Securitypraktikum WS 06/07

Stefan Klefisch,
Omid Haschemi,
Ulrich Grave,
Daniel Renoth

Inhaltsverzeichnis:

Bluetooth™

1. Über Bluetooth:

Bluetooth ist ein in den 1990er Jahren ursprünglich von Ericsson entwickelter Industriestandard gemäß IEEE 802.15.1 für die drahtlose (Funk-)Vernetzung von Geräten über kurze Distanz.

Bluetooth bietet eine drahtlose Schnittstelle, über die sowohl mobile Kleingeräte wie Mobiltelefone und PDA's als auch Computer und Peripheriegeräte miteinander kommunizieren können.

Ein solches Netzwerk wird auch als Wireless Personal Area Network (WPAN) bezeichnet. Hauptzweck von Bluetooth ist das Ersetzen von Kabelverbindungen zwischen Geräten.

1.1 Bluetooth Technik:

Klassen & Reichweite

Klasse	Max. Leistung in (mW)	Max. Leistung in (dBm)	Reichweite im Freien
Klasse 1	100 mW	20 dBm	~100 m
Klasse 2	2.5 mW	4 dBm	~50 m
Klasse 3	1 mW	0 dBm	~10 m

Tabelle 1-1: Bluetooth Klassen

Die Reichweite hängt stark von der Antennenbauform ab, sowie von Störungen und Hindernissen wie zum Beispiel Mauern, Wänden.

1.2 Architektur:

Ein Bluetooth-Netzwerk (Piconet) kann bis zu 260 Teilnehmer umfassen, acht Geräte können gleichzeitig aktiv sein (3bit adressiert) und 256 (8bit adressiert) währenddessen geparkt werden.
Alle nicht aktiven Geräte können im Parkmodus die Synchronisation halten und auf Anfrage im Netz aktiviert werden.
Das Piconetz besteht aus einem Master und bis zu sieben weiteren Teilnehmern (Slave). Der Master steuert die Kommunikation und vergibt Sendeslots an die Slaves.
Ein Bluetooth-Gerät kann in mehreren Piconetzen angemeldet sein, allerdings nur in einem Netz als Master. Bis zu zehn Piconetze bilden ein Scatternet (von to scatter = ausstreuen), wobei die Teilnehmer untereinander in Kontakt treten können. Hierbei wird jedes Piconet durch eine unterschiedliche Frequency-Hopping-Folge identifiziert. Die Datenrate leidet in diesem Scatternet jedoch meist erheblich.

1.3 Bluetooth Profile:

Austausch von Daten zwischen Geräten wird durch so genannte Profile realisiert. Bei Verbindungsaufbau tauschen die Geräte ihre Profile aus und legen somit fest, welche Dienste Sie für den jeweiligen Partner zu Verfügung stellen können und Daten oder Befehle sie dazu benötigen. Unten sieht man eine Auswahl einiger Profile, die für Bluetooth bereits implementiert worden sind.

ABKÜRZUNG	BEDEUTUNG	VERWENDET FÜR
AVRCP	Audio Video Remote Control Profile	Fernbedienung für Audio/Video
BIP	Basic Imaging Profile	Übertragung von Bilddaten
BPP	Basic Printing Profile	Drucken
CIP	Common ISDN Access Profile	ISDN Verbindungen über CAPI
CTP	Cordless Telephony Profile	Schnurlose Telefonie
DUN	Dial-up Networking Profile	Internet-Einwahlverbindung
ESDP	Extended Service Discovery Profile	Erweiterte Diensteerkennung
FAXP	FAX Profile	Faxen

FTP	File Transfer Profile	Dateiübertragung
GAP	Generic Access Profile	Zugriffsregelung
GAVDP	Generic AV Distribution Profile	Übertragung von Audio-/Videodaten
GOEP	Generic Object Exchange Profile	Objektaustausch
HCRP	Hardcopy Cable Replacement Profile	Druckanwendung
HSP	Headset Profile	Sprachausgabe per Headset
HFP	Hands Free Profile	Schnurlose Telefonie im Auto
HID	Human Interface Device Profile	Eingabe
INTP	Intercom Profile	Sprechfunk
LAP	LAN Access Profile (nur Version < 1.2)	PPP Netzwerkverbindung
OPP	Object Push Profile	Visitenkarten-/Terminaustausch
PAN	Personal Area Networking Profile	Netzwerkverbindungen
SAP	SIM Access Profile	Zugriff auf SIM-Karte
SDAP	Service Discovery Application Profile	Geräteauffindung
SPP	Serial Port Profile	Serielle Datenübertragung
SYNCH	Synchronisation Profile	Datenabgleich

