Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Studienarbeit

Sichere Übertragung im WLan mit mobilen Endgeräten (speziell unter Linux)

vorgelegt von
Lars Mählmann
am 11. August 2004

Studiengang Softwaretechnik

Betreuender Prüfer: Prof. Dr. Kai von Luck

Fachbereich Elektrotechnik und Informatik
Department of Electrical Engineering and Computer Science

Inhaltsverzeichnis

1. Einleitung **4**

2. Szenario **6**

3. Analyse **9**

3.1. Analyse 9

Probleme der PDAs lokal 9

Probleme der PDAs im WLAN 11

Systemanforderungen 12

Usability 14

Problemstellung bei WLan- Sicherheit 15

4. Design **16**

Ziel 16

Lösungsstrategie 16

Client-Server Architektur 17

Grobdesign Gesamtsystem 18

Die einzelnen Komponenten 19

Feindesign Mobiler Anteil 23

5. Prototyp/Realisierung **26**

SimPad SL 27

Linux und SimPad 28

Ausblick 29

6. Fazit **30**

Ausblick 31

A. Anhang **33**

Literaturverzeichnis **39**

Abbildungsverzeichnis

2.1. Angebote an den Gast 6
2.2. Check - in des Gastes 7
2.3. Checkout des Gastes 8

4.1. Möglichkeiten der Architektur 17
4.2. Netzwerkansicht für den Ferienclub 19
4.3. Komponentenmodel zur Netzwerkstruktur 20
4.4. Komponentenmodel zur Netzwerkstruktur 21
4.5. ein VPNTunnel in einem WLan-Netz 22
4.6. Ablauf einer Anmeldung mit einem mobilen Endgerät 24

5.1. Komponenten für das mobile Endgerät 26
5.2. das Simpad SL4 27
5.3. das Simpad SL4 mit Opie 28

1. Einleitung

> ***High-Speed-Internet im Hotel***
> *Vergessen Sie langsame Modems, Telefonadapter, kompliziertes Übertragen von Daten mit Ihrem Mobiltelefon - Die neue Technik Wireless LAN, die in den meisten neueren Notebooks von Haus aus schon integriert ist, machts möglich! Surfen und arbeiten Sie auf Ihren Reisen kabellos mit bis zu 11 MBit/Sekunde. Die mit Wireless LAN ausgerüsteten Hotels finden Sie unter www.WLAN-Germany.com. Buchen Sie dort mit hotel.de Ihre nächste Geschäftsreise und freuen Sie sich auf effizientes Arbeiten.* (hotel.de 2004)

Solche Anzeigen oder Ähnliche findet man inzwischen immer häufiger in Verbindung mit Urlaubsangeboten in Ferienclubs oder für Geschäftsleute. Viele Hotels bieten Wireless LAN als feste Service-Leistung für die Gäste an. Sei es für einen kurzen Blick auf die eMails des heutigen Tages, die Wettervorhersage oder überarbeitete Präsentationen die im Internet zur Verfügung gestellt werden.
Funknetze bringen bei aller Einfachheit der Technik auch gewisse Risiken mit sich. Eines dieser Risiken ist die Sicherheit des Netzwerkes und der mobilen Endgeräte. In diesem Dokument soll erörtert werden, wo die Probleme liegen und wie diese gelöst werden können.

Mobile Multimedia

Neue Fortschritte in der drahtlosen Netzwerkanschlußtechnologie und der rasanten Entwicklung bei mobilen Entgeräten führt zu einem neuen Service: dem sogenannten *mobile Multimedia*, darunter versteht man die individuelle Datenverarbeitung und Kommunikation über Funknetze mit Hilfe von kleinen und leistungsstarken Geräten, wie z.B. PDAs,Laptops oder Handys. Die damit verbunden Probleme: beschränkte Ressourcen(z.B. Batteriebetrieb), die verschiedenen Datenformate, Verarbeitung von einer grossen Menge Informationen oder auch teilweise klimatische Bedingungen, werden unter diesem Begriff zusammengefasst. Mit *mobile Multimedia* versucht man ein leistungstarken Handheld zu entwickeln, der diesen Anforderungen gerecht wird.(Havinga (2000))
Der Bereich von mobiler Unterhaltung und Multimedia(Musik,Film) ist sehr breit gefächert und wird zusätzlich erweitert durch Informations- und Kommunikationstechnologien. Der Zugriff auf diese unterschiedlichen Angebote soll durch mobile Multimedia abgedeckt werden.

Ferienclubs oder Hotels nutzen diesen Service, um ihren Gästen noch mehr Komfort zu bieten und stellen den Gästen ein Funknetz oder auch die jeweiligen Geräte zur Verfügung.

RoadMap

Im ersten Teil der Arbeit soll in einem Szenario dargestellt werden, welche Situationen in einem Ferienclub sein könnte und wie sich diese für die einzelnen Rollen (beteiligten Akteure) darstellt.Ich nehme dabei Bezug auf die Diplomarbeit von Andre Lüpke „Entwurf einer Sicherheitsarchitektur für den Einsatz mobiler Endgeräte“ (Lüpke 2004). Es soll erklärt werden, wie das Funknetzt genutzt wird und welche Art von Geräten zum Einsatz kommen.

Der nächste Abschnitt beschreibt die einzelnen Probleme und Sicherheitsanforderungen, die aus dem beschriebenen Szenario entstehen. Es soll aufgezeigt werden, wo die Probleme von WLan liegen und welche Sicherheitsrisiken und Gefahren damit verbunden sind. Weiter soll die Problematik veranschaulicht werden, die ein PDA mit sich bringt und welche Sicherheitsprobleme damit auftreten.

Als nächstes werden grundsätzliche Lösungsstrategien vorgestellt und in das Szenario eingebunden. An Hand von Sequenzdiagrammen und Anwendungsfällen werden die Lösungsstrategien auf ihre Vor- und Nachteile untersucht und die Folgen für das „Feriennetz“. Dabei wird im Speziellen ein Endgerät mit Linux als Betriebsystem betrachtet. Es soll geprüft werden, wie man mit Linux ein mobiles Endgerät sicher machen kann in Bezug auf die Anforderung die ein Ferienclub bzw. die Gäste an das Gerät stellen.

Im darauffolgenden Kapitel wird ein Prototype vorgestellt mit dem die vorher beschriebenen Thematiken umgesetzt und veranschaulicht werden. Es wird dargestellt in wie weit die Umsetzung möglich war, welche Probleme entstanden sind und welche Probleme neu entstanden sind.

Als letztes wird Fazit gezogen, was erreicht wurde und was noch offen geblieben ist. Desweiteren wird ein Ausblick darüber gegeben, wie die Zukunft der präsentierten Lösung aussehen könnte.

2. Szenario

In dem folgenden Beispiel beziehe ich mich auf den von Andre Lüpcke dargestellten fiktiven Ferienclub aus seiner Diplomarbeit (Lüpke 2004). In diesem Beispielszenario geht es um einen Ferienclub, der seinen Gästen die Möglichkeit bieten möchte, bestimmte Dienste über ein gelie- henes mobiles Endgerät ortsunabhängig nutzen zu können. Die Urlauber des Clubs erhalten dazu beim Einchecken, wenn sie sich eindeutig identifiziert haben, einen PDA über den sie diese Dienste in Anspruch nehmen können. Folgende Dienste möchte das Hotel, beispielsweise, den Gästen zur Verfügung stellen (siehe Abildung 2, Andre Lüpcke (Lüpke 2004)):

- Es soll ein Internetzugang zur Verfügung stehen
- Der Veranstaltungskalender des Clubes
- ein GPS-System für Ausflüge in der Umgebung
- als ein Reiseführer für die Umgebung
- Übersetzungsprogramm, Währungsumrechner
- einen Adressbuch für wichtige Ansprechpartner, wie z.B. Gästebetreuung, Ärtzte oder sogenannte Drittanbieter(Autovermietung).
- Kalender mit Erinnerungsfunktion für Reinigungszeiten, Abendessen, Kinderbetreuung oder für gebuchte Ausflüge

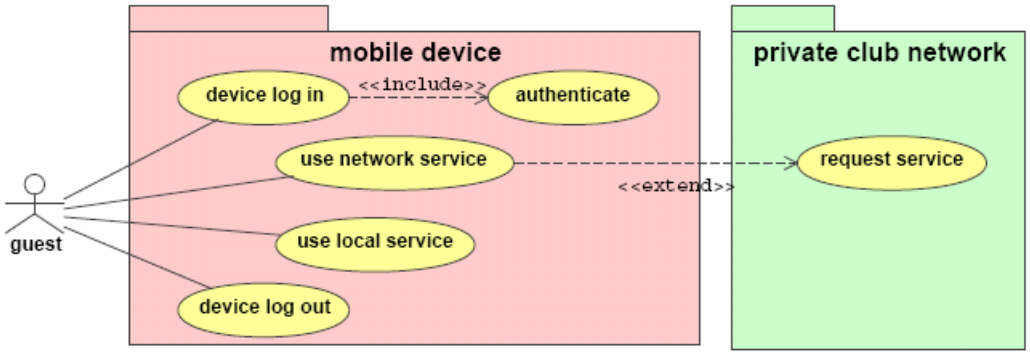

Abbildung 2.1.: Angebote an den Gast

Daraus ergeben sich sicherheitsrelevante Probleme, die im weiteren Verlauf genauer dargestellt werden sollen. Der Ablauf beim Verleih von so einem Gerät könnte folgendermassen ausssehen:

Der Gast bucht in einem Reisebüro oder direkt bei dem Ferienclub eine Reise über einen bestimmten Zeitraum, wobei sich daraus schon ergeben kann, welche Angebote für den Gast interessant sein dürften (soziale Stellung: Familie, Paare oder Singles), die beim Urlaub zur Verfügung stehen.

Wenn der Gast sich im Urlaub im Club anmeldet, wird ihm ein PDA zur Verfügung gestellt, über welchen der Gast sämtliche organisatorischen sowie informellen Fragen, Informationen oder Probleme lösen kann (siehe Abildung 2 nach Andre Lüpcke (Lüpke (2004))). Das kann zusätzlich die Vermittlung an Drittanbieter beinhalten, welche in Verbindung mit dem Hotel besondere Konditionen anbieten, da durch das Hotel und die Benutzung von *mobile Multimedia* eine Sicherheit darüber besteht, wer der Gast ist und das die Nutzung des Angebotes einfach ist. Dabei gibt es die Möglichkeit, das die Buchung direkt zwischen Gast und Anbieter erfolgt oder das Hotel die gesamte Organisation über deren Netz übernimmt.

