Bestimmung und Einordnung des Begriffs Mobilität und Untersuchung der Auswirkungen auf die Sicherheit von Betriebssystemen

Sven Lachmund
TU-München
lachmund@in.tum.de

21. Februar 2003

Zusammenfassung

Der Begriff der Mobilität ist im Rahmen unseres Projektes, das sich mit der Konzeption eines sicheren Betriebssystems für mobile Endgeräte beschäftigt, von zentraler Bedeutung. Zum einen ist der Begriff im Umfeld der Informatik und Informationstechnologie nicht allgemein definiert und zum anderen ist herauszufinden, inwieweit sich die Mobilität auf die Sicherheit, die Fokus in diesem Projekt ist, auswirkt. Dieses Dokument bietet eine Definition der Mobilität im Kontext des Projektes und betrachtet Auswirkungen der Mobilität auf die Sicherheitsanforderungen.

1 Einführung und Motivation

Durch die Entwicklung und Verbesserung der Kommunikationstechniken, der Zunahme der digitalen Informationsverarbeitung in jeglichen Bereichen und die Zunahme der Globalisierung steigt das Verlangen nach der Allgegenwärtigkeit von Computersystemen (Ubiquitous Computing, Pervasive Computing). Heute bekannte Ausprägungen von mobilen Endgeräten sind beispielsweise Mobiltelefone und Personal Digital Assistants (PDAs). Der Aspekt der Mobilität stellt für die IT-Sicherheit eine neue Herausforderung dar. Um in der Lage zu sein, die Auswirkungen der Mobilität auf die IT-Sicherheit erkennen zu können, ist der Frage, was die Mobilität für IT-Systeme bedeutet, nachzugehen.

Dieser Beitrag bestimmt zunächst den Begriff der Mobilität im Kontext der Informatik näher, um im Anschluss auf Bedrohungen einzugehen, die durch die Mobilität entstehen. Ferner werden zum Teil Lösungsansätze angesprochen, die vor den Bedrohungen schützen.

2 Allgemeine Definition der Begriffe Mobilität und mobil

Die beiden Begriffe *Mobilität* und *mobil* sind lateinischen Ursprungs. *Mobilität* bedeutet Beweglichkeit, geistige Beweglichkeit und *mobil* bedeutet beweglich, munter, die Fähigkeit besitzen, sich zu bewegen oder bewegt zu werden ([5, 4]). Diverse Fachgebiete, wie die Soziologie, Geographie oder Wirtschaft ([10]), verfeinern die Definition in ihrem Kontext, indem sie konkret beschreiben, welches Individuum die Beweglichkeit in welchem Umfeld besitzt. Eine derartige Definition gibt es im Bereich der Informatik und der Informationstechnologie nicht in diesem Ausmaß. Dieser Umstand motiviert die Fragestellungen des nächsten Kapitels.

3 Mobilität im Kontext der Informatik

Es stellt sich die Frage, welche Bedeutung der Begriff *mobil* für die Informatik hat. Ohne eine klare Vorstellung darüber kann die Mobilität im Security Engineering nicht adäquat berücksichtigt werden. Zur Konkretisierung einer Antwort wird im Folgenden das Individuum, das die Beweglichkeit aufweist, im Kontext der Informatik allgemein konkretisiert. Es wird der Frage nachgegangen, welche Individuen es in diesem Kontext gibt, die eine Beweglichkeit annehmen können und in welchem Medium sie sich bewegen. Die folgenden Individuen werden vor diesem Hintergrund betrachtet.

- Anwender
- System
- Endgerät
- Dienst
- Netz
- Code
- Protokoll
- Datum
- Kommunikation

Die Bedeutung der Mobilität für die Individuen wird im Folgenden untersucht.

Als System verstehen wir die Kombination mehrerer Komponenten zu einer Gesamtheit. Diese Gesamtheit nimmt in irgendeiner Form an einem Informationsverarbeitungsprozess teil. Der Begriff des mobilen Systems ist zu abstrakt, um die Auswirkungen der Mobilität darauf beschreiben zu können. Es ist erforderlich, die Auswirkung der Mobilität auf die Komponenten des Systems zu untersuchen, um eine konkrete Aussage erhalten zu können.

Der mobile Anwender zeichnet sich dadurch aus, dass er sich im Raum frei bewegt und sein zukünftiger Aufenthaltsort nicht unbedingt deterministisch ist. Er führt sein Endgerät i. d. R. mit sich, um an einem beliebigen Ort zu einer beliebigen Zeit der Informationsverarbeitung in verschiedensten Ausprägungsformen nachgehen zu können.