Tabelle 1-2: Bluetooth Profile

1.3.1 Bluetooth Profile - LAP:

Das Bluetooth-Profil LAP ermöglicht Bluetooth-Geräten den Zugang zu lokalen Netzwerken. Das Protokoll ist seit der Bluetooth-Spezifikation 1.2 nicht mehr im Bluetooth-Standard enthalten. Statt dessen soll für den Aufbau und die Kopplung von Netzwerken über Bluetooth-Verbindungen nur noch das Profil Personal Area Networking (PAN) zum Einsatz kommen.

Nur wenige ältere Bluetooth-Geräte bieten LAP an. Die meisten Netzwerkanwendungen von Bluetooth basieren von vornherein auf dem Profil PAN. LAP setzt auf ein weiteres Bluetooth-Profil auf, das Serial Port Profile (SPP).

Für das Bluetooth-Profil LAP sind zwei verschiedene Rollen definiert. Die Geräte die den Zutritt zu Netzwerken ermöglichen, werden als LAN-AP (Access-Point) bezeichnet. Geräte, die über einen LAN-AP auf ein LAN zugreifen wollen, werden hingegen als LAN-DT (Data-Terminal) bezeichnet.

1.3.2 Bluetooth Profile - PAN:

Über das Netzwerk-Profil PAN können im persönlichen Umfeld kleine Netzwerke gebildet werden. Durch Aufbau eines Ad-hoc-Netzwerkes können bis zu acht PCs aktiv miteinander Daten austauschen. Wie in einem lokalen Netzwerk (LAN) lassen sich Ressourcen wie Festplatten, Internetzugang und Drucker gemeinsam nutzen.

Über PAN ist auch die gemeinsame Nutzung eines DSL-Zuganges möglich. Dadurch können bis zu acht Geräte gleichzeitig auf eine bestehende DSL-Internetverbindung zugreifen.

Das Bluetooth-Profil PAN kennt zwei verschiedene Rollen. Ein PAN-AP (Access Point) kann anderen Bluetooth-Geräten, die als PAN-User (dt. Benutzer) bezeichnet werden, den Zugang zu bestehenden Netzwerken vermitteln oder als Master in einer PAN-Group (dt. PAN-Gruppe) arbeiten. Zu einem solchen spontan gebildeten Netzwerk können sich bis zu sieben PAN-User über einen PAN-AP zusammenschließen.

Zwei PAN-User können sich allerdings auch ohne Mitwirkung eines PAN-AP direkt miteinander verbinden.

2. Bluetooth Access-Point: **Belkin F8T030**

Merkmale :

- Kabellose Druckverbindungen zu einem USB-Drucker über Bluetooth und Ihr Netzwerk
- Unterstützt bis zu sieben Nutzer gleichzeitig
- Leichte Verwaltung mit integriertem Internet-Browser
- Reibungsloser Einsatz mit Desktop- oder PDA-Computer
- Durch das eingebaute Sicherheitssystem mit 128-Bit-Verschlüsselung und Authentifizierung erhalten Sie sicheren Zugriff auf jedes Bluetooth-Gerät
- Unterstützt alle Bluetooth v1.1-Geräte
- Leicht zu installieren
- Unterstützt Microsoft Windows 98 SE, Me, 2000, XP und Microsoft Pocket PC 2000 und Pocket 2002
- Bis zu 100 m Reichweite, je nach Umgebung, Anzahl der Benutzer und weiteren kabellosen Geräte in unmittelbarer Nähe.
- Inklusive Installations-Software für Windows

2.1 Entscheidungsfindung nach Kriterien:

- Anschaffungskosten
- Reichweite
- Beschaffung
- Funktionalität

Wir haben uns für den Access Point Belkin entschieden, da her eine hohe Reichweite bietet und recht günstig zu beziehen ist. Der D-Link z.B. ist alleine schon von seinen schwachen Reichweite von grade mal 20m ausgeschieden. Der Allnet wird nicht mehr hergestellt und ist demnach auch sehr schwer zu beschaffen.

