, E., Mühlhäuser M.: Audiobasierte Endgeräte für Ubiquitous Computing und geeignete Infrastrukturen. In: Praxis der Wirtschaftsinformatik: Ubiquitous Computing. dpunkt Heidelberg, 2003.

[2] Anderson, R., Kuhn M.: Tamper Resistance - a Cautionary Note. Second USENIX Workshop on Electronic Commerce, USENIX Press, 1996.

[3] Balfanz, D., Smetters, D., Stewart, P., Wong, H.: Talking to Strangers: Authentication in Ad-Hoc Wireless Networks. Symposium on Network and Distributed Systems Security (NDSS '02), Internet Society Publications, 2002

[4] Bluetooth Webseite: http://www.bluetooth.org (11/2003)

[5] BMBF futur Förderprogramm. Webseite: http://www.futur.de/de/index.htm (11/2003)

[6] Corner, M., Nobel, B.: Zero-Interaction Authentication. Annual International Conference on Mobile Computing and Networking, ACM Press, 2002.

[7] Eschenauer, L., Gligor, V. D., Baras, J.: On Trust Establishment in Mobile Ad-Hoc Networks. Security Protocols Workshop, Springer, 2003.

[8] Heinemann, A., Kangasharju, J., Lyardet, F., Mühlhäuser, M.: Ad Hoc Collaboration and Information Services Using Information Clouds. 3rd Workshop on Applications and Services in Wireless Networks, Institute of Computer Science and Applied Mathematics, 2003.

[9] IETF Working Group Authentication, Authorization and Accounting. Webseite: http://www.ietf.org/html.charters/aaa-charter.html (11/2003)

[10] Schechter, S., Hartemink, A., Parnell, T.: Anonymous Authentication of Membership in Dynamic Groups. Financial Cryptography, International Conference, Springer, 1999.

[11] Langheinrich, M.: Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, International Conference on Ubiquitous Computing, Springer, 2001.

[12] Langheinrich, M.: Privacy Awareness System for Ubiquitous Computing Environments. International Conference on Ubiquitous Computing, Springer, 2002.

[13] Schneier, B., Shostack, A.: Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards. USENIX Workshop on Smartcard Technology, USENIX Press, 1999.

[14] SicAri Webseite (ITO): http://www.ito.tu-darmstadt.de/projects/sicari/ (11/2003)

[15] Shankar, N., Arbaugh, W.: On Trust for Ubiquitous Computing. International Conference on Ubiquitous Computing, Springer Verlag, 2002.