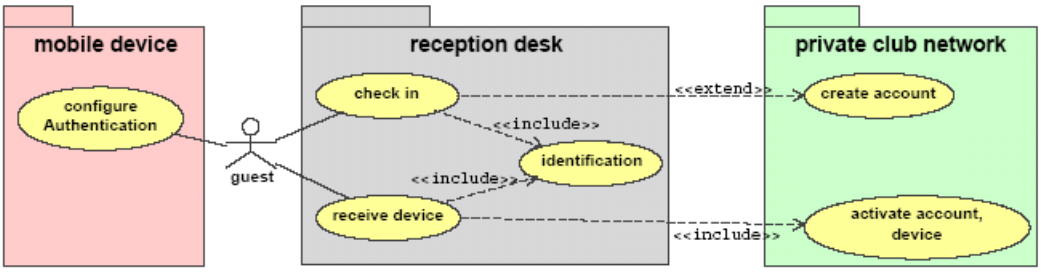

Abbildung 2.2.: Check - in des Gastes

Während des Aufenthaltes auf dem Gelände des Ferienclubs steht dem Gast ein Zugriff auf das Intranet des Clubes über ein WLan-Netz zur Verfügung. Desweiteren soll auch über das WLan der Zugriff auf das Internet vorhanden sein. Bei der Abreise wird das Gerät an der Rezeption wieder abgegeben und für den nächsten Gast vorbereitet(siehe Abbildung 2 nach Andre Lüpke (Lüpke (2004))).

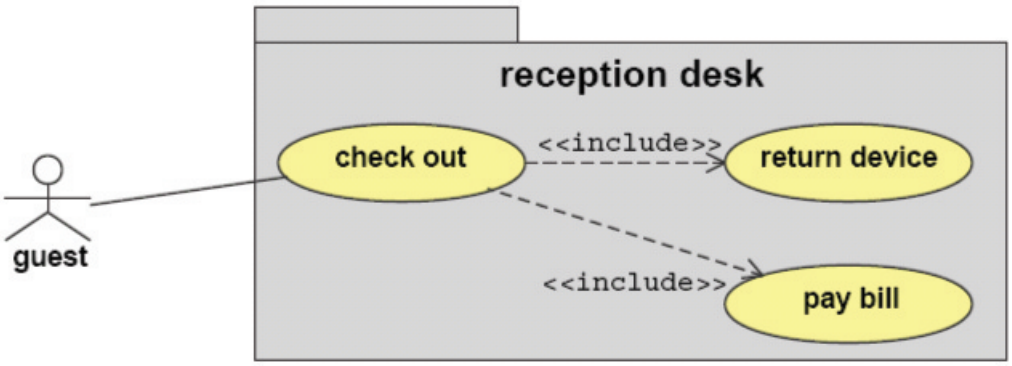

Abbildung 2.3.: Checkout des Gastes

3. Analyse

3.1. Analyse

In diesem Kapitel soll im folgenden die Sicherheitsproblematik eines PDAs im Ferienclub aufgezeigt und erklärt werden. Dabei ist zwischen den lokalen Problemen zu unterscheiden, das heisst, wie ist die Situation auf dem Gerät und muss was alles bedacht werden, und zum anderen die Sicherheitsaspekte im Netzwerk des Ferienclubs, die nicht nur den PDA lokal betreffen, sondern zusätzlich den Netzwerkverkehr zwischen dem PDA und dem „Clubserver“.

Probleme der PDAs lokal

Wenn der PDA an der Rezeption dem Gast ausgehändigt wird, muss für den Schutz der Daten des Benutzers die Software auf dem Gerät und für das Gerät selber Sorge getragen werden. Es gibt dabei mehrere Risikofaktoren, die zu beachten sind.

Funktionssicherheit, Software sollte nicht installiert oder gefälscht werden

Die installierte Software auf dem Gerät, welche zum Benutzen des Gerätes dient, muss geschützt werden, sei es vor Missbrauch oder falscher Bedienung. Es wäre vorstellbar, dass bei einer Famile das Kind mit dem Gerät „herumspielt“ und versehntlich die Softwareeinstellung verändert oder löscht.

Eine weitere Schwierigkeit besteht darin, dass der Gast keine eigenen Programme auf dem Gerät benutzen darf, um die Funktionstüchtigkeit des Gerätes nicht zu gefährden. Da auf dem Gelände eine Anbindung an das Hotelnetz und das Internet besteht, darf es nicht die Möglichkeit geben das Ferienclubnetz mit der aufgespielten Software zu verändern oder den Internetzugang für kriminelle Aktivitäten zu missbrauchen. Es wäre weiterhin vorstellbar, die installierten Programme so zu verändern, dass man andere Gäste des Ferienclubs behindert.

Datensicherheit

Es muss gewährleistet sein, dass die Software auf dem PDA nicht durch Fehler der Software in Zustände gebracht werden kann, in denen der Benutzer die Funktionalität verändern kann oder Zugriff auf andere Resourcen erhält.

Datenintegrität

Die Daten auf dem PDA dürfen nicht verändert oder gelöscht werden. Es darf nicht möglich sein sicherheitsrelevante Daten, wie z.B. Sicherheitszertifikate oder Benutzerkennungen, zu löschen oder zu verändern. Evtl. temporär gespeicherte Daten dürfen nicht lesbar sein und der Hauptspeicher sowie der Cache dürfen nicht veränderbar oder auslesbar sein.

Wichtig ist in diesem Zusammenhang auch die Konfiguration des Gerätes für den Betrieb im Ferienclub. Dazu gehören Netzwerkeinstellungen des WLans, Grundkonfigurationen wie z.B. Authentifizierungsdaten, Tastaturlayout, Spracheinstellungen.

Daten, die vom Ferienclub zur Verfügung gestellt worden sind, wie Notfallrufnummern, Adressen, etc., müssen geschützt sein.

Changedesk, Konfigurations-Managment

Eine weitere Problemquelle bietet die Aktualisierung der Softwarepakete und Sicherheitsupdates des Gerätes. Soll es in dem Club möglich sein, die eigenen eMails abrufen zu können, muss sichergestellt werden, dass keine aktuellen Viren oder Würmer auf das Gerät gelangen können. Weiter muss es möglich sein Mängel (Bugs) der vorhandenen Software zu beheben oder Programmaktualisierungen einzuspielen. Diese Problemestellung wird hier nicht weiter behandelt.

Systemverfügbarkeit

Das System sollte sicher sein vor Angriffen aus dem Internet. Werden von dem Gast aus dem WLan heraus Internetseiten aufgerufen, welche beispielsweise mobilen Code (Java Scropts) enthalten, muss gewährleistet sein, dass dieser Code auf dem Gerät nicht zu Systemabstürzen oder zu Sicherheitsproblemen führen kann. Ebenfalls muss sicher gestellt sein, dass einzelne Komponenten des PDAs, dessen Stablilität oder dessen Daten nicht gefährdet.

Diebstahl des Gerätes

Bei Diebstahl des Gerätes darf es für den Dieb nicht möglich sein, an die Daten des auf dem gestohlenen Gerätes heranzukommen. Es muss verhindert werden, dass die Daten des Gerätes nur durch Zugriff als „normaler“ Benutzer gefährdet werden. Weitherhin muss verhindert werden, dass man die Daten durch ein Rücksetzen in den Urzustand erhält. Die Datensicherheit muss auch bei Diebstahl gewährleistet sein. Bei Diebstahl muss der Benutzeraccount des PDAs im Hotelnetzwerk gesperrt werden können, damit auf dem Gelände der PDA nicht missbraucht werden kann.

Ausfall der Geräte

Ein Ausfall der Geräte kann nicht vermieden werden, aber durch vorzeitige Warnungen des Gerätes, auf Grund von Systemmeldungen, sollte es möglich sein, dem Ausfall beim Gast vorzugreifen und das Gerät frühzeitig auszutauschen. Das ist sinnvoll da man nicht sagen kann, wie sich der Ausfall einzelner Komponenten (Hard- oder Software) bemerkbar macht.

Probleme der PDAs im WLAN

Zu den oben beschriebenen Problemen auf dem PDA kommt die Problematik des Funknetzes noch hinzu. Das bedeutet im Wesentlichen, dass es grösser Probleme mit dem Funknetz selber geben kann oder die Gefahr des unerlaubte Mitlesen von Dritten im Netzwerk. Ebenso kann es zu unerlaubten Benutzen des WLans kommen. Die einzelnen Punkte werden hier genauer beschrieben.

Verfügbarkeit, Technische Probleme bei WLan

Ebenso wie die im oberen Kapitel beschriebene Problematik der lokalen Verfügbarkeit des PDAs, gibt es die dargestellte Problematik im WLan, wo diese sogar noch eine höhere Bedeutung erlangt, als auf dem PDA. Da es den Gästen überall auf dem Gelände möglich sein soll, während ihres Aufenthaltes Zugriff auf das Intranet zu haben, sollte das gesamte Netz sicher sein vor Störsendern, seien es baulichen Problemen oder auch Angreifern von aussen, welche versuchen in das Netz einzudringen. Ein weiterer Punkt ist die Performance des Netzes. Ist das Netz in der der Lage genügend Bandbreite zur Verfügung zu stellen, um allen Gästen ein komfortables „surfen“ zu ermöglichen und dabei zusätzlich sicher zu stellen

, dass das Netz nicht durch einen „Denial of Service“ [1] ausfällt. Eine Folge bei Ausfällen des Netzwerkes könnte ein Abbruch oder Misslingen von Transaktionen des Gastes sein und dass die Buchung einer Veranstaltung sich in einem nicht definierten Zustand befindet oder fremde Personen Zugang zu den Daten des Gastes bekommen. Ausserdem sollte beachtet werden, dass ein Gast im Urlaub durch diese Zustände verärgert wird und dieses Angebot nicht mehr in Anspruch nehmen wird.

Vertraulichkeit

Wenn der Gast Interesse an einzelnen Angeboten des Ferienclubs hat und diese buchen möchte, sollte dieser sicher sein können, dass die Daten an den Hotelserver gesendet werden und nicht von einer dritten Person gelesen werden.

Integrität

Der Gast reserviert für seine Familie einen Ausflug und sendet diese Daten an das System, dabei muss sichergestellt werden, dass ein weiterer Gast nicht die Möglichkeit hat die Daten dahingehend zu verändern, dass er ebenfalls mit auf der Reservierung auftaucht und damit die Daten nachträglich verändert. Es muss unmöglich sein nach dem Absenden der Daten diese zu verändern.

Authentizität

Werden vom Hotel Reservierungen, Wünsche oder andere Daten angenommen muss nachweisbar sein, von wem die Daten versendet worden sind und das dieses Person diesen Service nutzen darf. Es sollte protokollierbar sein wer, wann, was gesendet hat, um bei einem Missbrauch des Netzes auf diese Daten zurückgreifen zu können.