Das mobile Endgerät ist ein Hardware-Komponente, die mit Rechen-, Speicher- und Kommunikationsfähigkeit ausgestattet ist. Es ist mobil, d. h. es kann von seinem Anwender stets mitgeführt und an beliebigen Orten oder während des

Ortswechsels benutzt werden. Dabei sollen weitgehend alle Tätigkeiten des Anwenders orts- und zeitunabhängig durchgeführt werden können. Mit Tätigkeiten sind informationsverarbeitende Aktionen gemeint, die sich entweder komplett im Endgerät erledigen lassen oder zusätzlich die Kommunikation mit externen Systemen erfordern. Ein mobiles Endgerät hat üblicherweise eine netzunabhängige Stromversorgung mittels Batterie und kommuniziert über drahtlose Techniken mit anderen Systemen.

Möchte ein Endgerät einen Dienst in Anspruch nehmen, so muss es wissen, wo und wie er zu erreichen ist. Ein mobiler Dienst könnte zusammen mit dem System, auf dem er läuft, oder gar zusammen mit einer Infrastruktur, in der er angeboten wird, wandern. Dadurch ändert sich der Weg, den ein Endgerät zur Kommunikation mit dem Dienst im Netz durchschreiten muss. Um den Dienst nutzen zu können, muss bekannt sein, wo er zu erreichen ist.

Ein Netz ist die Summe aller es aufspannenden Kommunikationssysteme. Es wird zu einem mobilen Netz, wenn es dadurch seinen Aufenthaltsort wechselt, indem alle Kommunikationssysteme, die das Netz aufspannen, gemeinsam eine Ortsveränderung durchführen. Alle Kommunikationssysteme, die am Netz teilnehmen, müssen über seinen aktuellen Aufenthaltsort bescheid wissen, um hinzu gelangen oder bleiben zu können. Ein Kommunikationssystem kann jede Art von Netzknoten wie beispielsweise ein Endgerät, ein Router oder eine Bridge sein.

Der Begriff des mobilen Codes wurde in der Wissenschaft bereits eingängig untersucht ([3, 8, 9]) und bezeichnet einen ausführbaren Code, der auf ein anderes System gelangt, um dort ausgeführt zu werden.

Ein mobiles Endgerät greift im Rahmen der Datenkommunikation auf definierte Protokolle zu, damit es mit seiner Gegenstelle erfolgreich kommunizieren kann. Ein mobiles Protokoll kann man sich als ein Protokoll vorstellen, das von einem Netz, in dem es Anwendung findet, bereitgestellt wird. Das Endgerät kann das Protokoll bei Bedarf dynamisch herunterladen und benutzen während es sich in dem Netz befindet.

Ein Datum ist die Darstellung von Information in binärer Form. Es ist als Oberbegriff für die spezialisierteren Definitionen von Code und Protokoll zu sehen. Im Gegensatz zum Code und zum Protokoll ist es nicht ausführbar. Wenn ein Datum seinen aktuellen Aufenthaltsort verändert, ist es ein mobiles Datum. Als Beispiel ist ein Kommunikationsvorgang zu nennen, bei dem das Datum den Speicher des Endgerätes verlässt, durch ein Netz übertragen wird, um bei einem anderen Endgerät anzukommen.

Unter dem Begriff der mobilen Kommunikation versteht man in der Informationstechnik die Möglichkeit des Anwenders, unter der Verwendung seines mobilen Endgerätes ortsunabhängig zu kommunizieren. Dies setzt das Vorhandensein einer Kommunikationsinfrastruktur mit drahtloser Verbindung voraus, derer sich das mobile Endgerät bedient. Beispielsweise fällt jegliche Art von Funk und Mobiltelefonie darunter [6, 7].

Die Betrachtung der Mobilität von Systemen zeigt, dass es erforderlich ist, die Mobilität der einzelnen Komponenten des Systems zu betrachten. Dabei wird deutlich, dass sich jede Komponente nur in einem bestimmten Medium bewegen kann. Ist die Ausdehnung des Mediums eingeschränkt, ist auch die Mobilität der Komponente begrenzt, da die mobile Komponente auf die Existenz des Mediums angewiesen ist.
Nachdem die Mobilität der Komponenten in diesem Abschnitt definiert worden ist, zeigt der folgende die Auswirkungen der Mobilität auf die Sicherheit auf.

