Sicherheit bei spontan vernetzten mobilen Geräten

Dirk Timmermann, Clemens Cap, Marc Haase, Igor Sedov

Universität Rostock
Fakultät für Ingenieurwissenschaften
Albert-Einstein-Straße 2
18059 Rostock
{dirk.timmermann, marc.haase@etechnik.uni-rostock.de}
{clemens.cap, igor.sedov@informatik.uni-rostock.de}

Abstract: Ziel des Forschungsprojektes „Sicherheitsarchitektur und Referenzszenario für spontan vernetzte mobile Geräte“ der Universität Rostock ist die Untersuchung der besonderen Sicherheitsfragen im Bereich mobiler Geräte, die sich selbständig durch spontane Vernetzung mit anderen Geräten in Verbindung setzen. Es soll eine Hard- und Software-Sicherheitsarchitektur für diese Geräte entwickelt werden, die die geringe Prozessorleistung, die begrenzen Energieressourcen und die durch die spontane Vernetzung erst entstehenden Sicherheitsfragen berücksichtigt. Angesichts der leichten Abhörbarkeit der Radiowellen im drahtlosen Umfeld müssen zusätzliche kryptographische Protokolle für die Authentifizierung, Verschlüsselung und Zugriffssteuerung eingesetzt werden. Dies wird ebenfalls durch die geringere Prozessorleistung und niedrige Stromaufnahme auf mobilen Geräten erschwert.

1 Einleitung

Mobile Klein- und Kleinstgräte gehören inzwischen zu Gegenständen des täglichen Gebrauchs. Bislang war deren Funktionalität mangels Kommunikationsschnittstellen auf gerätespezifische Aufgaben reduziert. Jedoch durch die Integration von drahtlosen Kommunikationstechnologien in mobile Geräte besitzen diese nun die Möglichkeit zur spontanen Vernetzung und Dienstnutzung mit mobilen Geräten in der nahen Umgebung. Die daraus resultierenden neuartigen Kommunikations- und Anwendungsbereiche bringen wiederum neue Sicherheitsprobleme mit sich.

Im Rahmen des DFG Schwerpunktprogramms „Sicherheit in der Informations- und Kommunikationstechnik“ beschäftigt sich das Projekt „Sicherheitsarchitektur und Referenzszenario für spontan vernetzte mobile Geräte“ der Universität Rostock speziell mit den Sicherheitsfragen, die bei der *spontanen* Vernetzung von mobilen Geräten entstehen. Spontan bedeutet in diesem Zusammenhang, dass erst zum Zeitpunkt des Kommunikationsaufbaus Sicherheitsparameter zwischen den beteiligten Geräten ausgehandelt werden müssen. Eine vorherige Abstimmung oder Prä-Registrierung dieser Parameter, wie sie bei Public-Key-Infrastrukturen durchgeführt wird, ist aufgrund der Heterogenität von mobilen Geräten bezüglich der drahtlosen Kommunikationsschnittstellen, der Prozessorleistung, der Energieressourcen und der Benutzer unmöglich.

2 Forschungsziele des Projektes

Ziel des Projektes ist die Untersuchung der besonderen Sicherheitsfragen, die bei der spontanen Vernetzung zwischen mobilen Geräten auftreten. Aufgrund der vielfältigen Kommunikationsbeziehungen wird bei der Untersuchung zwischen Kommunikationsbeziehungen im privaten, lokalen und globalen Bereich unterschieden. Die jeweiligen Bereiche sind durch stark unterschiedliche Vertrauensbeziehungen zwischen Kommunikationspartnern charakterisiert. Diese beeinflussen die Auswahl einer für die jeweilige Situation angepassten Sicherheitsstrategie. Während im privaten Bereich von vertrauenswürdigen Geräten, die unter der Kontrolle des Benutzers stehen, ausgegangen werden kann, muss im lokalen Umfeld die Vertrauenswürdigkeit von Kommunikationspartnern bei Bedarf hergestellt und überprüft werden. Diese Überprüfung lässt sich mit Hilfe von Diensten z.B. aus dem globalen Bereich durchführen. Des Weiteren ist es bei der Kommunikation im lokalen Umfeld wünschenswert, identifizierende Daten zurückzuhalten um damit der Erstellung von Bewegungsprofilen entgegenzuwirken. Abbildung 1 stellt die genannten Beziehungen eines mobilen Gerätes zu den genannten Bereichen dar und zeigt ebenfalls die Kommunikationsbeziehungen zwischen den Bereichen.

Für den Aufbau von spontanen Kommunikationsbeziehungen sind neben einer dafür geeigneten Kommunikationstechnologie zusätzlich Software basierte Dienste für die Suche von Kommunikationspartnern, die Konfiguration von Sicherheits- und Verbindungsparametern und die Nutzung von angebotenen Dienstleistungen erforderlich. Die Entwicklung dieser Dienste erfolgt ebenfalls in diesem Projekt. Ein weiteres Forschungsziel ist die Untersuchung von Hard- und Software basierten kryptografischen Algorithmen und Protokollen bezüglich des Einsatzes in ressourcenarmen Systemen, wie sie mobile Geräte darstellen.