Systemanforderungen

Bei den genannten Problemen ging es um die Sicherheit des Netzwerkes und des PDAs. Aber zusätzlich ist zu bedenken, wie das vorgestellte Szenario in die Realität umgesetzt werden kann.

Dabei sind verschiedene Punkte, Probleme zu berücksichtigen:

[1] DoS (Denial of Service) oder DDoS (Distributed Denial of Service) sind Angriffe auf Server mit dem Ziel sie und ihre Dienste arbeitsunfähig zu machen.(dos 2004)

- Wartbarkeit
- Lebensdauer, Erweiterbarkeit
- Zuverlässigkeit
- Dokumentation

Wartbarkeit

Die Pflege des „virtuellen Ferienclubes“ im laufenden Betrieb muss sichergestellt sein. Wenn in der Hauptsaison einzelne Dienste des System ausfallen, muss es möglich sein diese ohne Auswirkungen auf den Gästeverkehr und zusätzliches Personal die Reparaturen durchzuführen oder im Falle des Ausfalles eines PDAs beim Gast diesen schnell zu reparieren oder für Ersatz sorgen zu können.

Lebensdauer, Erweiterbarkeit

Der „virtuellen Ferienclub“ sollte nicht für eine einzige Saison, sondern muss für einen längern Zeitraum ausgelegt sein . Das betrifft zum einen die Sicherheitsanforderungen, welche auf dem aktuellen Stand gehalten werden müssen und die mobilen Geräte, die extremen Belastungen durch die Vielzahl an Gästen und der Umgebung (z.B. Strand) ausgesetzt sind. Weiterhin ist die Erweitbarkeit für neue Serviceleistungen und Techniken zu gewährleisten. Das System sollte nicht von einem einzigen Anbieter abhängig sein, sondern eher auf standartisierten Lösungen beruhen. Eine Möglichkeit dazu könnte ein Open Source Projekt sein, welches eine breite Plattform von Anwendern und Entwicklern hat und somit eine gewisse Stabilität vorweisen kann.

Zuverlässigkeit

Das System funktioniert unter grosser Belastung ebenso wie mit wenig Auslastung. Die Performance darf für den Gast nicht unterschiedlich sein, sondern sollte auf Grund der Usability immer gut sein.

Dokumentation

Egal wie gut die Endgeräte und Dienste benutzbar sind, es muss eine ausführliche und gut verständliche Dokumentation geben. Bei Problemen in dem System steht diese als Anfangspunkt zur Verfügung, um das System zu verstehen und einzelne Designpunkte nachvollziehen zu können. Gut in diesem Zusammenhang wäre eine standartisierte Lösung, weil somit eine breite „Communitiy“ vorhanden ist, welche eine grosse Erfahrung zur Verfügung stellen kann.

Usability

Es sollte aber trotz der Risikobedenken und der geschilderten Probleme bedacht werden, dass der PDA für den Gast auch benutzbar bleibt. Es muss sicher gestellt sein, dass auch weniger technisch versierte Personen das Gerät bequem bedienen können. Die Sicherheitsaspekte haben nur dann einen Sinn, wenn das Gerät benutzt wird. Daher darf dem Gast keine 20stellige Pincode oder dergleichen aufgezwungen werden, wenn dieser sich im Hotelnetz anmelden möchte. Die Sicherheitsproblematik darf sich nicht zu Ungunsten des Gastes auswirken, da dieser den angebotenen Service sonst nicht nutzen wird.

Problemstellung bei WLan- Sicherheit

In der Analyse geht es darum ein sichere WLan zu entwickeln und es vor unbefugten Zugriffen von aussen abzusichern. Aber warum wird dieses nötig und warum nicht die vom Hersteller bei der Hardware mitgelieferte Sicherheitspaket benutzten? Ein WLan kennt keine physikalischen Grenzen wie Türen, Wände oder Bäume. Es ist möglich sich ausserhalb des Hotelgeländes zu bewegen und durch die Reichweite des Funknetzes diese auch ausserhalb zu benutzen und in das System einzudringen und angebotenen Dienste für sich zu nutzen.

> Die von den Herstellern in diesem Rahmen implementierten Sicherheitseinrichtungen reichen nicht aus, um die gesetzlich geforderten Schutzziele zu erfüllen(Kühn und Möller 2003)

In dem Bericht des Datenschutzbeauftragten von Hamburg wird erklärt, warum die Sicherheitseinrichtungen der Hersteller nicht ausreichen. (Datenschutz Hamburg (Kühn und Möller 2003)) Ich möchte an dieser Stelle nur kurz einen kleinen Einblick geben.

Es gibt drei Sicherheitsvorkehrungen:

- WEP (Wireless Equivalent Protected) : Mit Hilfe von WEP werden die Daten während der Funkübertragung mit 64 (effektiv 40) oder 128 (effektiv 104) Bit verschlüsselt. Seit 2001 ist es möglich durch Mithören von genügend großer Datenmenge den Schlüssel zu „knacken“.
- Versteckte SSID (Service Set Identifier): Mit dessen Hilfe ist es möglich den Acess Point vor fremden Clients zu verstecken. Die SSID wird aber regelmässig im Netzwerktraffic mitgesendet und somit abhörbar.
- MAC-Filterliste sind aus Ethernet bekannt und können im WLan ebenso geändert werden wie dort.

Bis zu dem heutigen Zeitpunk sind diese Sicherheitslöcher trotz der Weiterentwicklung des Standards IEEE 802.11 nicht behoben worden und können nicht als Sicherheitsvorkehrung gegen Angriffe auf das Netzwerk dienen.

4. Design

Im folgenden Kapitel wird dargestellt: Wie das Netzwerk des Ferienclubes aussehen könnte, beziehungsweise welche Möglichkeiten sich bieten um das angestrebte Szenario zu erreichen. Es sollen mehrere Lösungsstrategien vorgestellt werden, diskutiert werden wie diese in einem „virtuellen Ferienclub“ genutzt werden können und welche Komponenten dabei harmonieren und wie Linux als Betriebssystem auf dem PDA genutzt werden kann und die Vorteile die sich daraus ergeben.

Ziel

Bei den beschriebenen Sicherheitsbedenken aus der Analyse entstehen mehrere Anforderungen, die vom BSI folgendermassen beschrieben wurde:

> Absicherung der Clients insbesondere bei mobilen Clients, die sich in verschiedene Funk-LANs einbuchen können, sollten weitere lokale Schutzmaßnahmen implementiert werden, wie z. B.: Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc. (BSI 2003)

Lösungsstrategie

Als wichtiger Punkt in dem Aufbau des Sicherheitssystems sollte gesagt werden, dass der Schutz der Daten nicht teurer sein sollte als die Daten wert sind. Unterschieden wird die Lösung in den lokalen Teil, einem PDA, und dem Netzwerk hier der Ferienclub. Bei der weiteren Betrachtung einer Lösungsstrategie wird der technische Teil betrachtet und der soziale Anteil vernachlässigt, die einzelnen Rollen und Verantwortungen werden nicht direkt berücksichtigt.

Client-Server Architektur

Es ergibt sich die Frage, ob man ein sehr „schlanken“ Client und einen leistungstarken Server benutzt und somit die gesamte Rechenleistung auf den Server legt, um möglichst alles zentral zu verwalten. Der Vorteil liegt dabei dann in dem Administrationsaufwand für den Client, der damit sehr gering ausfällt und für den Gast als Anwender einfach bedienbar bleibt, da dessen Funktionalität eingegrenzt ist.

Die Alternative dazu wäre die Leistungsfähigkeit heutiger PDAs zu nutzen und mehr Applikationen auf den Client zu verteilen und somit den Server zu entlasten. Der Vorteil wäre dass der Gast auch ohne Zugriff auf das Hotelnetzwerk immer die Informationen zu seinem Urlaub „vorrätig“ hätte und eine höhere Mobilität erreicht. Damit muss aber die Sicherheit auf dem PDA erhöht werden, um zu gewährleisten, dass die verbesserte Mobilität nicht missbraucht werden kann.

In der Abbildung 4 sind mehrere Möglichkeiten der Abstufung zwischen einem schlanken Client und einem fat Client aufgeführt.

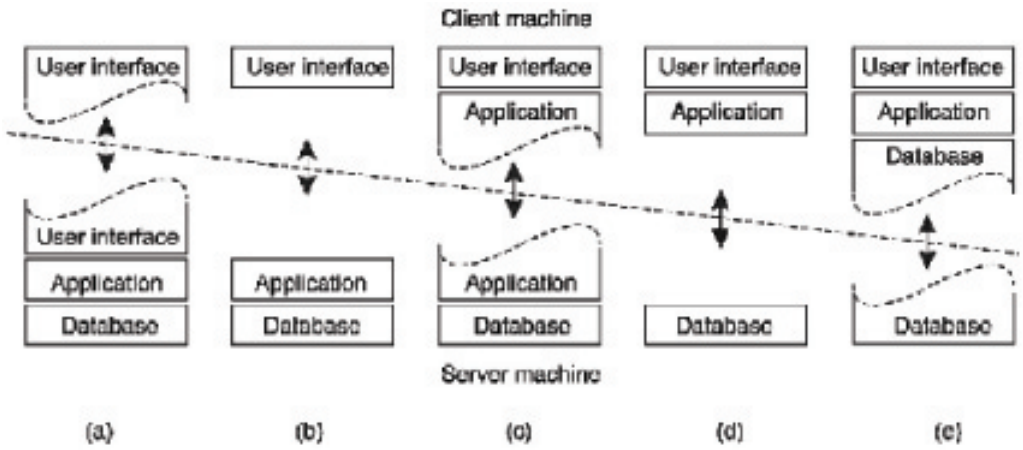

Abbildung 4.1.: Möglichkeiten der Architektur

Grobdesign Gesamtsystem

Eine mögliches Gesamtnetzwerk könnte wie folgt aussehen (siehe Abbildung 4): Das Gesamtsystem muss eine klare Trennung zwischen dem Wlan der Gäste und dem internen Hotelnetz vornehmen. Somit ist das Erlangen von internen Daten unterbunden. Der Netzwerkverkehr sollte über eine verschlüsselte Verbindungen im WLan stattfinden. Das Mithören von Netzwerkverkehr wird erschwert, wenn nicht sogar unmöglich. Für den Zugriff auf die angebotenen Dienste des Hotels muss der Gast sich authentifizieren. Der Zugriff darf nur aus dem internen Netz stattfinden, um das Risiko eines Missbrauchs oder Angriff auf das System von aussen zu verringern.