4 Auswirkungen auf die Sicherheit

Durch die Mobilität von Systemen eröffnen sich für die IT-Sicherheit neue Gesichtspunkte. Zusätzliche Bedrohungen entstehen den Komponenten und somit dem gesamten System. Dieser Abschnitt behandelt die Bedrohungen, denen die Individuen aus dem vorangegangenen Kapitel ausgesetzt sind und nennt fallweise beispielhaft mögliche Maßnahmen zum Schutz vor diesen Bedrohungen. Die Intention dieses Abschnitts ist aufzuzeigen, dass die Mobilität neue Sicherheitsfragen aufwirft, die es zu lösen gilt. Die Betrachtungen sind daher deskriptiv und informell. Sie können aber als Grundlage für die Erstellung eines systematischen Modells und einer Bewertung der Sicherheitsfragen und Maßnahmen dienen, was nicht Teil dieses Beitrags ist.

Die Mobilität des Anwenders ist eng verzahnt mit der Mobilität des Endgerätes. Nur wenn es der Anwender mit sich herumträgt, ist es mobil. Somit befindet sich das Endgerät in Abhängigkeit von der Zeit in unterschiedlichen Umgebungen, woraufhin es in unterschiedlichen Netzen sein kann.
Durch die häufige und spontane Benutzung kann es passieren, dass der Anwender sein Endgerät irgendwo liegen lässt. Aufgrund seiner Bauform ist das Endgerät in einem unbeobachteten Moment leicht zu entwenden. Unter Abwesenheit des Anwenders ist ein physikalischer Angriff auf das Endgerät uneingeschränkt möglich. Wird das Endgerät im eingeschalteten Zustand entwendet, oder gibt es keine Authentifikation beim Einschalten des Endgerätes, besteht die Gefahr, dass der Angreifer beispielsweise Daten auslesen oder Kommunikationsverbindungen oder die digitale Identität des Anwenders übernehmen kann. Befindet sich der Anwender nicht alleine an seinem aktuellen Aufenthaltsort, kann er bei seiner Arbeit am Endgerät beobachtet werden. Informationen können vom Display abgelesen oder Eingaben des Anwenders können beobachtet werden.
Mobilität bedeutet hier auch, dass das Endgerät zu unterschiedlichen Zeiten von verschiedenen Anwendern benutz wird (z. B. ein Endgerät für die ganze Familie). Es ist somit sicherzustellen, dass einem Anwender die Daten der anderen nicht zugänglich sind.
Durch die Mobilität des Endgerätes befindet es sich in verschiedenen Netzen. Für jedes Netz können unterschiedliche Erwartungen an die Sicherheit gestellt werden, da der Grad des Vertrauens differiert die verfügbaren Dienste differieren oder unterschiedliche Mechanismen zum Schutz vor Angriffen zur Verfügung stehen.

Auch die Netze haben unterschiedliche Anforderungen an die Endgeräte. Die Vertrauenswürdigkeit der Endgeräte differiert von Endgerät zu Endgerät oder es kann fallweise keine Aussage darüber getroffen werden, wenn das Endgerät dem Netz nicht bekannt ist. Aus der Sicht des Netzes besteht das Interesse, die Rechte des Endgerätes gering zu halten, damit ein potentiell böswilliger Anwender oder ein potentiell schadhaftes Endgerät keinen Schaden anrichten kann. Durch den spontanen Zusammenschluss diverser Endgeräte zu einem vorher nicht existenten Netz – einem sog. Ad-Hoc-Netz –, entsteht eine Beziehung der beteiligten Endgeräte zueinander, die in Bezug auf Vertrauenswürdigkeit schwer einzuschätzen ist. Auch hier verfolgen unterschiedliche Komponenten unterschiedliche Schutzziele, die es zu vereinen gilt.
Abhängig von der Umgebung, in der sich das Endgerät befindet, besteht der Wunsch, unterschiedliche Dienste zu nutzen oder anzubieten. Die Verwendung diverser Dienste kann zusätzliche Sicherheitsprobleme ergeben.

Im Rahmen der Authentifikation eines Dienstes ist heute häufig der Ort, an dem der Dienst angeboten wird (z. B. Name oder IP-Adresse des anbietenden Endgerätes) fester Bestandteil des Authentifikationsverfahrens. Um die Authentizität des Dienstes auch in seinem mobilen Umfeld gewährleisten zu können, sind geeignete Authentifikationsverfahren zu verwenden.

Die Mobilität eines Netzes wirkt sich auf die Anbindung des Netzes an seine Umgebung aus. Gemäß der Definition verändert sich das mobile Netz intern nicht, da all seine aufspannenden Endgeräte gemeinsam mobil sind, sodass sich ihre Beziehungen untereinander nicht ändern (das Hinzukommen oder Entfernen von Endgeräten aus dem Netz soll hier nicht betrachtet werden). Gibt es eine Anbindung an die Umgebung, können sich die Anforderungen an diese Anbindung durch die Mobilität des Netzes ändern, da die Anbindung über verschiedene Infrastrukturen realisiert werden kann. Die anbindende Gegenstelle muss zudem entscheiden können, welche Aktionen sie dem Netz erlauben kann und welche nicht.

