

Mobiler Einsatz – hoffentlich sicher

Stärken und Schwächen von Palm OS & Co.

Kai-Oliver Detken

Wie bei Desktop-Computern gibt es auch für Pocket PCs und Smartphones verschiedene, miteinander konkurrierende Betriebssysteme. Der große Unterschied zu Notebooks oder Desktops ist, daß man die Betriebssoftware auf den mobilen Computern nicht nach Belieben ändern oder austauschen kann. In der Regel entscheidet man sich beim Kauf des Gerätes also auch für das Betriebssystem. In einigen Fällen erlauben die Hersteller, später auf eine aktuellere Version der Betriebssoftware umzusteigen. Der Wechsel zu einer völlig anderen Softwareplattform ist dagegen nicht möglich. Zu hinterfragen sind zudem die Sicherheitsmerkmale der Systeme, da sie zunehmend im mobilen geschäftlichen Einsatz sind.

An Betriebssysteme für mobile Geräte werden im Vergleich zu herkömmlichen Betriebssystemen besondere Anforderungen gestellt. So muß z.B. das Betriebssystem eines Embedded Systems – etwa eines Antiblockiersystems in einem Fahrzeug – stabil und ausfallsicher laufen; bei der Inbetriebnahme von PDAs oder Smartphones erwartet der Benutzer eine schnelle Betriebsbereitschaft. Und da der Zugang zu mobilen Systemen für Fremde leichter möglich ist, erfordern „mobile Betriebssysteme“ auch besondere Sicherheitsvorkehrungen.

Angebote

Als Betriebssysteme für Mobiles sind vor allem Embedded Linux, Palm OS, Symbian OS sowie die Windows-Familie verbreitet.

Wenn von *Linux* die Rede ist, ist im Grunde eine Linux-Distribution gemeint; streng betrachtet ist Linux jedoch der Kernel. Dabei handelt es sich um einen „monolithischen“ Kernel, der allerdings so konfiguriert werden kann, daß nicht alle Hardwaretreiber und Merkmale als fest einkompilierte Instanzen schon bei der ersten Phase des Bootvorgangs zur Verfügung stehen. Es ist durchaus möglich, die notwendigen Treiber als Modul zu kompilieren und bei Bedarf zur Laufzeit nachzuladen. Man spricht hierbei von einem hybrid monolithischen Kernel. Dieser modulare Aufbau ermöglicht es, einen sehr kompakten Kernel mit minimaler Speicheranforderung zu bauen, der wiederum für den Einsatz im Embedded-Bereich von Interesse ist. Die Versionen für den Einsatz auf PDAs bzw. Smartphones fallen ebenso unter die Kategorie Embedded Linux. Sie sind für den Betrieb auf Systemen mit wenig RAM und geringer CPU-Leistung ausgelegt. Dabei werden alle gängigen Embedded-Architekturen unterstützt.

Die aktuelle Version von *Palm OS* mit dem Namen Cobalt 6.1 wird von Palmsource vertrieben. Sie ist eine komplett überarbeitete Konzeption und Entwicklung des Betriebssystems Garnet und eine Erweiterung der Version 5 des Betriebssystems. Der Kernel des Palm OS einschließlich der Version 4 basiert auf dem AMX Real Time Operating System (RTOS) von Kadak. Obwohl es sich dabei um einen Echtzeitkernel handelt, wird die Echtzeitfähigkeit unter Palm OS nicht eingesetzt. Aus Lizenzierungsgründen sind die APIs des Kernels nicht offengelegt. Bekannt ist allerdings, daß das Palm OS von den Eigenschaften wie z.B. Semaphore und Signalgruppen des AMX Gebrauch macht. Der Kernel unterstützt zwar volles Multitasking, stellt allerdings der Applikationsebene nur einen einzigen Task zur Verfügung. Hier kann zu einem Zeitpunkt nur eine Anwendung ausgeführt werden.

Die aktuelle Version Cobalt 6.1 wurde laut Palmsource als eine hochgradig modulare, skalierbare und standardbasierte Plattform speziell für neuartige Smartphones und andere drahtlose Endgeräte konzipiert und entwickelt. Dabei wurde das Betriebssystem komplett auf die ARM-Architektur portiert und zeichnet sich vor allem durch die Multitasking-Multithreading-Fähigkeit aus.

Bei *Symbian OS* handelt es sich um ein Betriebssystem des gleichnamigen Konsortiums, das aus namhaften Herstellern wie Nokia, Ericsson, Panasonic und weiteren besteht. Es stellt die Weiterentwicklung des Betriebssystems Epoc dar, das früher auf Psion-Geräten eingesetzt wurde. Version 9.1 wurde Anfang 2005 von Symbian vorgestellt, verbreitet sind allerdings die Versionen 7.0, 7.0s und 8.0 auf den neuesten Smartphones der zweiten und dritten Generation der genannten Gerätehersteller. Man kann

Symbian OS als ein offenes Betriebssystem bezeichnen, da durch ein Lizenzierungsmodell Lizenzabnehmer, die meist identisch mit den Geräteherstellern sind, den kompletten Betriebssystemquellcode zur Verfügung gestellt bekommen. So können Anpassungen an die spezifische Hardware vorgenommen werden, und die Entwicklung eines eigenen Betriebssystems ist nicht notwendig.

