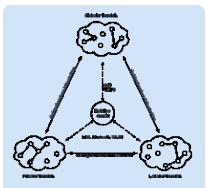
Titel

Sicherheitsarchitektur und Referenzszenario für spontan vernetzte mobile Geräte

DFG Schwerpunktprogramm "Sicherheit in der Informations- und Kommunikationstechnik"

Kurzbeschreibung



Ad-hoc Kommunikationsbeziehungen von mobilen Geräten

Ziel des Projektes ist die Untersuchung der besonderen Sicherheitsfragen bei der Kommunikation zwischen mobilen Geräten und der drahtlosen Umgebung im privaten, lokalen und globalen Bereich bei spontaner Vernetzung. Im Rahmen des Projektes erfolgt eine grundlegende, theoretische und praktische Untersuchung von Sicherheitsproblemen in Abhängigkeit von der durchzuführenden Transaktion, der aktuellen Umgebung, Ressourcen der Kommunikationspartner und der drahtlosen Kommunikationstechnologie. Das angestrebte Ziel ist die Entwicklung von Lösungsmodellen unter der Berücksichtigung der erweiterten Kommunikationsmöglichkeiten mobiler Geräte und der daraus resultierenden heterogenen Kommunikationsbeziehungen. Die entwickelten Lösungsmodelle werden anhand einer Simulations- und Evaluationsumgebung für drahtlose Netzwerke überprüft.

Die bisher durchgeführten Sicherheitsuntersuchungen konzentrierten sich im wesentlichen auf Kommunikationsbeziehungen zwischen zwei Geräten, Sicherheit von drahtlosen Kommunikationstechnologien und Gerätearchitekturen für mobile Geräte.

Die im dritten Bearbeitungszeitraum neu durchzuführenden Sicherheitsuntersuchungen konzentrieren sich jetzt auf die Kommunikationsbeziehungen zwischen einem mobilen Gerät und der drahtlosen Umgebung. In dieser Umgebung befinden sich Einzelgeräte und mehrere miteinander über spontane Vernetzung kommunizierende mobile Geräte, die durch unterschiedliche Kommunikationstechnologien, Ressourcen und Funktionalität charakterisiert sind.

Das zukünftige Arbeitsprogramm gestaltet sich wie folgt: Zu Beginn des dritten Bearbeitungszeitraumes wird eine grundlegende Analyse von Kommunikationsbeziehungen zwischen einem personenbezogenen mobilen Gerät und Geräten im privaten, lokalen und globalen Bereich (Abbildung 1) anhand von ausgewählten Kommunikationsmodellen durchgeführt. Zu jedem Modell werden die spezifischen Sicherheitsprobleme analysiert und konzeptuelle Lösungsmöglichkeiten erarbeitet.

Das angestrebte Ziel ist die Schaffung einer vertrauenswürdigen Kommunikation unter Berücksichtigung der Sicherheitsanforderungen

- der durchzuführenden Transaktion,
- der aktuellen Umgebung,
- der Ressourcen der Kommunikationspartner und
- der drahtlosen Kommunikationstechnologie

im jeweiligen Kommunikationsmodell.

Dafür wird ein Konzept zur adaptiven, transparenten Selektion von Kommunikations- und Sicherheitstechnologien entwickelt und anschließend in einer ebenfalls zu entwickelnden Simulationsumgebung überprüft. Diese setzt auf existierenden Simulationswerkzeugen auf und wird um die zusätzlich erforderlichen Sicherheitsfunktionen erweitert. Gleichzeitig erfolgt ebenfalls eine Erweiterung der bereits vorhandenen Evaluationsumgebung um die zu untersuchenden Kommunikationsmodelle, sodass erfolgreich simulierte Lösungsansätze nahtlos auf die Evaluationsumgebung übertragen werden können. Die erzielten Ergebnisse des Projektes werden abschließend einer umfassenden Sicherheitsanalyse unterzogen. Begleitend dazu findet die Realisierung und Integration des in den vorangegangenen Projektzeiträumen spezifizierten und partiell implementierten kryptografischen Co-Prozessors statt.