Die Gäste benutzen einen eigenen Internetzugang, um die Netzwerklast für das interne Hotelnetz nicht zu überlasten. Weiterhin wird der Schaden durch unbeabsichtigte Maleware (Viren,Würmer) von Hotelgäste, die sich auf dem Hotelnetz installieren, minimiert. Über die Firewall lassen sich restriktive Regel erstellen, damit die Gäste nur bestimmte Dienste wie Internet und Mail benutzen. Durch die Authentifizierung des Gastes bei Anmelden in das Netz ist der Zugriff unberechtigter Personen auf die Angebote des Clubs unterbunden.

Es bietet sich an eine demilitarisierte Zone (DMZ) einzuführen, in der die Server stehen, auf welchen die Angebote an die Clubgäste installiert sind. Der Gast hat auf diese Zone nur Zugriff im Clubnetz von seinem PDA aus.Dabei könnte der Zugriff über eine Applikation oder eine gesicherte Internetverbindung stattfinden. Dem Hotelpersonal wird der Zugriff auf die Daten nur über bestimmte Dienste wie SSL oder verschlüsselte Verbindungen erlaubt. Grundsätzlich ist jeder Verkehr aller Protokolle vom WLan und dem internen Netz verboten, sofern es nicht explizit erlaubt wird.

Komponentenentwurf

Der Komponentenentwurf beruht darauf, dass ein mobiles Endgerät zur Verfügung steht, welches die nachfolgend beschriebenen Eigenschaften erfüllt. Darunter fallen beispielseise Multiuserfähigkeit, verschlüsselte Verbindungen mit ssh und Rechteverwaltung bei der Softwareinstallation und Deinstallation. Der mobile Client muss zusätzlich über die nötige Hardware verfügen um eine Funkverbindung zu einem Access Point und somit in ein Netzwerk aufbauen zu können. Der vorgestellte Netzwerkentwurf kann in mehrere Komponenten unterteilt werden, die modular aufgebaut sind und miteinander kommunizieren. Der mobile Client soll als sogenannter „Fat-Client“ benutzt werden können. Es soll möglich sein Daten des Ferienclubs auf dem Gerät speichern zu können um somit auch ausserhalb des Hotels diese Daten zu benutzen (siehe Abbildung 4).

Folgende Komponenten werden benötigt um den Gästen eine sichere Verbindung zu den Hotelservicen anzubieten:

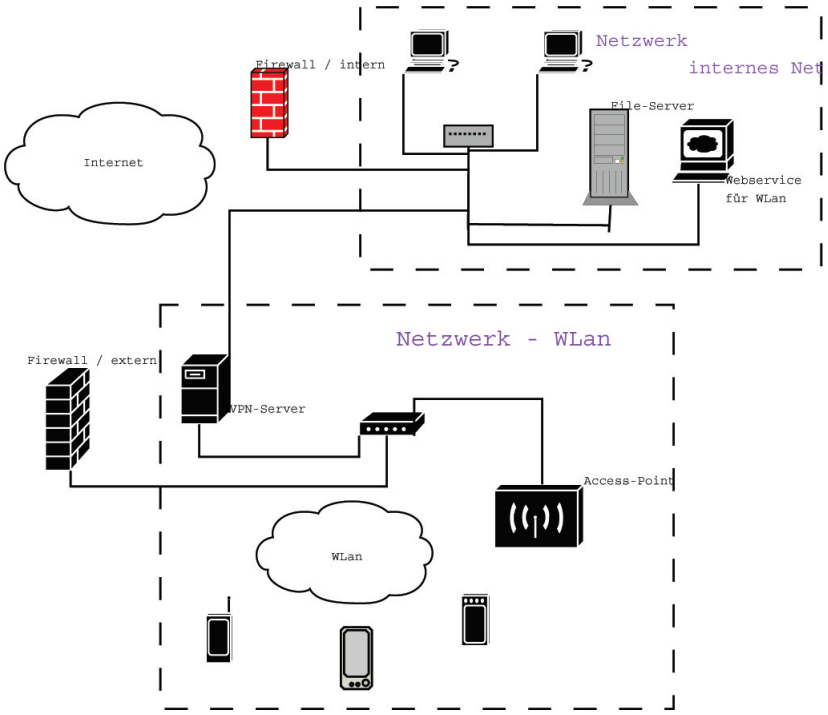

Abbildung 4.2.: Netzwerkansicht für den Ferienclub

- einen Access Point um eine Verbindung mit dem Netzwerk herstellen zu können.
- ein Secure Access mit dem die Daten im Netzwerkverschlüsselt werden und somit das „Mithören“ des Datenverkehrs unterbinden.
- ein Benutzerauthentifizierung im Netzwerkwerk sowie auf dem Client um unabhänig vom Hotelnetz den PDA auch ausserhalb des WLans nutzen zu können.
- im Netzwerk werden verschiedene Dienste angeboten wie z.B. Veranstaltungskalender, Internet, Drittanbieter, etc . . . .
- bei lokaler Nutzung werden Dienste, wie Kalender, Bildbetrachter zur Verfügung gestellt, die kein Netzwerk Zugriff benötigen.

Die einzelnen Komponenten

Es wird erklärt, wie die Komponenten aussehen, wie diese eingesetzt werden und warum. Bezugenommen wird dabei auf die Grafik 4.

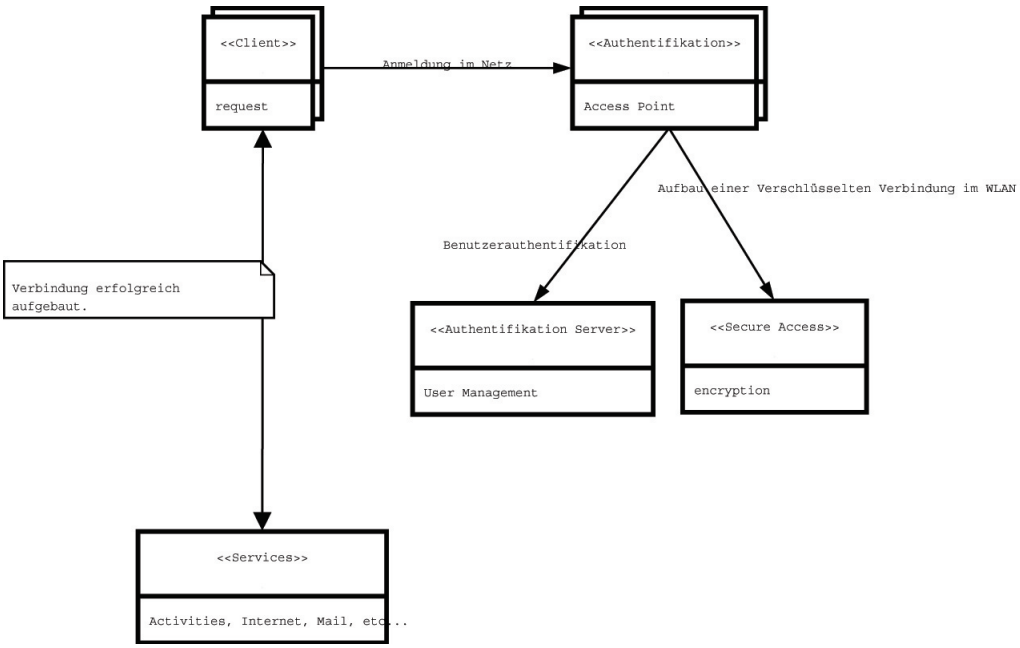

Abbildung 4.3.: Komponentenmodel zur Netzwerkstruktur

Access Point

Als Access Points kommen hier ein handelsübliche Router, die dem PDA Zugang zu dem Netzwerk des Ferienclubs ermöglichen und flächendeckend über das Clubgelände verteilt sind. Die Geräte unterstützen den Standard IEEE (Institute of Electrical and Electronics Engineers) 802.11. Die angebotenen Sicherheitsmöglichkeiten wie Mac-Filterung, verstecken der ESSID oder WEP-Verschlüsselungen werden eingeschaltet um die Sicherheit bei dem Access Point über dessen eigene Möglichkeiten zu erhöhen. Diese Massnahmen verhindern zwar nicht den Einbruch in ein Netzwerk, erschweren diesen aber.

Secure Access

Für die Verschlüsselung der Daten wird ein VPN-Server (Virtuelles Private Network) benutzt, der eine verschlüsselte Verbindung in dem Netzwerk gewährleistet (siehe Abbildung 4 von Florian Müller (Müller 2002)). Über den Access-Point baut der Client, in diesem Fall der PDA, eine Verbindung zu dem VPN-Server auf, welcher die Daten über einen sogenannten VPN-Tunnel verschlüsselt.

Eine VPN-Verschlüsselung hat den Vorteil, dass diese Technik schon vielfach in kabelgebundenen Netzwerken zu Einsatz gekommen ist und sich bewährt hat.

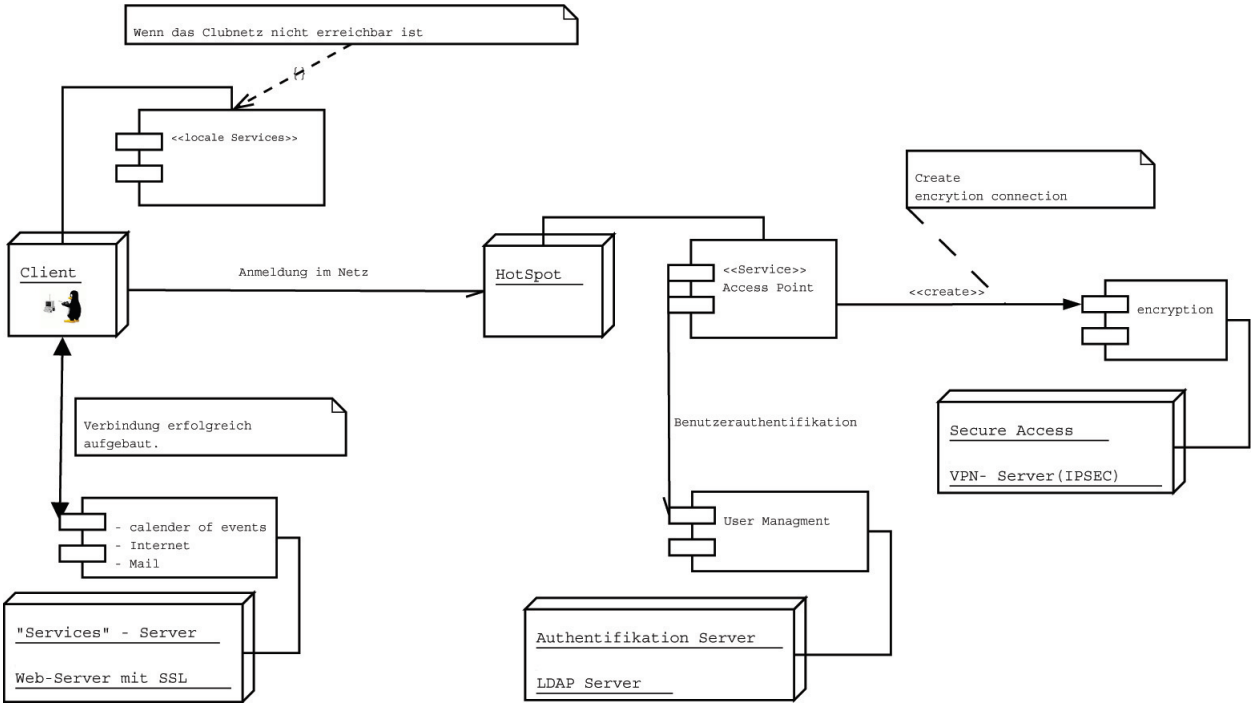

Abbildung 4.4.: Komponentenmodel zur Netzwerkstruktur

Benutzerauthentifizierung im Netzwerk

Die Benutzeranmeldung erfolgt mit Hilfe eines *Kerberosservers*. Der Kerberosserver vereinfacht durch sein Konzept der Ticketerstellung eine einfache Bedienung durch den Gast, da er sich nur einmal Anmelden muss, um die verschiedenen Dienste nutzen zu können. Da nicht jeder Gast „technisch versiert"ïst, wird somit gewährleistet, dass die Passwortabfrage zur Buchung von kostenpflichtigen Diensten so einfach wie möglich gehalten wird.

