Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Studienarbeit

Sicheres Wlan im Ferienclub

vorgelegt von
Roman Bartnik
am 23. März 2005

Studiengang Softwaretechnik

Betreuer: Prof. Dr. Kai von Luck

Fachbereich Elektrotechnik und Informatik
Department of Electrical Engineering and Computer Science

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einleitung

1.1. Motivation

In dem Grade, in dem mobile Endgeräte in Anwendungsszenarien verwendet werden, steigt der Bedarf an sicheren Kommunikationswegen. Es existieren viele Endgeräte, die eine drahtlose Verbindung vorsehen, jedoch ohne Berücksichtigung der Sicherheit. In dieser Arbeit wird eine Möglichkeit vorgestellt, PDA's sicher an interne Netze anzuschließen, so daß auf dieser Basis die von André Lüpke an der HAW entworfene Architektur[1] eingesetzt werden kann.

1.2. Szenario

In einem Ferienclub soll es Gäste ermöglicht werden, über mobile Endgeräte Informationen einzuholen und rechtsverbindliche Vereinbarungen einzugehen. Hierbei werden die PDA's personalisiert und den Gästen bei ihrer Ankunft an der Rezeption, als eine Art Clubausweis, ausgehändigt. Während ihres Urlaubs können die Gäste die gebotenen Möglichkeiten auf dem gesamten Clubgelände nutzen. Ihre PDA's halten dabei dauerhaften Kontakt zu den Servern des Clubs.

1.3. Aufgabenstellung und Ziele

Ziel ist es, die über das drahtlose Medium laufende, Kommunikation vor Abhören und Verfälschen zu sichern. Die Kommunikation mit den Servern des Clubs soll auf autorisierte Geräte beschränkt werden. Die Sicherung der Endgeräte wurde in (Mählmann 2004) untersucht, während (Lüpke 2004) eine Anwendungsarchitektur vorstellte. Da wie in (Lüpke 2004) ausgeführt, die Sicherheit der Daten und Anwendungen auf den PDAs, aufgrund des verwendeten Betriebssystemes nicht zu gewährleisten ist, konzentrierte sich die Arbeit auf Serveranwendungen.

[1] (Lüpke 2004)

(Mählmann 2004) betrachtete die Möglichkeiten ein mehrbenutzerfähiges Betriebssystem mit Verwaltung von Benutzerrechten, zur Erhöhung der Sicherheit auf den mobilen Geräten, zu verwenden. Dadurch wird es unter anderem möglich die Konfiguration der Geräte und das Ausführen fremder, möglicherweise schädlicher, Software zu verhindern. Dies beugt ungewollten Ausfällen der Services vor. [2] Die Arbeit geht von einer sicheren Netzverbindung zwischen PDA s und dem internen Clubnetz aus, ohne weiter darauf einzugehen.

Diese Arbeit beschreibt eine entsprechende Netzwerkarchitektur, die mit erhältlichen Softwarekomponenten auskommt. Diese Architektur soll danach in einer Testumgebung realisiert werden.

1.4. Gliederung

In Kapitel 2 werden die Anforderungen der Gäste und Betreiber dargelegt, sowie technische Anforderungen an die Funktionalität und Sicherheit, die sich daraus ergeben. Darauf aufbauend, wird in Kapitel 3 ein Design beschrieben.

Kapitel 4 stellt einige Techniken vor, die zur Umsetzung des Designs verwendet werden können. Als letztes wird in Kapitel 5 beschrieben, wie sich die Umsetzung in der Laborumgebung gestaltete und welche Techniken gewählt wurden.

[2] Schneier hat einen Artikel zu Sicherheit auf Clientseite geschrieben (Schneier 2000)

2. Analyse

2.1. Szenariobeschreibung

Das Szenario entspricht dem bereits in (Lüpke 2004) und (Mählmann 2004) behandeltem fiktiven Ferienclub. Der Club bietet seinen Gästen die Möglichkeit, über entliehene mobile Endgeräte, bestimmte Dienste ortsunabhängig zu nutzen.

Es werden dem Gast beispielsweise Informationen zu Veranstaltungen im Club, sowie interessante Ereignisse mitgeteilt. Eine weitere Möglichkeit sind Reservierungen von Clubanlagen (z.B. ein Tennisplatz) oder ein Reiseführer. Diesen Diensten ist gemein, daß sie unverbindlich oder rein informativ sind, sowie keine persönlichen Daten erfordern.

Zusätzlich zu diesen Diensten, stehen dem Gast auch Möglichkeiten zur Verfügung, die eine Rechtsverbindlichkeit nach sich ziehen. Dies sind typischerweise geschäftliche Transaktionen, wie Käufe oder das Buchen von kostenpflichtigen Dienstleistungen. Diese Dienste werden, in Anlehnung an (Lüpke 2004), “kritische Dienste” genannt.

2.2. Anforderungen des Gastes

Der Gast verbringt seinen Urlaub im Club und es ist sein Hauptanliegen, sich über die vorhandenen Möglichkeiten zu informieren und sie zu nutzen. Die für seinen PDA angebotenen Anwendungen, bieten ihm eine Möglichkeit dazu. Wenn er überzeugt ist, daß sie ihm Vorteile bringt und er der Technik vertraut, wird er das System nutzen.

Dieses Vertrauen kann man erreichen, indem man die Risiken für den Gast minimiert und ihm die getroffenen Maßnahmen mitteilt. Hierbei sollte vielleicht zwischen wahrgenommenen und tatsächlichen Risiken unterschieden werden. Die tatsächlichen Risiken ergeben sich aus $Eintrittswahrscheinlichkeit * Schaden$, während bei den wahrgenommenen Risiken zusätzliche Faktoren vor das Produkt aus Eintrittswahrscheinlichkeit Schaden gesetzt werden müssen. (Schneier 2004)

Schutz der persönlichen Daten

Der Gast soll das System nutzen, wobei teilweise persönliche Daten erforderlich werden. Diese müssen nun vor dem Zugriff unberechtigter Dritter geschützt werden, damit keine negativen Konsequenzen für den Gast entstehen.

Schutz vor Fehlabrechnungen

Die werden Leistungen in Anspruch genommen, die Rechtsverbindlichkeiten nach sich ziehen. Es ist natürlich im Interesse des Gastes, das ihm nicht unberechtigter Weise Leistungen in Rechnung gestellt werden. D.h., unter anderem, muß ihm die Natur einer Buchung vor Augen geführt werden, wenn sie den Charakter einer Willenserklärung hat. Es müssen Nachweise erzeugt werden, anhand derer sich die Herkunft der Kosten aufschlüsseln lässt. Ausserdem muß das System verhindern, das Dritte mutwillig falsche Buchungsinformationen einspielen.

Verlässlichkeit des Buchung

Hat der Gast eine Leistung gebucht, erwartet er ihre Erfüllung. So muß eine bestellte Konzertkarte auch zum vereinbarten Termin zur Verfügung stehen. Wenn er die Erfahrung macht, daß Buchungen verloren gehen, wird sie wieder über andere Wege abschließen.

Aktuelle und zutreffende Informationen

Wenn der Gast seine Zeitplanung nach den Informationen des Terminplans ausrichtet, müssen diese natürlich auch korrekt sein. Ebenso wird er es nicht akzeptieren, wenn er eine Veranstaltung, aufgrund eines veralteten Terminplanes, verpasst. Macht der Gast einmal die Erfahrung, das er einen Termin verpasst, oder umsonst besucht, wird er den Informationen nicht vertrauen und bei den Angestellten, oder in Prospekten, nach einer Bestätigung oder aktuelleren Information zu suchen.

Verfügbarkeit

Der Gast will in seinem Urlaub möglichst wenig Zeit mit der Planung seiner Aktivitäten verbringen. Hierbei bietet das System durch seine Automatisierung den Vorteil, das er Leistungen zeitnah buchen kann. Wonach er sich wieder andern Tätigkeiten widmen kann. Allerdings muss das System auch verfügbar sein, und nur kurze Wartezeiten enthalten. Denn

sollte es sich herausstellen, das Leistungen mehrmals nicht gebucht werden konnten, wird der Gast wieder auf die Reservierung durch das Personal zurückgreifen.

Einfache Bedienung

Die Bedienung des Systems muss so einfach wie möglich sein. Sie darf dem Gast keine unverstandenen Hindernisse in den Weg stellen. Jeder nötige Lernaufwand und jeder zusätzliche Schritt, den der Kunde ausführen muss, ist ein Hinderniss auf dem Weg zur Akzeptanz.

Man muss nun die Balance zwischen Benutzerfreundlichkeit und Sicherheit finden. Der Kunde möchte natürlich ein sicheres System, es ist ihm vielleicht nur nicht bewusst, wieweit sich sein Verhalten auf die Sicherheit auswirkt.

Der Autor nimmt an, das man den Benutzer von der Notwendigkeit überzeugen kann, sich beim Einschalten des Gerätes, nach einer längeren Pause und beim Abschließen von Verträgen gegenüber seinem Endgerät oder dem Server zu identifizieren. Bei einer weiteren Passwortabfrage, halte ich die Akzeptanz beim Kunden bereits für zweifelhaft.

Geringes Risiko

Die Abschnitte 2.2 und 2.2 enthalten den größten potentiellen Schaden für den Kunden, und damit auch den Club. Gefolgt von 2.2 und 2.2 bei deren Nichterfüllung der Gast Zeit verliert, welche in einem Urlaub eine sehr begrenzte Ressource ist.

Um das Vertrauen des Kunden zu erwerben, muss man einerseits die tatsächlichen Risiken auf ein für den Clubbetreiber und den Kunden akzeptables Maß senken, sowie den Kunden davon überzeugen das dem tatsächlich so ist. Das heisst, Marketing betreiben, um das wahrgenommene Risiko an das tatsächliche Risikonivaeu anzugleichen.[1]

2.3. Anforderungen des Betreibers

Akzeptanz des Systems durch den Gast

Da der Clubbetreiber natürlich möchte, dass sein System genutzt wird, ist eine Anforderung, daß die Kunden es akzeptieren können. Damit macht er sich die Anforderungen im vorhergehenden Kapitel zu eigen. Um dieses Ziel zu unterstützen, kann die Clubverwaltung auch

[1] Wahrgenommenes (Subjektives)Risiko wird hier nicht weiter behandelt.

einige der Risiken für den Kunden übernehmen, solange dabei die Anforderung “Sicherheit vor Betrug” nicht gefährdet wird.

Sicherheit vor Betrug

Das System muss sich rechnen, d.h. die Risiken müssen so gering sein, das die eintretenden Schäden nicht die Gewinne übersteigen. Die Schäden durch Betrug sind vielfältig:

- Angreifer können versuchen sich Leistungen zu erschleichen.
- Angreifer können versuchen anderen Kunden Leistungen anzurechnen
- Angreifer können versuchen, Daten auszuspähen
- . . .

Diese Angriffe verursachen direkte Schäden, wie bei der Leistungserschleichung, bei der der Club Leistungen ohne Gegenleistung erbringt und indirekten Schaden durch Imageverlust oder eine gestärkte Konkurrenz, bei Belastung eines fremden Kundenkontos und Datenausspähung.