Ergebnisse

Erstes Arbeitspaket (AP1)
Im Rahmen des Projektes wurden Sicherheitsuntersuchungen bezüglich mobiler Geräte und drahtloser Kommunikationstechnologien mit dem Schwerpunkt auf spontane Vernetzung durchgeführt. Folgende Ergebnisse mit eigenen Veröffentlichungen wurden erzielt:

- Entwicklung und Referenzimplementierung eines generischen Sicherheitsmodells „Advanced Security Manager“
- Untersuchung von Anonymitätsaspekten bei der Nutzung von drahtlosen Kommunikationstechnologien

Zweites Arbeitspaket (AP2)
Basierend auf den erzielten Ergebnissen des ersten Arbeitspaketes konzentrierten sich die nachfolgenden Untersuchungen des zweiten Arbeitspaketes (AP2) auf Ad-hoc Netzwerke. Hierbei wurden insbesondere Kommunikationsmodelle in drahtlosen Sensornetzwerksystemen untersucht. Als Ergebnis wurde ein

- Algorithmus zur Erhöhung der Verfügbarkeit von drahtlosen Sensornetzwerksystemen

entwickelt und anhand einer dafür implementierten Simulationsumgebung überprüft. Das in diesem Algorithmus angewandte Cluster Modell wurde auf das Bluetooth Service Discovery Protokoll übertragen mit dem Ziel einer

- sicheren und energieeffizienten Dienstsuche in Bluetooth-Netzwerken.

Drittes Arbeitspaket (AP3)
Parallel zu den theoretischen Untersuchungen erfolgte im dritten Arbeitspaket (AP3) der Aufbau einer drahtlosen Evaluationsumgebung zur experimentellen Forschung und Überprüfung der von uns neu entwickelten Algorithmen und Verfahren für Ad-hoc Netzwerke. Dazu wurden folgende Arbeiten durchgeführt:

- Aufbau einer Bluetooth Infrastruktur
- Realisierung von Bluetooth Sensorknoten und Entwicklung eines angepassten Bluetooth Protokoll-Stacks
- Entwicklung einer Middleware Architektur
- Integration eines biometrischen Sensors
- Entwicklung eines kryptografischen Co-Prozessors für mobile Kleingeräte

Viertes Arbeitspaket (AP4)
Im vierten Arbeitspaket (AP4) wurde aus den erzielten Ergebnissen zusammenfassend das Konzept eines sicheren Bürgergerätes für den e-Government Bereich abgeleitet. Des Weiteren flossen diese in die Entwicklung eines Prototypen ein, der auf der CeBIT 2003 präsentiert wird.

- Entwicklung eines CDA (Citizen Digital Assistant) Konzepts
- Arbeiten im Zuge der CeBIT 2003 Präsentation am gemeinsamen Prototypen des SPP Sicherheit

Laufzeit

- **2001 – 2003**

Bearbeiter

Dipl.-Ing. Marc Haase

Prof. Dr.-Ing. Dirk Timmermann
E-Mail
Tel.: +49 381 498 7250
Fax: +49 381 498 118 7251
Raum: W1205