Windows Compact Edition (CE) ist ein modulares 32-bit-Betriebssystem für mobile Endgeräte von Microsoft. Der wesentliche Unterschied zu anderen Windows-Betriebssystemen sind die geringen Anforderungen an Hardwareressourcen. Auf Basis von Windows CE 3.0 wurde 2000 Windows Pocket PC entwickelt.

	Embedded Linux	Palm OS	Symbian OS	Windows-Familie
Marktausrichtung	universell	PDA's	Smartphones	universell
Konfigurierbarkeit	hoch	gering	gering	hoch
Footprint (min. Speicherbedarf)	250 - 700 kbyte	keine Angabe	ca. 200 kbyte	300 kbyte (CE) 5 Mbyte (XP)
Multitasking	ja	nur auf Betriebssystemebene	ja	ja
Programmierung	wie für Desktop-Systeme	spezielles API	spezielles API	wie für Desktop-Systeme
Handschrifterkennung	optional	integriert	integriert	integriert

Vergleich von Betriebssystemen für Mobiles

Windows Pocket PC bietet ein vereinfachtes Benutzerinterface, optimierte Performance, neue und verbesserte Anwendungen und vor allem neue Multimedia-Funktionen.

Nach Windows Pocket PC folgte Windows Mobile 2003 mit verbesserter Netzkonnektivität, erweiterten vordefinierten Konfigurationen, verbessertem Speichermanagement und Shared Source.

Windows CE kann auf unterschiedlichsten Plattformen mit verschiedensten Features laufen und unterstützt die Prozessortypen Intel x86, MIPS, ARM und Hitachi-SH-Prozessoren. Microsoft bietet ab Pocket PC Version 2002 wegen des zu hohen Kompatibilitätsaufwandes für Hardware und Software nur noch ARM-basierte Geräte an. Microsoft Pocket PC basiert auf dem Kern von Windows CE 3.0. Dies führt zu der Betriebssystemreihe Windows CE, die von Microsoft Hardware vertrieben wird. Die aktuelle Version ist Windows CE 5.0.

Sicherheitsaspekte

Bei Linux kann man davon ausgehen, daß es auf PDA's genauso sicher ist wie als Desktopvariante. Durch die konsequente Umsetzung des Multiuser-Konzeptes besitzt ein Benutzer generell wenige Rechte auf dem System. Er hat, ähnlich wie auf einem Desktopsystem, keinerlei Befugnis, an ausführbaren System- bzw. Konfigurationsdateien Änderungen vorzunehmen. Nur der Super-User „Root“ genießt uneingeschränkte Rechte auf das System, was wiederum Risiken birgt. Das Ausführen eines nicht vertrauenswürdigen Codes durch den Super-User kann durchaus fatale Folgen haben. Möglich ist eine Infizierung des gesamten Systems mit Viren.

Deshalb sollte die Benutzung des Systems mit Super-User-Rechten generell vermieden werden.

Auch wenn Linux-Betriebssysteme einen sehr guten Schutz vor Datenmißbrauch gewährleisten und bis jetzt die besten Sicherheitsmerkmale für mobile Endgeräte bieten, sind einige Schwachstellen vorhanden wie die Möglichkeit, eine Synchronisation ohne Authentisierung vornehmen zu können. Viren und Würmer sind stets vorhanden, wenn auch nicht direkt für mobile Linux-Distributionen.

Für Palm OS Cobalt wurde die Sicherheit völlig neu entwickelt. Basis ist ein sicherer Kernel, der auf einem Capabilities-Modell beruht. Hierfür vergibt der Kernel während des Bootvorganges gewisse Berechtigungen an die sog. Systemmanager: Autorisierungsmanager, Authentisierungsmanager, Cryptographic Provider Manager (CPM) und Certificate Manager.

Nur die berechtigten Systemmanager können mit anderen Systemkompo-

nenten kommunizieren. Laut Palm-source sind mit der Einführung von Cobalt 6.1 die meisten Schwachstellen behoben. Mangels Geräten mit diesem Betriebssystem gibt es aber noch keine Erfahrungswerte.

Das Sicherheitssystem des Symbian OS ermöglicht Authentisierung, Datenintegrität und Datenverschlüsselung. Hierbei werden sowohl symmetrische Verschlüsselungsalgorithmen wie DES, AES, RC2, RC4, RC5 und PKCS#7 als auch asymmetrische Verfahren wie RSA, DAS und DH unterstützt. Weiterhin gehören kryptografische Hash-Funktionen zum Funktionsumfang. Für eine sichere Kommunikation bietet Symbian OS kryptografische Protokolle wie SSL/TLS, IPsec und WTLS. Zudem stellt es eine Applikation und Schnittstellen zur Handhabung und Speicherung von digitalen Zertifikaten für den Einsatz bei SSL/TLS usw. bereit. Außerdem ermöglicht das Installationswerkzeug von Symbian OS eine sichere Installationsprozedur.