Verbindlichkeit von Buchungen

Wenn der Gast eine Buchung getätigt hat, ist diese für ihn, wie den Club, verbindlich. Es wird also verhindert, das der Gast nach erfolgter Leistungserbringung des Clubs die Buchung erfolgreich abstreiten kann. Das System muss also Möglichkeiten beinhalten, die einen Nachweis der erfolgten Buchung durch den Gast erlauben.

2.4. Forderungen an die Datenübertragung

Die bisher genannten Anforderungen gelten für das Gesamtsystem. Die sichere Übermittlung der Daten betreffen nur einige der Punkte. Da dies, als ein Teil der Infrastruktur, kaum direkten Kontakt mit dem Benutzer hat. Andere Punkte betreffen es allerdings besonders, da ein Ausfall auf dieser Ebene alle oberen Teile des Systems betrifft.

Einfache Bedienbarkeit

Der Gast muss sich ohnehin mehrmals beim System anmelden. (Endgerät, persönliche Identifikation bei Geschäftsabschlüssen), so daß eine weitere Eingabeaufforderung vermutlich nicht akzeptiert wird. Daher sollte die Authentifikation des Endgerätes keine explizite Handlung des Benutzers erfordern. Dies kann man durch eine Einbindung in die lokale Benutzeranmeldung erreichen. Solange der Benutzer sich nicht am lokalen Gerät neu authentifizieren muss, muss er dies auch nicht gegenüber dem Netzwerk.

Isolation der einzelnen Benutzer

Da jeder Gast einen Zugang bekommt, muss ein Angreifer keine technischen Hürden überwinden, um Zugang zum öffentlichen Clubnetz zu bekommen, er muss nur einen Urlaub buchen. Daher muss jedes ausgegebene Endgerät als potentieller Angreifer betrachtet werden. Dies ist nichts neues, ein großer Anteil von Angriffen werden aus dem Inneren von Systemen ausgeführt. Um diesen Einfluss zu minimieren, sollen die Endgeräte keinen direkten Kontakt untereinander erlauben.

Isolation des Netzes von nicht autorisierten Benutzern

Da die Leistungen nur von Clubgästen genutzt werden sollen, sind fremde Geräte vom Netzzugang auszuschliessen.

Verfügbarkeit

Die Verbindung mit dem Clubnetz ist dauerhaft verfügbar, da ein Kunde, der bei seinem ersten Versuch etwas über das Clubnetz zu erledigen enttäuscht wird (durch zu lange Wartezeiten z.B.), schnell zu anderen Möglichkeiten greifen wird.

Zuverlässigkeit

Auf Benutzerebene sollte die Ausfallwahrscheinlichkeit über die durchschnittliche Transaktionsdauer niedrig sein, um die Akzeptanz der Technik nicht zu gefährden. Daher sollte der Status der VPN-Verbindung überwacht werden, um sie im Bedarfsfall ohne Benutzerinteraktion wieder aufzubauen.

2.5. Anforderungen aus der Informatik

Modularität

Die Unterteilung eines grossen Themenkomplexes in eigenständige Bereiche(Module), mit definierten Schnittstellen. Diese Aufteilung ist sinnvoll, damit Änderungen an Teilen des Systems sich nur in den betroffenen Modulen auswirken. Änderungen können z.B. bei der Hinzunahme weiterer Dienste, sowie zur Anpassung an erweiterte Sicherheitsanforderungen, nötig werden.

Wiederverwendbarkeit

Das Design für die sichere Infrastruktur soll gänzlich durch das Verbinden vorhandener Teilkomponenten realisiert werden, um die Vorteile der Wiederverwendbarkeit zu nutzen. Hierbei ist besonders die Möglichkeit, auf vorhergehende Analysen der Komponenten zurück zugreifen, zu erwähnen. Dies ist im Bereich der Sicherheit ein nicht zu unterschätzender Vorteil, da z.B. bei Algorithmen nur durch ausführlicher Analysen ein Vertrauen in ihre Sicherheit gewonnen werden kann.

Erweiterbarkeit und Wartbarkeit

Nach der Fertigstellung eines Systems ist es unvermeidlich, daß sich die Umgebungsbedingungen sowie die Anforderungen ändern. D.h. es muss möglich bleiben, neue Funktionen einzubauen und veraltete Komponenten zu ersetzen. Das Beheben von Fehlern sollte ohne Expertenwissen möglich sein. (Lüpke 2004, 23)

Portabilität

Unter Portabilität versteht man die Möglichkeit ein Design in verschiedenen Umgebungen zu implementieren. Hierdurch erreicht man eine Unabhängigkeit von verschiedenen Hard– und Softwareherstellern. [2]

[2] (Lüpke 2004, 23)

Sicherheit

Um zu verdeutlichen, als was Sicherheit hier verstanden werden soll, kann man sich an die Definition des Bundesministeriums für Sicherheit in der Informationstechnik halten. Es beschäftigt sich hauptsächlich mit Bedrohungen beim Betrieb von Informationssystemen und ihrer Gegenmaßnahmen.

> Zustand eines IT–Systems, in dem die Risiken, die beim Einsatz dieses IT-Systems aufgrund von Bedrohungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.

(BSI 1992, Anhang F, Glossar)

Unter der Bedrohung wird der Verlust von Verfügbarkeit, Integrität oder Vertraulichkeit verstanden.

> A single design flaw with respect to security may render all security measures useless. (Tanenbaum und Steen 2001, 413)

> Building all kinds of security mechanisms does not relly make sense unless it is known how those mechanisms are to be used, and against what. (Tanenbaum und Steen 2001, 413)

Verfügbarkeit

> Mit Verfügbarkeit bezeichnet man den Tatbestand, daß Funktionen eines IT–Systems ständig bzw. innerhalb einer vorgegebenen Zeit die von Funktion zu Funktion unterschiedlich sein kann, zur Verfügung stehen und die Funktionalität des IT–Systems nicht vorübergehend bzw. dauerhaft beeinträchtigt ist. in diesem Zusammenhang kann auch die Verfügbarkeit von Informationen bzw. Daten bedeutend sein. (BSI 2003, Kap. 3.1)

Während man auf reiner Softwareebene natürlich nicht gegen alle Einschränkungen der Verfügbarkeit verhindern kann, so gibt es hier natürlich doch einige Maßnahmen, die man treffen kann.

Die Akzeptanz der Technik dürfte stark davon abhängen, das sie unterbrechungsfrei zur Verfügung steht. Wenn ein Gast erst einige Male erfolglos versucht hat das System zu benutzen, wird er wohl auf die weitere Nutzung der Mobilen Dienste verzichten und den PDA auf dem Zimmer lassen, oder wieder abgeben. (Reine Hypothese)

Integrität

> Unter der Integrität von Informationen versteht man die Tatsache, daß Informationen nur von Befugten in beabsichtigter Weise verändert und nicht unzulässig modifiziert werden können. Von dieser Grundbedrohung sind auch Programme betroffen, da die Integrität nur bei ordnungsgemäßer Verarbeitung und Übertragung garantiert werden kann. Häufig wird unter dem Begriff “Integrität” außer der Unversehrtheit der Daten auch noch die Vollständigkeit, die Widerspruchsfreiheit und die Korrektheit verstanden. Vollständig bedeutet, daß alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den gemeinten Sachverhalt unverfälscht beschreiben. (BSI 2003, Kap. 3.1)

> Das Verfälschen, das unbefugte Mitlesen und sogar das unbefugte Speichern von Daten auf ihrem Weg durch ein modernes Kommunikationsnetz lassen sich nicht ausschließen, Sicherungsmaßnahmen können jedoch verhindern, daß dadurch relevante Schäden entstehen. (Jakob 1999, Kap. 25 2.1)

Wenn über ein Netz Geschäfte abgeschlossen werden, muss man davon ausgehen können, das sie im selben Zustand, in dem sie den Empfänger erreichen, auch den Sender verlassen haben. Sollten sie im Transit von Angreifern verändert werden können, ist es nicht mehr möglich Verträge abzuschließen.

Vertraulichkeit

> Unter der Vertraulichkeit von Informationen versteht man die Tatsache, daß die Informationen nur Befugten zugänglich ist und kein unbefugter Information stattfinden kann. Von dieser Grundbedrohung können auch Programme als Informationen im weiteren Sinn betroffen sein, z.B. wenn ein Verfahren, dessen Vorschrift durch ein Programm dargestellt wird, geheim gehalten werden soll. (BSI 2003, Kap. 3.1)

In diesem Zusammenhang vielleicht nicht der wichtigste Sicherheitsaspekt, andererseits dürfte einem Clubbetreiber daran gelegen sein, das seine Konkurrenten nicht das Konsumverhalten und das Umsatzvolumen in seinem Club in Echtzeit auslesen können. Weiterhin könnten die Terminkalender reicher Touristen willkommene Informationen für Vertreter (Können sich aber auch einfach an Brennpunkten aufhalten) oder Räuber sein. (Gast A auf Individualtour in der Stadt)

Authentizität

Die eindeutige Identifikation von Benutzern, oder die eindeutige Identifikation, der Herkunft von Daten.

Auf Netzwerkebene soll sichergestellt sein, das nur zahlende Gäste die angebotenen Dienste nutzen. Auf Anwendungsebene ist der auch im Nachhinein Mögliche Nachweis über die Herkunft von Bestelldaten, wichtig für den Nachweis des Vertragsabschlusses.

Verschiedene der in A vorgestellten Angriffe lassen sich vermeiden, wenn die Authentizität von Daten und Benutzern festgestellt werden kann.

Fehlertoleranz

Fehlertoleranz ist eine wichtige Voraussetzung um Zuverlässigkeit und Verfügbarkeit zu erhalten. Diese Eigenschaften wiederum sind wichtige Bausteine eines sicheren Systems.

Die Hauptfunktionen der Netzwerkinfrastruktur, sollten auch gewährt bleiben, wenn Fehler in einzelnen Komponenten auftreten. Hierfür sind folgende Konzepte wichtig:[3]

1. Verfügbarkeit (Availiability)[4]
2. Zuverlässigkeit (Reliability)
3. Sicherheit (Safety)
4. Wartbarkeit (Maintainability)

Zuverlässigkeit

> Reliability refers to the property that a system can run continuously without failure. In contrast to availability, reliability is defined in terms of a time interval, instead of an instant in time. (Tanenbaum und Steen 2001)

Während die Verfügbarkeit in allen Schichten der Architektur, notwendig ist, da ein Ausfall in jeder Schicht zur Folge hat, das der Benutzer nicht die gewünschte Aktion ausführen kann, kann eine geringe Zuverlässigkeit in den niedrigeren Schichten in den nächsthöheren ausgeglichen werden. Es ist die Frage auf welcher Ebene dies geschehen sollte.