Veröffentlichungen

2003

- Haase, M.; Burchardt, H.; Golatowsk, F.: Bluetooth Sensornetzwerk auf der Basis von Mikrocontroller gesteuerten Sensorknoten. Embedded World 2003, München, 2003.
- Sedov, I.; Haase, M.; Maibaum, N.; Cap, C.; Timmermann, D.: Citizen Digital Assistant (CDA) - Ein sicherer Zugang zu e-Government – Diensten. PIK Sonderheft zur CeBIT 2003, 2003.
- Sedov, I.; Haase, M.; Preuss, S.; Cap, C; Timmermann, D.: Time and Energy Efficient Service Discovery in Bluetooth. In: Procedings of the 57th IEEE Vehicular Technology Conference, Jeju, Korea 2003.
- Sedov, I.; Haase, M.; Buchholz, H.; Preuss, S.; Cap, C.: Ad Hoc Network Protection by the Advanced Security Manager. In: Procedings of the IEEE 58th VTC Conference,Wireless Security Session, Orlando, Florida, USA, 2003, (eingereicht)
- Sedov, I.; Buchholz, H.; Cap, C.; Preuß, S.: Security for Service Discovery. The Eight International Conference on Personal Wireless Communications, IFIP WG 6.8 - Mobile and Wireless Communications, Italy (eingereicht), 2003.
- Golatowski, F.; Blumenthal, J.; Handy, M.; Haase, M.; Burchardt, H.; Timmermann, D.: Softwarearchitektur für Sensornetzwerke. 4. Iuk-Tage Mecklenburg-Vorpommern, Rostock, 2003.
- Sedov, I.: Kontextabhängige Sicherheit auf Kleinstgeräten. Workshop InfoSpaces, 2003.

2002

- Buchholz, H.: Sicherheit in Ad-hoc Netzwerken. Diplomarbeit, Rostock, 2002.
- Burchardt, H.: Intelligentes Sensornetzwerk. Diplomarbeit, Rostock, 2002.
- Haase, M; Handy, M.; Zugenmaier, A; Hohl, A.: Anonymität in drahtlosen Ad-hoc Netzwerken. Technischer Bericht, 2002.
- Haase, M.; Handy, M.; Timmermann, D.: Low-Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection. 4th IEEE International Conference on Mobile and Wireless Communications Networks, Stockholm, 2002.
- Schmalisch, M; Ploog, H.; Timmermann, D.: Kriterien zur optimalen Auswahl von Elliptic Curve Cryptography als Hard- oder Softwarelösung. Embedded Intelligence 2002, Band 1, S. 489-498, Nürnberg, 2002.
- Schmalisch, M.; Ploog, H.; Timmermann, D.: Laufzeitoptimierte VHDL Bibliothek zur Verifikation und Simulation kryptographischer Prozessoren. GI/ITG/GMM Workshop - Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen, ISBN: 3-8265-9859-8, S. 154 - 162, Tübingen, 2002.
- 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.
- Sedov, I.; Haase, M.: CeBIT 2003 Prototyp: Hardware und Middleware Spezifikation, Technischer Bericht, Universität Rostock, 2002
- Cap, C.; Maibaum, N.: Digital Identity and it's Implications for Electronic Government. In: Towards the E-Society - E-Commerce, E-Business, and E-Government, Kluwer Academic Publishers, Boston ISBN 0-7923-7529-7, 2002.
- Cap, C; Maibaum, N.; Heyden, L.: JavaCard-kontrollierter, sicherer Zugriff auf persönliche Dokumente und Berechtigungen. GI-Edition - Lecture Notes in Informatics; Sigrid Schubert, Bernd Reusch and Norbert Jesse (Hrsg.), Informatik bewegt, Informatik 2002, Proceedings of the 32th Annual Meeting of the GI, pages 433-436.
- Preuß, S.: JESA Service Discovery Protocol. Second International IFIP-TC6 Networking Conference:Networking, Springer, Lecture Notes in Computer Science Vol. 2345 May 19-24, 2002.
- Maibaum, N.; Mundt, T.: JXTA: A Technology Facilitating Mobile Peer-To-Peer Networks. In: Proceedings of the International Mobility and Wireless Access Workshop (MobiWac 2002), 12th October 2002, Forth Worth, Texas, USA, IEEE Computer Society Order Number PR01843, Pages 7 - 13, ISBN 0-7695-1843-5.
- Timmermann, D.: Sicherheit, Kommunikation und Energie: Offene Fragen wirklich mobiler Systeme. Eingeladener Vortrag, Gemeinsames Symposium der DFG Schwerpunktprogramme "Softwareagenten" und "IuK-Sicherheit", Schloss Dagstuhl, Wadern, 2002.

