Bluetooth Security - Gruppe Defcon

Jan Bremer
Christian Armbrust
Malte Rademacher
Christian Bruns
Sven Markmann

Inhalt

ABBILDUNGSVERZEICHNIS....2

1 ..... SICHERHEITSANFORDERUNGEN IN DRAHTLOSEN KOMMUNIKATIONSNETZEN... 4

1.1 VERGLEICH DRAHTGEBUNDENER MIT DRAHTLOSER TECHNIK....5
1.2 DARSTELLUNG ALLGEMEINER SICHERHEITSASPEKTE....6
1.3 WELCHE KONZEPTE EXISTIEREN ZUR LÖSUNG DER O.G. SICHERHEITSPROBLEMATIKEN (ALLGEMEINE ERKLÄRUNG):....7

2 ..... UNTERSUCHUNGEN DER IM SEMINAR VERWENDETEN DRAHTLOSEN TECHNOLOGIEN BEZÜGLICH IHRER SICHERHEIT 8

2.1 SICHERHEITSANALYSE WLAN....8
2.1.1 Einleitung 8
2.1.2 Sicherheitsoptionen des WLAN-Standards (802.11(b)) 8
2.1.3 WLAN Sicherheitslücken.... 11
2.1.4 Verbesserungmöglichkeiten der WLAN-Sicherheit 12
2.1.5 Lösung mittels Virtual Private Network (VPN).... 13
2.2 BLUETOOTH SICHERHEIT 15
2.2.1 Einleitung 15
2.2.2 Sicherheitsmodi.... 15
2.2.3 Der Sicherheitsmanager.... 16
2.2.4 Architekturübersicht 17
2.2.5 Sicherheitslevel der Dienste.... 18
2.2.6 Verbindungseinrichtung 18
2.2.7 Umgang mit dem Protokoll-Stack.... 19
2.2.8 Schlüsselmanagement.... 20
2.2.9 Verschlüsselung.... 24
2.2.10 Authentisierung 25
2.2.11 Sequence-Chart.... 26

3 ..... SICHERHEITSKONZEPT FÜR DAS IANT (GENOS). 32

3.1 BESCHREIBUNG....32
3.2 MODI DES GENOS-SERVERS: 34
3.3 SICHERHEITSEINSTELLUNGEN DES 1050 AP....34
3.4 GENOS KONFIGURATION IM IANT....37
3.5 DIE INTEGRATION VON WLAN UND BLUETOOTH MIT GENOS....38
3.6 KURZDARSTELLUNG DER FUNKTIONSWEISE EINES RADIUS SERVERS....39
3.7 IST GENOS DAS RICHTIGE PRODUKT FÜR DAS IANT? 39

4 .....QUELLENANGABEN:. 41

Abbildungsverzeichnis

ABBILDUNG 1: WEP VERSCHLÜSSELUNG 9
ABBILDUNG 2 WEP ENTSCHLÜSSELUNG 10
ABBILDUNG 3 SHARED KEY AUTHENTISIERUNG 11
ABBILDUNG 4 BLUETOOTH SICHERHEITSARCHITEKTUR 17
ABBILDUNG 5 FLUSSDIAGRAMM SICHERHEITSABFRAGE 19
ABBILDUNG 6 BLOCKSCHALTBILD EINER BLUETOOTH VERBINDUNGSAUFNAHME 21
ABBILDUNG 7 MASTER UND INITIALIZATION SCHLÜSSEL ERZEUGUNG MIT DEM E22 ALGORITHMUS 22
ABBILDUNG 8 UNIT UND COMBINATION KEY ERZEUGUNG MIT DEM E21 ALGORITHMUS 23
ABBILDUNG 9 SCHLÜSSELALGORITHMUS E3 FÜR DEN ENCRYPTION KEY 23
ABBILDUNG 10 BESCHREIBUNG DES VERSCHLÜSSELUNGSPROZESSES 24
ABBILDUNG 11 BESCHREIBUNG DES AUTHENTISIERUNGPROZESSES 25
ABBILDUNG 12 BLUETOOTH PAIRING SEQUENCE CHART 26
ABBILDUNG 13 GENOS SCHICHTENMODELL 33
ABBILDUNG 14 GENOS AP-KONFIGURATION 35
ABBILDUNG 15 GENOS NETZSTRUKTUR 37
ABBILDUNG 16 GENOS-RADIUS INTEGRATION 38
ABBILDUNG 17 RADIUS KOMMUNIKATION 39

1 Einleitung

Ziel unseres Projektes war es, ein umfassendes Sicherheitskonzept für alle drahtlosen Verbindungen des IANT zu erstellen. Zum Einstieg in die Sicherheitsanforderungen haben wir uns sowohl in die drahtlose Netzwerktechnik, als auch in die drahtgebundene Netztechnik eingearbeitet. Dazu betrachteten wir die Sicherheitsanforderung in drahtlosen- gegenüber drahtgebundener Datenkommunikation. Die allgemeinen Lösungsansätze wurden herausgestellt und zur Basis einer weiteren Betrachtung herangezogen.
Im Folgenden verglichen wir WLAN mit Bluetooth und beleuchteten die Sicherheitsmechanismen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit.
Letztlich erstellten wir ein Vorschlag für das IANT auf Basis des Sicherheitskonzeptes von Genos. Darin zeigten wir die Probleme bei der Inbetriebnahme mit der bereits vorhandenen Hardware auf.

2 Reflexion

Rückblickend ist zu sagen, dass die Teamarbeit in unserer Gruppe sehr gut funktioniert hat. Anfänglich haben wir uns sehr nahe an den Projektplan gehalten und haben in Teams die einzelnen Aufgaben erledigt. Zum Ende hin sind wir vom Projektplan abgewichen, da sich bestimmte Fragen als zu schwierig für die Bearbeitung in der geplanten Zeit erwiesen. Außerdem war es für uns im Hinblick auf die Präsentation sinnvoll, das Projekt mehr auf einzelne Personen aufzuteilen, um vertiefende Beiträge ermöglichen zu können.
Praktische Erfahrungen mit der Bluetoothtechnik konnten wir in unserer Arbeit leider nur begrenzt sammeln. So blieb die praktische Arbeit mit Bluetooth auf den Datenaustausch zwischen unseren Notebooks sowie das Mitschneiden eines Parings beschränkt. Die Notebooks hingegen haben uns hinsichtlich gegenseitiger Kommunikation, Dokumentation, Informationsaustausch sowie Informationsbeschaffung sehr geholfen.

3 Sicherheitsanforderungen in drahtlosen Kommunikationsnetzen

Der sehr offene Zugang zu drahtlosen Kommunikationsnetzen macht die Sicherheitseinstellungen zu den signifikantesten Faktoren die untersucht und verstanden werden müssen. Nur so ist es möglich das ganze Potential drahtloser Kommunikation auszuschöpfen. Die meisten verfügbaren Technologien nutzen heutzutage das Radio-Frequenz-Spektrum. Dieses Frequenzband ist ohne großen Aufwand von nahezu Jedermann abhörbar und einer großen Anzahl Störungen unterworfen. Da drahtlose Kommunikation momentan schon für geschäftliche Zwecke genutzt wird und in naher Zukunft noch viel stärker eingebunden werden soll ist dieser ungeschützte Zustand nicht akzeptabel und der Bedarf an Sicherheits-Konzepten groß.

Sicherheit ist die Kombination von Prozessen, Prozeduren und Systemen, die benutzt werden, um Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

- **Vertraulichkeit** (Confidentiality):
  Der Schutz gegen die unberechtigte Kenntnisnahme von Informationen. Dies schließt auch den Schutz von Informationen ein, die für sich "harmlos" erscheinen, aber dazu benutzt werden können, um Zugriff auf vertrauliche Informationen zu erhalten (z. B. Systemkonfigurations-dateien).

- **Integrität** (Integrity):
  Die Sicherstellung der Korrektheit (Unversehrtheit) von Daten (Datenintegrität) bzw. der korrekten Funktionsweise von Systemen (Systemintegrität). Daten dürfen ohne Berechtigung weder modifiziert noch gelöscht werden können. Dies schließt unter anderem auch beispielsweise Dateiattribute, Sicherungskopien (Backups) und Dokumentationen ein. Ein System muss sich zu jedem Zeitpunkt logisch korrekt verhalten. Dies schließt v. a. auch die logische Vollständigkeit jeglicher Teile der Hardware und Software, die Sicherheitsfunktionen implementieren, ein.

- **Verfügbarkeit** (Availability):
  Alle verarbeiteten Daten sowie die zur Verarbeitung notwendigen Systeme und Betriebsmittel müssen jederzeit verfügbar und funktionsbereit sein, wenn ein autorisierter Benutzer darauf zugreifen will. Dies schließt beispielsweise jegliche Hardware, Programme, Funktionen und für Daten auch Archive und Sicherungskopien (Backups) ein.

Im Allgemeinen, sollte ein sicheres mobiles Gerät folgende Funktionen besitzen:

- **Authentisierung:** Die Identität des Benutzers muss validiert werden.

- **Encryption:** Um Lauschangriffe auf die Datenkommunikation auszuschließen.

- **Zugangskontrolle:** Um sicherzugehen, dass Benutzer nur zu den Informationen Zugang bekommen, für die sie autorisiert sind.

- **Diebstahlsicherung:** Zentral gesteuerte Abschaltung der Geräte, wenn sie einem nicht authentisierten Benutzer in die Hände fallen.

Den Benutzern der mobilen Technologien muss durch Sicherheitslösungen ein hohes Maß an Vertrauen gegeben werden, dass sie sichergehen können, dass ihre Daten adäquat geschützt werden. Zum Beispiel nutzen viele Menschen heutzutage das Internet für die vielfältigsten Aufgaben, aber die wenigsten haben Vertrauen Zahlungen über das Internet abzuwickeln.

3.1 Vergleich drahtgebundener mit drahtloser Technik

In kabelbasierten Netzwerken bieten die Kabel, welche die Geräte miteinander verbinden einen gewissen physischen Schutz gegen Manipulationen. Die Kabel selbst befinden sich normalerweise innerhalb eines Gebäudes, welches durch gewisse Zugangskontrollen geschützt ist. Innerhalb der Räume, wo sich die Geräte befinden, sind die Kabel frei zugänglich. Um die Kabel zu erreichen muss ein potentieller Angreifer also in das Gebäude einbrechen und dann den entsprechenden Raum suchen. Um an die Daten zu gelangen, muss er das Kabel anzapfen, ohne dass dies für den Benutzer sichtbar ist.

In mobilen, kabellosen Netzen werden die Daten nun nicht mehr über Kabel, sondern offen über die Luft übertragen und sind somit in einem gewissen räumlichen Umkreis (bei WLAN bis zu 300m) einfach zu empfangen. Es kann sogar sein, dass die Übertragung außerhalb eines Gebäudes empfangbar ist. Die Datenübertragung ist also über die Luftschnittstelle sehr viel leichter zugänglich, als bei einem verkabelten Netz. Angesichts der leichten Abhörbarkeit im drahtlosen Umfeld sind eine Authentisierung, Verschlüsselung und Zugriffssteuerung mit starker Kryptographie erforderlich. Beim WLAN Standard 102.11b wird dieses durch das WEP Wired Equivalent Privacy Verschlüsselungsverfahren (auf welches wir im Unterpunkt WLAN allgemein näher eingehen) realisiert. Ohne Verschlüsselung ist es beispielsweise leicht möglich in der Nachbarschaft bei einem Funk-LAN mit einer eigenen Wireless LAN Karte Zugriff auf fremde Daten zu bekommen und diese zu manipulieren.

Die größte Gefahr für die Sicherheit von Funknetzen geht dabei nicht unmittelbar von der Funk-Hardware aus. Durch Unwissenheit und Fehlverhalten bei der Einrichtung der Netzwerkhardware untergraben die Anwender vielmehr selbst die Sicherheitsmechanismen. Denn die in den gängigen Standards definierten Schutzvorkehrungen werden von vielen meist nur ungenügend eingesetzt.

Da sich die einzelnen Kommunikationsnetze drahtlosen Kommunikationsnetze auf der RF-Schnittstelle überlagern können und es so zu Interferenzen kommen kann, ist eine sehr sorgfältige Planung und Installation bei benachbarten Netzen nötig. Die Sendestärken der Antennen müssen aufeinander abgestimmt werden.

Bei Adhoc-Netzwerken besteht zusätzlich die Herausforderung, dass sich die Teilnehmer beim Aufbau des Netzwerkes noch nicht kennen, also ist es nicht möglich auf gemeinsamen Informationen beispielsweise eine geheimer Schlüssel, aufzubauen. Möglicherweise verwenden sie sogar verschiedene Sicherheitsstandards. Eine Attacke, die speziell auf mobile Netzwerke abzielt, ist die Location- Attack. Das Ziel dieses Angriffs ist es, den Standort eines Geräts zu bestimmen damit Aussagen über den Aufenthaltsort einer Person zu machen. Des weiteren kann diese Person auch in Beziehung zu anderen Geräten und somit Personen gebracht werden. Diese Attacke ist besonders problematisch, da eine Person rund um die Uhr, auch im privaten Bereich, ohne großen finanziellen Aufwand überwacht und der Standort mit hoher Genauigkeit bestimmt werden kann. Diese Informationen könnten für vielerlei Angriffe verwendet werden: Erpressung oder einfach zum Aufbauen eines Profils einer bestimmten Person.

Nach Angabe der Deutschen Telekom werden Wireless LANs nie ganz die Sicherheit von Kabelnetzen erreichen. Sie halten den Security-Anforderungen an unternehmensweite Kabelnetze aber weitestgehend stand und überzeugen durch hohe Flexibilität.

3.2 Darstellung allgemeiner Sicherheitsaspekte

In fast allen Bereichen in denen Bluetooth zur Anwendung kommt, werden private oder persönliche Daten der Benutzer verwaltet oder verwendet. Es ist daher besonders wichtig, dass sich kein fremder User in ein Netz bzw. einen Rechner einloggen und auf dessen Daten zugreifen kann. Neben der Verunreinigung durch sog. „Viren“ und der unbemerkten Verfälschung wären die Daten auch vor der Löschung nicht sicher. Eine zusätzliche Gefahr ergibt sich, wenn ein fremder User durch Imitation eines Bekannten in ein Netz eindringt und unter Ausgabe einer falschen Identität unbemerkt Zugriff auf Daten und ggf. weitere Netzte erlangt (Account- Missbrauch). Auch ohne Login kann es für potentielle Angreifer möglich sein, in den Besitz vertraulicher Daten zu gelangen, sie zu verfälschen und zu „infizieren“. Die Funkschnittstelle könnte abgehört werden oder Daten auf dem Weg vom Absender zum Empfänger manipuliert werden. Bei verschlüsseltem Verkehr kann durch Überwachung der Funkschnittstelle immerhin noch ein Überblick über die Aktivitäten des Netzes aufgezeichnet werden und daraus ggf. ein Rückschluss gezogen werden. Bei mobilen Bluetoothteilnehmern kann ein Bewegungsprotokoll erstellt werden, welches kritische Gewohnheiten eines Nutzers verrät.