[3] (Tanenbaum und Steen 2001)
[4] Siehe Abschnitt 2.5 auf Seite 15

Sicherheit

> Safety refers to the situation that when a system temporarily fails to operate correctly, nothing catastrophic happens. (Tanenbaum und Steen 2001, 363)

Im behandeltem Teilsystem ist der unberechtigte Zugang zum Netzwerk und das Ausspähen von Daten zwei der möglichen katastrophalen Ereignisse. Diese sollen auch im Fehlerfall verhindert werden.

Während Sicherheit (Security) die Minimierung von Risiken durch Angreifer und Systemfehler beinhaltet, bedeutet Sicherheit (Safety), das auch der Ausfall von Einzelkomponten nicht zu einer Erhöhung der Risiken führt. “Safety” ist also ein integraler Bestandteil von “Security”.

Wartbarkeit

> Finally, maintainability refers to how easy a failed system can be repaired. A highly maintainable system may also show a high degree of availability, especially if failures can be detected and repaired automatically. (Tanenbaum und Steen 2001)

Da die Nichtverfügbarkeit des Systems sehr schnell zur Nichtakzeptanz führen könnte, sollten defekte Elemente des Netzwerkes schnell repariert werden können, wenn nicht andere Maßnahmen zur Erhöhung der Verfügbarkeit getroffen wurden.

3. Design

> Simply stating that a system should be able to protect itself against all possible security threats is not the way to actually build a secure system. What is first needed is a description of security requirements, that is a security policy. (Tanenbaum und Steen 2001, 415)

Es wird ein System entworfen, das die Anforderungen aus Kapitel 2 für die Strecke von den PDAs zum Clubnetzwerk umsetzt. Hierfür wird betrachtet, wie man die Endgeräte, den Gateway ins Clubnetz und die Verbindung zwischen ihnen einrichtet. Der Hauptpunkte ist die Absicherung der Daten, die über das WLAN verschickt werden.

3.1. VPN

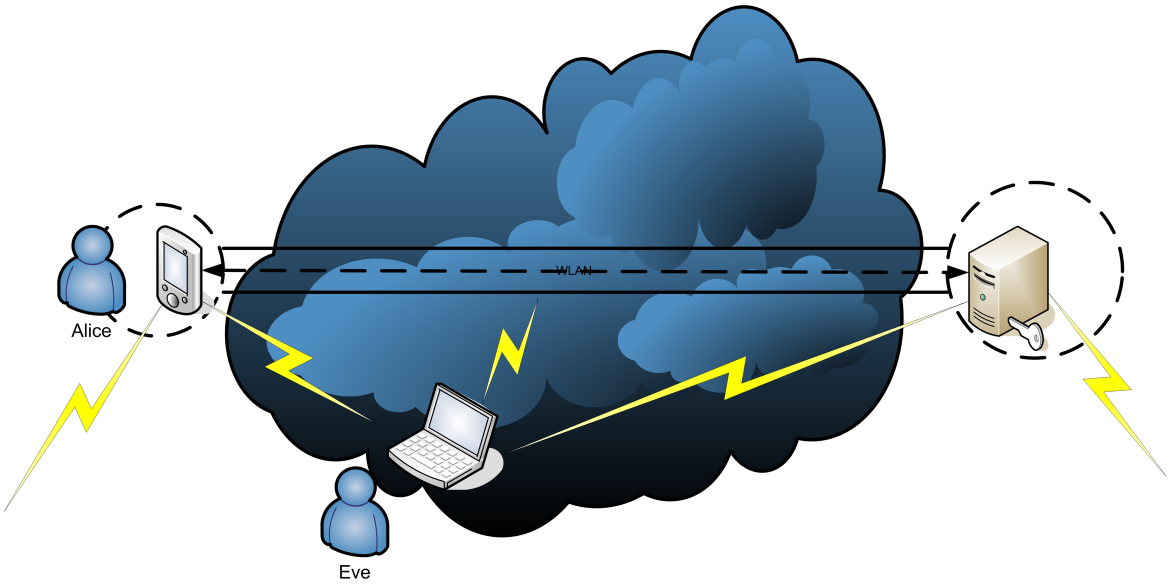

Abbildung 3.1.: Ein PDA hat einen Tunnel zum Gateway aufgebaut. Beide Teilnehmer sind jedoch nicht gegen weiteren Netzverkehr aus dem öffentlichen WLAN abgeschirmt

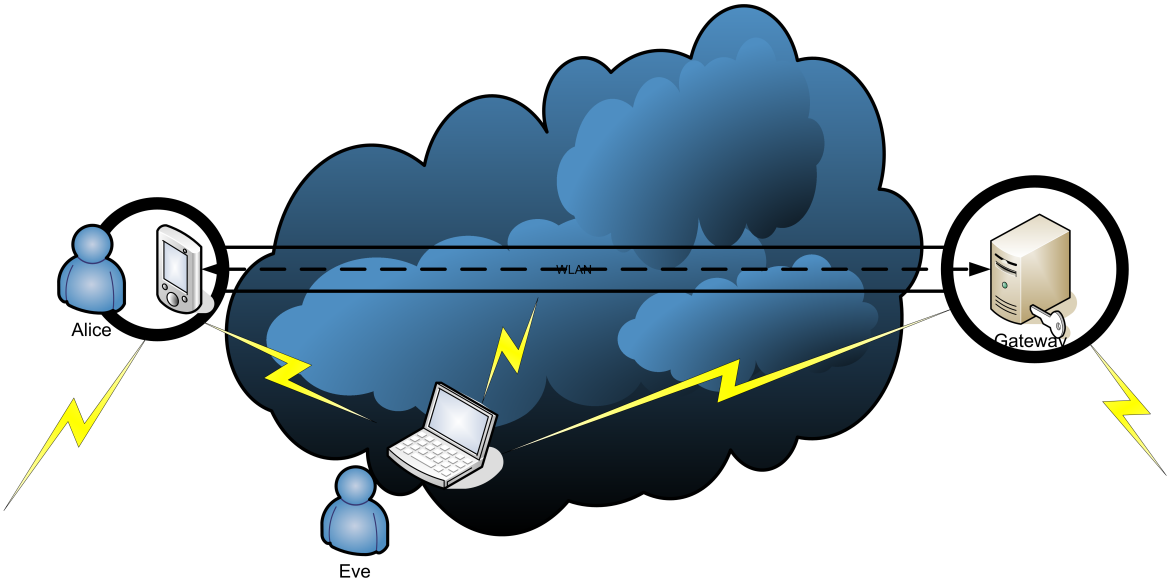

Abbildung 3.2.: Ein PDA hat einen Tunnel zum Gateway aufgebaut. Beide Endpunkte sind jedoch auch mit weiteren Maßnahmen gesichert

Um die Anforderungen der Integrität, Vertraulichkeit und Authentizität zu erfüllen, wird zwischen den einzelnen PDAs und dem Gateway je ein kryptographisch abgesicherter Tunnel (VPN) eingerichtet.

> Ein Tunnel bezeichnet in der EDV das Übertragen der Daten eines Netzwerkprotokolls, eingebettet in ein anderes Netzwerkprotokoll. Tunnel werden verwendet um gesicherte, verschlüsselte Verbindungen über ungesicherte Computernetze aufzubauen (s. VPN) oder um Firewalls und andere Sicherheitsmaßnamen zu umgehen. (Wikipedia 2005a)

Hierbei stellen die PDA's einzelne Endpunkte einer verschlüsselten Verbindung dar, während der Gatewayrechner für alle PDA's der Endpunkt ist, der die Verbindung ins Clubnetz bietet, und somit als Server auftritt.

> Ein Virtuelles Privates Netzwerk (VPN) ist ein Computernetz, das zum Transport privater Daten ein öffentliches Netzwerk (zum Beispiel das Internet) nutzt. Teilnehmer eines VPN können Daten wie in einem internen LAN austauschen. (Wikipedia 2005b)

Das VPN stellt sich für die PDA's dar, als ob sie der einzige Teilnehmer in ihrem Netz sind, das durch einen Router mit dem Clubnetz verbunden ist.

Durch den Tunnel sind die Daten im Transit gesichert, wodurch die Endpunkte zum nächsten Angriffspunkt werden und gesondert gesichert werden müssen. (Siehe Abb. 3.1)

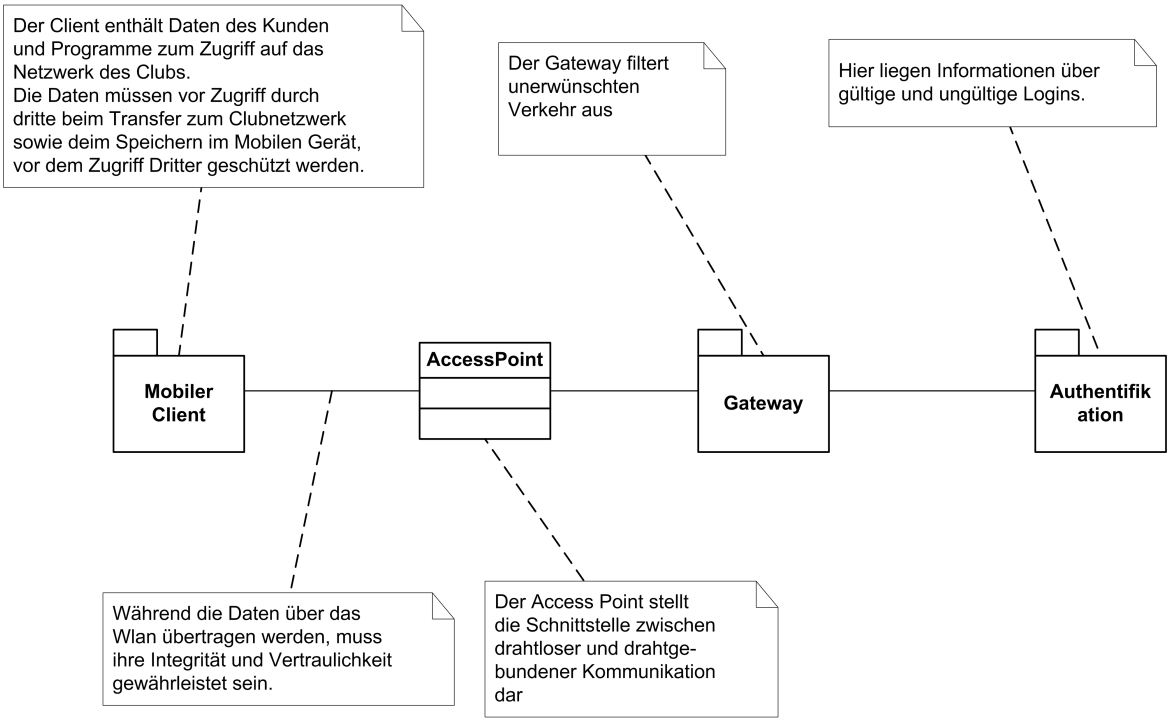

Abbildung 3.3.: Verwendete Komponenten

Dies wird durch verschiedene Konfigurationen auf PDA– und Serverseite erreicht, wodurch die Verletzlichkeit gegenüber ungesichertem Verkehr sinkt. (siehe Abb. 3.1)

Im folgenden werden die Endpunkte PDA und Gatewayrechner, mit den erforderlichen Konfigurationen beschrieben, um den Tunnel und die Endpunkte zu sichern.