Ein weiterer Vorteil besteht darin, dass kein Passwort im Netzwerk übertragen wird, sondern nur auf dem PDA und dem Server „verglichen" wird. Es ist möglich, eine Unterscheidung bei der Ticketerstellung vorzunehmen. Denkbar ist z.B. eine Unterscheidung zwischen kostenlosen(z.B. Internetnutzung) und kostenpflichtigen Diensten (z.B. Tagesausflug) vorzunehmen.

Wie ein VPN-Server ist ein Kerberosserver eine bewährte Technik in Netzwerken und wird in verschiedenen Betriebssystemen zur Benutzerverwaltung eingesetzt (z.B. Windows 2000 Server).

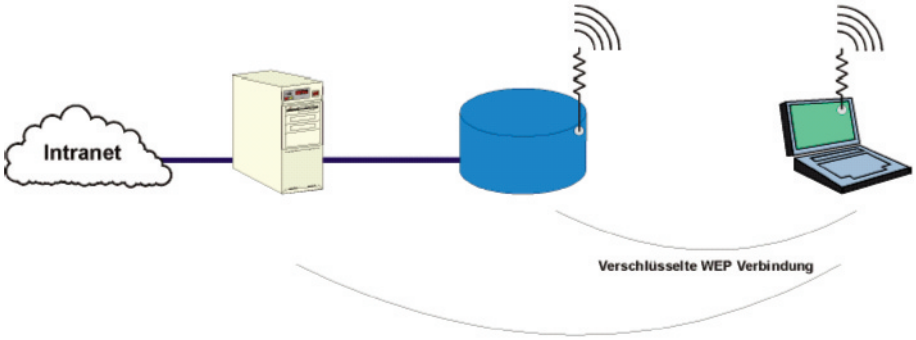

Abbildung 4.5.: ein VPNTunnel in einem WLan-Netz

Benutzerauthentifizierung lokal, auf dem PDA

Die Anmeldung lokal auf dem PDA erfolgt wie auf einem Desktop Linux System. Es erfolgt eine Einschränkung bei der Passwortwahl (z.B. mindestens sechs Zeichen, keine Wörter aus Wörterbüchern und Sonderzeichen wie *!*) und das Passwort wird verschlüsselt auf dem PDA hinterlegt (/etc/shadow). Das Passwort ist wie auf einem „herkömmlichen “ Linux nur durch den *Administrator (root)* zurücksetzbar. Um das Passwort synchron zur Netzwerkanmeldung zu halten, muss die Möglichkeit der Passwortänderung durch den Gast deaktiviert werden.

Bei einer Kompromitierung des Passwortes muss die Änderung an der Hotelrezeption vorgenommen werden. Bei einem gestohlenen PDA muss der Dieb den Account des Administrators erhalten und erhält auf Grund der verschlüsselten Passwörter keinen Zugriff auf die Daten des Gastes. Umgekehrt kann der Dieb nicht mit Hilfe des Benutzeraccounts die Konfiguration des PDAs auslesen.

Angebotene Dienste des Ferienclubs

Die Angebote im Ferienclub sollten attraktiv sein für alle Gäste und möglichst einfach bedienbar. Bei der Nutzung des Internets muss eine Wiedererkennung der graphischen Oberfläche bestehen, damit die Gäste auch das Angebot des Internets nutzen. Einfaches Starten der Internetanwendung und eine gute Verfügbarkeit sind wesentlich für die Nutzung. Damit wäre es möglich, einen Veranstaltungskalender ins Intranet zu stellen, der von den Gästen benutzt wird. Es wäre keine weitere Erklärung nötig, um die Bedienung des Veranstaltungskalenders zu ermöglichen. Ein Internetkalender, z.B. in dem Buchung eines Tennisplatzes möglich ist, könnte die Auslastung der Tennisplätze verbessern und wäre bequem vom „Pool“ aus zu buchen. Ein weiteres Angebot wäre die Nutzung der Geräte, um z.B. am Strand mit anderen Hotelgästen Computerspiele zu spielen auch die Verabredung zum Frühstück oder zum

Abendessen wären möglich. Die Verwaltung kann, wie von Andre Lüpke (Lüpke 2004) beschrieben, serverseitig stattfinden oder unter Linux in dem Profil auf dem PDA. Dort stehen Anwendungen, wie Adressbuch und Terminkalender zur Verfügung, um die persönlichen Daten zu verwalten.

Auf dem PDA kann man dem Gast alles zur Verfügung stellen was dem Gast die Benutzung des PDAs erleichtert, wie z.B. die Bedienung in der Landessprache des Urlaubers. Es muss eine Hilfe vorhanden sein, die angepasst ist auf die Grösse des Displays und, wenn nötig, den Benutzer interaktiv durch die einzelnen Dialoge führt. Es kann den Urlauber ausserhalb des Ferienclubes Unterstützung bieten, wie einen Stadtplan und Touristenführer, um auf Besonderheiten und besondere Gepflogenheiten in Restaurants (z.B. Höhe des Trinkgeldes) aufmerksam zu machen. Es kann auch bei Tagesausflügen mit dem geliehenen Auto ein GPS anbieten. Bei genügend grossem Speicher ist es möglich zusätzlich als *mp3-Player* zu dienen. Bei Urlaubern mit digitaler Kamera wird es möglich, Urlaubsphotos „auszulagern“ und später an der Rezeption als Bildabzug ausdrucken zu lassen. Serviceinformationen, wie Erinnerungsfunktion und Memos oder Wetterbericht etc, können vom Hotel im Intranet angeboten und zur späteren Nutzung auf dem PDA abgelegt werden.

Feindesign Mobiler Anteil

Auf dem Linux PDA gibt es eine Vielzahl von Programmen, die man vom *Windows CE Betriebssystem* bekannt sind und somit eine gute Bedienbarkeit ermöglichen. Der Vorteil bei vielen Anwendungen wie z.B. *PIM* (sogenannte Officeanwendungen) sind durch die Benutzerverwaltung personalisierbar und können von dem Gast auch ausserhalb des Ferienclubs benutzt werden. Auf Grund einer Benutzerverwaltung auf dem Gerät ist ein größeres Angebot von Leistungen verfügbar, da die Systemeinstellungen für die einzelnen Anwendungen dem Gast nicht zugänglich sind und somit nicht veränderbar. Denkbarbar wäre z.B. durch unsachgemässe Bedienung, sei es vielleicht durch die Kinder einer Familie oder mit Absicht. Der Aufwand zur Administration kann dadurch als sehr gering eingestuft werden. Zusätzlich ist es möglich, den PDA mit einem unterschiedlichen Profil für verschiedene Kategorien von Urlaubern vorzubereiten (Familien, Singel oder Paare).

Bei Diebstahl kommen Diebe nicht einfach an die Systemkonfigurationen des Hotels oder die Daten der Gäste. Ein „einfacher“ Hardwarereset reicht nicht aus. Das Passwort des Administrators (*root*) zu erhalten ist nur unter zur Hilfe nahme von Werkzeugen wie bei Linux Desktopsystemen möglich, was aber durch die Aktualisierung des Systemes (*Sicherheitspatches*) zusätzlich erschwert werden kann. Das Passwort des Gastes zu erfahren wird dadurch erschwert, dass dieses verschlüsselt im Dateisystem abgelegt sind. Hiermit wird es schwerer für den Dieb das Gerät als Werkzeug zum Einbruch in das Hotelnetzwerk zu missbrauchen (wenn der Diebstahl vom Gast noch nicht gemeldet wurde, z.B. auf Tagesausflügen).

Weiterhin ist es für den „einfachen Benutzer“ nicht erlaubt Geräteeinstellung zu verändern (Einstellung des WLan-Netzwerkes, . . .).

Im Fall eines Ausfalles der Software kann an der Rezeption des Hotels innerhalb kürzester Zeit ein neues *Image* des Gerätes aufgespielt werden, was nach einer Schulung durch die Techniker auch von anderen Hotelangestellten durchgeführt werden kann, wodurch die Wartung vereinfacht wird.

Sequenzdiagramme

Die Anmeldung eines Gastes könnte wie folgt aussehen(4):

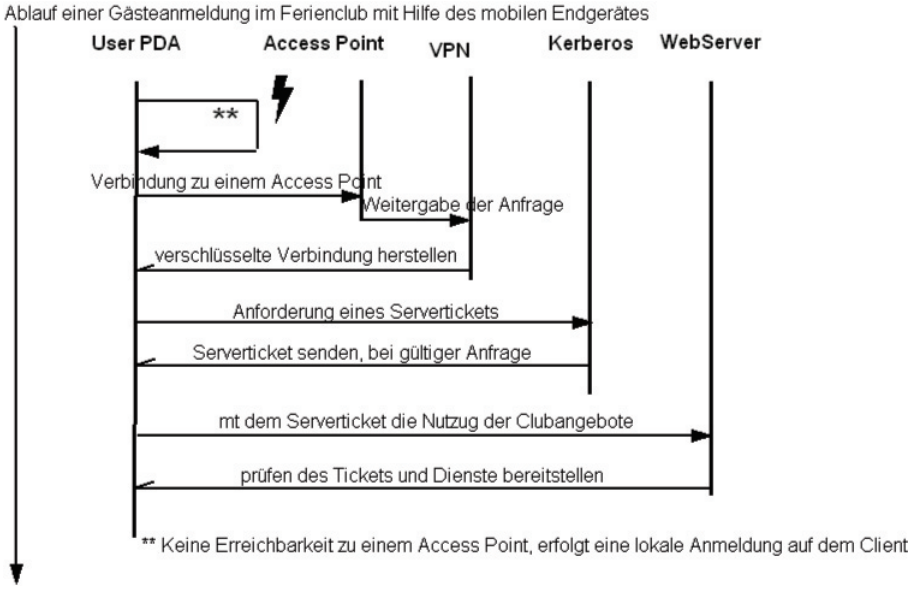

Abbildung 4.6.: Ablauf einer Anmeldung mit einem mobilen Endgerät

- Der Gast befindet sich nicht auf dem Feriengelände und hat somit keinen Zugriff auf das WLan. Er kann sich mit seinem Passwort lokal auf dem PDA anmelden und diesen wie ein „herkömmlichen PDA“ nutzen.
- Auf dem Feriengelände wird eine Verbindung zu einem *Hotspot* aufgebaut.
- Der *Hotspot* prüft, ob es ein gültiges Gerät des Ferienclub ist.
- Ist die Authentifizierung des Gerätes erfolgreich, wird die Anfrage des PDAs an den *VPN-Server* weitergeleitet.
- Der PDA baut eine Verbindung zu dem *VPN-Server* auf und hat somit eine verschlüsselte Verbindung zu dem Netzwerk aufgebaut.