Die Funkschnittstelle bietet weitere Möglichkeiten in den sicheren Betrieb eines Bluetoothsystems einzugreifen ohne die Privatsphäre der Benutzer zu stören. Durch

das stören einer Verbindung durch einen Störsender, wird zwar nicht die Vertraulichkeit von Daten berührt, aber der Betrieb des Systems unmöglich. Die einzige Möglichkeit, das Stören durch Störsender zu unterbinden ist eine sichere Abschirmung der betreffenden Gebäude bzw. der betreffenden Räume. Dies könnte z.B. durch integrierte Metallgitter in den Wänden erzielt werden, ähnlich dem Faraday´schen Käfig. Bei ressourcenbegrenzten Geräten (etwa durch Batteriebetrieb) kann durch ständige Anfragen die Betriebszeit störend verkürzt werden.

3.3 Welche Konzepte existieren zur Lösung der o.g. Sicherheitsproblematiken (allgemeine Erklärung):

Es gibt mehrere Möglichkeiten zur Lösung der o.g. Sicherheitsproblematiken. Ein erster Versuch für ein sicheres Netz wäre eine Teilnehmeridentifizierung anhand eindeutiger Merkmale, wie z.B. der MAC Adresse. Diese würden in eine Access Control List (ACL) eingetragen. Versucht ein Client mit einer fremden MAC – Adresse sich anzumelden, wird er abgewiesen. Eine Schwachstelle hierbei wäre die Möglichkeit mit Hilfe von Software diese MAC zu ändern. Authentisierung wäre der nächste Schritt in Richtung eines sicheren Netzes. Die Authentisierung könnte z.B. softwareseitig anhand von Passwörtern, bzw. hardwareseitig mit Hilfe von Smart Cards o.ä. gelöst werden. Weiterhin könnten verschiedene Nutzergruppen für verschiedene sicherheitsrelevante Bereiche geschaffen werden. So könnte verhindert werden, dass z.B. Netze missbraucht werden, oder Daten von Unbefugten eingesehen oder geändert würden. Bei Datenübertragungen im Netz ist es wichtig die Nutzlast zu verschlüsseln z.B. WEP (Wired Equivalent Privacy). Hierbei wird mit verschiedenen Schlüssellängen gearbeitet, nämlich 64Bit oder 128 Bit. Dabei sind 24 Bit jeweils der so genannte Initialisierungsvektor (eine von der Hardware von Datenpaket zu Datenpaket veränderte zufällige Zahl) und der Rest (40 bzw. 104 Bit) wird vom Anwender definiert.

Sichere End-zu-End Verbindungen über das IP Protokoll können mit Hilfe von VPN (Virtual Private Network) realisiert werden. Dabei wird im Falle von WLAN eine sichere Verbindung zwischen jedem WLAN Client und einem VPN Gateway im Netzwerk hergestellt. In diesem Fall verhalten sich die Access Points transparent, die eigentliche Authentisierung der Clients findet nämlich im Netzwerk statt, nicht im Funk. Die übertragenen Daten können hierbei unter Verwendung sicherer Verschlüsselungen, wie z.B. IPsec verschlüsselt werden.

Ein sehr einfaches Merkmal zur Sicherheitserhöhung ist die Begrenzung der Reichweite der Accesspoints. Bei Bluetooth ist dies schon durch den Standard gegeben, der eine Reichweite von ca. 10 m beinhaltet. Im WLAN besteht des weiteren die Möglichkeit die Funktionalität abzuschalten. Ist die Übertragung der SSID (System Set Identifier oder „Network Name“) unterdrückt, so kann sie nicht von Clients aus dem Netz ermittelt werden. Nur mit passender SSID können sich allerdings Clients ins Netz einloggen. Das Frequency Hopping im Bluetooth ist auch als Sicherheitsaspekt zu sehen. Hierbei wird pro Sekunde 1600 die Frequenz geändert. Will man das Signal abhören, so muss der potentielle Angreifer sich erst mit dem Signal synchronisieren.

4 Untersuchungen der im Seminar verwendeten drahtlosen Technologien bezüglich Ihrer Sicherheit

4.1 Sicherheitsanalyse WLAN

4.1.1 Einleitung

Im Folgenden Kapitel werden die im 802.11 bzw. 802.11b Standard definierten Sicherheitsmechanismen aufgeführt und erläutert. Der Standard bietet darüber hinaus Möglichkeiten, diese Mechanismen mittels proprietärer Lösungen zu erweitern. Der letzte Abschnitt wird auf Probleme dieser Sicherheitsoptionen eingehen.

4.1.2 Sicherheitsoptionen des WLAN-Standards (802.11(b))

4.1.2.1 Access Control List (ACL)

Da jede WLAN-Netzwerkkomponente eine weltweit eindeutige Hardware- bzw. MAC-Adresse besitzt, ist es prinzipiell möglich, in einem WLAN MAC-Adressen nur bestimmte MAC-Adressen für die Kommunikation zu autorisieren. Dies wird mittels einer sogenannten Access Control List (ACL) realisiert. Diese ACLs besitzen jedoch den Nachteil, dass sie "per Hand" konfiguriert werden müssen und somit für viele Einsatzszenarien ausscheiden. Ein weiteres Problem besteht darin, dass die MAC-Adresse im Klartext übertragen wird und diese Barriere folglich überwindbar ist, was jedoch mit nicht unerheblichen Aufwand verbunden ist.

4.1.2.2 (Extended) Service Set Identifier ((E)SSID)

IEEE 802.11 bietet die Möglichkeit, einen Netzwerknamen zu vergeben. Für diesen sogenannten (Extended) Service Set Identifier ((E)SSID) gibt es zwei Betriebsmodi: Bei Angabe der Kennung "Any", akzeptiert die WLAN-Komponente beliebige ESSIDs potentieller Kommunikationspartner. Im zweiten Modus wird der Netzwerkname des Partners überprüft und nur Teilnehmer mit dem gleichen ESSID können an der Kommunikation teilnehmen. Da der ESSID im Klartext über das Netz gesendet wird, kann er von Außenstehenden mit einfachen Mitteln in Erfahrung gebracht werden. Es ist anzumerken, dass einige Access-Points die Möglichkeit bieten, des Senden des Netzwerknamens im Klartext zu unterbinden.

4.1.2.3 Wired Equivalent Privacy (WEP)

Bei WEP handelt es sich um ein Verfahren, das mit symmetrischen Schlüsseln arbeitet. Im WLAN-Standard sollen mittels des Wired Equivalent Privacy-Protocols

- Authentisierung
- Integrität
- Verschlüsselung

sichergestellt werden. Dazu wird ein 40 oder 104 Bit (aufgrund von "Firmenstandards" existieren mittlerweile auch längere Schlüssel) langer Schlüssel verwendet, welche bei allen an einem bestimmten WLAN beteiligten Rechnern manuell eingetragen werden müssen. Zu beachten ist, dass alle Rechner dieses WLANs den selben Schlüssel verwenden. Im Folgenden wird zunächst das Verfahren der Verschlüsselung sowie Entschlüsselung näher betrachtet, welches ein Sicherstellen der Integrität einschließt. Danach wird in einigen Worten auf die

Authentisierung eingegangen, die ebenfalls auf dem Verschlüsselungsverfahren basiert.

4.1.2.4 WEP Verschlüsselung

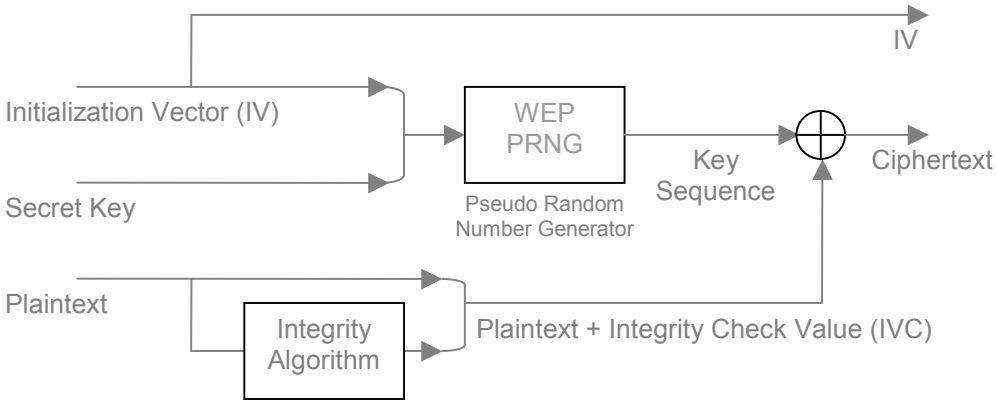


Abbildung 1: WEP Verschlüsselung

Das Verschlüsselungsverfahren sowie die Sicherstellung der Integrität wird in Abbildung 1 veranschaulicht. (RSA Verschlüsselungsalgorithmus mit variabler Schlüssellänge von Ron Rivest). Ist die WEP-Verschlüsselung aktiviert, werden alle Daten, die von WLAN-Komponenten versendet werden nach dem in dargestellten Schema verschlüsselt. Als Eingangsdaten (linke Seite) werden dabei ein 24 Bit langer, so genannter Initialisierungsvektor (IV), der geheime Chiffrierschlüssel (Secret Key) sowie die Daten im Klartext (Plaintext) verwendet. Der Initialialisierungsvektor wird in der Regel für jede Nachricht generiert und, wie oben dargestellt, letztendlich zusätzlich zu der verschlüsselten Nachricht im Klartext übertragen. Darüber hinaus werden der IV zusammen mit dem WEP-Schlüssel einem Zufallszahlengenerator zugeführt (WEP PRNG) der mit Hilfe eines spezifizierten Algorithmus daraus eine Schlüsselsequenz (Key Sequence) erzeugt, die im Endeffekt den Klartext verschlüsselt.

Wie man leicht nachrechnen kann, ergibt sich aus der Länge des IV zusammen mit der verwendeten Schlüssellänge eine Gesamtschlüssellänge von 64 bzw. 128 Bit, die man i.a. auch auf WLAN-Produkten findet. Aus dem zugeführte Klartext wird zunächst mittels eines im Standard definierten Integritätsalgorithmus (Integrity Algorithm) eine 32 Bit Checksumme berechnet, die danach den unverschlüsselten Daten angehängt wird. Wie die Abbildung zeigt, wird aus dem daraus entstehendem Datenstrom zusammen mit der generierten Schlüsselsequenz eine XOR-Verknüpfung gebildet, deren Ausgang die verschlüsselten Daten (Ciphertext) erzeugt. Wie oben angedeutet werden diese chiffrierten Daten zusammen mit dem IV anschließend versendet.

4.1.2.5 WEP Entschlüsselung

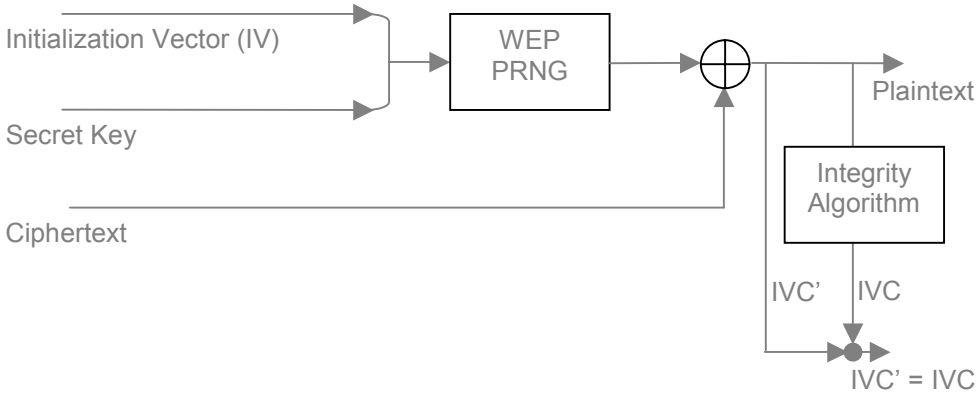


Abbildung 2 WEP Entschlüsselung

Da es sich hier um ein symmetrisches Chiffrierverfahren handelt, verläuft die Entschlüsselung der Daten in analoger Weise zur Verschlüsselung. Wie in Abbildung 2 dargestellt wird wiederum aus (diesmal aus empfangenem) Initialisierungsvektor sowie dem bekannten geheimen Schlüssel ein Gesamtschlüssel gebildet, der dem Zufallszahlengenerator zugeführt wird. Am Ausgang dieses Generators wird folglich die identische Schlüsselsequenz erzeugt, wie schon auf Senderseite. Anschließend wird diese Sequenz mit dem Verschlüsselten Text einer XOR-Operation unterzogen (zweimal identische XOR-Operation ergibt wieder die ursprünglichen Daten).

Die sich ergebenden Daten bestehen aus der Integritätschecksumme (IVC') sowie der Nachricht im Klartext. Schließlich wird mittels Integritätsalgorithmus und Klartextnachricht ebenfalls eine Checksumme (IVC) berechnet und diese mit dem empfangenen Wert IVC' verglichen. Stimmen beide Werte überein, kann davon ausgegangen werden, dass die Nachricht auf dem Übertragungsweg nicht verändert wurde.

4.1.2.6 WEP Authentisierung

Bezüglich der Authentisierung wird zwischen zwei Betriebsarten unterschieden: "Open System" sowie "Shared Key". Im ersten Fall findet keine Authentisierung statt, im letzteren Fall authentisieren sich die WLAN-Komponenten mittels eines Challenge-Response-Verfahrens (Herausforderungs-Antwort). Dieses Verfahren soll im Folgenden anhand von Abbildung 3 kurz erläutert werden. Es ist zu beachten, dass Authentisierung nur zusammen mit aktivierter WEP-Verschlüsselung gewählt werden kann.

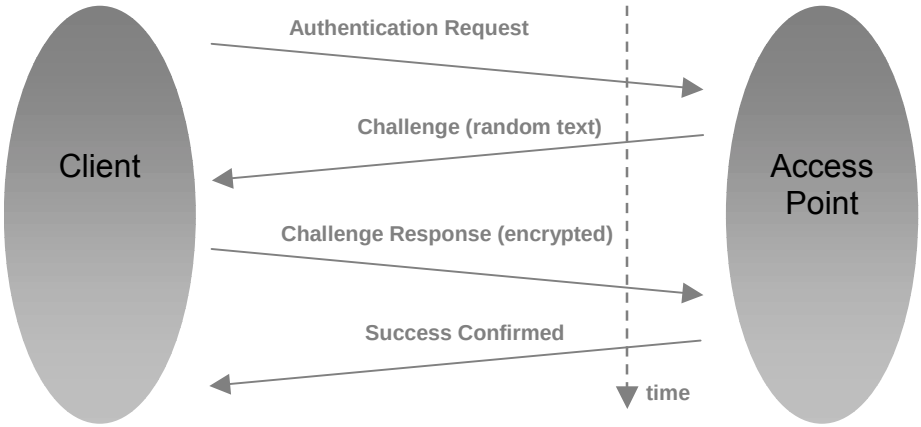


Abbildung 3 Shared Key Authentisierung

Zunächst sendet der Client einem Access Point (AP) eine Authentisierungsanfrage (Authentication Request). Diese wird vom entsprechenden Access Point mit einem sogenannten Challenge beantwortet. Bei dem Challenge handelt es sich um einen vom AP generierten Zufallstext, der unverschlüsselt zusammen mit dem Initialisierungsvektor übertragen wird.
Dieser Zufallstext wird nun vom Client mittels des symmetrischen Schlüssels sowie des RC4-Algorithmus (wird auch für Verschlüsselung verwendet, s.o.) chiffriert und der verschlüsselte Text anschließend and den Access Point zurückgesendet (Response).
Da dem Access Point der Klartext sowie der Schlüssel ebenfalls bekannt sind, kann er eine identische Operation durchführen und letztendlich die empfangene Response mit dem selbst errechneten Wert vergleichen. Stimmen beide Daten überein, kann der AP davon ausgehen, dass der Client den korrekten Schlüssel besitzt und somit der ist, der er vorgibt zu sein – der Client hat sich authentisiert.