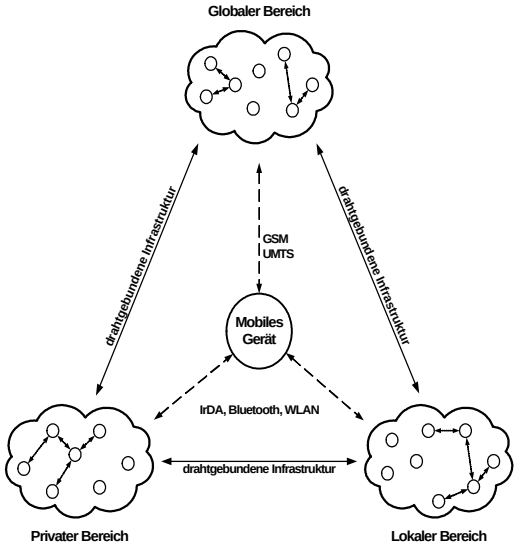

Abbildung 1

Im Rahmen des Projektes erfolgt eine grundlegende, theoretische und praktische Untersuchung von Sicherheitsfragen bei spontaner Vernetzung in Abhängigkeit von der durchzuführenden Transaktion, der aktuellen Umgebung, den Ressourcen der Kommunikationspartner und der drahtlosen Kommunikationstechnologie. Das angestrebte Ziel ist die Entwicklung von Sicherheitsmodellen für mobile Geräte unter Berücksichtigung der erweiterten Kommunikationsmöglichkeiten mobiler Geräte und der daraus resultierenden heterogenen Kommunikationsbeziehungen. Die entwickelten Sicherheitsmodelle werden anhand einer seit Projektbeginn aufgebauten und ständig weiterentwickelten Simulations- und Evaluationsumgebung für drahtlose Netzwerke überprüft.

3 Aktivitäten des Projektes

Dieser Abschnitt gibt einen kurzen Überblick über die im Projekt bereits abgeschlossenen und noch laufenden Forschungsaktivitäten.

Ausgangspunkt bildete die Untersuchung der drahtlosen Kommunikationstechnologien IrDA, Bluetooth, IEEE 802.11b und GSM hinsichtlich ihrer Sicherheitseigenschaften und -mechanismen. Parallel dazu wurden Hardware-Plattformen von mobilen Geräten bezüglich der genannten Kriterien bewertet. Diese Arbeiten wurden mit der Entwicklung von Referenz- und Bedrohungsszenarien für spontan vernetze mobile Geräte [Se00] abgeschlossen. Aus den Bedrohungsszenarien wurde anschließend ein generisches Sicherheitsmodell „*Advanced Security Manager*“ [Bu02] entwickelt und für die Bluetooth-Kommunikationstechnologie implementiert und evaluiert. Als mobile Testplattform wurde ein mit Linux ausgestatteter PDA eingesetzt.

Im Zusammenhang mit diesen Arbeiten wurde ebenfalls der Einfluss von drahtlosen Kommunikationstechnologien auf die informationelle Selbstbestimmung des Benutzers untersucht. Hierbei wurde deutlich, dass sowohl Bluetooth als auch IEEE802.11b identifizierende Daten bei der Kommunikation preisgeben [HHT03].

Basierend auf den bis dahin erzielten Ergebnissen konzentrierten sich die nachfolgenden Untersuchungen auf *Ad-hoc Netzwerke*. Hierbei wurden insbesondere Kommunikationsmodelle in drahtlosen Sensornetzwerksystemen untersucht. Als Ergebnis wurde ein Algorithmus zur Erhöhung der Verfügbarkeit von drahtlosen Sensornetzwerksystemen [Ha02b] entwickelt und anhand einer dafür implementierten Simulationsumgebung überprüft. Das in diesem Algorithmus angewandte Cluster Modell wurde in [SH03b] auf das Bluetooth Service Discovery Protokoll übertragen. Damit lässt sich eine sichere und energieeffiziente Dienstsuche in Bluetooth-Netzwerken [Se03a] durchführen.

Begleitend zu den theoretischen Untersuchungen erfolgte der *Aufbau einer drahtlosen Evaluationsumgebung* zur experimentellen Forschung und Überprüfung der von uns neu entwickelten Algorithmen und Verfahren für Ad-hoc Netzwerke. Als drahtlose Kommunikationstechnologie wird Bluetooth eingesetzt. Die Entwicklungsumbebung enthält sowohl PC gesteuerten Bluetooth Knoten, als auch selbst entwickelte Bluetooth-Sensorknoten (BlueNode), die durch Mikrocontroller gesteuert sind und für die ein angepasster Bluetooth-Protokoll-Stack entwickelt wurde [Ha03a, Bur02].