3.2. Mobiler Client

Die Endgeräte enthalten Daten, für die Vertraulichkeit und Integrität wichtig sind. Damit sie allerdings einen Nutzen bringen, müssen sie über ein Funknetz mit den Servern des Clubs ausgetauscht werden.

Der Gateway und der entsprechende Client sind die einzigen Teilnehmer des Wlans, die den Verkehr lesen sollen. Dies lässt sich erreichen, indem man zwischen jedem Client und dem Gateway eine VPN–Verbindung aufbaut. Damit dies jedoch Wirkung zeigt, darf der Client keine Informationen über die ungesicherte Schnittstelle übertragen.

Hieraus ergibt sich, daß der Client zwei Komponenten braucht, um am Clubnetz teilzunehmen, diese müssen ausserdem durch das OS des Endgerätes vor Konfigurationsänderun-

gen durch den Kunden geschützt werden, damit die Sicherungsmaßnahmen nicht unterlaufen werden. Ein Schutz vor absichtlicher Kompromittierung ist vor allem zum Schutz der VPN–Zugangsdaten notwendig, da der Kunde seine eigenen Zugangsdaten einfach weitersagen kann.

Schlüsselaustauschdienst und VPN-Client

Der VPN-Client dient als Endpunkt eines Tunnels zum Gateway, über den Verbindungen zum Clubnetzwerk laufen. Vor der Einrichtung des Tunnels authentifiziert sich der Schlüsselaustauschdienst gegenüber dem VPN-Server und überprüft seinerseits die Identität des Gatewayrechners. Zusätzlich zur gemeinsamen Authentifikation wird ein Sitzungsschlüssel ausgetauscht, mit dem die spätere Kommunikation zwischen Client und Server verschlüsselt wird.

Der aufgebaute Tunnel bietet nun anderen Anwendungen eine abhörsichere Netzwerkschnittstelle mit authentifizierten Endpunkten zur Kommunikation.

Diese Schnittstelle kann die Integrität, Authentizität und Vertraulichkeit der Daten während der Übertragung durch das Wlan gewähren.

Packetfilter

Damit die, während der Übertragung durch den Tunnel/das VPN, gewonnene Sicherheit nicht durch Schwächen an den Endpunkten verlorengeht, wird das Kommunikationsverhalten des PDA's sehr restriktiv konfiguriert.

Es werden nur Netzwerkverbindungen erlaubt, die zum Nutzen der Clubdienste nötig sind. Andere Verbindungsversuche, ob von lokalen Anwendungen oder aus dem Netzwerk, werden abgelehnt.

Der VPN-Client und der Schlüsselaustauschdienst sind die einzigen Anwendungen, die Zugriff auf die unverschlüsselte Netzwerkschnittstelle benötigen. Datenverkehr anderer Anwendungen, der unverschlüsselt abläuft, ist eine Gelegenheit, Informationen zu gewinnen und eventuell vorhandene Programmierfehler in den Anwendungen auszunutzen.

Der Packetfilter beschränkt nun den möglichen unverschlüsselten Verkehr auf die zur Authentifikation und Schlüsselaustausch nötigen Daten, sowie den verschlüsselten Verkehr auf Kommunikation mit bekannten Clubservern und Proxies.

3.3. Accesspoint

Der Accesspoint muss den Gastgeräten auf dem gesamten Gelände Zugang zum Clubnetz zu ermöglichen. Da eine Authentifikation der Geräte im VPN-Protokoll stattfindet, müssen die Accesspoints diese nicht unterstützen. Vertrauliche Daten werden hierdurch nicht gefährdet, da diese nur über den VPN–Kanal übertragen werden.

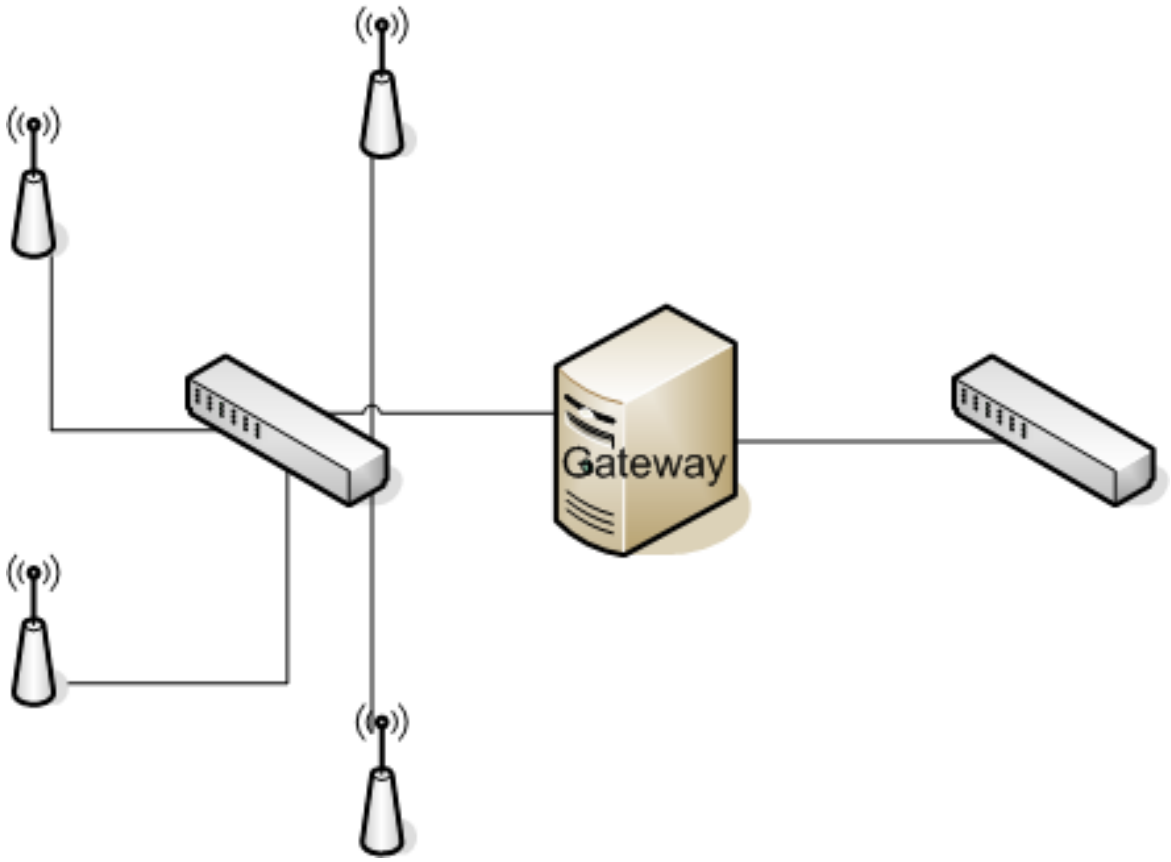

Abbildung 3.4.: Mehrere Accesspoints an der externen Gatewayschnittstelle

Ab einer gewissen Grösse des Geländes werden mehrere Accesspoints nötig, damit die Abdeckung gewährleistet ist. (siehe Abb. 3.3 auf Seite 23) Diese bilden dann ein offenes Netz, mit dem Gateway als Schnittstelle in das geschlossene Netzwerk.

3.4. Gateway

Der Gateway steht zwischen dem gänzlich offenen Funkbereich und den Servern des Clubnetzes. Er hat mehrere Aufgaben:

- Abhalten von nicht–authentifizierten Geräten
- Vertraulichkeit der Daten
- Isolieren der PDA's voneinander
- Routen der Daten zu den internen Clubservern

Diese Aufgaben werden von unterschiedliche Komponenten erfüllt:

- Packetfilter
- Schlüsselaustauschdienst
- VPN–Server

Diese drei Komponenten müssen korrekt konfiguriert werden und zusammenarbeiten, um die Aufgaben zu erfüllen.

Um zu vermeiden, das nichtzahlende Personen das Netz nutzen, leitet er nur den Verkehr von authentifizierten Benutzern weiter, deren Daten er nur verschlüsselt annimmt, um ein Belauschen der Kommunikation zu verhindern. Die nötigen Authentifikationsdaten erhält er vom Authentifikationsserver.

Schlüsselaustauschdienst

Der Schlüsselaustauschdienst auf dem Gateway, ist das Gegenstück zum Schlüsselaustauschdienst auf einem PDA. Er hat jedoch nicht nur Informationen um einen Gegenpunkt zu authentifizieren, sondern erhält vom Authentifikationsserver die Informationen, die nötig sind um jeden zugelassenen PDA zu identifizieren. Sollten Geräte verloren gehen, werden ihre Zugangsdaten als ungültig markiert und der Gateway erlaubt ihnen keine weiteren Verbindungen in das Clubnetz. Ausserdem hat er Zugriff auf geheime Informationen, mit denen er sich gegenüber den PDA 's authentifizieren kann.

Ist die gegenseitige Authentifikation erfolgreich, wird ein Sitzungsschlüssel, der nur dem anfragenden PDA und dem Schlüsselaustauschdienst bekannt ist, erzeugt und dem VPN–Server übergeben, der die weitere Kommunikation verwaltet.

VPN-Server

Der VPN–Server stellt zusammen mit dem VPN–Client auf dem PDA den Tunnel zur Verfügung, über den die Anwendungsdaten laufen. Diese Verbindung wird mit dem ausgehandelten Sitzungsschlüssel verschlüsselt. Den Anwendungen bietet er die Möglichkeit, den Tunnel wie eine normale Netzwerkschnittstelle zu nutzen und somit Daten vor Mithören und Verfälschen während der Übertragung zu sichern.