4.1.3 WLAN Sicherheitslücken

WLAN-Systeme bergen in aktuellen standardkonformen Implementierungen große Sicherheitslücken. Die wichtigsten Schwachstellen werden in diesem Abschnitt aufgeführt.

- **Kein Schlüsselmanagement:** Zunächst einmal kann man die Verteilung der symmetrischen Schlüssel problematisch betrachten. Dies ist nicht nur mit einem hohen administrativen Aufwand verbunden, sondern die Geheimhaltung der verwendeten Schlüssel darf, besonders in großen Netzen, in Frage gestellt werden. Da alle Stationen den selben Schlüssel verwenden, ist das Bekannt werden eines Schlüssels kritisch für das gesamte Netz. Wie o.a. werden die Schlüssel manuell in die WLAN-Komponenten eingetragen. Dieser physische Zugriff hat häufig zur Folge, dass die verwendeten Schlüssel selten oder nie gewechselt werden.
- **Manipulierbare MAC-Adressen:** Da die MAC-Adressen sehr einfach abgehört werden können und mit einigem Aufwand für ein Gerät

beliebig konfigurierbar sind, sind somit auch die durch die o.a. Access-Control-List gegebenen Addressfilter überwindbar.

- **Schwachstellen des WEP-Protokolls:** Die Mechanismen, mit denen bei WEP Verschlüsselung, Integrität sowie Authentisierung sichergestellt werden sollen, besitzen folgende Sicherheitsprobleme:
  - **40 Bit ist zu kurze Schlüssellänge:** Eine aufgezeichnete komplett verschlüsselte Nachricht kann selbst mit einem handelsüblichen Computer innerhalb weniger Tage durch Ausprobieren aller möglichen Schlüssel dechiffriert werden. Eine Person ist somit nach erfolgreicher Schlüsselermittlung in der Lage, alle Daten des speziellen WLANs mitzulesen, zumindest solange, bis der Schlüssel geändert wird (was häufig nie der Fall ist). Schlüssel der Länge 104 Bit sollten hingegen bisher eine ausreichende Sicherheit gegen diese Art der Entschlüsselung gewährleisten.
  - **Datenpakete fälschbar:** Wie in und dargestellt, ist die Schlüsselsequenz (Key Sequenz) am Ausgang des Zufallszahlengenerators abhängig von Initialisierungsvektor sowie dem Schlüssel. Sollte ein potentieller Angreifer jemals in Besitz einer gültigen Schlüsselsequenz gelangen, ist er damit in der Lage, bis zum nächsten Schlüsselwechsel beliebig Pakete in das Netz einzuschleusen, d.h. gültige Chiffredaten zu erzeugen. Eine solche Key Sequence kann leicht erzeugt werden, falls zu einer verschlüsselten Nachricht der Klartext bekannt ist. Mittels XOR kann somit aus diesem Klartext mit angehängter Checksumme (kann selber errechnet werden, da Integrity Check Algorithm im Standard spezifiziert) eine Schlüsselsequenz bestimmt werden. Diese Sequenz kann nun für nachfolgende Paketverschlüsselung verwendet werden, wobei diese zwar alle den gleichen Initialisierungsvektor verwenden, dies jedoch insofern kein Problem darstellt, da allein der Sender den IV festlegt. Eine zu Chiffrierdaten gehörige Klartextnachricht kann zum Beispiel sehr einfach durch Abhören einer Authentisierung erhalten werden. Es ist u beachten, das bei dieser Methode der Angreifer nicht in Besitz des geheimen Schlüssels gelangt.

4.1.4 Verbesserungmöglichkeiten der WLAN-Sicherheit

Zunächst wird noch einmal die besondere Sicherheitsproblematik beim Einsatz von WLANs in universitären Netzen herausgestellt.
Universitäre Netze besitzen i.A. folgende Charakteristika

- große, heterogene Benutzergruppen
  - viele unkritische Nutzer
  - einige potentielle Angreifer mit hohem Fachwissen unter den Nutzern
- begrenzte Anzahl symmetrischer Keys zur Verschlüsselung
- SSIDs (Netzwerknamen) und Keys sind "offenes Geheimnis"
- Eigenes Notebook im WLAN: Abhören des Netzwerkdatenverkehrs einer Funkzelle möglich und unvermeidbar

Daraus folgt, dass WLAN bereiche selbst als unsichere Bereiche anzusehen sind, vergleichbar mit dem Internet. Eine ausreichende Sicherheit könnte durch aufgesetzte Sicherheitsmaßnahmen wie z.B. Virtueller Privater Netzwerke (VPN) erreicht werden.
Protokolle, die zur Erstellung von Verbindungen für VPN sind zum Beispiel:

4.1.4.1 Point to Point Tunneling Protocol (PPTP)

- Protokoll zur Realisierung virtueller privater (Multiprotokoll-) Netzwerke (VPN) auf Layer 2
    - Authentisierung der Nutzer mittels PAP oder CHAP (individuell verschlüsselt) oft jedoch nur MS-CHAP
    - Einsatz bereits an einigen WLAN-Universitäten erprobt (Beispielsweise Universität Karlsruhe, siehe www.uni-karlsruhe.de/Uni/RZ/Netze/DUKATH)

4.1.4.2 IPSec

- übergreifender, plattform- und herstellerunabhängiger Standard für sichere Kommunikation mit TCP/IP auf Layer 3 (transparent für Nutzer)
- Features:
    - Authentifikation der Nutzer / Paketabsender, Vertraulichkeitswahrung durch individuelle Verschlüsselung
    - Zugriffskontrolle
    - Schutz vor Angriffen durch eine Wiederholung früherer Kommunikation
    - Key Management: Austausch und Erneuerung von Schlüsseln manuell oder automatisch per IKE (Internet Key Exchange)

4.1.4.3 Lösung mittels Virtual Private Network (VPN)

Um Zugriff auf das LAN zu erlangen, muss sich ein Client zunächst mittels der VPN-Technologie als berechtigt erweisen. Nach erfolgreicher Anmeldung im Virtual Private Network erhält der entsprechende Client eine IP Adresse des Netzes und hat anschließend Zugriff auf das Intranet sowie das Internet.

VPN ermöglicht eine sichere (verschlüsselte) Verbindung zum jeweiligen Zielnetz. Generell gewährleistet das VPN-Verfahren, einen Computer unabhängig von seinem Standort sich in ein Zielnetz zu integrieren. Erforderlich ist dabei nur eine VPN Client-Software für das jeweilige Betriebssystem sowie ein Account auf dem VPN Server des Zielnetztes. Während des Aufbaus einer VPN Verbindung wird ein verschlüsselter Kanal ("Tunnel") zum Zielnetz erstellt, über den anschließend Login-Information sowie andere Daten übertragen werden.

4.1.4.3.1 VPN Software

Wie schon oben erwähnt gibt es verschiedene Protokolle, die zur VPN-Verbindungserstellung verwendet werden können. So zum Beispiel IPSec (Internet Protocol Security) oder PPTP (Point-to-Point Tunneling Protocol).
PPTP ist sowohl in Windows 2000 als auch in Windows XP integriert, somit ist keine zusätzliche Software notwendig. IPSec hingegen ist zumindest in Windows 2000 noch nicht enthalten, sodass eine entsprechende Software installiert werden muss.

Diese Software ist für die gängigen Betriebssysteme verfügbar (Linux, Windows 95/98/ME/2000/XP, MacOS X, Palm OS, Windows CE3, Solaris, etc.).

4.1.4.3.2 VPN Sicherheit

Mit dem o.g. verschlüsselten Kommunikationstunnel können mittels VPN Datenpakete beliebiger Protokolle verschlüsselt und verpackt über das Netz versandt werden. Dabei wird TCP/IP als Transportmittel verwendet.

Im Folgenden werden die von IPSec gebotenen Sicherheitsfunktionen kurz dargestellt:

- **Authentisierung**: Zur Identitätsprüfung wird ein gemeinsames Schlüsselwort festgelegt der so genannte "Pre-Shared-Key". Die Internet-Key-Exchange-(IKE) Funktion verschlüsselt diesen Schlüssel automatisch. Stimmt der Code zwischen Client und Server überein, wird anschließend ein zweiter verschlüsselter Kanal aufgebaut, über den der eigentliche Datenaustausch stattfindet.
- **Vertraulichkeit**: Mit Hilfe bewährter Verschlüsselungsverfahren z.B. DES- (56 Bit) oder Triple-DES (168 Bit) (symmetrische Verfahren) kann bei IPSec die Vertraulichkeit der Datenkommunikation sichergestellt werden.
- **Integrität**: Auch bei IPSec werden wird die Integrität der Daten mittels einer Checksumme geprüft. Dabei wird mit sogenannten "Hash-Algorithmen" z.B. MD-5 oder SHA-1 verwendet.

Wegen seiner umfangreichen Verschlüsselungsverfahren wird die Verwendung von IPSec beim Aufbau einer VPN-Verbindung empfohlen.

Beispiel-Konfigurationsanleitungen für VPN-Clients sowohl für PPTP als auch IPSec können zum Beispiel unter den Adressen

http://www.wireless.ethz.ch/silva/wlan/installation/vpn_install bzw.
http://wlan.informatik.uni-bremen.de/

eingesehen werden.

4.2 Bluetooth Sicherheit

4.2.1 Einleitung

Bluetooth Signale lassen sich wie z.B. WLAN leicht abhören. Darum waren in der der Bluetooth-Spezifikation besondere Sicherheitsmechanismen erforderlich um Lauschangriffen entgegenzuwirken und das Verfälschen von Absenderangaben bei Nachrichtenübertragung entgegen zu wirken
Insbesondere die Sicherungsschicht stellt Merkmale zur Verfügung, mit der Authentisierung und Verschlüsselung von Daten möglich ist.

4.2.2 Sicherheitsmodi

Bluetooth enthält zur Authentisierung von Geräten 3 verschiedene Sicherheitsmodi. Je nach Gerät und Sicherheitsbedarf werden die verschiedenen Modi genutzt.

Modus 1
Der Modus 1 bezieht sich auf fehlende Sicherheitsvorkehrungen und wird eingesetzt, wenn auf den entsprechenden Geräten keine sicherheitskritischen Applikationen ausgeführt werden.
In diesem Modus ignorieren die Geräte die Sicherheitsfunktionen der Sicherheitsschicht, so dass der Zugriff auf Datenbanken freigegeben wird, die keine sensitiven Daten enthalten. Diese Datenbanken enthalten z.B. Daten von Visitenkarten oder Terminkalendern (vCard bzw. vCalendar).

Modus 2
Der Modus 2 bietet Sicherheit auf der Dienstebene und ermöglicht bei parallel ablaufenden Applikationen oder Prozessen mit verschiedenen Sicherheitsanforderungen, die entsprechenden Zugriffsverfahren.

Modus 3
Der Modus 3 bietet Sicherheit auf der Sicherungsebene, durch die der Link Manager für alle Applikationen bei der Verbindungseinrichtung für Sicherheitsvorkehrungen auf einem einheitlichen Niveau sorgt. Dieser Modus ist zwar weniger flexibel, jedoch lässt er sich durch das gemeinsame, hohe Sicherheitsniveau leichter als Modus 2 implementieren, in dem jede Applikation ihren eigenen Sicherheitslevel hat.

Beim Sicherheitsmodus 2 lassen sich die Sicherheitsstufen für Geräte und Dienste separat festlegen. Für Geräte gibt es 2 Stufen des Vertrauens, trusted (vertrauenswürdig) und untrusted (nicht vertrauenswürdig).
Vertrauenswürdige Geräte stehen in einer festen Beziehung zueinander (paired devices) und haben unbeschränkten Zugriff auf alle Dienste.

Nicht vertrauenswürdige Geräte stehen in keiner permanenten Beziehung, bzw. Verbindung, weshalb sie nicht vertrauenswürdig sind. Es kann Fälle geben, in denen Geräte in einer festen Beziehung zueinander stehen, jedoch trotzdem untrusted sind. In diesen Fällen wird der Zugriff auf Dienste beschränkt.
Es lässt sich auch der Trust-Level eines Gerätes so setzen, dass es nur Zugriff auf einen Dienst, bzw. eine Gruppe von Diensten hat.
Die Anforderungen für Autorisierung, Authentisierung und Verschlüsselung werden je nach Zugriff der Geräte unabhängig von einander festgelegt:

- Bei Diensten, die Autorisierung und Authentisierung erfordern, wird nur trusted devices der Zugriff erlaubt, alle anderen Geräte müssen sich manuell autorisieren.
- Dienste, die nur eine Authentisierung erfordern
- Dienste, die für alle offen stehen

Ein Sicherheitsansatz ist der Einsatz eines Sicherheitsmanagers, der während der Einrichtung einer Verbindung abgefragt wird. Der Sicherheitsmanager kann so vertrauenswürdigen Geräten, nach Abfrage der internen Datenbank, Dienste und Zugriffe der entsprechenden Sicherheitsstufe ermöglichen.

Diese Abfrage des Sicherheitsmanagers kann jedoch keine vorhandenen netzwerkspezifischen Sicherheitsvorkehrungen ersetzen. Bei extrem strengen Anforderungen, müsste die Sicherheit durch Sicherheitsmechanismen auf der Anwendungsschicht ergänzt werden.

Ein charakteristisches Merkmal der Bluetooth Sicherheitsarchitektur ist, dass Anwendereingriffe beim Zugriff auf Dienste möglichst vermieden werden. Nur wenn Geräten eine beschränkte Nutzung von Diensten gewährt werden soll, sind Anwendereingriffe notwendig, oder wenn vertrauenswürdige Beziehungen zu Geräten eingerichtet werden sollen, die unbeschränkten Datenzugriff erlauben.

4.2.3 Der Sicherheitsmanager

Der Sicherheitsmanager, der die Sicherheitsarchitektur implementiert, muss mehrere Datenbanken verwalten.
Die Dienstedatenbank enthält für alle Dienste die entsprechenden Einträge, die im Zusammenhang mit der Sicherheit stehen, die entweder verbindlich (**V**) oder optional (**O**) sind.