2.2 Access-Point Konfiguration:

Für den AP besteht ein webbasierendes Konfigurationsinterface. Es ist recht simple aufgebaut für die einfache Handhabung. Alles ist recht deutlich definiert. Zugang zum Administrationsinterface erhält man über eine feste IP-Adresse (141.28.68.197).

Nach dem Login gibt es verschieden Konfigurationspunkte.

- **LAN**
- **Bluetooth**
- **USB**
- **Security**
- **Utilities**

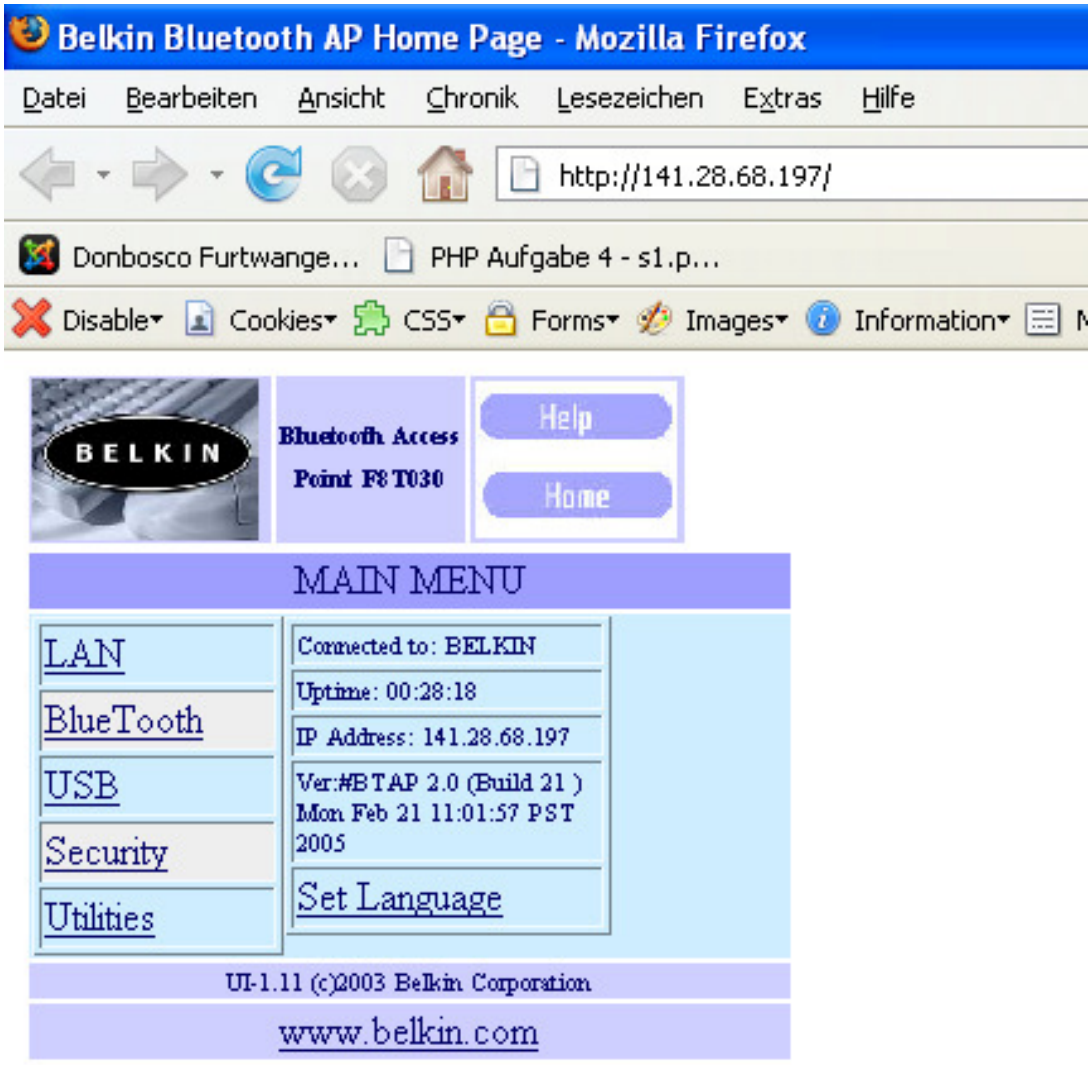

Bild 1-1: Startseite Interface

2.2.1 LAN:

Bild 1-2: LAN Einstellungen

Unter dem Menüpunkt befinden sich sämtliche Netzwerkgrundeinstellungen wie die MAC Adresse, der Hostname, entsprechende IP-Adresse, die Subnetmask, Router IP, DNS und Domain. Über den Button „Change" lassen sich fast alle Einstellung ausgenommen der MAC Adresse ändern bzw. konfigurieren.

- ## 2.2.2 Bluetooth:

Darunter sind Informationen über den Status der Bluetooth-Verbindungen zu finden. Ebenfalls die Adresse, den Linkstatus, die Anzahl der aktuellen Verbindungen und des Netzwerkverkehrs mit Auflistung von eingehenden und ausgehenden Paketen.

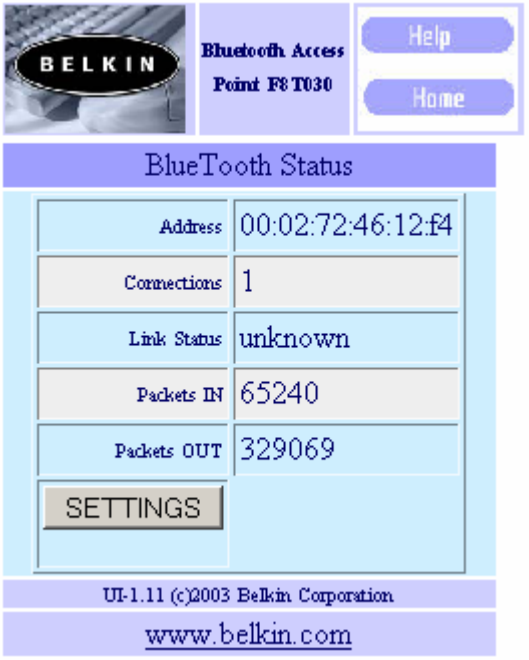

Bild 1-3: Bluetooth Status

Über den Button „Settings" können folgende Einstellungen vorgenommen werden wie auf Bild 4: Bluetootheinstellungen zu sehen sind.