Packetfilter

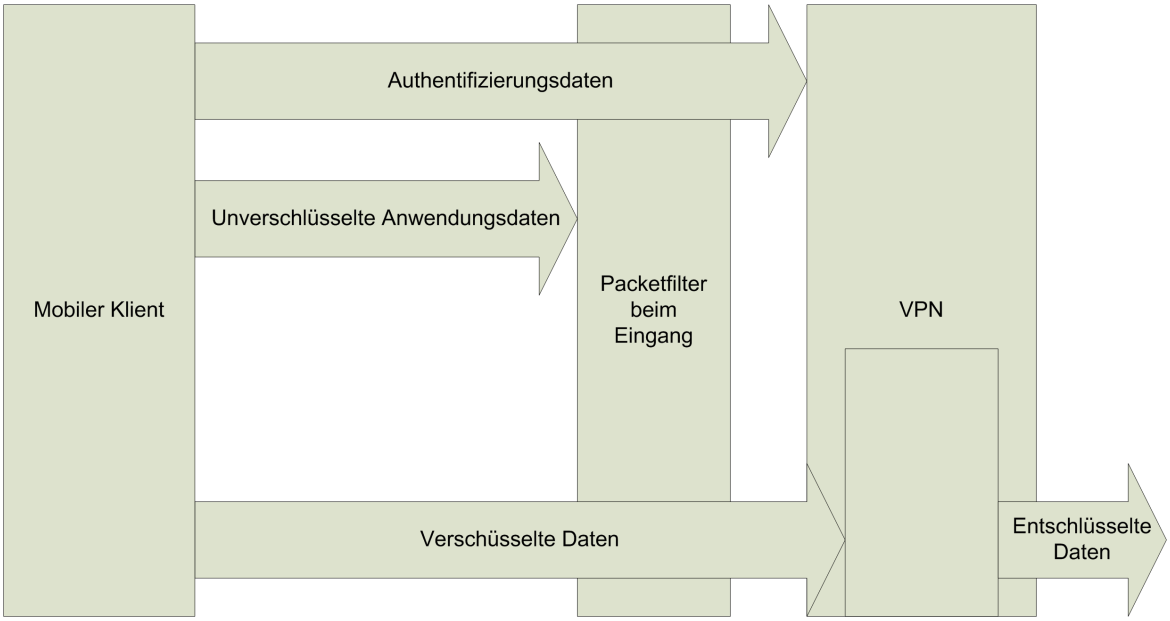

Abbildung 3.5.: Regeln über eingehende Pakete auf der Gatewaynetzwerkschnittstelle

Es wurde im Kapitel 3 gefordert, daß die Endgeräte möglichst restriktiv entscheiden, welche Daten weitergeleitet werden und welche Daten den Anwendungen präsentiert werden. Hierfür sollen die PDA's von allen anderen Netzwerkteilnehmern isoliert werden, die nicht für die Bereitstellung von Diensten nötig sind.Ausserdem soll keine Kommunikation über die unverschlüsselte Schnittstelle laufen, die nicht zur Authentifikation nötig sind.

Um diese Ziele zu erreichen, wird auf dem Gatewayrechner ein Packetfilter eingerichtet, der Netzwerkverbindungen nach Portnummer und Quell– bzw. Zieladresse filtert. In Tabelle 3.1 sind alle gültigen Quell/Ziel–Verbindungen aufgeführt.

Für den IP–Stack auf dem Client, ist der VPN–Tunnel nur eine von mehreren Netzwerkschnittstellen, über die Daten versendet werden. Da die Endgeräte vor anderen Netzwerkteil-

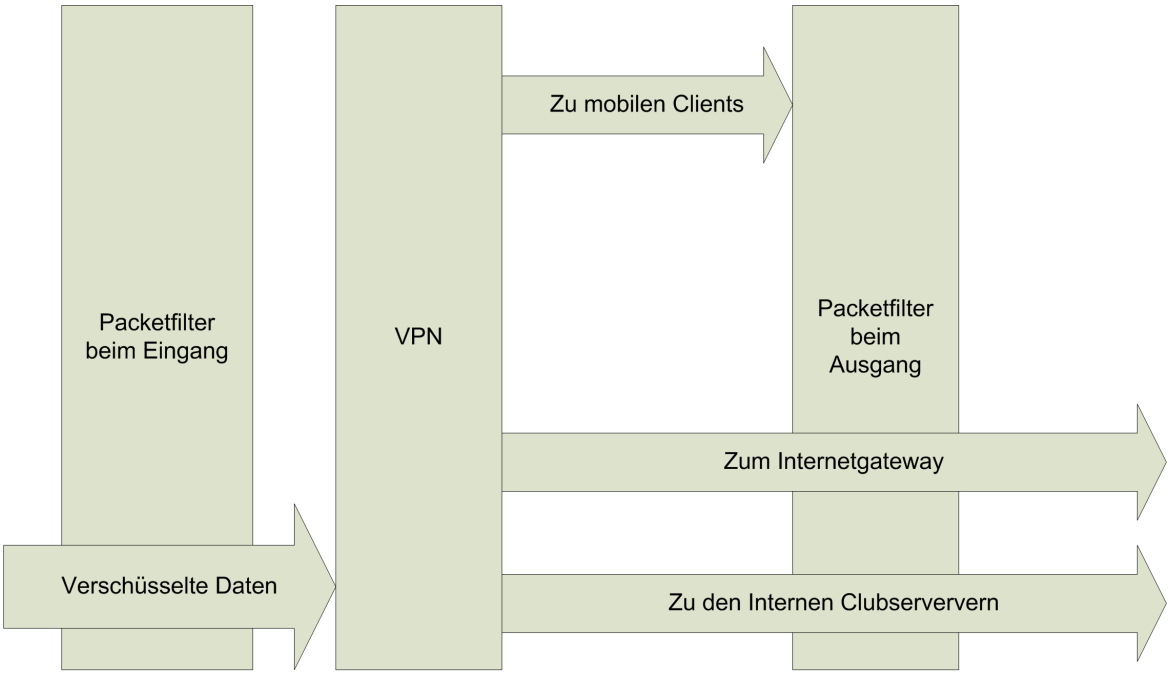

Abbildung 3.6.: Regeln über ausgehende Pakete auf der Gatewaynetzwerkschnittstelle.

nehmern isoliert werden sollen, werden Pakete eines PDAs, nicht in das VPN eines anderen PDAs geroutet.

Der Packetfilter ist der zentrale Punkt über den alle Netzwerkdaten des Gatewayrechners laufen. An diesem Punkt setzt die Kontrolle über den Datenfluss an. Er kontrolliert ob die Kombination von End– und Zielpunkt, sowie die Art der Übertragung (verschlüsselt oder nicht) erlaubt ist. Gültige Kombinationen sind in Tabelle 3.1 auf Seite 27 festgelegt. Hierbei sind die Fälle unverschlüsselter und verschlüsselter Verkehr gesondert aufgeführt.

- Unverschlüsselte Daten dürfen nur zum Aufbau der verschlüsselten Verbindung versendet werden.
- Die Daten eines PDA dürfen keinen PDA als Ziel haben
- Die Daten eines PDA dürfen nur die festgelegten Clubserver als Ziel haben.
- Daten die Clubserver als Ziel haben, dürfen nur über die verschlüsselte Verbindung laufen

	PDA 1	PDA 2	Gateway	Anwendungsserver	Internet–Gateway
Unverschlüsselt					
PDA 1	Kein Bedarf	Nein	Ja	Nein	Nein
PDA 2	Nein	Kein Bedarf	Ja	Nein	Nein
Gateway	Ja	Ja	Kein Bedarf	Ja	Ja
Anwendungsserver	Nein	Nein	Ja	Kein Bedarf	Nein
Internet–Gateway	Nein	Nein	Ja	Nein	Kein Bedarf
Verschlüsselt					
PDA 1	Kein Bedarf	Nein	Ja	Ja	Ja
PDA 2	Nein	Kein Bedarf	Ja	Ja	Ja
Gateway	Ja	Ja	Kein Bedarf	Kein Bedarf	Kein Bedarf
Anwendungsserver	Nein	Nein	Ja	Kein Bedarf	Kein Bedarf
Internet–Gateway	Nein	Nein	Ja	Nein	Kein Bedarf

Tabelle 3.1.: Zulässige Quell– und Zielverbindungen

3.5. Authentifikationsserver

Eines der Ziele dieses Systems ist es, das nur vom Club ausgegebene mobile Geräte, sich mit dem Netz des Clubs verbinden können. Auch für diese sollen Einschränkungen gelten, falls sie aus dem Einflussbereich der legitimen Gäste verschwinden, oder falls Gäste ihre Geräte nicht abgeben. Einmal erzeugte Accounts müssen also eine begrenzte Gültigkeitsdauer haben, sowie bei Bedarf widerrufen werden.

Diese Verwaltung der Benutzerkonten übernimmt ein zentraler Authentifikationsserver, der dem Gateway die Informationen zur Verfügung stellt. Um effektiv zu bleiben, muss er seinerseits aktuelle Informationen erhalten.

Wie ihm diese zur Verfügung gestellt werden, soll hier nicht ausgeführt werden. Es muss einen Prozess geben, der ihm Ereignisse wie ausgegebene Geräte, gestohlene Geräte und abgereiste Gäste mitteilt. Eine weitere Möglichkeit wären auf 48h begrenzte Schlüssel, die über eine Schnittstelle, die physischen Zugang erfordert, erneuert werden.

Da dieser Server die Zugangsdaten sämtlicher Endgeräte enthält, sollte er soweit wie möglich isoliert werden. Die einzigen benötigten Schnittstellen sind die zum Gatewayserver und ein Zugang zur Pflege der Zugangsdaten.

Es gibt mehrere Möglichkeiten zum Überprüfen der Accountdaten, wobei eine wichtige Eigenschaft ist, daß auch bei Ausfall des Authentifikationsservers keine ungültigen Logins akzeptiert werden. D.h. bei jedem Verbindungsversuch muss überprüft werden, ob der Authentifikationsserver erreichbar ist, bevor ein Tunnel aufgebaut wird.

3.6. Netze

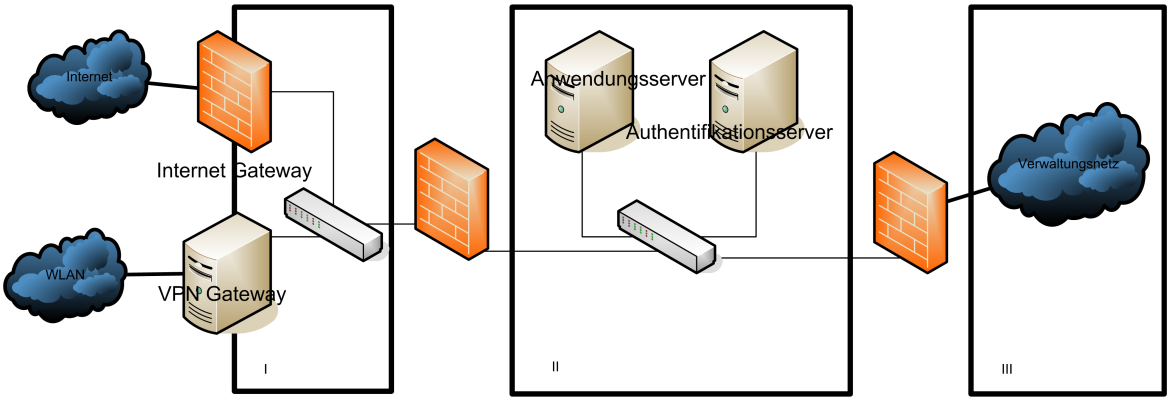

Abbildung 3.7.: Verschiedene Netze

III Internes Verwaltungsnetz: Zum Betrieb des Clubs notwendig

II Dienstleistungsserver: Hier werden die Services für die Kunden angeboten. Information, Bestellung, Autorisierung.

WLAN Der Zugang für die Kunden

Internet

Die gesamte Infrastruktur des Clubs wird in mehrere voneinander getrennte Netze aufgeteilt, nach den Bedürfnissen ihrer Nutzer und dem Schutzbedarf der Daten. Es gibt Komponenten, die an den Schnittstellen sitzen und die Kommunikation verwalten. Eine Beschreibung dieses Aufbaus steht auch schon in Mählmann2004 und Lüpke2004.