Eintrag	**Status**
Authorization required	V
Authentification required	V
Encryption required	V
PSM Value (Protocol / Service Multipexer)	V
Broadcasting allowed	O

Die Information über die Vertrauenswürdigkeit der Geräte muss in einem festen Speicher im Gerät gespeichert werden. Wird dieser aus irgendeinem Grund gelöscht, werden die gelöschten Geräte wieder als unbekannt eingestuft.

In der Gerätedatenbank werden wie in der Dienstdatenbank ebenfalls verbindliche (V) und optionale (O) Einträge gespeichert.

Eintrag	**Status**	**Inhalt**
BD_ADDR	V	48-Bit-MAC-Adresse
Trust level	V	trusted / untrusted
Link Key	V	Bitfeld (max 128bit)
Device Name	O	Zeichenkette, die sich nutzen lässt, um Namensanforderungen zu vermeiden

4.2.4 Architekturübersicht

Die Bluetooth Sicherheitsarchitektur stellt einen flexiblen Rahmen zur Verfügung, in dem klar festgelegt ist, wann z.B. der Benutzer einbezogen wird (durch Eingabe einer PIN).

Des Weiteren ist festgelegt, welche Aktionen die Protokollschichten durchführen müssen, um bestimmte Sicherheitsüberprüfungen ausführen zu können.

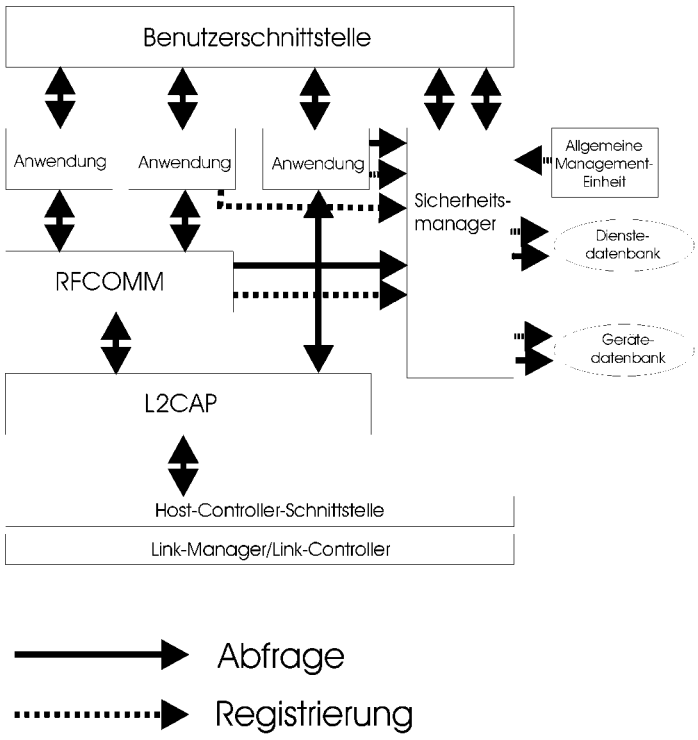


Abbildung 4 Bluetooth Sicherheitsarchitektur

Die Schlüsselkomponente der Bluetooth Sicherheitsarchitektur ist der Sicherheitsmanager, der für die Ausführung der folgenden Aufgaben zuständig ist:

- Speicherung von Informationen über Dienste, die im Zusammenhang mit der Sicherheit stehen
- Speicherung von Informationen über Geräte, die im Zusammenhang mit der Sicherheit stehen
- Bearbeitung und Beantwortung von Zugriffsanforderungen durch Anwendungen
- Erzwingen der Autorisierung und/oder Verschlüsselung vor der Verbindung mit einer Anwendung
- Initiieren oder verarbeiten von Eingaben eines Gerätebenutzers, um vertrauenswürdige Beziehungen auf der Geräteeben einzurichten

- Initiieren des Pairings und Aufforderung an den Benutzer zur PIN – Eingabe, wobei die PIN – Eingabe auch durch eine Anwendung erfolgen kann.

Mit dem zentralen Sicherheitsmanager bietet sich die Möglichkeit flexible Zugriffsverfahren leicht zu implementieren, da die Schnittstellen zu Protokollen einfach bleiben und sich diese, wie oben abgebildet, auf Frage-Antwort- und Registrierungsprozeduren beschränken.

4.2.5 Sicherheitslevel der Dienste

Das Sicherheitsniveau eines Dienstes wird durch 3 Attribute bestimmt:

- Erforderliche Autorisierung. Der Zugriff wird nur trusted devices gewährt, bzw. untrusted devices nach einer Autorisierungsprozedur. Die Autorisierung erfordert immer eine Authentisierung, bei der verifiziert wird, ob es sich bei dem entfernten Gerät um das richtige handelt.
- Erforderliche Authentisierung. Vor der Verbindung mit einer Anwendung muss das entfernte Gerät authentisiert werden.
- Erforderliche Verschlüsselung. Die Verbindung muss in den verschlüsselten Mode umgeschaltet werden, bevor der Zugriff auf den Dienst gestattet wird.

Diese Attributinformationen werden in der Dienstedatenbank des Sicherheitsmanagers gespeichert. Wenn keine Registrierung stattgefunden hat, wird eine Vorgabe Sicherheitsstufe genutzt. Bei ankommenden Verbindungen sind laut Vorgabe Autorisierung und Authentisierung nötig, bei abgehenden nur Authentisierung.

4.2.6 Verbindungseinrichtung

Um ohne Benutzereingriffe unterschiedliche Anforderungen hinsichtlich der Verfügbarkeit von Diensten erfüllen zu können, muss die Authentisierung nach der Festlegung der Sicherheitsstufe des angeforderten Dienstes stattfinden.
Die Authentisierung erfolgt, wenn eine Verbindungsanforderung für den Dienst übertragen wird. Die folgenden Ereignisse treten beim Zugriff auf ein vertrauenswürdiges Gerät nacheinander auf:

- Die Verbindungsanforderung erfolgt über L2CAP
- L2CAP fordert beim Sicherheitsmanager den Zugriff an
- Der Sicherheitsmanager fragt die Dienstedatenbank ab
- Der Sicherheitsmanager fragt die Gerätedatenbank ab
- Falls erforderlich erzwingt der Sicherheitsmanager die Authentifizierung und Verschlüsselung
- Der Sicherheitsmanager erlaubt den Zugriff
- L2CAP fährt mit der Einrichtung der Verbindung fort

Dabei kann die Authentisierung in beide Richtungen stattfinden, so dass sich der Client beim Server authentisieren muss, oder umgekehrt.

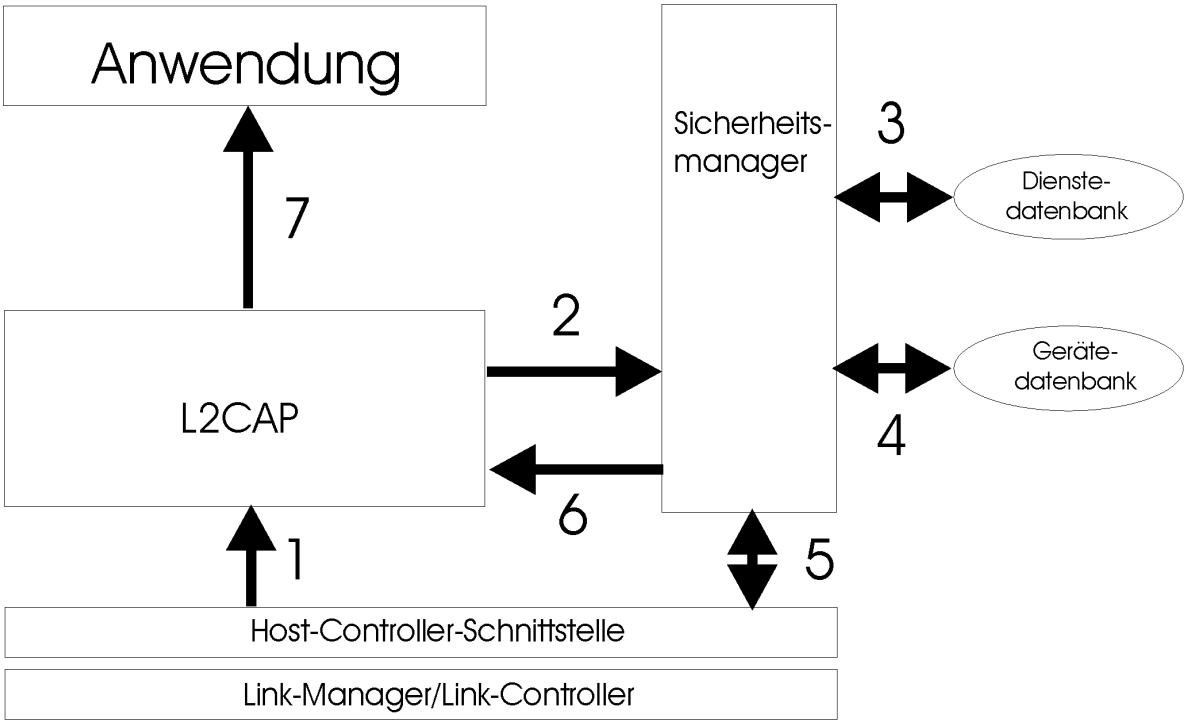


Abbildung 5 Flussdiagramm Sicherheitsabfrage

Auch wenn die Bluetooth Sicherheitsarchitektur nicht auf den Modus 3 (Sicherheit auf der Verbindungsebene) abgestimmt ist, kann sie trotzdem diesen Modus leicht unterstützen. Der Sicherheitsmanager kann dem Link Manager befehlen, dass die Authentisierung erzwungen wird, bevor eine Basisbandverbindung durch das HCI hergestellt wird. Vor dem Übergang von Modus 2 auf Modus 3 sind jedoch einige Schritte erforderlich, damit nicht vertrauenswürdige Geräte keinen Zugriff erhalten.
Der Sicherheitsmanager muss alle Verbindungscodes für nicht vertrauenswürdige Geräte, die im Funkmodul gespeichert sind, entfernen. Dazu kann er den HCI einsetzen.

4.2.7 Umgang mit dem Protokoll-Stack

Für ankommende Verbindungen ist die Zugriffssteuerung der L2CAP – Ebene und manchmal auch der darüber liegenden Multiplex Protokollen (z.B. RFCOMM) erforderlich. Beim Empfang des Verbindungswunsches stellt das Protokollobjekt beim Sicherheitsmanager eine Anfrage, beider die übermittelten Multiplex Informationen weitergereicht werden. Der Sicherheitsmanager entscheidet, ob die Verbindung initiiert werden darf, oder nicht. Er antwortet dann dem Protokollobjekt.
Falls der Zugang von Seiten des Sicherheitsmanagers gewährt wird, wird die Prozedur zur Einrichtung einer Verbindung fortgesetzt. Wird der Verbindungswunsch abgelehnt, wird die Verbindung beendet.

Der Sicherheitsmanager speichert Informationen über bestehende Authentisierungen. Dadurch werden multiple Authentisierungsprozeduren innerhalb einer Sitzung auf der der LMP-Ebene (dh. über Funk)vermieden. Dazu ist zwar während der Verbindung ein weiterer Funktionsaufruf erforderlich, jedoch entfällt, falls notwendig, eine weitere Authentisierungsprozedur.

4.2.8 Schlüsselmanagement

Die Sicherheitsfunktionen auf der Verbindungsebene werden durch vier Einheiten bedient. Die Bluetooth Device Address (**BD_ADDR)** ist eine vom IEEE definierte 48-bit Adresse, die für jedes Bluetoothgerät einmalig ist. Der **Private Authentication Key** (Link Key) ist eine 128-bit Zufallszahl, die für Authentisierungszwecke verwendet wird. Der **Private Encryption Key** wird die für Verschlüsselung verwendet wird und hat eine Länge von 8- 128 Bits. Und die Zufallszahl **RAND** ist eine sich häufig ändernde 128-bit lange Pseudozufallszahl, die durch die Bluetooth Systeme selbst gebildet wird.

Alle die Sicherheit betreffenden Transaktionen zwischen zwei oder mehr Beteiligten werden über den Link Key durchgeführt. Der Link Key ist eine 128-bit Zufallszahl, sie wird im Authentisierungsprozess und als Parameter verwendet, wenn der Encryption Key abgeleitet wird. Die Lebenszeit eines Link Keys hängt davon ab, ob es ein semipermanenter oder temporärer Schlüssel ist. Ein semipermanenter Schlüssel kann, nachdem die gegenwärtige Sitzung vorüber ist, verwendet werden um andere Bluetoothteilnehmer zu authentisieren, die ihn teilen. Ein temporärer Schlüssel lebt nur bis die gegenwärtige Sitzung beendet wird. Temporäre Schlüssel werden allgemein bei den point-to-multipoint Verbindungen verwendet, in denen gleiche Informationen mehreren Empfängern übermittelt werden.

Es gibt einige weitere Schlüsselarten, die in Bluetooth definiert werden. Link Keys können in Abhängigkeit von der Anwendung Combination Keys, Unit Keys, Master Keys oder Initialization Keys sein. Zusätzlich zu den Link Keys gibt es den Encryption Key. Der Unit Key wird separat bei der Aufnahme der ersten Verbindung erzeugt. Der Combination Key wird von den Informationen von zwei Teilnehmereinheiten abgeleitet und er wird für jedes neue Bluetooth Teilnehmerpaar erzeugt. Der Master Key ist ein temporärer Schlüssel, der den gegenwärtigen Link Key ersetzt wenn die Master Einheit, Informationen mehr als einem Empfänger übermitteln möchte. Der Initialization Key wird während des Initialisierungsprozesses als Link Key verwendet.

Die Länge des Codes der persönlichen Identifikationsnummer (PIN), der in den Bluetooth Geräten verwendet wird, kann zwischen 1 und 16 Oktetts liegen. Der normale 4-digit Code ist für einige Anwendungen genügend, aber für Anwendungen mit einem höheren Sicherheitsbedarf werden längere Codes benötigt. Der Pin- Code eines Gerätes kann fest vorgegeben sein, er muss dann nicht manuell eingegeben werden, wenn dieses Gerät mit einem zweiten eine Verbindung aufnehmen soll. Bei Geräten für höhere Anwendungen muss während der ersten Initialisierung der Verbindung, der PIN bei beiden Geräten manuell eingegeben werden (engl. Pairing) dies dient der Generierung eines Link Keys, wenn Geräte gepairt sind (ein Link Key beiden Geräten bekannt ist) fällt die neue Eingabe der Pin für diese Verbindung weg.