Die Entwicklung von Diensten für mobile Geräte zur Suche von Kommunikationspartnern, zur Suche und Nutzung von entfernten Diensten erfolgt auf Basis einer Middleware Architektur [SH02a] [Go03]. Diese bietet ebenfalls die Integration eines biometrischen Sensors zur Authentifizierung von Benutzern gegenüber mobilen Geräten.

Aus den bis dahin erzielten Ergebnissen wurde zusammenfassend das *Konzept eines sicheren Bürgergerätes für den e-Government Bereich* abgeleitet [Se02a, SH02b]. Des Weiteren flossen diese in die *Entwicklung eines Prototypen* ein, der auf der CeBIT 2003 präsentiert wurde [Wo03].

4 Zukünftige Arbeiten

Forschungsschwerpunkt der nächsten 2 Jahre ist die Analyse von Ad-hoc Kommunikationsbeziehungen mobiler Geräte im privaten, lokalen und globalen Bereich. Dieser Bereich zeigt gegenwärtig ein sehr starkes Wachstumspotential. Klassische Ad-hoc Topologien werden durch die Integration von heterogener Kommunikationsschnittstellen, die eine gleichzeitige Kommunikation über unterschiedliche drahtlose Kommunikationstechnologien ermöglichen, flexibler und bieten damit die Möglichkeit, die bestehenden eingeschränkten Sicherheitsarchitekturen in Ad-hoc Netzwerken zu erweitern.

Zur Überprüfung der weiterentwickelten Sicherheitsarchitekturen wird gerade an einer kombinierten Simulations- und Evaluationsumgebung für drahtlose Ad-hoc Netzwerke gearbeitet. Durch den Einsatz von virtuellen Kommunikationsschnittstellen lassen sich komplexe Ad-hoc Netzwerke bereits auf PC Basis bezüglich ihres realen Funkverhaltens simulieren.

Literaturverzeichnis

[Bu02] Buchholz, H.: *Sicherheit in Ad-hoc Netzwerken.* Diplomarbeit, Rostock, 2002.

[Bur02] Burchardt, H.: *Intelligentes Sensornetzwerk*. Diplomarbeit, Rostock, 2002.

[Go03] Golatowski, F.; Blumenthal, J.; Handy, M.; Haase, M.; Burchardt, H.; Timmermann, D.: *Service-Oriented Software Architecture for Sensor Networks.* International Workshop on Mobile Computing, IMC 2003; Rostock; Germany June 17-18, 2003.

[HHT03] Handy, M.; Haase, M.; Timmermann, D.: Anonymitätsaspekte bei Bluetooth und WLAN IuK Tage Mecklenburg-Vorpommern, Rostock, 2003

[Ha02b] Haase, M.; Handy, M.; Timmermann, D.: *Low-Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection*. 4th IEEE International Conference on Mobile and Wireless Communication Networks, Stockholm, 2002.

[Ha03a] Haase, M.; Burchardt, H.; Golatowsk, F.: *Bluetooth Sensornetzwerk auf der Basis von Mikrocontroller gesteuerten Sensorknoten*. Embedded World 2003, München, 2003.

[Se00] Sedov, I.; Cap, C.; Haase, M.; Timmermann, D.: Sicherheitsarchitektur für mobile spontan vernetzte Geräte. Workshop Bedrohungsszenarien im Rahmen des SPP Sicherheit in der Informations- und Kommunikationstechnik, Bremen, Dezember 2000.

[Se01a] Sedov, I.; Cap, C.; Haase, M.; Timmermann, D.: Hardware Security Concept for Spontaneous Network Integration of Mobile Devices. In: Lecture Notes in Computer Science, Springer Verlag 2001

[Se02a] Sedov, I.; Maibaum, N.; Cap, C.: *A Citizen Digital Assistant for e-Government*. In: Lecture Notes in Computer Science Vol. 2456, S. 284 - 287, Springer, 2002.

[SH02b] Sedov, I.; Haase, M.; Maibaum, N.; Cap, C.; Timmermann, D.: *Citizen Digital Assistant (CDA) - Ein sicherer Zugang zu e-Government – Diensten.* PIK Praxis in der Informationsverarbeitung und Kommunikation, 26. Jahrgang1/03 2003.

[SH03b] Sedov, I.; Haase, M.; Preuss, S.; Cap, C; Timmermann, D.: *Time and Energy Efficient Service Discovery in Bluetooth*. In: Proceedings of the 57th IEEE Vehicular Technology Conference, Jeju, Korea 2003.

[Wo03] Wohlgemuth, S.; Gerd tom Markotten, D.; Jendrike, U.; Müller, G.: *DFG-Schwerpunktprogramm „Sicherheit in der Informations- und Kommunikationstechnik“*. It-Information Technology, Methoden und innovative Anwendungen der Informatik und Informationstechnik, 45(1), 2003.