- Blumenthal, J.; Timmermann, D.: Middleware für mobile spontan vernetzte Sensornetzwerke. Startkolloquium DFG-Schwerpunktprogramm Basissoftware, Karlsruhe, 2002.
- Timmermann, D, Golatowski, F.; Ploog,H.; Bannow, N.: JSM: A small Java processor core for smart cards and embedded systems. In: Satellite Workshop Proceedings, Java in Embedded Systems, ARCS 2002, ISBN: 3-8007-2686-6, S. 135-140, Karlsruhe, 2002.
- Timmermann, D.; Handy, M.: Energie, Sicherheit und Mobilität in Smart Environments.Ladenburger Kolleg, Ladenburg, 2002.

2001

- Sedov, I.; Haase, M.; Cap, C.; Timmermann, D.: Hardware Security Concept for Spontaneous Network Integration of Mobile Devices. In: Lecture Notes in Computer Science Vol. 2060, Springer, 2001.
- Haase, M.; Sedov, I.; Cap, C.; Timmermann, D.: SmartBadge:Your Wireless Identity. Posterpräsentation, Berliner Kolloquium im Rahmen des DFG SPP Sicherheit, 2001.
- Cap, C.; Maibaum, N.; Heyden, L.: Extending the Data Storage Capabilities of a Java-based Smartcard. 6th IEEE Symposium on Computers and Communications, ISBN 0-7695-1177-6; ISSN 1530-1346, Hammamet,Tunesia, 3-5 July, 2001.
- Mundt, T.; Preuß, S.: Adaptive Service Chaining. In: Proceedings of 7th International Conference on Information Systems Analysis and Synthesis (ISAS 2001), July 2001, Orlando, Florida.
- Timmermann, D, Schmalisch, M.; Ploog, H.;: Beschleunigung von Elliptic Curve Cryptography durch algorithmische Optimierung. Workshop DFG Graduiertenkolleg "Verarbeitung, Verwaltung, Darstellung und Transfer multimedialer Daten - Technische Grundlagen, Gesellschaftliche Implikationen", erschienen in: Rostocker Informatik-Berichte, Universität Rostock, ISSN: 0233-0784, S. 59-68, 2001.
- Timmermann, D, Golatowski, F.; Preuss, S., Ploog, H. Geithner,T.; Cap, C.: Integration of Java Processor Core JSM into SmartDev(ices). 8th IEEE International Conference on Emerging Technolgies and Factory Automation, Proceedings, ISBN: 0-7803-7241-7, S. 699-702, Antibes Juan les Pins (France), 2001.
- Timmermann, D.; Handy, M.: Living in a smart environment. Ladenburger Kolleg, Ladenburg, 2001.
- Timmermann, D.; Ploog, H.; Schmalisch, M.: Anwendung einer Librayoptimierten VHDL-Kodierung für mobile ISDN-Verschlüsselung. 14. Mikroelektroniktagung 2001, ÖVE-Schriftenreihe Nr.26, ISBN: 3-85133-022-6, S.185-190, Wien, 2001.
- Timmermann, D.;.Golatowski, F.; Bannow, N.: Hardwareunterstützung für Java-Cards: Der Javaprozessor JSM. 14. Mikroelektroniktagung 2001, ÖVE-Schriftenreihe Nr.26, ISBN: 3-85133-022-6, S.141-146, Wien, 2001.
- Timmermann, D.; Ploog, H.; Flügel, S.: Improved ZDN-Arithmetic for Fast Modulo Multiplication. ICCD 2001, International Conference on Computer Design: VLSI in Computers & Processors, ISBN: 0-7695-1200-3, S. 166-171, Austin (TX, USA), 2001.
- Timmermann, D.; Schmalisch, M.: Grundlagen der Elliptic Curve Cryptography. 3. IuK-Tage Mecklenburg-Vorpommern, Rostock, 2001.
- Timmermann, D.; Schmalisch, M.: Einführung in die Elliptic Curve Cryptography. 10. Symposium Maritime Elektronik, S. 125-128, Rostock, 2001.
- Timmermann, D.; Ploog, H.: Mobile Sicherheit durch effiziente Public-Key-Verschlüsselung. 3. IuK-Tage Mecklenburg-Vorpommern, Rostock, 2001.
- Timmermann, D.; Ploog, H.; Ahrens, A.: Nicht triviale Sicherheitsprobleme im E- und M-Commerce. 3. IuK-Tage Mecklenburg-Vorpommern, Rostock, 2001.
- Timmermann, D.; Ploog, H.; Ahrens, A.: Erhöhung der Sicherheit von Public-Key Implementierungen auf Smart Cards gegen Timing-Angriffe. 10. Symposium Maritime Elektronik, S. 137-140, Rostock, 2001.
- Timmermann, D.; Golatowski, F.; Bannow, N.; Hildebrandt, J.; Ploog, H.: JSM - Ein Java Prozessor für eingebettete Systeme: Aufbau, Implementierung und Rapid-Prototyping. 10. Symposium Maritime Elektronik, S. 185-188, Rostock, 2001.
- Wegner, T.: Internet Security - Auf dem Wege zur ganzheitlichen Sicherheit im CampusNetz. 3. Iuk-Tage Mecklenburg-Vorpommern, Rostock, 2001.
- Wegner, T.: Ganzheitliche Sicherheit im DV-Netzen - Ein IP-Paketfilter als ein Baustein zur Schaffung einer ganzheitlichen Sicherheitsarchitektur in einem bestehenden Intranet. 10. Symposium Maritime Elektronik, S. 85-88, Rostock, 2001.