Die Verbindungsaufnahme erfolgt nach dem folgenden Schema:

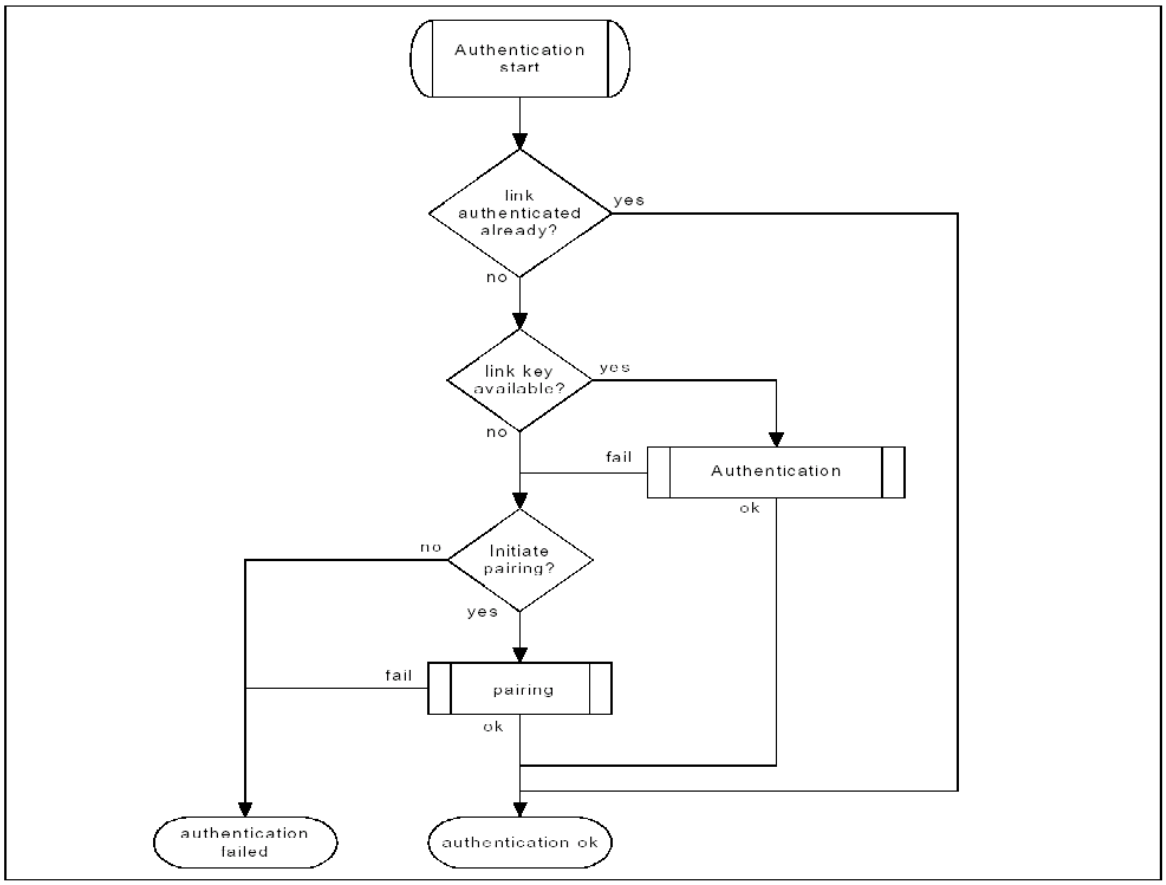


Abbildung 6 Blockschaltbild einer Bluetooth Verbindungsaufnahme

Der Initialization Key ist erforderlich, wenn zwei Einheiten ohne vorherige Verbindung in Kontakt treten wollen. Der Initialization Key wird durch den Algorithmus E22 erzeugt, der den PIN- Code, die Bluetooth Device Address des Gegenübers und die 128-bit Zufallszahl (RAND) als Eingänge verwendet. Der resultierende 128-bit Initialization Key wird für den Schlüsselaustausch während der Erzeugung eines Link Keys verwendet. Nach dem Schlüsselaustausch wird der Initialization Key verworfen.

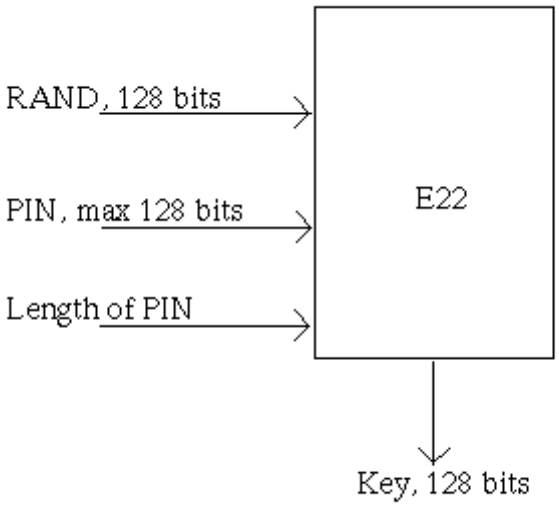


Abbildung 7 Master und Initialization Schlüssel Erzeugung mit dem E22 Algorithmus

Der Unit Key wird mit dem Algorithmus E21 erzeugt, wenn die Bluetooth Einheit zum ersten Mal in Betrieb genommen wird. Nachdem er generiert worden ist, wird er im Permanentspeicher der Einheit gespeichert und wird nur selten geändert. Eine Bluetooth Einheit kann den Unit Key des Gegenübers als Link Key zwischen diesen Einheiten verwenden. Während des Initialisierungsprozesses entscheidet die Anwendung, welche beteiligte Einheit seinen Unit Key als Link Key zur Verfügung stellt. Wenn eine der Einheiten nur sehr eingeschränkten Speicher hat (keinen Unit Key speichern kann), wird immer ein neuer Link Key generiert.

Der Combination Key wird während des Initialisierungsprozesses erzeugt, wenn die Einheiten entschieden haben, einen solchen zu verwenden. Er wird durch beide Einheiten gleichzeitig erzeugt. Zuerst erzeugen beide Einheiten eine Zufallszahl. Mit dieser Zufallszahl und ihrer Bluetooth Device Address generieren sie über den E21 Algorithmus den Combination Key. Danach tauschen die Einheiten sicher ihre Zufallszahlen aus und errechnen den zwischen ihnen zu verwendenden Combination Key.

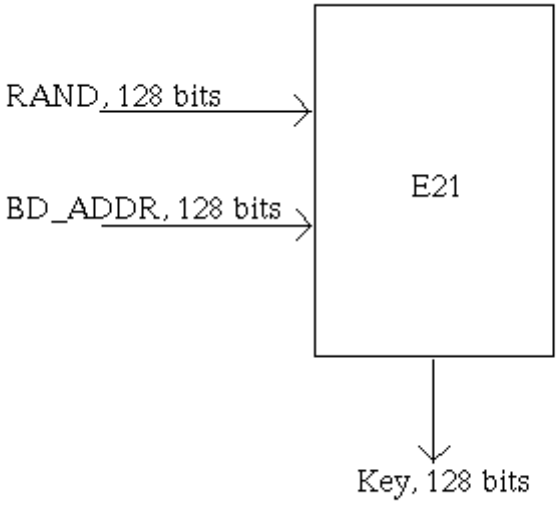


Abbildung 8 Unit und Combination Key Erzeugung mit dem E21 Algorithmus

Der Master Key ist der einzige temporäre Schlüssel der Gruppe der Link Keys. Er wird durch die Master Einheit erzeugt, indem der E22 Algorithmus auf zwei 128-bit Zufallszahlen angewendet wird. Ergebnis ist hier eine 128-bit Zufallszahl. In erster Linie wird der E22 Algorithmus verwendet, um sicherzustellen, dass der Master Key wirklich eine Zufallszahl ist. Eine dritte Zufallszahl wird dann den Slaves übermittelt und mit einem Schlüsselalgorithmus und dem gegenwärtigen Link Key wird von Master und Slaves ein Overlay berechnet. Der neue Link Key (der Master Key) wird dann, bitweise XORed mit dem Overlay zu den Slaves geschickt. Mit der Umkehroperation erhalten damit die Slaves den Master Key. Dieses Verfahren muss mit jedem Slave durchgeführt werden, mit dem der Master den Master Key verwenden will.

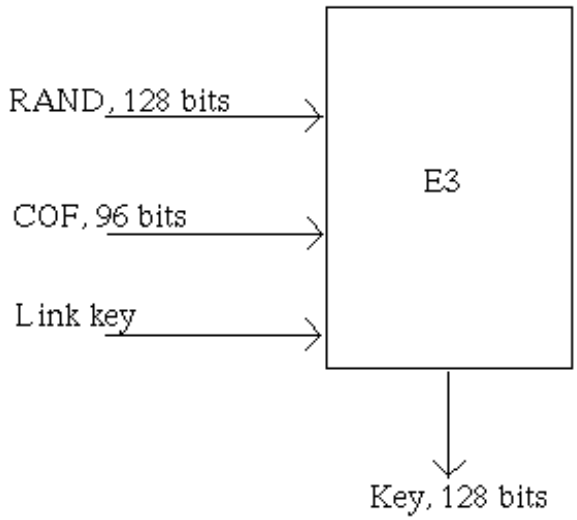


Abbildung 9 Schlüsselalgorithmus E3 für den Encryption Key

Der Encryption Key wird vom gegenwärtigen Link Key, der 96-bit Ciphering Offset Number (COF) und einer 128-bit Zufallszahl erzeugt. Die COF basiert auf dem

Authenticated Ciphering Offset (ACO), der während des Authentisierungsprozesses erzeugt wird. Wenn der Link Manager (LM) die Verschlüsselung aktiviert, wird der Encryption Key erzeugt. Er wird jedes Mal automatisch geändert, wenn die Bluetooth Einheit in den Encryptionmodus geschaltet wird.

4.2.9 Verschlüsselung

Das Bluetooth Verschlüsselungsystem verschlüsselt die Nutzlasten der Pakete. Dieses wird mit einer Stream Cipher E0 getan, die für jede Nutzlast synchronisiert wird. Die Stream Cipher E0 besteht aus dem Nutzlast Schlüsselgenerator, dem Key Stream Generator und dem Encryption/Decryption Teil. Der Nutzlast Schlüsselgenerator kombiniert die Eingangbits in einer passenden Reihenfolge und verschiebt sie auf die vier linear rückgekoppelten Schieberegister (LSFR) des Key Stream Generators. Die Key Stream Bits werden hier durch eine Methode, die vom Summation

Stream Cipher Generator von Massey und Rueppel abgeleitet wurde, generiert.

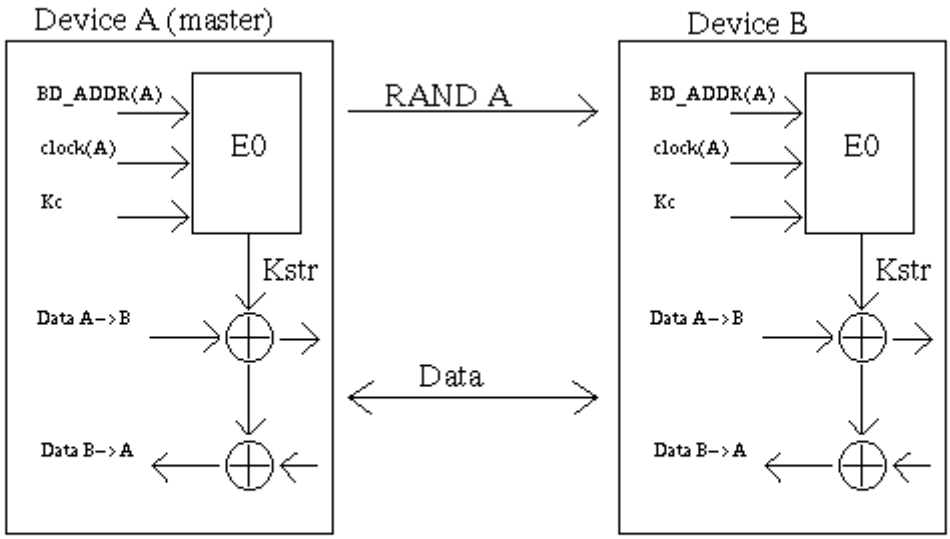


Abbildung 10 Beschreibung des Verschlüsselungsprozesses

In Abhängigkeit davon, ob eine Einheit einen semipermanenten Link Key oder ein Master Key verwendet, werden verschiedene Verschlüsselungmodi eingesetzt. Wenn ein Unit Key oder ein Combination Key verwendet werden, wird Broadcastverkehr nicht verschlüsselt. Einzeln adressierter Verkehr kann entweder verschlüsselt werden oder nicht. Wenn ein Master Key verwendet wird, gibt es drei mögliche Modi. In Verschlüsselungmodus 1, wird nichts verschlüsselt. In Verschlüsselungmodus 2 wird Broadcastverkehr nicht verschlüsselt, aber der einzeln adressierte Verkehr wird mit dem Master Key verschlüsselt. Und in Verschlüsselungmodus 3, wird der gesamte Verkehr mit dem Master Key verschlüsselt.

Da die Encryption Keygröße von 8 Bits bis 128 Bits variieren kann, muss über die Größe des Encryption Key, der zwischen zwei Einheiten verwendet wird, verhandelt werden. In jeder Einheit gibt es einen Parameter, der die maximale mögliche Schlüssellänge definiert. In Verhandlung um die Schlüsselgröße schickt der Master seinen Vorschlag für die Schlüsselgröße zum Slave. Der Slave kann diese entweder annehmen und bestätigen, oder einen anderen Vorschlag senden. Dieses wird fortgesetzt bis eine Übereinstimmung erreicht ist, oder eine der Einheiten die Übermittlung abbricht. Der Abbruch der Verhandlung wird durch die verwendete Anwendung initiiert. In jeder Anwendung wird eine minimale annehmbare Schlüsselgröße festgelegt und wenn die Anforderung durch den anderen Teilnehmer nicht erfüllt wird, bricht die Anwendung die Verhandlung ab. Dieses ist notwendig, um zu verhindern, dass ein böswilliger Teilnehmer die zu verwendende Schlüssellänge zu niedrig einstellt.

Der Verschlüsselungsalgorithmus verwendet vier linear rückgekoppelte Schieberegister (LFSRs) mit den Längen 25, 31, 33 und 39, mit der Gesamtlänge von 128. Der 128-bit Ausgangswert der vier LFSRs wird vom Key Stream Generator errechnet, der den Encryption Key, eine 128-bit Zufallszahl, die Bluetooth Device Address der Einheit und den 26-bit Wert des Taktgebers verwendet.

4.2.10 Authentisierung

Der Bluetooth Authentisierungsschema verwendet eine Challenge- Response Strategie, in der ein 2-Schritt Protokoll verwendet wird, um zu überprüfen, ob die Einheit gegenüber den geheimen Schlüssel kennt. Das Protokoll verwendet symmetrische Schlüssel, also basiert eine erfolgreiche Authentisierung darauf, dass beide Teilnehmer den gleichen Schlüssel teilen. Als zusätzliches Produkt wird der Authenticated Ciphering Offset (ACO) in beiden Einheiten berechnet und gespeichert, der der Erzeugung des Encryption Keys dient.