- Der nächste Schritt ist die Anmeldung des Gastes, um die Dienste im Club nutzen zu können. Es wird eine Anfrage an den *Benutzerauthentifizierungsserver* gestellt, wo das Passwort des Gastes abgefragt wird, mit welchem der Gast sich im Netzwerk und auf dem PDA selbst anmeldet.
- Bei erfolgreicher Anmeldung wird ein „Ticket“ erstellt, mit dem der Gast die Angebote des Ferienclubes nutzen kann.
- An dem Webserver wird als letzter Schritt das Ticket auf Gültigkeit überprüft.

Der Gast bleibt solange in dem Netzwerk angemeldet, bis er sich ausserhalb der Reichweite der *Hotspots* befindet. Eine weitere Möglichkeit der Abmeldung besteht durch eine explizite Abmeldung des Gastes am PDA. Das Ticket selber hat nur eine bestimmte Gültigkeitsdauer, die sich selbst maximal zweimal verlängern kann. Danach muss sich der Gast wieder neu anmelden.

5. Prototyp/Realisierung

Dieses Kapitel beschreibt, wie die im oberen Kapitel beschriebene Lösung auf einem mobilen Endgerät umgesetzt wurde. Der Schwerpunkt liegt dabei auf dem Client.

Der Client soll als „mobiles Endgerät“ innerhalb des Funknetzwerkes benutzt werden können und zusätzlich soll es möglich sein die Daten auf dem Hotelserver mit denen auf dem PDA abzugleichen. Der Vorteil ist das der Gast die Möglichkeit hat ausserhalb des Ferienclubes sich über Angebote und Veranstaltungen zu informieren oder zusätzlich über Änderungen und Mitteilung informiert zu sein. Um diese Anforderungen zu erfüllen, benötigt dieser Client eine Anzahl von Komponenten, wie sie in Abbildung 5 dargestellt sind.

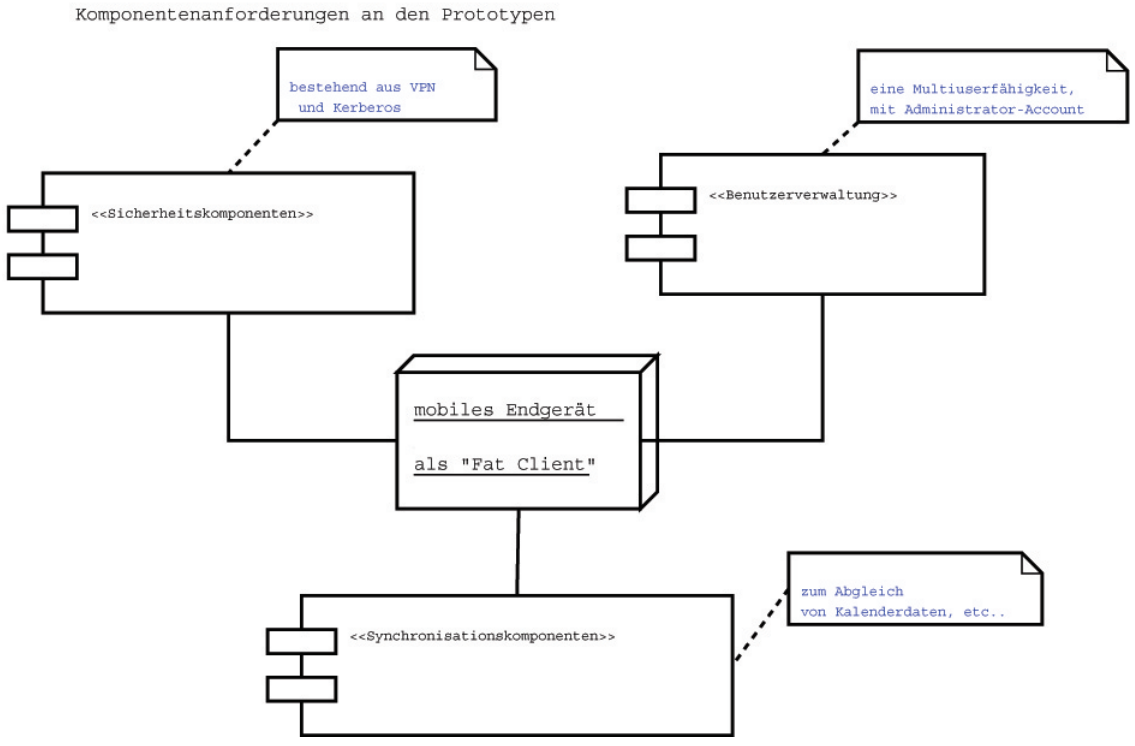

Abbildung 5.1.: Komponenten für das mobile Endgerät

Die *Benutzerverwaltung* auf dem Gerät wird benötigt um eine Trennung zwischen Anwender

(Gast) und der Administration zu gewährleisten. Der Gast soll nicht die Möglichkeit haben die Einstellungen oder einzelnen Softwarekomponenten zu verändern.

Die *Sicherheitskomponenten* dienen zur sichern Anmeldung und Übertragung von Daten in dem Ferienclub. Um diese Komponenten einzurichten wird ein Benutzeraccount (Administrator) benötigt womit diese einzurichten sind, damit der Gast oder fremde Personen keinen Zugriff drauf haben um nicht versehntlich oder mit Absicht diese Daten zu verändern (z.B. Zugangsdaten zum Hotelnetz). Auf eine Implementation der Kerberos-Anmeldung musste verzichtet werden, da keine geeignete Umgebung mit Anmeldungsserver zur Verfügung stand.

Die *Synchronisationskomponenten* dienen zum Abgleich der Daten im Hotelnetz mit denen auf dem PDA. Es ist dabei möglich die *PIM-Anwendungen* des Systemes zu benutzen oder ein eigenes Programm zu benutzen.

Auf eine Serverimplementierung wird hier verzichtet, da diese nur als Umgebung für den PDA genannt wird.

SimPad SL

Als PDA kommt ein Siemens Simpad SL4 zum Einsatz. Dieser unterstützt USB1.1, IrDA Infrarot Interface (IrDA V1.1), PC-Karte PCMCIA Typ II, SmartCard SmartCard Leser gemäss ISO7816 (Teil 1-3) und optional WLAN (Wireless Local Area Network) nach 802.11b um sich mit Funknetzen zu verbinden. Eine Besonderheit im Vergleich zu den anderen PDAs ist das 8.4 Zoll TFT (aktive Matrix SVGA Auflösung (800 x 600 pixels)). Womit es weitgehends möglich ist die Browsertechnologien des Desktops Computers zu nutzen(Abildung 5).

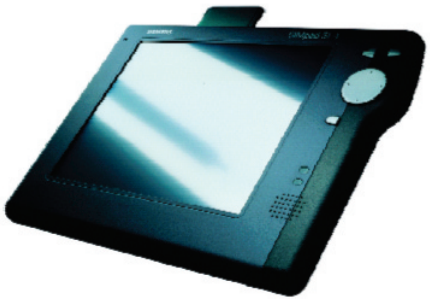

Abbildung 5.2.: das Simpad SL4

Linux und SimPad

Das Linux für den Simpad entstand aus dem „familiar linux“[1], welches entwickelt wurde für ältere Produkte als dem Simpad (iPAQ, Zaurus, Assabet, etc . . .).

Daraus entstand das Projekt „Opensimpad“. Das erste Linux wurde von zwei Siemensmitarbeitern (Juergen Messerer und Walter Schweizer) aus der Schweiz entwickelt. Als grafische Oberfläche wurde *TinyX* benutzt. Das Dateisystem war *CRAMERFS*, das immer noch eingesetzt wird und den Nachteil, hat nur lesbar zu sein.

Parall dazu entstand Opie. Opie ist ein grafisches Frontend auf den QT-Bibilotheken von TrollTech.(Siehe Abbildung 5) [2] beruht.

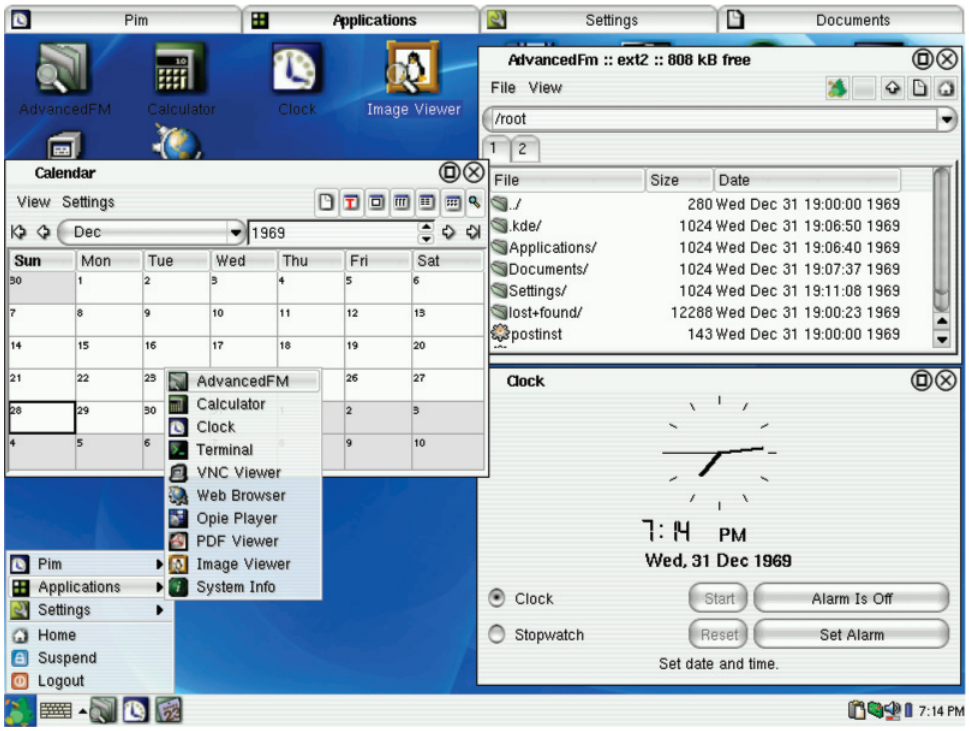

Abbildung 5.3.: das Simpad SL4 mit Opie

Eine installierbares Image ist auf der Homepage `www.opensimpad.org/download` erhältlich und ist ca. 16 MB gross. Danach kann man mit der Debian ähnlichen Paketverwaltung *ipkg* Software nachinstallieren.