Die Bedrohungen beim Einsatz von mobilem Code (z. B. Überschreiben des Adressraums eines Prozesses (Buffer Overflow)) und deren Vermeidung (z. B. Sandboxing oder Code-Inspektion) werden in der Literatur bereits ausführlich diskutiert ([3, 8, 9]). Es wird daher davon abgesehen, diese Thematik hier tiefer zu beleuchten.

Der hinter dem mobilen Protokoll steckende Code muss vertrauenswürdig sein, da er sonst aufgrund seiner hohen Privilegien sämtliche Schutzmechanismen des Kerns unterlaufen kann. Dieses Problem ähnelt dem des mobilen Codes. Unterschiedlich ist allerdings die Ausführungsumgebung. Während der mobile Code (z. B. in Form eines Agenten) üblicherweise im User-Mode ausgeführt wird, läuft das Protokoll in einem höher privilegierten Modus ab.

Nach der obigen Definition das mobilen Datums ergeben sich keine neuen Bedrohungen für das Datum. Auch in immobilen Systemen werden Daten mit Hilfe der Datenkommunikation versandt. Zur Erreichung der gewünschten Schutzziele sind je nach Sensibilität der Daten die üblichen Maßnahmen zur Wahrung der Vertraulichkeit, Integrität und Authentizität zu ergreifen. Die gewünsch-

ten Schutzziele können abhängig vom aktuellen Aufenthaltsort der Daten sein. Befinden sie sich in einer vertrauenswürdigen Umgebung, sind die Schutzziele durchaus geringer.
Auch hier sei auf die Literatur zu diesem Thema verwiesen ([3, 8, 9]).

5 Fazit

Durch die Überführung eines Systems in ein mobiles System ergeben sich zusätzliche Bedrohungen, die durch geeignete Maßnahmen beseitigt werden müssen. Um die Bedrohungen erkennen zu können, ist es erforderlich, die Auswirkungen der Mobilität auf die Komponenten des Systems zu untersuchen. Im Bereich der Betriebssysteme spielen mit der Mobilität Sicherheitsaspekte herein, die es bei der Konzeption des sicheren Betriebssystems zu berücksichtigen gilt.

Danksagung

Besonderer Dank geht an Herrn Prof. Dr. Uwe Baumgarten für die tatkräftige Unterstützung in Form von anregenden und hilfreichen Diskussionen.
Dieser Beitrag ist im Rahmen des Projekts LucaOS im Schwerpunktprogramm Sicherheit der DFG entstanden. Dank geht daher an die DFG für die Förderung des Projektes.

Literatur

[1] Uwe Baumgarten, Claudia Eckert, and Harald Görl. Trust and confidence in open systems: Does security harmonize with mobility? In *9th ACM SIGOPS European Workshop „Beyond the PC: New Challenges for the Operating System“*. ACM, September 2000.

[2] Hakima Chaouchi and Guy Pujolle. A new policy based management of mobile ip users. *LNCS 2345 Springer*, pages 1099–1104, 2002.

[3] Claudia Eckert. *IT-Sicherheit, Konzepte — Verfahren — Protokolle*. Oldenbourg Verlag, München, 2001.

[4] Merriam-Webster OnLine The Language Center (Hersg.). Merriam-webster dictionary. http://www.m-w.com/, Dezember 2002.

[5] Dudenredaktion [Hrsg.]. *Duden, Die deutsche Rechtschreibung, Band 1.* Dudenverlag, Mannheim – Leipzig – Wien – Zürich, 22 edition, 2000.

[6] Klaus Lipinski [Hrsg.]. *Lexikon Mobilkommunikation.* MITP-Verlag GmbH, Bonn, 1999.

[7] Ralf Reichwald [Hrsg.]. *Mobile Kommunikation – Wertschöpfung, Technologien, neue Dienste.* Betriebswirtschaftlicher Verlag Dt. Th. Gabler GmbH, Wiesbaden, 2202.

[8] Andrew S. Tanenbaum. *Moderne Betriebssysteme.* Pearson Studium, München, zweite edition, 2002.

[9] Andrew S. Tanenbaum and Maarten van Steen. *Distributed Systems – Principals and Paradigms.* Prentice Hall, New Jersey, USA, 2002.

[10] wissen.de Online-Lexikon (Hersg.). Wissen.de-lexikon. http://www.wissen.de, Dezember 2002.