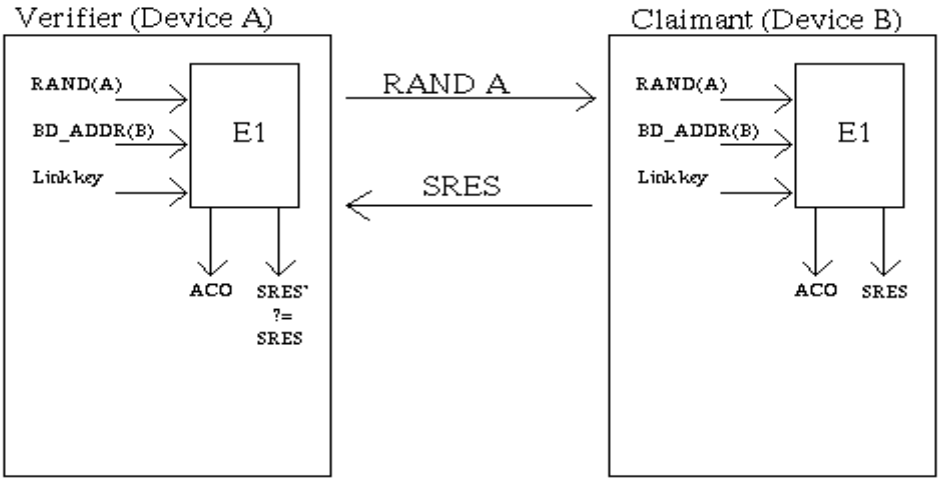


Abbildung 11 Beschreibung des Authentisierungprozesses

Zuerst schickt der Verifier dem Antragsteller eine Zufallszahl (RES). Dann verwenden beide Teilnehmer die Authentisierungsfunktion E1 mit der Zufallszahl, der Bluetooth Device Address des Antragstellers und dem gegenwärtigen Link Key, um eine Antwort (SRES) zu erhalten. Der Antragsteller sendet die Antwort zum Verifier, der dann die Gleichheit überprüft.
Bei der gegenseitigen Authentisierung läuft diese Prozedur zweimal nacheinander ab, wobei jedes Gerät einmal den Part des Verifiergerätes und einmal den des Antragstellers übernimmt. Bei bestimmten Applikationen wird nur eine einseitige Authentisierung benötigt. Der Link Manager (LM) koordiniert die Authentisierungswünsche der Anwendungen und bestimmt, in welche(r) Richtung(en) die Authentisierungsprozedur abzulaufen hat/abläuft.
Wenn die Authentisierung nicht erteilt werden kann (SRES' ≠ SRES), muss ein bestimmter Zeitabschnitt vergehen bis ein neuer Authentisierungsantrag gestellt werden kann. Der Zeitabschnitt verdoppelt sich mit jedem abgelehnten Versuch von der gleichen Adresse, bis die maximale Wartezeit erreicht ist. Die Wartezeit verringert sich exponentiell auf ein Minimum, wenn keine Authentisierungsversuche während eines Zeitabschnitts abgelehnt werden.

4.2.11 Sequence-Chart

Ein Connection Setup mit Pairing läuft folgendermaßen ab (die Connection Request Phase hat vorher stattgefunden):

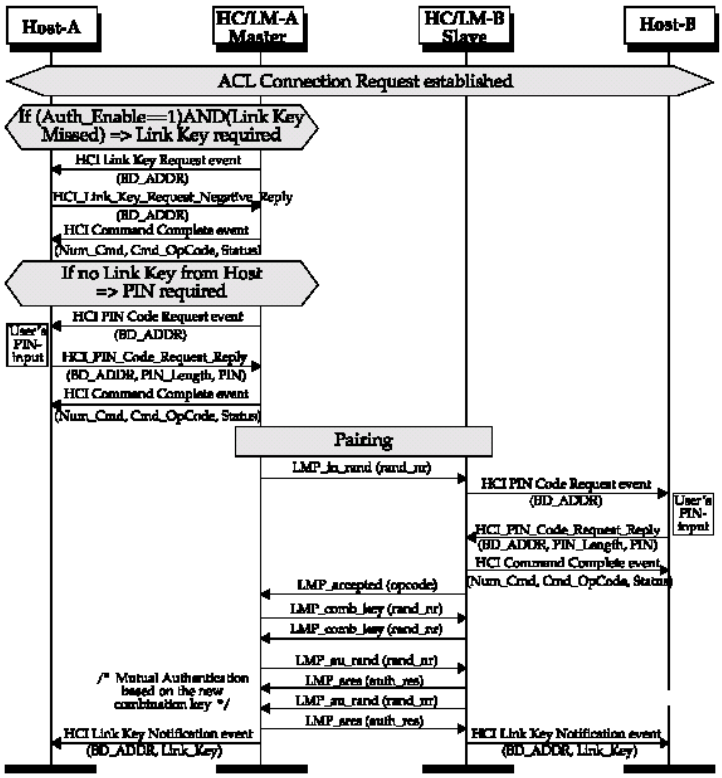


Abbildung 12 Bluetooth Pairing Sequence Chart

Das Programm Spylite protokolliert die Schnittstelle zwischen Host und Host Controller/ Link Manager. Ein Protokoll einer Verbindungsaufnahme mit Pairing der Schnittstelle HC/LM- B~ Host- B ist hier als Beispiel angefügt:

13:17:19.067 GKI freeq 0 (0:2) 1 (0:1) 2 (0:13) 3 (0:8) 4 (0:91)
13:17:19.708 --
13:17:19.708 **RCVD Event from HCI. Name: HCI_Connection_Request** (Hex Code: 0x04 Param Len: 10)
Parameters
BD_ADDR of remote : 00-04-61-80-3c-f5
Device Class of remote : 12-01-0c
Link Type : 1 (0x01)
[Das HCI (Host Controller Interface) stellt eine Befehlsschnittstelle zum Baseband-Controller und zum Link Manager zur Verfügung. Diese Schnittstelle bietet ein einheitliches Verfahren für den Zugriff auf Bluetooth-Basisband-Fähigkeiten.][BTSPEC S. 45: Between master and slave(s), different types of links can be established. Two
link types have been defined:
• Synchronous Connection-Oriented (SCO) link 0x00
• Asynchronous Connection-Less (ACL) link 0x01]

13:17:19.728 **SENT Command to HCI. Name: HCI_Accept_Connection_Request** (Hex Code: 0x0409 Param Len: 7)
Parameters
BD_ADDR of remote device : 00-04-61-80-3c-f5
Role (0 = master, 1 = slave) : 1 (0x01)
[Der Sender akzeptiert hier die Verbindungsanfrage, bestätigt die BD_ADDR des Gegenübers und nimmt die Rolle des Sklaven ein]

13:17:19.728 **RCVD Event from HCI. Name: HCI_Command_Status** (Hex Code: 0x0f Param Len: 4)
Parameters
Status : Success (0x00)
Num HCI Cmd Packets : 1 (0x01)
Command Opcode : HCI_Accept_Connection_Request (0x0409)
[Der Gegenüber bestätigt den empfangenen Befehl]

13:17:19.738 **RCVD Event from HCI. Name: HCI_Connection_Complete** (Hex Code: 0x03 Param Len: 11)
Parameters
Status : Success (0x00)
Connection Handle : 40 (0x0028)
BD_ADDR of remote : 00-04-61-80-3c-f5
Link Type : 1 (0x01)
Encryption Mode : 0 (0x00)
[An diesem Punkt ist die Baseband-Connection vollständig aufgebaut (ohne Encryption)]

13:17:19.758 **SENT Command to HCI. Name: HCI_Read_Clock_Offset** (Hex Code: 0x041f Param Len: 2)
Parameters
Connection Handle : 40 (0x0028)
[Mit dem Befehl HCI_Read_Clock_Offset (Connection_Handle) kann der BT Master den Taktgeber-Versatz der BT Sklaven lesen. Der Taktgeber-Versatz ist wichtig, um die Paging Prozedur bei einem neuen Anschlussversuch zu beschleunigen.]
[BTSPEC S.1057: Using the command HCI_Read_Clock_Offset (Connection_Handle) the BT Master can read the Clock Offset of the BT Slaves. The Clock Offset can be
used to speed up the paging procedure in a later connection attempt.]

13:17:19.758 **RCVD Event from HCI. Name: HCI_Page_Scan_Repetition_Mode_Change** (Hex Code: 0x20 Param Len: 7)
Parameters
BD_ADDR of remote : 00-04-61-80-3c-f5
Page Scan Repetition Mode : 1 (0x01)
[Der Sender gegenüber gibt bekannt, dass er den Modus in dem er Pager scant, ändert]

13:17:19.768 **RCVD Event from HCI. Name: HCI_Command_Status** (Hex Code: 0x0f Param Len: 4)
Parameters
Status : Success (0x00)
Num HCI Cmd Packets : 0 (0x00)
Command Opcode : HCI_Read_Clock_Offset (0x041f)

13:17:19.778 **RCVD Event from HCI. Name: HCI_Max_Slots_Changed** (Hex Code: 0x1b Param Len: 3)
Parameters:
Connection Handle : 40 (0x0028)
Max Slots : 5 (0x05)

13:17:19.788 **RCVD Event from HCI. Name: HCI_Read_Clock_Offset_Complete** (Hex Code: 0x1c Param Len: 5)
Parameters:
Status : Success (0x00)
Connection Handle : 40 (0x0028)
Clock Offset : 14066 (0x36f2)
BTM_InqDbRead: bd addr [000461803cf5]

13:17:19.808 **RCVD Event from HCI. Name: HCI_Command_Status** (Hex Code: 0x0f Param Len: 4)
Parameters:
Status : Success (0x00)
Num HCI Cmd Packets : 1 (0x01)
Command Opcode : HCI No Operation (0x0000)

13:17:19.808 **SENT Command to HCI. Name: HCI_Change_Connection_Packet_Type** (Hex Code: 0x040f Param Len: 4)

Parameters:
Connection Handle : 40 (0x0028)
Packet Type : 0xcc18 (DM1 DH1 DM3 DH3 DM5 DH5)
[Der Packet Typ wird geändert]

13:17:19.818 **RCVD Event from HCI. Name: HCI_Command_Status** (Hex Code: 0x0f Param Len: 4)
Parameters:
Status : Success (0x00)
Num HCI Cmd Packets : 1 (0x01)
Command Opcode : HCI_Change_Connection_Packet_Type (0x040f)

13:17:19.828 **SENT Command to HCI. Name: HCI_Write_Link_Policy_Settings** (Hex Code: 0x080d Param Len: 4)
Parameters
Connection Handle : 40 (0x0028)
Link Policy Settings : 15 (0x000f)
[Dieser Befehl ändert die Link Policy Einstellungen. Der Link Policy Settings Parameter stellt das Verhalten des lokalen Link Managers ein für den Fall, dass er einen Request von einer Remotevorrichtung empfangen wird oder er die Sklaverolle ändern soll. Der lokale Link Manager weist Requests automatisch ab oder stellt sie selbst, je nach der Einstellung der Link Policy.]

13:17:19.848 **RCVD Event from HCI. Name: HCI_Connection_Packet_Type_Changed** (Hex Code: 0x1d Param Len: 5)
Parameters
Status : Success (0x00)
Connection Handle : 40 (0x0028)
Packet Type : 0xcc18 (DM1 DH1 DM3 DH3 DM5 DH5)

13:17:19.878 **RCVD Event from HCI. Name: HCI_Command_Complete** (Hex Code: 0x0e Param Len: 6)
Parameters
Num HCI Cmd Packets : 1 (0x01)
Cmd Code : 0x080d (HCI_Write_Link_Policy_Settings)
Status : Success (0x00)
Connection Handle : 40 (0x0028)

13:17:19.878 **SENT Command to HCI. Name: HCI_Write_Link_Supervision_Timeout** (Hex Code: 0x0c37 Param Len: 4)

Parameters
Connection Handle : 40 (0x0028)
Timeout (625us units) : 32000 (0x7d00)
[Der Timeout Parameter wird geändert, dieser dient der Feststellung von Verbindungsverlusten]

13:17:19.888 **RCVD Event from HCI. Name: HCI_Command_Complete** (Hex Code: 0x0e Param Len: 6)

Parameters
Num HCI Cmd Packets : 1 (0x01)
Cmd Code : 0x0c37 (HCI_Write_Link_Supervision_Timeout)
Status : Success (0x00)
Connection Handle : 40 (0x0028)

13:17:19.898 **RCVD Event from HCI. Name: HCI_PIN_Code_Request** (Hex Code: 0x16 Param Len: 6)

Parameters
BD_ADDR of remote : 00-04-61-80-3c-f5
btm_sec_pin_code_request() BDA: 00:04:61:80:3c:f5
[Der PIN Code- Request wird verwendet, um anzuzeigen, dass ein PIN- Code angefordert werden muss, um einen neuen Link Key zu generieren. Der Host muss mit PIN- Code- Request- Reply oder dem PIN- Code- Request- Negative- Reply- Befehl reagieren abhängig davon, ob der Host den Host- Controller mit einem PIN- Code versorgen kann oder nicht.]
[BTSPEC S.754: The PIN Code Request event is used to indicate that a PIN code is required to create a new link key. The Host must respond using either the PIN Code Request Reply or the PIN Code Request Negative Reply command, depending on whether the Host can provide the Host Controller with a PIN code or not.
Note: If the PIN Code Request event is masked away, then the Host Controller will assume that the Host has no PIN Code.]

13:17:31.225 **SENT Command to HCI. Name: HCI_Pin_Code_Request_Reply** (Hex Code: 0x040d Param Len: 23)
Parameters
BD_ADDR of pin code device : 00-04-61-80-3c-f5
PIN Length : 8 (0x08)
PIN Code : 00 00 00 00 00 00 00 38 37 36 35 34 33 32 31
[Der PIN_Code_Request_Reply Befehl wird verwendet, um auf einen PIN- Code-Request vom Host Controller zu antworten. Er spezifiziert den Pin- Code, der für eine Verbindung zu verwenden
ist. Der PIN- Code- Request wird erzeugt, wenn eine Remotevorrichtung um ein Pairing bittet.]
[BTSPEC S.580: The PIN_Code_Request_Reply command is used to reply to a PIN Code
request event from the Host Controller, and specifies the PIN code to use for a connection. The PIN Code Request event will be generated when a connection with remote initiating device has requested pairing.]

13:17:31.235 **RCVD Event from HCI. Name: HCI_Command_Complete** (Hex Code: 0x0e Param Len: 10)
Parameters
Num HCI Cmd Packets : 1 (0x01)
Cmd Code : 0x040d (HCI_Pin_Code_Request_Reply)
Status : Success (0x00)
BD_ADDR of pin code device : 00-04-61-80-3c-f5

13:17:31.385 **RCVD Event from HCI. Name: HCI_Link_Key_Notification** (Hex Code: 0x18 Param Len: 23)

Parameters

BD_ADDR of remote : 00-04-61-80-3c-f5
Link Key : 0c fb 5b 1b 41 15 eb 9f cd c6 32 40 ea be e5 21
btm_sec_link_key_notification() BDA: 00:04:61:80:3c:f5
TYPE: 0

[Der Link- Key- Notification- Event wird verwendet, um dem Host anzuzeigen, dass ein neuer Link Key für den Anschluss mit dem Gegenüber erzeugt worden ist. Der Key_Type Fallparameter informiert den Host darüber, welche Schlüsselart (Combination Key, lokaler Unit Key oder remote Unit Key)(hier: Combination Schlüssel) verwendet wird.]