Es stehen zwei unterschiedliche Images zur Verfügung:

[1] www.handhelds.org
[2] www.trolltech.com

- Ein Image mit Opie, welches ein gut und einfach zu bedienendes Linux zur Verfügung stellt(siehe 5)
- Ein Image mit X11 Oberfläche und stark orientiert an dem Desktop Linux, wobei viel selber konfiguriert werden muss

Eine genaue Beschreibung der Installation ist im Anhang zu finden. Das Opensimpad Linux bringt viele Sicherheitsfeatures mit. Zur lokalen Authentifizierung benutzt man die Multiuserfähigkeit von Linux. Für den Zugang von aussen steht ein normaler ssh Zugang zur Verfügung, mit dem es möglich, ist den Simpad bequem über einen Desktop-PC zu administrieren.

Als Firewall steht das bekannte Werkzeug *ip-Tables*, von Linux-Server oder Desktop Geräten bekannt, zur Verfügung.

Für Multimediaanwendung erhält man für Musik den *xmms* in einer angepassten Version für PDAs zur Verfügung. Für Filme kann man wählen zwischen *xine* oder *mplayer*. Für die PIM Anwendungen ist es entscheidend, welches Image man installiert hat. Bei *Opie* ist es eine kleinere Version vom *KDE-Office*, bei dem anderen Image sind es die *Gnome Anwendungen*.

Die Konfiguration der einzelnen Komponenten kann über ein graphisches Dialogfenster erfolgen oder aus einer Kommandozeile heraus und den einzelnen Konfigurationsdateien. Die Struktur vom Linux gleicht der von einem Desktop Linuxsystem. Es gibt das Verzeichniss */etc, /var,/usr, /home* in denen die Konfiguration, die Anwendungen und die Protokolldateien liegen. Es ist weiterhin möglich, sich mit Hilfe eines Crosscompilers einen neuen Kernel zu bauen. Dies kann insbesondere interessant sein, um mehrere Sicherheitsmodule in den Kernel zu integrieren (wurde nicht getestet.). Auch die Anbindung mit *NFS* ist möglich.

Ausblick

Es bleibt abzuwarten, wie sich Linux als PDA-System etabliert. Im Moment ist die Situation diese, dass man sein PDA selber mit Linux „bespielen“ muss und es schwierig ist Geräte , wie den Zaurus von Sharp, zu kaufen und auch im Firmenumfeld im Einsatz zu finden. Die Entwicklung schreitet stetig voran und das Interesse an diesen Geräten wächst. Allerdings wird wohl der „Durchbruch“ erst dann erfolgen, wenn grosse Hersteller von PDAs diese mit einem Linux Betriebsystem ausliefern. Zur Frage der Sicherheit bleibt zu sagen, dass die Entwicklung sich im Moment nicht stark von der auf Server- oder Desktopsystemen unterscheidet, da sie aus denselben Modulen bestehen.

6. Fazit

Zusammenfassend kann gesagt werden, dass Linux als Betriebsystem auf einem PDA eine durchaus berechtigte Alternative zu Windows CE darstellt.

Zu der in der Diplomarbeit von Andre Lüpke (Lüpke 2004) dargestellten Lösung mit einem Windows CE Pocket PDA gibt es mehrere Vorteile, die Linux gegenüber Windows im PDA-Betriebssystembereich bietet. Es muss aber gesagt werden, dass die Entscheidung für Linux gewisse Probleme und Risiken birgt, die es zu beachten gilt.

An erster Stelle wären da die Gäste eines Ferienclubs, die ein einfach zu bedienendes Gerät erwarten, welches sich standardkonform zu Windows verhält und es beim „Einchecken“ des Gastes keiner Einführung bedarf, in der die Vorzüge des Systemes erklärt werden. Die Akzeptanz des Gerätes muss gewährleistet werden, was bei nicht jeder Anwendung zum derzeitigen Zeitpunkt vorhanden ist (z.B. Flash, Java-Script bei Internet Browsern). Bei dem Aspekt Sicherheit kann gesagt werden, dass Linux als sehr sicher gilt, es müssen nur die wöchentlich angegebenen Sicherheitspatches immer in das bestehende System eingepflegt werden, was zu einem hohen administrativen Aufwand führen kann.

Es gibt im Linux Bereich eine breite Anwendergruppe, die sich aktiv mit der Weiterentwicklung von Linux auf PDAs beschäftigt, aber nicht von den Herstellern. Das betrifft zum einen die Hilfestellungen bei Problemen sowie die Garantiegewährleistung. Der wohl wichtigste Punkt ist aber, dass der Haupteil der Anwendungen sich in der Testphase befindet oder noch nicht auf den Punkt Sicherheit untersucht wurde und es keine Aussagen zu dem Betrieb in einem grossen Netzwerk gibt. Insbesondere gilt das für Kerberos und VPN Technologien.

> Das Implementieren von Sicherheitslösungen ist keine triviale Angelegenheit, . . . Neben den vielen zu berücksichtigenden Aspekten, kommen noch teilweise recht umständlich zu bedienende Software . . . hinzu (Lüpke 2004).

Diese gilt nicht nur für Windows, sondern auch für Linux. Das Betriebssystem bringt von sich aus viele Werkzeuge von sich aus mit, aber die Schwierigkeit der Konfiguration bleibt.

Es stellte sich aber bei Testen des oben beschriebenen Prototypes mehrere Vorteile ein. Es ist recht einfach ein PDA mit Linux zu installieren. Insbesondere das Verteilen von einem *Image* auf mehrer PDAs ist über das Netzwerk, USB und eine serielle Schnittstelle durchführbar. Hinzu kommt eine einfache Nachinstallation von einzelnen Komponenten wie

beispielsweise *VPN*. Die Netzwerkeinstellung für das WLAN sind im Vergleich zu Windows einfacher und klarer strukturiert. Durch die oben beschriebenen Werkzeuge für *Firewalls* und *ssh* ist es möglich, den Rechner nach aussen hin abzusichern und eine verschlüsselte Netzwerkverbindung aufzubauen.Weiterhin liefert Linux die einzelnen Komponenten, welche in der Komponentenanylse geforderten Sicherheitsbestandteile mit und es werden keine zusätzlichen Fremdanbieter gebraucht, die in das System integriert werden müssen.

Der aber grösste Vorteil besteht darin, dass Linux im Gegensatz zu Windows CE als Mehrbenutzerbetriebssystem verwendet werden kann und somit viele Probleme der oben Beschrieben gelöst werden können (Systemweite Einstellungen können nicht von Gästen ausgelesen werden, Software kann nicht von Fremden installiert oder verändert werden). Das Betriebsystem stellte sich als sehr stabil laufend heraus auch beim Abstürzen einzelner Anwendungen wie z.B. ein Internetbrowser lies sich das System weiterhin bedienen. Die sogennaten PIM Anwendungen sind konform zu Windows bekannten Produkten und verfügen über eine gute Bedienung. Die breite Anwender- und Entwicklungsgemeinde stellt eine gute Hilfe zur Verfügung und die dazugehörige Dokumentation, wie man es von Servern oder Desktopsystemen kennt.

Das System ist im Laborbetrieb gut einsetzbar gewesen, allerdings werden wohl erst in einer Ferienclubumgebung die Schwächen in der Sicherheit und Funktionalität der Software erkennbar.

Ausblick

An dieser Stelle soll kurz darauf eingegangen werden was im Zusammenhang mit einem PDA und Linux als Betriebsystem auf diesem Gerät noch zusätzlich möglich sein könnte und was im weiteren noch untersucht werden kann.

Da die heutigen PDAs viele verschiedene Kommunikationsschnittstellen bieten, wie Infrarot oder Bluetooth wäre es interessant zu sehen ob man unter Linux diese Techniken nutzen kann um beispielsweise in einem Museum die Information zu einzelnen Kunstgegenständen auf den PDA zu überspielen oder im Hotel bestimmte Daten direkt von Mitarbeitern zu erhalten (ohne Umweg über das Hotelnetz).

Die Sicherheitskomponenten, wie Biometrischer Fingerabdruck würden eine weitere Untersuchung des PDA mit Linux interessant gestalten, da somit die Benutzung des Gerätes für den Gast vereinfacht werden könnte. Die Benutzung von Smart Cards oder USB-Sticks zur Benutzerauthentifikation könnten ebenfalls ein weiterer Sicherheitsaspekt sein den es zu untersuchen gilt.

In Verbindung mit den neuen WLan-Standarts*Temporary Key Integrity Protocol (TKPI)* oder *Advanced Encryption Standart (AES)* wäre eine weitere Untersuchung des hier vorgestellten

Entwurfes interesant. Weiterhin könnte man darüber nachdenken, wie man Teile der Daten auf dem PDA verschlüsselt ablegen könnte.

Zusätzlich ist es sinnvoll sich zu überlegen welche Anwendungen man dem Gast lokal auf dem PDA, unter Linux, weiterhin anbieten kann. Es wäre z.B. denkbar dem Gast ein Netzwerkspiel zur Verfügung zu stellen mit dem dieser mit anderen Gästen spielen kann oder auch eine Kommunikatisplattform bieten um sich über Dienste des Hoteles auszutauschen.

Sieht man sich die Benuzerakzeptanz von mobilen Endgeräte und die steigende Beliebtheit des WLans und auch von Linux an, wird es wohl in Zukunft mehr Dienstleistung geben, die für den Zugriff in diesem Bereich ausgelegt sind. Ebenso steigen aber auch die Sicherheitsprobleme in diesem Zusammenhang und es muss abgewartet werden, wie und ob man diese Probleme zum heutigen Stand bewältigen kann.