	Verwaltungsnetz	Anwendungsserver	WLAN	Internet
Verwaltungsnetz	Angebote			
Anwendungsserver	Abrechnungsdaten			
WLAN		Authentifikationsanfragen, Bestelldaten		
Internet		Webzugang		

Tabelle 3.2.: Informationsfluss

4. Techniken

Es gibt verschiedene Möglichkeiten, die Funktionalitäten, die die im Kapitel 3 beschriebenen Komponenten erfordern, zu implementieren. Bei der Auswahl muss man sowohl darauf achten, daß die geforderte Funktionalität vollständig erhalten ist, als auch, daß das Protokoll sowie die Implementation den geforderten Sicherheitsbedürfnissen entspricht.

Dies für die im folgenden beschriebenen Protokolle im einzelnen zu untersuchen, sprengt nicht nur den Rahmen dieser Arbeit, sondern leidet auch noch darunter, das man Sicherheit nur schwer positiv nachweisen kann.[1] So ist auch für viele der heutigen kryptographischen Algorithmen nicht bekannt, ob erfolgreiche Angriffe mit einem geringeren Aufwand, als ein Brute–Force Angriff erfordert, existieren. Es ist nur bekannt, wieviele Personen bis jetzt erfolglos versucht haben, einen solchen zu finden.

Unter diesem Gesichtspunkt, sollte man ältere Protokolle, die bereits mehreren Untersuchungen standgehalten haben bevorzugen. (Schneier 2004, 107 ff.)

In diesem Kapitel werden zuerst einige Authentifikationsprotokolle mit ihren Stärken und Schwächen vorgestellt, im Vergleich zu den in den Kapiteln 2 und 3 geforderten Aufgaben. Danach werden mehrere vorhandene Tunnellösungen beschrieben, zusammen mit Erwähnungen durchgeführter Sicherheitsuntersuchungen, ihrer Unterstützung der in 4.1 aufgeführten Protokolle, sowie ihrer Zusammenarbeit mit zentralen Authentifikationsdatenbanken.

4.1. Authentifikation

- Kein Übertragen von Zugangsdaten
- Eindeutige Identifikation
- Keine Abhängigkeit der Schlüsselentropie von Passworten
- Wechselnde Schlüssel

[1] Weitergehende Betrachtungen zu Sicherheit im WLAN sind in (Postel u. a. 2004)

Kerberos

Ein Kerberosserver ist eine zentrale Instanz, die Clients auf Anfrage Nachweise ihrer Identität und der Berechtigung auf gewisse Server zuzugreifen ausstellt (Tickets). Die Struktur dieser Tickets garantiert es, das nur der anfragende Client sowie der gewünschte Server die Autorisierungskommunikation lesen können. Es ermöglicht auch, das nur einmalige Anmeldung mit Benutzerinteraktion nötig ist, alle weiteren Anfragen an Server im Verbund kann durch SW auf Clientseite automatisiert werden, ohne das ein Passwort gespeichert werden muss.

Dieses Protokoll wird ausführlich in (Vale u. a. 2004) und in (Hübner 2004) vorgestellt.

In Zusammenhang mit dieser Arbeit wäre Kerberos eine geeignete Lösung, leider unterstützen noch nicht genug VPN-Clients Kerberos als Authentifizierungsprotokoll.

Zusammenfassung:

- sichere Kommunikation
- Lange erprobt
- Freie Implementierungen des Authentifikationsservers
- Integration mit Servern nur auf 2 Plattformen (Linux ab Kernel 2.6 und FreeBSD mit Isakmpd Racoon)
- Integration auf Clients erst ab Linux Kernel 2.6

X509-Zertifikate

Zertifikate ermöglichen ebenfalls eine sichere Authentifizierung der Benutzer, ohne Passworte zu übertragen. In (Postel u. a. 2004) werden einige Probleme mit der Praktikabilität erwähnt. Zum Beispiel den nötigen Aufbau einer Infrastruktur, sowie Schwierigkeiten bei oft wechselnden Clientzertifikaten. In diesem fiktivem Ferienclub ist eine PKI ohnehin vorgesehen, da sie für die verbindlichen Geschäfte der Gäste zuständig ist. Die Zertifikate werden ohnehin gewechselt, sobald ein Gerät an die Verwaltung zurückgegeben wird.

Im Falle von kompromittierten Zertifikaten, muss die Certificate Revocation List (CRL) aktualisiert werden, bevor sie der IKE als ungültig zurück weist. Es müssen Maßnahmen definiert werden, die ein zeitnahes aktualisieren der CRL als Ziel haben. Bei Erstellen des Revocation Certificates wird überprüft, ob dieses erfolgreich an den Gatewayserver übermittelt wurde.

Wie man in 4.1 sieht, können auch bei nur einem Rechner, der die Zertifikate nutzt, unerwünschte Nebenwirkungen auftreten, wenn die Zertifikate nicht bei jeder Nutzung mit einer

	Zentrale Speicherung	Lokale Speicherung
Neue Benutzer	Kein Login(Fehler)	Login(korrekt)
Gültige Benutzer	Kein Login(Fehler)	Login(korrekt)
Abgelaufene Benutzer	Kein Login(Korrekt)	Kein Login(korrekt)
Kompromittierte Zertikate	Kein Login(Korrekt)	Login(Fehler)

Tabelle 4.1.: Fehlerauswirkungen bei Unterbrechung der Verbindung zwischen PKI-Verwaltung und Gateway

zentralen Instanz verglichen werden. (Unberechtigte Nutzer, können mit kompromittierten Zertifikaten das Netz nutzen) Der Nachteil liegt in der geringeren Verfügbarkeit, da auch gültige Zertifikate nicht mehr überprüft werden können, was zu einem Ausfall des Netzzugangs für alle berechtigten Benutzer führt.

Zusammenfassung:

- Infrastruktur vorhanden
- In Anbetracht der Verwendung als Unterschrift ist ein gemeinsames Zertifikat für Infrastruktur und Benutzerauthentifizierung nicht gut

Shared Secret

Clients haben ein Passwort, mit dem sie Daten so verschlüsseln, daß nur der Server sie entschlüsseln kann. in Diesem Fall ist “shared” nur auf Client und Server bezogen, nicht auf eine grössere Gruppe.

Hierbei gibt es zwei Möglichkeiten:

Das Shared Secret ist aus einem Passwort abgeleitet Hierbei hängt die Entropie des Schlüssels von der des Passwortes ab, wodurch hohe Bit-Anzahlen im kryptographischem Algorithmus relativiert werden.

Hinterlegter Schlüssel Oder das Shared Secret wird auf dem PDA hinterlegt, bevor er dem Benutzer ausgehändigt wird. Ein Problem hierbei ist, das sämtliche Kommunikation über die Nutzungszeit mit einem einzigen kryptographischem Schlüssel erfolgt.

4.2. Transportsicherheit

Da diese Arbeit die Absicherung des Netzwerkes auf unterer Ebene beschreiben will, wird nicht weiter auf die Möglichkeiten der Verschlüsselung auf Anwendungs–, Session–, oder Verbindungsebene eingegangen, die immer noch eingesetzt werden können, da z.B. SSL auch eine Benutzerauthentifikation zur Verfügung stellt.

IpSec

Was ist IpSec

IpSec ist eine Sammlung von Protokollen, die Authentifizierung und Vertraulichkeit auch für IP–Netzwerke garantieren sollen. Diese Protokolle sind[2]:

AH – Authentication Header Garantiert Authentizität, durch Signierung der Pakete. Voraussetzung ist ein gemeinsamer Schlüssel

ESP – Encapsulation Payload Garantiert vertrauliche Übertragung, durch Verschlüsseln der Paketdaten mit wählbaren kryptographischen Verfahren. Voraussetzung ist ein gemeinsamer Schlüssel.

IPcomp Komprimiert die Paketdaten vor dem Verschlüsseln

IKE – Internet Key Exchange AH und ESP brauchen einen gemeinsamen Schlüssel. IKE erlaubt es zwei Systemen gegenseitig einen solchen auszuhandeln.

IpSec bietet zwei Arbeitsmodi an:

Tunnelmodus Pakete werden auf einem Teilabschnitt der Übertragung verschlüsselt. Dies kann der Weg zwischen zwei Gateways sein, oder zwischen dem Client und dem Gateway zum gesicherten Netz.

Transportmodus Die Pakete werden zwischen Client und Zielrechner verschlüsselt.

[2] (NetBSD-Team 2005)

Wie authentifiziert IpSec

IpSec hat zwei Möglichkeiten, sich auf einen gemeinsamen Schlüssel zu einigen: Pre–Shared–Keys, oder die Verwendung eines IKE–Daemons. Da für jeden Verbindungsaufbau einen neuen Sitzungsschlüssel auszuhandeln, sollte man einen solchen verwenden. Die verschiedenen Implementierungen dieses Daemons unterstützen verschiedene Methoden der gegenseitigen Authentifikation.

PKI Wird von den meisten Varianten unterstützt, auch von der bei Linux 2.4.xx verwendeten Variante.

Kerberos Wird von den Daemons unter FreeBSD und Linux 2.6 unterstützt

Von diesen Varianten wäre Kerberos sinnvoll, da es ein auf Sicherheit ausgelegte Methode zur zentralen Authentifikation ist. Kerberos wird allerdings erst von neueren Varianten von IKE–Daemons unterstützt, die noch nicht auf allen PDA–Plattformen portiert wurden.

Fazit

> Even with all the serious critisisms that we have on IPsec, it is probably the best IP security protocol available at the moment. (Schneier und Ferguson 2000, 1)

In ihrer Arbeit “A Cryptographic Evaluation of IPsec” kommen Schneier und Ferguson zu dem Schluss, daß trotz einiger Schwächen, die sie vor allem seiner Komplexität anlasten, IPSec momentan das wohl sicherste Verfahren ist. hierzu trägt auch bei, das es momentan wahrscheinlich am intensivsten untersucht wird, da es als verpflichtender Teil der IPv6 Spezifikation ein wichtiger Teil des zukünftigen Internets sein wird.[3]

> We strongly discourage the use of IPsec in its current form for protection of any kind of valuable information, and hope that future iterations of the design will be improved. However, we even more strongly discourage any current alternatives, and recommend IPsec when the alternative is an insecure network. Such are the realities of the world. (Schneier und Ferguson 2000, 99)

[3] (Postel u. a. 2004), (Schneier und Ferguson 2000)

PPtP

Was ist PPtP

Ein von Microsoft entwickeltes Protokoll, um den sicheren Zugang zum Firmennetzwerk über Einwahlknoten zu ermöglichen. Authentifikation erfolgt über MS-CHAPv2, nachdem sich die erste Version nicht als ausreichend sicher erwiesen hat.

Welche Anmeldeverfahren hat PPtP

PPtP bietet verschiedene Varianten der Benutzerauthentifikation an, die jedoch alle gewisse Schwächen haben.