[BTSPEC S. 756: The Link Key Notification event is used to indicate to the Host that a new Link Key has been created for the connection with the device specified in BD_ADDR. The Host can save this new Link Key in its own storage for future use. Also, the Host can decided to store the Link Key in the Host Controller's Link Key Storage by using the Write_Stored_Link_Key command. The Key_Type event parameter informs the Host about which key type (combination key, local unit key or remote unit key)(here: combination key) that has been used during pairing. If pairing with unit key is not supported, the Host can for instance discard the key or disconnect the link.]

5 Sicherheitskonzept für das IANT (Genos)

5.1 Beschreibung

Da das IANT Genos Server zur Bluetooth Authentifikation einsetzt, haben wir uns dafür entschieden, dass Produkt genauer zu untersuchen und die eingebauten Sicherheitsfeatures mit den allgemeinen Bluetooth Sicherheiskonzepten zu vergleichen. Leider ist detailliertes Informationsmaterial (vor allem technische Informationen) zu Genos rar und so stützt sich die Untersuchung alleine auf die Materialien die im Institut vorhanden sind und auf wenige relevante Internetseiten (wir haben auch telefonisch Kontakt mit red-m aufgenommen).

Die Genos 2.1 Software ist momentan die einzige zentrale Management und Sicherheitslösungssoftware für Bluetooth und WLAN am Markt.
Sie nutzt ein fünf Schichten Netzwerk Konzept. So muss ein unauthorisierter Nutzer erst einmal jede Schicht für sich durchbrechen. Das Genos Konzept baut darauf auf, dass jede darauf folgende Schicht einen noch stärkeren Schutz bereithält.

Die fünf Sicherheitsschichten in Genos sind (siehe Grafik 1):

1. Device Authorization: Verhindert den Zugriff auf das Netzwerk von nicht autorisierten Geräten.

2. Link-Level Authentifikation und Encryption: Schützt die Luftschnittstelle und verhindert „Eavesdropping“.

3. Benutzer und Netzwerk Sicherheit: Verhindert erneut den Zugriff auf das Netzwerk, aber diesmal von nicht autorisierten Benutzern.

4. Firewall: Stellt sicher, dass die Benutzer nur Zugang zu bestimmten Diensten haben.

5. VPN Server: Dieser bietet eine weitere Benutzer Authentifikation und Verschlüsselung an, zusätzlich zu Standart VPN Lösungen.

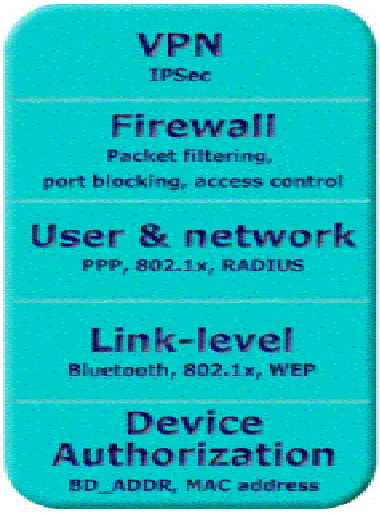


Abbildung 13 Genos Schichtenmodell

Hier noch einmal eine Auflistung in Stichworten, aller Sicherheitsfeatures, die die Genos Software anbietet:

- Geräte Level Adressen Prüfung
- Link level Authentifikation and Encryption (im Falle von Bluetooth sind das PIN, link keys und Geräte Pairing)
- Zugangskontrolle, basierend auf den angebotenen Diensten, Benutzer Lokation im Netzwerk, Vergabe von Geräte und Benutzer Privilegien.
- Netzwerk Level Authentifikation mit LDAP[1] und RADIUS[2]
- IP Zugangskontrolle und integrierte Firewall, anpassbare „Wireless Firewall“
- Netzwerk Adressen Translation (NAT)
- VPN Unterstützung mit PPTP and Ipsec / VPN Data Encryption, die die robuste IPSec 3DES Encryption benutzt
- 64 und 128 bit dynamische WEP Key Encryption für alle WiFi Anwendungen, die das 802.1x Protokoll benutzen und alternative 128 bit Encryption für Bluetooth
- eingebauter IPSec Server
    - MD5[3] (Message Digest) Authentifikation
    - 3DES[4] (Data Encryption Standart) Encryption
    - IKE[5]Zertifikate
- Paketfilterung and Port Blocking Firewall, einschließlich:
    - HTTP Web Traffic

  - Email
  - VPN
  - FTP

- 802.1x (802.11b Module) Zertifikatbasiertes (EAP/TLS) Login, stellt dynamische sessionbasierte WEP Keys sicher, Genos nutzt folgende Protokolle hierfür:

  - EAP/TLS[6]
  - 802.1x/EAPOL[7]
  - RADIUS/EAP/TLS

- Zentrales WEP Key Management (802.11b)

- PPP Authentifikation, die PAP[8], CHAP[9] and MS-CHAP (Bluetooth) benutzt

- Zentrales Bluetooth PIN Key Management

- Zentral verwaltete Geräte Adress Tabelle zur Geräte Autorisation

5.2 Modi des Genos-Servers:

1. Gateway Mode: Jeglicher Verkehr der „Wireless“ Domäne passiert zuerst den Genos Server. Dies hat den Sicherheitsvorteil, dass die „Wireless“ Domäne vom Rest des Netzwerks getrennt wird.

2. Indirect Mode: In diesem Modus wird der Verkehr der „Wireless“ Domäne direkt vom AP in das Netzwerk geleitet. Zu diesem Netzwerk hat der Genos Server auch Zugriff und kontrolliert so den drahtlosen Zugriff.

5.3 Sicherheitseinstellungen des 1050 AP

Uns lagen sehr ausführliche Informationen über die Konfiguration, des im IANT benutzten Access Point 1050 AP (von der Firma Red-M, die Genos betreibt), mit Genos vor. Es folgt eine detaillierte Auflistung der Sicherheitsfeatures die Genos im Access Point implementiert hat (siehe Grafik 2):

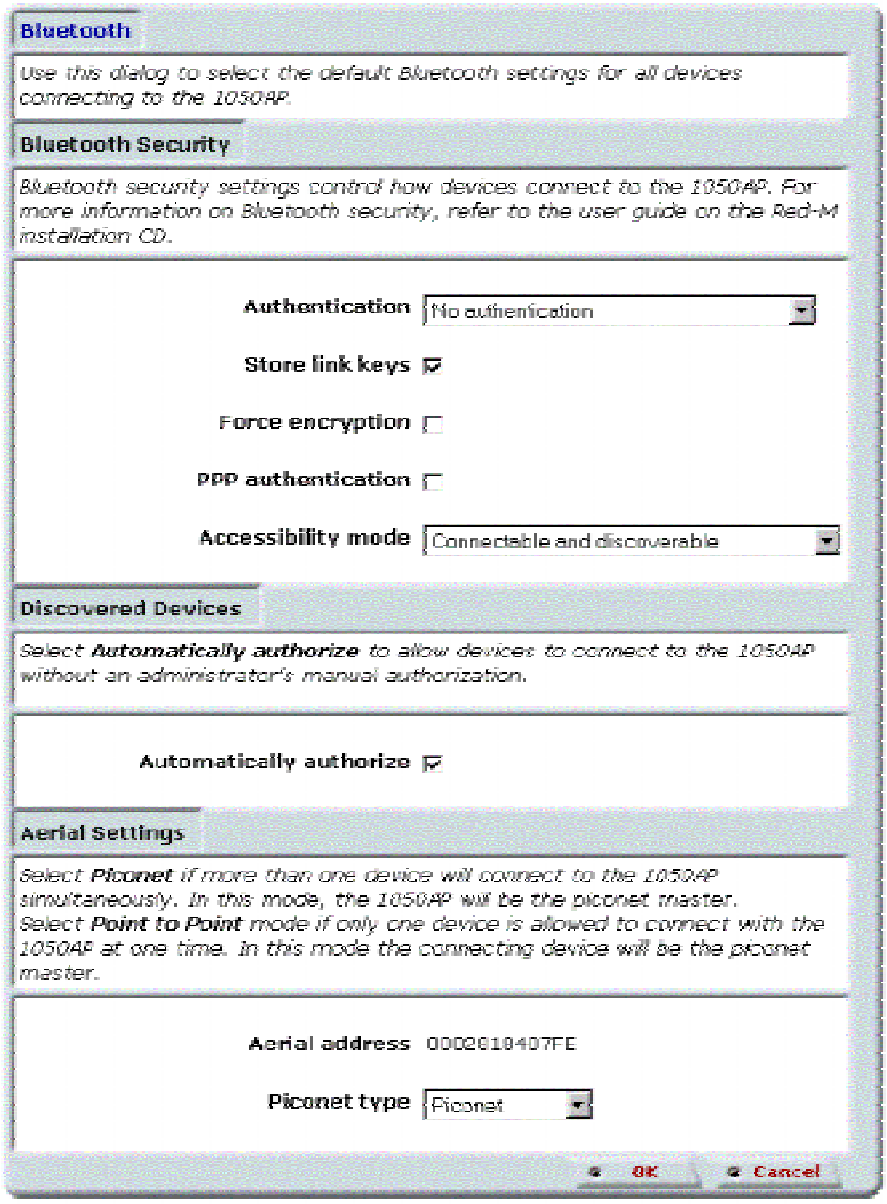


Abbildung 14 Genos AP-Konfiguration

Generell gilt, dass die Sicherheitseinstellungen für jedes Bluetooth Gerät individuell getroffen werden können. So können manche Sicherheitseinstellungen für ein bestimmtes Gerät gelten, andere wiederum nicht.

Bluetooth Authentifikation: Hierbei handelt es sich um eine Implementatierung der bereits bekannten Bluetooth Authentifikation. Der Administrator muss den Passkey des Bluetooth Gerätes in die dafür vorgesehene Dialogbox auf einem Access Point eintragen. Es gibt auch die Möglichkeit der automatischen Authentifikation. Wird dieses gewählt muss der Administrator nicht mehr jedes neue Gerät manuell authentisieren. Wählt sich das Bluetooth Gerät das erste Mal auf dem AP ein, findet das schon bekannte Pairing statt. Eine Sicherheitseinstellung erlaubt es, dass der erzeugte Link Key nicht gespeichert wird. Das bedeutet, Benutzer müssen ihren Passkey bei jedem Verbindungswunsch neu eingeben.

Genos hält an dieser Stelle aber vier verschiedene Authentifikationsmöglichkeiten bereit:

- Keine Authentifikation:
- Authentifikation mit Pairing
- Authentifikation nur für in der Vergangenheit gepairte BT Geräte
- Authentifikation mit Pairing, aber nur in den folgenden 5 Minuten

Wenn Authentifikation in einer der oben genannten Optionen eingeschaltet ist, kann Encryption auf der Luftschnittstelle angewählt werden. Es werden alle Links zwischen dem AP und den Bluetooth Geräten nur noch verschlüsselt übertragen.

Der Genos Server besitzt die Möglichkeit PPP Authentifikation zu benutzen. Dieses Feature kann zusätzlich oder anstatt der normalen Bluetooth Authentifikation und Encryption eingesetzt werden. Die PPP Authentifikation fordert den Bluetooth Benutzer auf, jedes Mal wenn er eine Verbindung zu einem Bluetooth Access Point aufnehmen möchte, seinen Benutzernamen und sein Passwort einzugeben.
Wenn die PPP Authentifikation eingestellt wird, benutzt Genos das CHAP[9] Protokoll um die Benutzer zu authentifizieren

Erreichbarkeitsmodus des Access Points: Es gibt in Genos drei verschiedene Einstellungsmöglichkeiten, die entscheiden, ob ein Bluetooth Gerät den Access Point entdecken und sich mit ihm verbinden kann.

- Die Default Einstellung ist „Connectable and Discoverable“. In diesem Modus können BT Geräte Informationen mit dem AP austauschen und bei einem Scan von Bluetooth Geräten in Reichweite wird der Access Point angezeigt.
- „Connectable and Non-Discoverable“ bedeutet, dass ein Bluetooth Gerät den Access Point bei einem Scan nicht entdeckt, aber mit ihm verbinden kann, um Informationen auszutauschen, wenn ihm die Adresse des Access Points bekannt ist.
- Im „Non-Connectable and Non-Discoverable“ Modus ist der Access Point bei Scans nicht zu sehen und kein BT Gerät kann sich mit ihm verbinden. Dieser Modus ist besonders zu empfehlen, wenn der Access Point gerade konfiguriert wird oder neue Benutzer hinzugefügt werden, um Missbrauch zu vermeiden.

Luftschnittstellen Einstellung: Man kann mit dem AP ein Piconetz aufbauen oder aber eine Punkt zu Punkt Verbindung. Im Piconetz Modus fungiert der Access Point als Master und mehrere Bluetooth Geräte können mit ihm gleichzeitig kommunizieren. Bei dem Punkt zu Punkt Betrieb kann sich nur ein Bluetooth Gerät mit dem Access Point verbinden und der Access Point nimmt hierbei die Rolle des Slaves ein.

5.4 Genos Konfiguration im IANT

Das IANT nutzt momentan fünf Bluetooth Access Points vom Typ 1050 AP von Red-M. Als Bluetooth Authentifikations Server wird Genos 2.1 eingesetzt. Die Bluetooth Access Points werden in folgender Konfiguration verwendet (siehe Grafik 3):

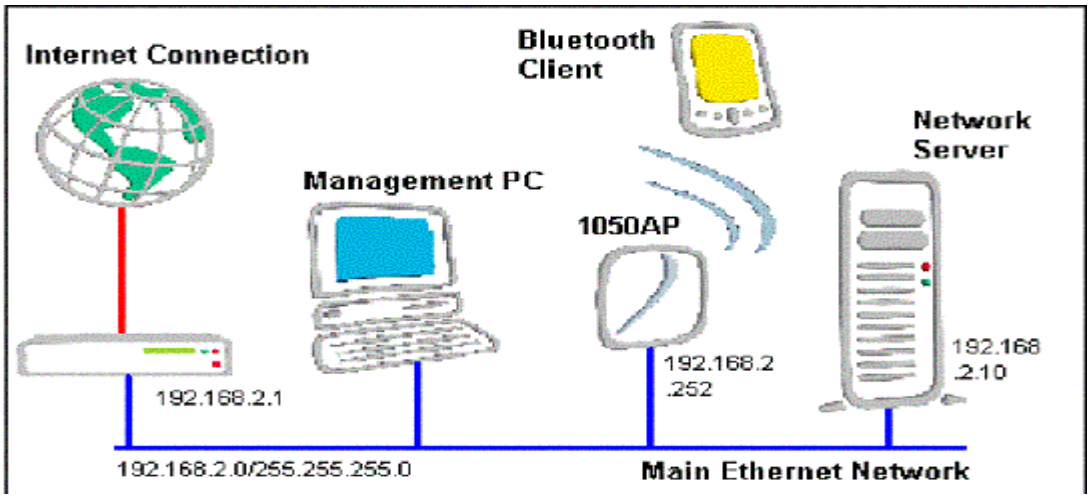


Abbildung 15 Genos Netzstruktur

Die Bluetooth Geräte bekommen Ihre IP Adressen von dem DHCP Server (hosted auf einem Network Server). Die gesamten Netzwerk Informationen (z.B. DNS, Default Gateway), werden vom DHCP Server geliefert.