A. Anhang

Die hier aufgeführte Anleitung stammt von c0rnholio (c0rnholio 2004).
Weitere Dokumentation zum Simpad findet man auf der Opensimpadseite www.opensimpad.org (Simpad 2004).

```
(Hier als Beispiel von CE3.0 auf CE4.0 mit
Windows Desktop-Rechner)

Version 0.1

Erstellt: 25.07.03 c0rnholio
Reviewed: 26.07.03 isi

Danke an Gerhard Islinger für
den Review und Verbesserung!!!

DISCLAIMER: ----------- Alle hier gemachten
Angaben sind ohne Gewähr!!! Wer aus seinem
SIMpad einen Briefbeschwerer macht ist selbst
schuld!!! Ich kann keine Garantie für d
ie Richtigkeit dieser Angaben geben!!!


Vorbereitung:
-------------
- Entsprechendes Image besorgen:
http://simpad.silentservices.de/simpad-faq.html#Q24

- serload herunterladen:
http://prdownloads.sourceforge.net/simpad/serload.zip?download

- COM1 auf dem Rechner freimachen
(also Active-Sync und/oder andere Programme,
die den Port belegen, beenden.)

- Bootloader für SLx herunterladen und in Verzeichnis entpacken:
http://prdownloads.sourceforge.net/simpad/
```

```
bloader-2.5.3-SL4.tar.gz?download

- Alle Dateien in ein Verzeichnis packen
(der einfachheit wegen hier: c:\simpad) -
Kaffee (o.ä.) bereithalten

- !! Als erstes vor allen Updates das SIMpad
ans Netzteil anschließen !! Wenn bem Laden in
den Flash-Speicher der Strom ausgeht, _hat_ man
einen Briefbeschwerer!

- Etwas Geduld mitbringen! Auch wenn normalerweise
alles in maximal einer Stunde durch ist,
speziell die Installation über die serielle
Schnittstelle kann _lange_ dauern. Es sind Fälle
aufgetreten, in denen das Pad mehrere Stunden
scheinbar "hing"...


Installation des neuen Bootloaders:
-----------------------------------
Schritt 1: Das SIMpad mit dem Kabel an
die Schnittstelle "COM1" des Desktops anschliessen

Schritt 2: DOS-Box öffnen und in das Verzeichnis
c:\simpad wechseln

Schritt 3: Serload starten: serload loader_bl.alt

Schritt 4: Nach Aufforderung von serload einen Reset (kleiner
"RESET"-Knopf auf der Rückseite) am Pad durchführen. Der
Download/Installation des Bootloaders sollte jetzt beginnen

Schritt 5: Nachdem serload sagt,
das das Pad jetzt resettet werden soll, dies natürlich tun

Schritt 6: Serload erneut starten: serload loader_bl

Schritt 7: Schritt 4 und 5 entsprechend wieder durchführen

Schritt 8: Serload beenden (CTRL-C) und DOS-Box schliessen.
Hyperterminal (o.ä.) starten, auf COM1 mit 38400,8,n,1, ohne
Flow-Control einstellen.

Schritt 9: Pad resetten und die Keyboard-Taste
(die unter den runden Joypad) gedrückt halten.
Im Hyperterminal erscheint jetzt das Bootmenü
des SIMpad’s. In den ersten Zeilen steht
```

```
die Versionsnummer des Bootloaders. Diese sollte
dann jetzt 2.5.3 lauten. Wenn nicht: Goto
Schritt 1!


Möglichkeit 1: Installation des Images mit Serload
--------------------------------------------------
Nachdem der Bootloader wie oben beschrieben
erneuert wurde, kann man nun das Image übertragen.
Das Funktionsprinzip ist das selbe wie bei der
Installation des Bootloaders.

Schritt 1: DOS-Box öffnen und in das Verzeichnis
c:\simpad wechseln

Schritt 2: Serload starten: serload imagename
(der Imagename ergibt sich aus dem heruntergeladenen
Image (siehe Vorbereitung) oder durch
Umbenennung des selbigen...Ihr wisst was ich meine...)

Schritt 3: Kaffee holen und warten...
Im DOS-Fenster könnt ihr den Fortschritt des Vorgangs
beobachten. Die Übertragung des Images und das
anschliessende Flashen dauert ca. 20-40 Minuten...

Schritt 4: Nachdem der Vorgang abgeschlossen ist,
fordert Serload wieder zum Reset auf. Kleines
Knöpfchen an der Rückseite drücken und beobachten,
wie das SIMpad das neue Image bootet.

Schritt 5: 3 Kreuze machen, das Update ist komplett!


Möglichkeit 2: Installation des Images über das Netzwerk
---------------------------------------------------------
Wer eine zur NE2000 (NE2K) kompatible 16bit
PCMCIA-Netzwerkkarte hat, der kann sich
das Warten auf serload ersparen. Die Installation
über das Netzwerk mit BootP unf TFTP geht
ziemlich fix. Ich benutze für TFTP Pumpkin
(http://www.klever.net/) und für BootP BootP-Desktop
(http://www.weird-solutions.com/). Auf die
Konfiguration der beiden Tools gehe ich hier jedoch
nicht ein. Jeder andere TFTP und BOOTP Server
sollte auch funktionieren.

Wenn alles soweit eingerichtet ist, kann es losgehen.
```

```
Schritt 1: Das SIMpad per Hyperterminal
(o.ä. Prog.) anschliessen, mit den Einstellungen
"38400,8,n,1,No Flow-Control". Reset Knopf drücken
und den Tastatur-Knopf gedrückt halten.
Im Hyperterminal erscheint jetzt das Bootmenü des
SIMpads. Wenn die Karte funktioniert, sollte
das Pad in den oberen Meldungen in
Hyperterminal eine IP-Adresse zugewiesen bekommen
haben.

Schritt 2: Wenn der TFTP und BootP Server läuft
sollte jetzt im Bootmenü die "Boot from Network"
Option angewählt werden (Taste ’n’)

Schritt 3: Das Pad überträgt jetzt das Image
 über das Netzwerk, was recht fix geht, und
fängt anschliessen mit dem Flash-Vorgang an.

Schritt 4: Kaffee holen und warten...Dauert
in der Regel 10-15 Minuten, kann aber auch
mal länger dauern...

Schritt 5: Wenn der Vorgang abgeschlossen ist,
fordert das Pad im Hyperterminalfenster zum
Reset auf. Danach bootet das neue Image wie
durch Wunderhand...


Möglichkeit 3: Installation des Images direkt über das Pad
-----------------------------------------------------------
Es besteht die Möglichkeit ein Image direkt
über das Pad zu installieren.

Schritt 1: Factory-Reset durchführen damit
genug Speicher frei wird.

Schritt 2: Unter Device-Settings->Memory, den
Schiebeschalter soweit wie möglich
(am besten ca. 50 MB für Storage) nach
rechts schieben.

Schritt 3: Internetverbindung herstellen

Schritt 4: Das Software-Update Tool des Pad’s starten un den
Anweisungen folgen.

Schritt 5: Nachdem das Tool den Download durchgeführt hat,
_NICHT_ auf Weiter klicken!
```

Im Root-Verzeichnis des Pad’s befindet sich
jetzt eine recht große Binary Datei. Dies sollte
namensgleich durch das gewünschte Image ersetzt
werden (Per CF-Karte kopieren z.B.)

Schritt 6: Nachdem das Image auf das Pad kopiert wurde,
im Update-Tool auf weiter klicken.
Das Tool installiert nun das gewünschte Image...
Zeit für Kaffee...

Möglichkeit 4: Installation über das Software Update Tool des Pad’s
---
Da gibt es eigentlich nicht wirklich viel zu zu schreiben.

Schritt 1: Internetverbindung etablieren.

Schritt 2: Sicherstellen, das genügend freier Speicher
auf dem Pad vorhanden ist (ca 30 MB freier Datenspeicher).
Notfalls Factory-Reset durchführen und
Internetverbindung wiederherstellen.

Schritt 3: Per Registry Editor den Schlüssel
"HKEY_LOCAL_MACHINE\SOFTWARE\Version"
auf S842-SI-GER-107 (für das deutsche CE.Net 4.0)
ändern.

Schritt 4: Das Software-Update Programm
starten und den Anweisungen folgen.

Schritt 5: Kaffee holen und auf Komplettierung warten...

Anhang: Einige Links...

SIMpad-FAQ:
http://simpad.silentservices.de/

SIMpad-Info’s:
http://home.netsurf.de/gerhard.islinger/simpad/

SIMpad-Forum bei Palmtop-Magazin:
http://www.palmtop-magazin.de/board/tablett/

Linux und Tools für’s SIMpad:
http://www.opensimpad.org/

Opensimpad Forum:

http://forum.opensimpad.org/

Literaturverzeichnis

dos 2004 WIKIPEDIA, der freien E. (Hrsg.): *Denial of Service*. 2004. – URL http://de.wikipedia.org/wiki/Denial_of_Service. – Zugriffsdatum: 2004-03-21

Simpad 2004 SEITE, Simpad H. (Hrsg.): *Linux auf dem Simpad*. 2004. – URL http://www.opensimpad.org/. – Zugriffsdatum: 2004-08-11

c0rnholio 2004 SEITE, Simpad H. (Hrsg.): *Linux auf dem Simpad installieren*. 2004. – URL http://simpad.silentservices.de/. – Zugriffsdatum: 2004-08-11

BSI 2003 INFORMATIONSTECHNIK, Bundesamt für Sicherheit in der (Hrsg.): *Sicherheit im Funk-Lan*. 2003. – URL www.bsi.bund.de. – Zugriffsdatum: 2004-02-22

Havinga 2000 HAVINGA, Paul J. ; MULTIMEDIA, Mobile (Hrsg.): *Mobile Multimedia*. 2000. – URL http://wwwhome.cs.utwente.nl/~havinga/thesis/. – Zugriffsdatum: 2004-03-21

hotel.de 2004 HOTEL.DE AG (Hrsg.): *Newsletter*. 2004. – URL http://media.hotel.de/Hotels-in/WLAN_Hotel.htm. – Zugriffsdatum: 2004-02-22

Kühn und Möller 2003 KÜHN, Ulrich ; MÖLLER, Frank: WLan: die neue Offenheit / Datenschutz Hamburg. 2003. – Forschungsbericht

Lüpke 2004 LÜPKE, Andre: *Entwurf einer Sicherheitsarchitektur für den Einsatz mobiler Endgeräte*, Hochschule für Angewandte Wissenschaften Hamburg, Dissertation, April 2004. – URL http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/diplom/luepke.pdf. – Zugriffsdatum: 2004-08-09

Müller 2002 MÜLLER, Florian: Sicherheit in WLans / Technische Universität Carola-Wilhelmina zu Braunschweig, Institut für Betriebssysteme und Rechnerverbund. nov 2002. – Forschungsbericht