PAP Übertragt Benutzernamen und Passwörter im Klartext

CHAP Ein Challenge/Response–Verfahren, das den Benutzernamen im Klartext überträgt

MS–CHAPv2 Die aufgrund von Schwächen von MS–CHAPv1 weiterentwickelte Variante

Von diesen Verfahren wäre MS–CHAPv2 am geeignetsten, jedoch bleiben einige Schwächen, die Bruce Schneier und Mudge zu dem Schluss kommen lassen:

> Microsoft has improved PPTP to correct the major security weaknesses described in [. . .]. However, the fundamental weakness of the authentication and encryption protocol is that it is only as secure as the password chosen by the user. As computers get faster and distributed attacks against passwordfiles become more feasible, [. . .] Since authentication and key-exchange protocols which do not allow passive dictionary attacks against the user's password are possible [. . .] it seems imprudent for Microsoft to continue to rely on the security of passwords. Our hope is that PPTP continues to see a decline in use as IPSec becomes more prevalent. (Schneier u. a. 1999, 11)

L2tP

L2tP vereint die Eigenschaften von Ciscos Entwicklung L2F mit Microsofts PPtP, mit IPSec als verschlüsselnder Komponente. Es ist eine Erweiterung des Point–to–Point Protokoll, das laut Cisco bereits ein Teil von vielen VPNs ist.

Zu den Nachteilen im Rahmen dieser Arbeit zählen:

- Abhängig von einer PK–Infrastruktur

- Wenige open–source Implementierungen
- Langer Protokollstack und hoher Overhead

Wohingegen die Vorteile die in (Postel u. a. 2004, 84) aufgeführt werden, namentlich:

- Einfache Benutzung
- Weite Verbreitung

durch die Rahmenbedingungen des Szenarios grösstenteils nebensächlich werden. Die Endgeräte werden vom Club ausgewählt und den Kunden vorkonfiguriert ausgehändigt. [4]

OpenVPN

OpenVPN ist eine Lösung, die auf Basis der OpenSSL–Authentifikations– und Verschlüsselungsmethoden einen IP–Tunnel zur Verfügung stellt. Er hat einige Möglichkeiten, die es erlauben, den Client zu konfigurieren. Clientsoftware ist unter anderem für Linux und Windowsplattformen erhältlich, jedoch nicht für das alle PDAs.[5] Sollte eine Portierung auf die gewählte Plattform erfolgen, kann man über die Verwendung nachdenken, da OpenVPN bereits Kerberos unterstützt[6].

[4] Quellen für diesen Abschnitt sind (Team 2003) und (Postel u. a. 2004, 84)
[5] (Yonan)
[6] (Speel 2004)

5. Prototyp

5.1. Laborumgebung

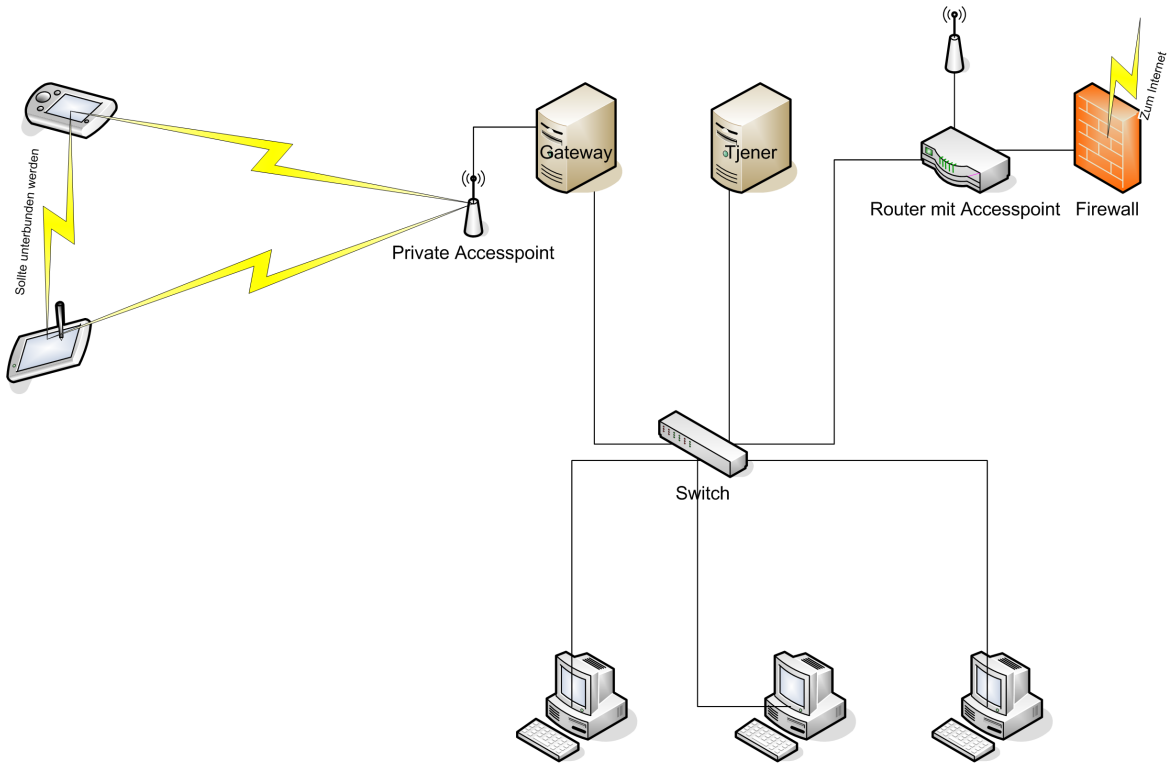

Abbildung 5.1.: Vorhandene Struktur in der Testumgebung

Das Labornetzwerk besteht aus einem geswitchten Netzwerksegement, das über einen NAT-Router mit einer Firewall der Hochschule für Angewandte Wissenschaften Hamburg verbunden ist. Dieser Router hat einen eingebauten Accesspoint mit WEP-Verschlüsselung und ausgeschaltetem SSID-Broadcast. Die drahtlosen Geräte erscheinen im Netzwerk jedoch gleichberechtigt mit den Clients die über Kabel mit dem Switch verbunden sind. IP–Adressen werden über einen DHCP-Server vergeben, auf dem auch ein LDAP-Verzeichnisdienst zur Benutzerverwaltung läuft.

Gatewayrechner

Der Gatewayrechner ist ein handelsüblicher Intel–PC. Es wurde die Linuxdistribution “Debian GNU/Linux 3.1 (Sarge)” mit einem Kernel der Version 2.6.8-2-686 als Betriebssystem gewählt. Da die nötigen Funktionen auch auf anderen Betriebssystemen vorhanden sind, ist es kein Problem, auch ein anderes Betriebssystem zu installieren.

Accesspoint

In den Gatewayrechner ist eine SMC2802 PCI–Wlankarte mit einer Übertragungsrate von 54Mbit eingebaut, und Unterstützung für den “Master–Mode” mit dem sie die Funktion eines Accesspoints übernehmen kann.

PDA

Als PDA kommt ein Siemens Simpad SL4 zum Einsatz das nach den Vorgaben von Mählmann (2004) eingerichtet ist. Dieses unterstützt Wireless Lan 802.11b mit Hilfe einer PCMCIA WLAN–Karte.

Authentifikationsserver

Die Funktion des Authentifikationsservers übernimmt eine mit Certificate Authority auf dem Gatewayrechner.

5.2. Einrichtung

Der IpSecdienst auf dem Simpad sollte von den IpSec–Modulen des 2.4er Kernels übernommen werden. Die Funktion des Authentifikationsserver wurde mit OpenSSL realisiert. Der IpSECdienst auf dem Gatewayrechner wird von den 2.6er Kernelmodulen und dem IKE–Server “Raccoon” zur Verfügung gestellt.

Für den Prototypen wurden der Authentifikationsserver, und der Gatewayrechner eingerichtet. Hiermit besteht die Möglichkeit Authentifikationsdaten für Gäste zu erzeugen, die mit einer begrenzten Gültigkeitsdauer versehen sind. Bei Bedarf können die Clientzertifikate auch widerrufen werden. Clients können sich mit den ihnen zugeteilten Zertifikaten anmelden.

Authentifikationsserver

OpenSSL wurde mit Hilfe der Debianpaketverwaltung installiert wurde[1] Es wurde ein selbstsigniertes Zertifikat generiert, daß zur Beglaubigung aller weiteren Zertifikate dient:

```
openssl genrsa -out ca-key.pem 1024
openssl req -new -key ca-key.pem -out ca.csr
openssl x509 -req -days 365 -in ca.csr \
       -signkey /root/ca/ca-key.pem -out ca.pem
```

Alle weiteren Zertifikate werden mit “ca-key.pem” signiert. Das Zertifikat “ca.pem” wird an alle Teilnehmer des Systems verteilt, die die Gültigkeit von Zertifikaten überprüfen müssen.

Die Zertifikate für den Gatewayrechner und die PDA s unterscheidet sich nur in der Gültigkeitsdauer, die bei den Gästen von 365 Tagen auf die Dauer des Aufenthaltes gekürzt wird. Damit die Zertifikate später widerrufen werden können, werden sie archiviert. [2]

Sollte ein Gerät verloren gehen, wird das, auf ihm enthaltene Zertifikat zurückgerufen.[3]

Wlantreiber

Der Treiber der WLAN–Karte benötigt zuerst ein Firmware–Image des Herstellers, das unter /usr/lib/hotplug/firmware/isl3890 liegen muss.

```
/sbin/lsmod | /bin/grep -q prism54 || /sbin/modprobe prism54
```

Die Karte wird danach im Mastermodus gestartet dient als Accesspoint im IP–Bereich 192.168.0.xxx, auf Kanal 3. WEP–Verschlüsselung ist ausgeschaltet, da die Sicherheit über IpSEC erreicht werden soll.

```
ifconfig eth1 promisc netmask 255.255.255.0 192.168.0.1 up
iwconfig eth1 channel 3
iwconfig eth1 mode "Master"
iwconfig eth1 essid "Clubnetz"
# iwconfig eth1 key FFFFFFFFFFFFFFFFFFFFFFFFFF
iwconfig eth1 key off
```

[1] `apt-get install openssl`
[2] Die Befehle zum Generieren von Server– und Client–Zertifikaten sind in B.3 und B.4 aufgeführt.
[3] Siehe Abschnitt B.5

IPsec auf Serverseite

Es wird der IKE–Server Raccoon und die IpSEC–Kernelmodule des Kernels 2.6 installiert. Die Konfiguration [4] erfolgt dergestalt, das aus dem WLAN kommende Anfragen nach einem Tunnel erfolgreich sind, wenn sich der anfragende PDA mit einem gültigem Zertifikat ausweisen kann. Zur Überprüfung dienen eine gültige Unterschrift der eigenen Certificate Authority und eine Certificate Revocation List (CRL) die von der CA gepflegt wird.

IpSec auf Clientseite

Dieser Abschnitt beschreibt die gewünschte Konfiguration auf Clientseite: Auf dem PDA sollen die IpSec–Module des 2.4er Kernels mit dem ipkg Befehl. dem IKE-Server “isakmpd” des Free S/Wan Projektes wird das eigene Zertifikat mit dem privaten Schlüssel, sowie das Zertifikat des Gatewayservers bekanntgegeben.