Anwendungen, die auf einem Windows-CE-basierten System ausgeführt werden, operieren mittels der Memory Management Unit (MMU) in getrennten Speicherbereichen. Windows CE kann bis zu 32 Prozesse gleichzeitig verwalten. Alle Prozesse werden in einem eigenen Thread betrieben. Windows CE zählt damit zu den thread-sicheren Betriebssystemen. Die wichtigsten unterstützten Sicherheitsmechanismen sind u.a. das Security Support Provider Interface (SSPI), Kryptografie, digitale Signaturen, Smartcards, Windows NT LAN Manager (NTLM), SSLv2 und SSLv3 sowie Private Communication Technology (PCT). Für sichere Kommunikation unterstützt Windows CE auch die Microsoft Cryptographic API (CAPI). Das Teilsystem Windows CE Smartcard unterstützt CAPI und ein Gerätetreibermodell, um Smartcard-Anwendungen zu realisieren. Zusätzlich erleichtert die PC/SC-Unterstützung die Portierung bestehender Smartcard-Treiber. Das Smartcard-Teilsystem stellt eine Verbindung zwischen der Smartcard-Hardware und der Smartcard-Anwendung her. Die APIs dazu befinden sich in DLLs.

Das Problem bei Windows CE ist, daß Anwendungen, die für eine bestimmte Hardwareplattform entwickelt wurden, nicht ohne weiteres portierbar sind. Microsoft sorgte auch mit seinen Benennungen der einzelnen Betriebssysteme für Irritierungen. Somit hat man sich mit Windows CE 5.0 auf die alte Namensgebung zurückbesonnen. Microsoft Pocket PC besitzt keinerlei Möglichkeit, Daten auf dem mobilen Endgerät zu verschlüsseln. Es grenzt weder Speicherblöcke noch Applikationen wirkungsvoll voneinander ab. Jede Applikation kann ihre Prioritäten anpassen, andere Applikationen beenden, auf deren Speicherbereiche zugreifen oder auch den Wechsel in den Stromsparmodus unterbinden. Paßwörter können vom Nutzer deaktiviert werden und sind oft in der Standardeinstellung bereits deaktiviert. Auch können externe Speicher, etwa eine SD-Karte, von einem Angreifer einfach aus dem Endgerät entnommen und die darauf gespeicherten Daten gestohlen werden. Es sind gefälschte Dialoge möglich, da das

Betriebssystem ActiveX und Java unterstützt, mit deren Hilfe ein gefälschter Dialog aufgebaut werden kann. Des Weiteren besteht die Möglichkeit, auf dem mobilen Endgerät mobilen Code auszuführen.

Bewertung

Trotz zahlreicher Erneuerungen in Bezug auf Sicherheit und Anpassungen an die neuartigen Smartphones wird Palm OS Cobalt 6.1 von keinem Gerätehersteller auf diesem Sektor eingesetzt. Die Unterstützung für NAND-Flash-Speicher für automatische Backups bei einem leeren Akku sowie der USB-on-the-go für einen direkten Datenaustausch zwischen den mobilen Endgeräten könnten eigentlich für einen Einsatz des neuen Palm OS sprechen. Dennoch setzen die Hersteller bislang weiterhin auf Palm OS 5.x, so daß die Zukunft des Betriebssystems auf dem Smartphone-Sektor noch unklar ist. Auf der anderen Seite hat Palmsource angekündigt, daß eine künftige Version des

Palm OS Cobalt auf einem Linux-Kernel basieren wird. Dabei beabsichtigt Palmsource nicht die Offenlegung der Palm-Quellen, sondern die Erstellung einer Ebene oberhalb eines freien Linux-Kernels mit dem von Palm gewohnten Look & Feel und der Middleware. Als Beweggründe werden neuere und attraktivere Lizenzierungsmodelle genannt. Zudem glaube man an eine führende Rolle von Linux im Bereich der mobilen Geräte.

Im Vergleich zu Palm OS und Pocket PC bietet Symbian OS einen besseren Schutz. Das mobile Endgerät mit Symbian kann im Firmennetz mit Hilfe von Access-Control-Listen administriert werden; durch das Synchronisieren der Daten auf zugelassenen Servern läßt sich der Zugriff durch andere Management-Server unterbinden.

Fazit: Schon die üblichen Lizenzkosten legen die Benutzung eines freien Betriebssystems wie Linux nahe; dessen Sicherheitsvorteile verstärken diesen Trend noch, so daß in Zukunft mehr aus diesem Bereich zu erwarten sein wird. (we)