Vorträge im Rahmen des SPP Sicherheit

- Sedov, Igor; Cap, Clemens H; Haase, Marc; Timmermann, Dirk: Security Aspects Personal Area Networks. Vortrag, Workshop "Spontane Vernetzung/drahtlose Kommunikation im Rahmen des SPP Sicherheit", Rostock, 2001.
- Haase, Marc; Timmermann, Dirk; Sedov, Igor; Cap, Clemens H.: Drahtlose Kommunikationstechnologien. Vortrag, Workshop "Spontane Vernetzung/drahtlose Kommunikation im Rahmen des SPP Sicherheit", Rostock, 2001.
- Haase, Marc; Sedov, Igor; Timmermann, Dirk; Cap, Clemens H.: Mehrstufige Sicherheitsarchitektur für spontan vernetzte mobile Geräte. Vortrag, Kolloquium des SPP Sicherheit, Böblingen, 2001.
- Haase, Marc; Sedov, Igor; Timmermann, Dirk; Cap, Clemens: Sicherheitsarchitektur und Referenzszenario für spontan vernetzte mobile Geräte. Vortrag, Kolloquium des SPP Sicherheit, IBM Research, Zuerich, 2002.
- Haase, Marc; Sedov, Igor; Timmermann, Dirk; Cap, Clemens: Sicherheitsarchitektur und Referenzszenario für spontan vernetzte mobile Geräte. Vortrag, Kolloquium des SPP Sicherheit, Rostock, 2002.

Kontakt
Fakultät für Informatik und Elektrotechnik
Institut für Angewandte Mikroelektronik und Datentechnik
Haus 1, Raum 1207 (Sekretariat)
Richard Wagner Str. 31
18 119 Rostock-Warnemünde
Telfon: +49 381 498 72 51
Fax: +49 381 498-118 72 51

Schnelleinstieg
Publikationen
Anfahrt
Kontakt
Laborpraktikum
Lehrangebot
Highlights
Projekte