5.5 Die Integration von WLAN und Bluetooth mit Genos

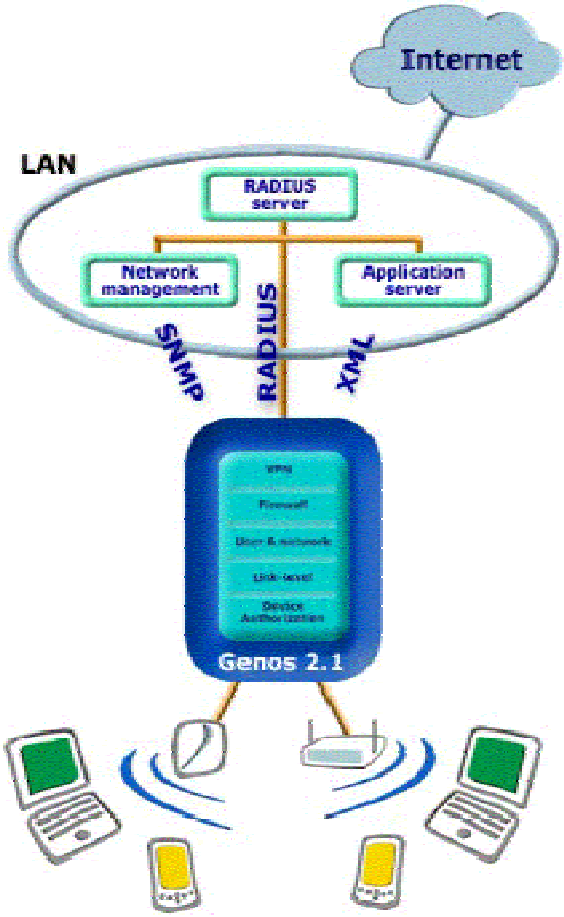


Abbildung 16 Genos-Radius Integration

Der Genos Server kann so konfiguriert werden, dass er sich in eine bestehende WLAN Architektur integrieren lässt. Hierfür wird der Genos Server vor den für WLAN benutzten Authentifikations Server (RADIUS) geschaltet. Jeglicher „Wireless Network“ Verkehr, muss so den Genos Server passieren. Die IP des RADIUS Servers wird in den Genos Server eingetragen. So kann Genos die Anfragen von drahtlosen Geräten, die ihm nicht bekannt sind, zur Überprüfung an den RADUS Server weiterleiten. Erst wenn der RADIUS Server das Gerät auch nicht identifizieren kann, wird es abgewiesen. So lässt sich eine ganzheitliche Sicherheitsarchitektur für den gesamten drahtlosen Netzwerkverkehr bilden (siehe Grafik 4).

Genos unterstützt nur WLAN Access Points von bestimmten Herstellern.
Diese sind:

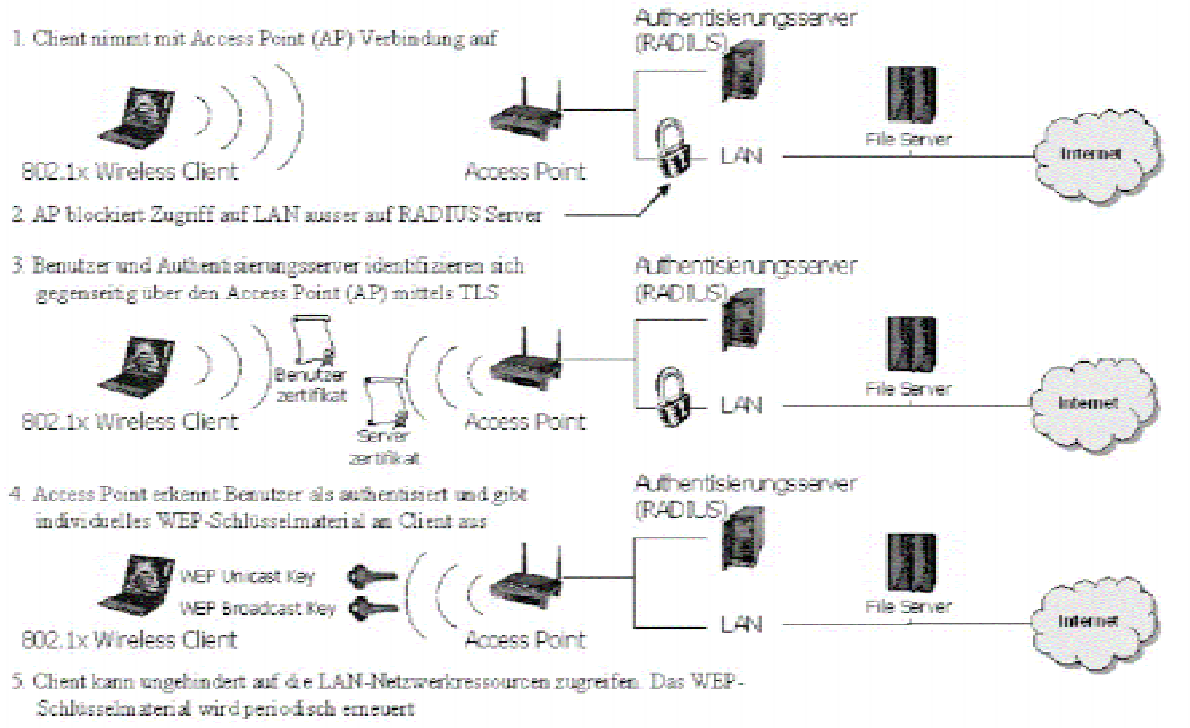
- Cisco
- Intel
- 3Com
- Symbol

Das IANT benutzt momentan WLAN Access Points von Lucent Technologies. Diese sind nicht kompatibel mit Genos.

Das IANT hat keinen RADIUS Server implementiert. WLAN und Bluetooth werden parallel betrieben, jedes für sich mit eigenem Sicherheitskonzept. Ein Sicherheitskonzept, dass Bluetooth und WLAN vereint, liegt also nicht vor, ist aber für die Zukunft zu empfehlen (z.B. RADIUS integriert in Genos). Im Hinblick darauf, dass das RRZN in naher Zukunft alle WLAN Aktivitäten kontrollieren wird, lohnt es sich wahrscheinlich nicht mehr jetzt noch eine eigene Lösung zu implementieren.

5.6 Kurzdarstellung der Funktionsweise eines RADIUS Servers

Die unten stehende Grafik soll kurz verdeutlichen, wie ein RADIUS Server funktioniert:



Quelle: 11b+1x=11i oder die drahtloseNetzwerksicherheits-Mathematik der Zukunft? Gerhard Hassenstein

Abbildung 17 Radius Kommunikation

5.7 Ist Genos das richtige Produkt für das IANT?

In unseren Untersuchungen haben wir gezeigt, dass Genos softwareseitig alle Sicherheitsfeatures die Bluetooth von Haus mitbringt implementiert hat. Es verwendet die neusten Protokolle und Algorithmen und ist somit zukunftssicher und auf dem aktuellsten Stand was Sicherheitstechnik betrifft. Darüber hinaus bietet Genos noch eine Vielzahl zusätzlicher Sicherheitskonzepte an, mit denen es möglich ist eine Bluetooth Kommunikation über einen Access Point sicherer zu gestalten.
Auch für ein gemeinsames Sicherheitskonzept von WLAN und Bluetooth im Parallelbetrieb bietet Genos eine Lösung an. Die einzige Funktion, die nach unseren Kenntnisstand nicht in Genos implementiert ist, aber zu unserem Sicherheitskonzept gehört, ist eine Audit Funktion, mit der alle Netzaktivitäten aufgezeichnet werden, um sie später bei Bedarf einsehen zu können.

Trotzdem gibt es zum heutigen Zeitpunkt, nach unseren Recherchen, kein vergleichbares Produkt auf dem Markt. Genos eignet sich sehr gut, um die Sicherheitsanforderungen des IANT´s zu erfüllen.

Es ist an dieser Stelle noch darauf hinzuweisen, dass Genos nur softwareseitig für ein sicheres Netzwerk sorgt. Wie in Kapitel 1 gezeigt wurde, müssen noch Maßnahmen unternommen werden, die das IANT vor Störsendern schützt. Außerdem muss die Sendeleistung der Access Points angepasst werden und die Access Points selbst müssen vor unerlaubten Zugriffen geschützt werden, nur dann erreicht man ein ganzheitliches Sicherheitskonzept.

5.8 Glossar

[1] LDAP: Lightweight Directory Access Protocol
LDAP ist ein TCP/IP-basiertes Directory-Zugangsprotokoll, das sich im Internet und in Intranets als Standardlösung für den Zugriff auf Netzwerk-Verzeichnisdienste für Datenbanken, E-Mails, Speicherbereiche und andere Ressourcen etabliert hat. LDAP ist von der IEFT standardisiert und bietet einen einheitlichen Standard für Verzeichnisdienste (DS).

[2] RADIUS Server: Der Remote Authentication Dial-in User Service, kurz RADIUS genannt, ist ein Werkzeug, mit dem sich Remote-Access-Sicherheitskonzepte flexibel und zentral einrichten lassen. RADIUS folgt einem Client/ Server-Modell. Bei der Anmeldung eines Benutzers sendet der Remote Access Server die Verbindungsanfrage eines Benutzers zum zentralen RADIUS-Server weiter, der dann im Namen des Remote Access Servers die Authentisierung und Autorisierung des Benutzers überprüft und bestätigt.

[3] MD5: Der Algorithmus benutzt als Eingang einen String beliebiger Länge und liefert als Ausgabe einen 128 bit „Fingerprint“ des Strings, anhand dessen der String eindeutig erkannt wird. Stichwort Digitale Signatur

[4] 3DES (Triple DES): Verbesserung des symmetrischen DES-Verschlüsselungsverfahrens, bei dem der DES-Algorithmus dreimal angewendet wird, um eine höhere Sicherheit zu erreichen.

[5] IKE (Internet Key Exchange Protocol): IKE dient bei IPSec der Authentifizierung und dem Schlüsselaustausch.

[6] EAP/TLS: Mit Hilfe des Extensible Authentication Protocols (EAP) können zwei Kommunikationspartner vor der eigentlichen Authentifizierung aushandeln, welche Authentifizierungsmethode angewandt werden soll.
EAP beschreibt in einem einfachen Request-Response-Verfahren den Austausch der Authentifizierungsdaten vom Benutzer zum Authentisierungsserver und dessen Antwort. Dabei können beliebige Authentifizierungs-mechanismen, wie CHAP, Kerberos, SecurID oder wie bei Genos SSL-TLS benutzt werden.

[7] EAPOL: Die EAP-Nachrichten müssen selbst noch einmal ummantelt sein, um das Frame-Netz als Medium nutzen zu können. Das so genannte »EAP over LAN«-Protokoll (EAPOL) verteilt die Nachrichten physikalisch zwischen Switch, Client und RADIUS-Server und benachrichtigt alle Teilnehmer über den Session-Status per »Start«- und »Logoff«-Nachricht.

[8] PAP Password Authentication Protocol: Eine Methode für das Validieren der Identität von Benutzern, die sich bei einem Point-to-Point Protocol (PPP)-Server anmelden. Das PAP-Verfahren wird in der Regel eingesetzt, wenn der Benutzername und das Kennwort, das vom Benutzer eingegeben wird, unverschlüsselt an ein anderes Programm gesendet werden müssen.

[9] CHAP: Kurz für Challenge Handshake Authentication Protocol, eine Authentisierungsart, in dem der Authentisierungsdienst (gewöhnlich ein Netzserver) dem Client, einen Schlüssel, für den Usernamen und das Kennwort zuschickt. Dieser aktiviert die Verschlüsselung, um bei der Übertragung des Usernamens und des Kennworts gegen abhorchen geschützt zu sein. Vergleichbar mit PAP.

6 Fazit

Bei unseren Untersuchungen der Sicherheitsfeatures, die in WLAN und Bluetooth integriert haben wir gezeigt, dass die WLAN Sicherheit basierend auf WEP unzureichend ist. Gerade in größeren Institutionen ist es nicht möglich den symmetrischen Schlüssel geheim zu halten. Eine ausreichende Sicherheit bietet hier ein VPN. Ein VPN beinhaltet aber auch Nachteile. Besonders der erhöhte administrative Aufwand und der zusätzliche finanzielle Belastung für diese Infrastruktur fallen hierbei negativ auf. Wie ausführlich ausgeführt basiert die Bluetooth Sicherheit auf Authentisierung und Encryption. Die Verschlüsselungsmaßnahmen sind sicherer einzustufen, als die von WLAN. Man kann aber an der kompletten Bluetooth Sicherheitsarchitektur eine ganz prägnante Schwachstelle erkennen. Es lassen sich nur Geräte authentifizieren, nicht deren Anwender. Sofern keine Schutzmaßnahmen auf der Anwendungsschicht angewendet werden, ist immer Missbrauch und unautorisierter Zugang möglich. Abschließend sind wir zu dem Schluss gekommen, dass eine sichere Infrastruktur in der Größenordnung eines Instituts nur mit sehr viel Aufwand individuell angepasst werden kann. Insbesondere wenn man Bluetooth und WLAN parallel nutzen möchte. Die momentan sicherste Lösung ist es den Genos Server in der Kombination mit einem Radius Server einzusetzen. So erreicht man ein ganzheitliches Sicherheitskonzept, welches Bluetooth und WLAN vereint. Genos verwendet die neusten Protokolle und Algorithmen und ist somit zukunftssicher und auf dem aktuellsten Stand was Sicherheitstechnik betrifft. Darüber hinaus bietet Genos noch eine Vielzahl zusätzlicher Sicherheitskonzepte an, mit denen es möglich ist Kommunikation über einen Access Point sicherer zu gestalten.

7 Quellenangaben:

- Bluetooth - Sicherheitsmodelle der Bluetooth Spezifikation – Nathan J. Muller – 2001
- Wireless Security – Randall K. Nichols, Panos C. Lekkas – 2002
- http://www.niksula.cs.hut.fi/~jiitv/bluesec.html
- Bluetooth Spezifikation - Bluetooth_11_Specifications_Book
- Security Weakness in Bluetooth - Markus Jakobsson, Susanne Wetzel
- Security of Bluetooth: An Overview of Bluetooth Security - Marjaana Träskbäck
- http://www.edcwireless.com/BTgenos.htm
- http://www.e-mediation.com.my/Inside_genos.pdf
- http://www.red-m.com/products/genos/core/
- http://www.red-m.com/support/1050ap/documents/default.asp
- Sicherheit im Funk-LAN (WLAN, IEEE 802.11) - Bundesamt für Sicherheit in der Informationstechnik - Juli 2002
- http://standards.ieee.org/getieee802/802.11.html - IEEE 802.11(b) WLAN Standards