[4] Konfigurationsdateien, siehe B.1

6. Fazit und Ausblick

6.1. Fazit

Diese Arbeit hat gezeigt, daß sich die wesentlichen Bedrohungen, der drahtlosen Übertragung abwenden lassen. Die hierfür notwendigen Maßnahmen betreffen die Betriebssystemebene. Der Prototyp hat gezeigt, daß es zwar viele Bausteine gibt, mit denen sich das Ziel erreichen ließe. Jedoch waren nicht alle auf dem PDA verfügbar. Eine Netzwerkinfrastruktur, die die gestellten Anforderungen erfüllt, war dennoch zu realisieren. Die Entscheidungen für bestimmte Techniken, wurden jedoch zu einem großen Teil durch die Verfügbarkeit der Software auf der Zielplattform beeinflußt.

Aufgrund der hohen Konfigurationskomplexität ist es jedoch schwierig zu sagen, ob die Sicherheit, die die Werkzeuge für VPN und Authentifikation bieten, nicht durch falsche Optionen preisgegeben wurden.

6.2. Ausblick

Es wäre wünschenswert, wenn die Authentifikationsdaten auf dem PDA nicht im Klartext vorliegen müssten, um verwendet zu werden. hierfür wäre eine stärkere Einbindung in den Authentifikationsprozess des Benutzers nötig, oder die Nutzung von biometrischen Verfahren. So könnte z.B. eine Kamera aus den Gesichtsdaten einen Schlüssel zur Ver/Entschlüsselung des Zertifikats generieren.

Es gäbe auch alternative Methoden der Schlüsselverwaltung. So könnte jedes Gerät, das sich in einem definierten Bereich befindet, einen neuen Schlüssel erhalten, wenn sein Besitzer erkannt wurde und er im Besitz des Gerätes ist.[1]

[1] Im Besitz bedeutet: Position von Gerät und Gast stimmen überein.

A. Angriffe

There are four types of security threats to consider (Pfleeger 1997):

- Interception
- Interruption
- Modification
- Fabrication

Tanenbaum und Steen (2001)

A.1. Unerlaubte Nutzung der Bandbreite

Ist der Zugang zum Internet nicht durch Authentifizierung gesichert, so kann dieser auch von unbefugten Personen genutzt werden. Entweder Clubgäste, die ihn nicht bezahlen, oder clubfremde Personen, die sich noch im Empfangsbereich eines Accesspoints befinden. Durch die geringe Bandbreite einer Wlans kann dies auch die Verbindungen anderer Gäste zu den Clubservern beeinträchtigen.

A.2. DOS–Angriff auf den Authentifizierungsdienst

Auch wenn durch die begrenzte räumliche Ausdehnung eines WLans die Gefahr von DDOS nicht gegeben ist, so können doch Schwächen im Authentifizierungsdienst dazu führen, das er von unrechtmäßigen Benutzern unerreichbar gesetzt wird. Dies würde dazu führen, das rechtmässige Benutzer keine Verbindungen mehr aufbauen können, da sie sich nicht mehr authentifizieren können. Sollte man versuchen, diese Gefahr durch Cachen von Authentifizierungsinformationen zu umgehen, würde man es ermöglichen, daß kompromitierte Informationen weiterhin als gültig anerkannt werden.

A.3. DOS–Angriff auf die Accesspoints

Ein Angreifer flutet den genutzten Frequenzbereich, mit unnützen Daten. Bei gültigen WLAN-Paketen würde die Kollisionserkennung die nutzbare Datenrate stark nach unten regeln. Da die Sendestärke geregelt ist und WLAN auf einer frei nutzbaren Frequenz übertragen wird, ist fraglich was als Gegenmassnahme möglich ist, ausser den Störer vom Clubgelände zu verweisen.

A.4. Passives Abhören

Radiowellen, durch die die Daten übertragen werden, sind ein offenes Medium. Jeder Angreifer kann die übertragenen Pakete empfangen. Um die übertragenen Informationen trotzdem vertraulich zu halten, ist es notwendig kryptographische Verfahren anzuwenden.

Hierbei sind die in üblicher WLAN-Hardwaretechnik mitgelieferten Techniken nicht ausreichend, da sie starke Mängel haben.

A.5. Man in the Middle

Dieser Angriff ist erfolgversprechend, wenn sich Client und Server nicht kennen, und keine Möglichkeit haben ihre Identität zu überprüfen. Da in diesem Szenario die Möglichkeit besteht, allen Endgeräten über einen sicheren Kanal Informationen zu geben, die eine Eindeutige Identifikation des Kommunikationspartners zu geben, sollte man diese Gefahr minimieren können.

B. Konfigurationsdateien und Code

B.1. Racoon

```
path certificate "/etc/racoon/certs";
listen
{
  isakmp 192.168.0.1;
  isakmp 10.0.2.50;
}

# Eintrag für Clients mit unbekannten IPs
remote anonymous {
        exchange_mode main;
        generate_policy on;
        passive on;
initial_contact on;

        doi ipsec_doi;
        certificate_type x509 "sc.pem" "sk.pem";
        verify_cert on;
        my_identifier asn1dn;
        peers_identifier asn1dn;
        verify_identifier off;
        lifetime time 60 min;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm md5;
                authentication_method rsasig;
                dh_group modp1024;
        }
}
```

```
sainfo anonymous {
        # pfs_group modp1024;
        encryption_algorithm 3des;
        authentication_algorithm hmac_md5;
        compression_algorithm deflate;
}
```

B.2. Generieren des CA–Zertifikates

```
openssl genrsa -out ca-key.pem 1024
openssl req -new -key ca-key.pem -out ca.csr
openssl x509 -req -days 365 -in ca.csr \
       -signkey /root/ca/ca-key.pem -out ca.pem
```

B.3. Generieren des Raccoon–Zertifikates

```
openssl genrsa -out gateway-key.pem 1024
openssl req -new -key gateway-key.pem -out gateway.csr
openssl x509 -req -days 365 -in gateway.csr \
       -CA /root/ca/ca-key-cert.pem -CAkey /root/ca/ca-key.pem \
       -out gateway-certificate.pem
```

B.4. Generieren eines Gast–Zertifikates

```
# Usage:
#   makecert <guestname> <duration>
mkdir /root/guests/cert/${1}
cd /root/guests/cert/${1}
mkdir certs
cd certs

echo "Generate Key"
openssl genrsa -out ${1}.pem 1024
echo "Generate CSR"
```

```
openssl req -new -key ${1}.pem -out ${1}.csr
echo "Generate Cert"
openssl x509 -req -days 14 -in ${1}.csr \
       -CAkey /root/ca/ca-key.pem \
       -CA /root/ca/ca-key-cert.pem\
       -trustout \
       -out ${1}-cert.pem
```

B.5. Aktualisieren der CRL

```
# Generate a CRL
openssl ca -gencrl -out crl.pem


openssl ca -revoke <certificate> -crl\_compromise JJJJMMTTSSMMSSZ
```

Literaturverzeichnis

BSI 1992 INFORMATIONSTECHNIK, Bundesamt für Sicherheit in der: *Grundschutzhandbuch*. Bundesamt für Sicherheit in der Informationstechnik, 1992. – URL http://www.bsi.de/

BSI 2003 INFORMATIONSTECHNIK, Bundesamt für Sicherheit in der: *Grundschutzhandbuch*. Bundesamt für Sicherheit in der Informationstechnik, 2003. – URL http://www.bsi.de/

Hübner 2004 HÜBNER, Prof. Dr.-Ing. M.: *IT–Sicherheit*. 2004

Jakob 1999 JAKOB, Dr.: *Tätigkeitsberichte des Bundesamtes für Datenschutz*. Bd. 17: *17ter Tätigkeits bericht*. Bundesamt für Datenschutz, 1999. – URL http://www.bfd.bund.de/information/tb9798/kap00/Start.html

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

Mählmann 2004 MÄHLMANN, Lars: *Sichere Übertragung im WLan mit mobilen Endgeräten (speziell unter Linux)*, Hochschule für Angewandte Wissenschaften Hamburg, Diplomarbeit, jun 2004. – URL http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/studien/maehlmann.pdf

NetBSD-Team 2005 NETBSD-TEAM, The: NetBSD Documentation: NetBSD IPsec. (2005). – URL http://www.netbsd.org/Documentation/network/ipsec/. – Zugriffsdatum: 2005-02-21

Pfleeger 1997 PFLEEGER, Charles P.: *Security in Computing*. Prentice-Hall, 1997

Postel u. a. 2004 POSTEL, Patrick ; SCHÜNEMANN, Sebastian ; ZDRZALEK, Jaroslaw: *Sicherheit in kommerziellen WLANSystemen*. Berliner Tor 5 / Hamburg / Germany, HW Hamburg, Diplomarbeit, 2004

Schneier 2000 SCHNEIER, Bruce: The Fallacy of Trusted Client Software. In: *Information Security Magazine* (2000), August

Schneier 2004 SCHNEIER, Bruce: *Secrets and Lies*. Dpunkt Verlag, August 2004. – SchNE b 00:1 1.Ex

Schneier und Ferguson 2000 SCHNEIER, Bruce ; FERGUSON, Niels: A Cryptographic Evaluation of IPsec. 3031 Tisch Way, Suite 100PE, San Jose, CA 95128, USA, 2000. – Forschungsbericht. – URL `citeseer.ist.psu.edu/ferguson00cryptographic.html`

Schneier u. a. 1999 SCHNEIER, Bruce ; MUDGE ; WAGNER, David: Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). In: *Secure Networking - CQRE (Secure) '99*, URL `http://www.schneier.com/paper-pptpv2.html`, 1999, S. 192–203

Speel 2004 SPEEL, Hans-Cees: Meet OpenVPN. In: *Linux Journal* (2004), December. – URL `http://www.linuxjournal.com/article/7949`

Tanenbaum und Steen 2001 TANENBAUM, Andrew S. ; STEEN, Maarten V.: *Distributed Systems: Principles and Paradigms*. Prentice Hall PTR, 2001. – ISBN 0130888931

Team 2003 TEAM, Cisco: *Layer 2 Tunnel Protocol*. Cisco Systems, Inc., USA: Cisco Systems, Inc. (Veranst.), Januar 2003. – URL `http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.pdf`

Vale u. a. 2004 VALE, Marshall ; ALTMAN, Jeffrey ; HILL, Paul ; MCGUIRE, Scott: *Documentation for the krb5-1.4 release*. http://web.mit.edu/kerberos/: MIT (Veranst.), 2004. – URL `http://web.mit.edu/kerberos/www/`. – Zugriffsdatum: 2005-03-21

Wikipedia 2005a WIKIPEDIA: Tunnel_EDV. In: *Wikipedia. Die Freie Enzyklopädie* 2005-02-20 (2005), Februar

Wikipedia 2005b WIKIPEDIA: VPN. In: *Wikipedia. Die Freie Enzyklopädie* 2005-02-20 (2005), Februar

Yonan YONAN, Jim: *Project Info - OpenVPN*. Web. – URL `http://sourceforge.net/projects/openvpn/`