Bild 1-4: Bluetootheinstellungen

Vergabe des "FriendlyName", eines Alias für den Access Point. Hier in diesem Fall wurde Belkin gewählt. Unter diesem Alias ist der Access Point unter Bluetooth sichtbar.

Des Weiteren kann die maximale Anzahl der Clients beschränkt werden in der Scala von
0 – 7.

Zuletzt kann das PAN Profil aktiviert bzw. deaktiviert werden.

- **2.2.3 USB:**

Welcher Statusinformationen liefert über den Zustand der USB Verbindungen an Ports 0 und Port 1, welche für den Anschluss von Druckern konzipiert sind. Es können maximal 2 Drucker an dem F8T030 betrieben werden.

- **2.2.4 Security:**

Hier werden sicherheitsrelevante Parameter vergeben. Diese untergliedern sich nochmals in weitere Punkte wie

  - **Bluetooth User Verwaltung :** *(Bild 1-5: Bluetooth User Verwaltung)*
    - Anzeigen aller User
    - Hinzufügen und ändern von User
    - Löschen einzelner User
    - Aktivieren bzw. Deaktivieren des Usermodus

Bild 1-5: Bluetooth Userverwaltung

- **Bluetooth Passwort :**
  - Setzen eines neuen Passwortes

- **Sicherheitsmanager :** *(Bild 1-6: Bluetooth User Verwaltung)*
  - Setzen eines Zugangspasswort
  - Zugangsschutz aktivieren bzw. deaktivieren

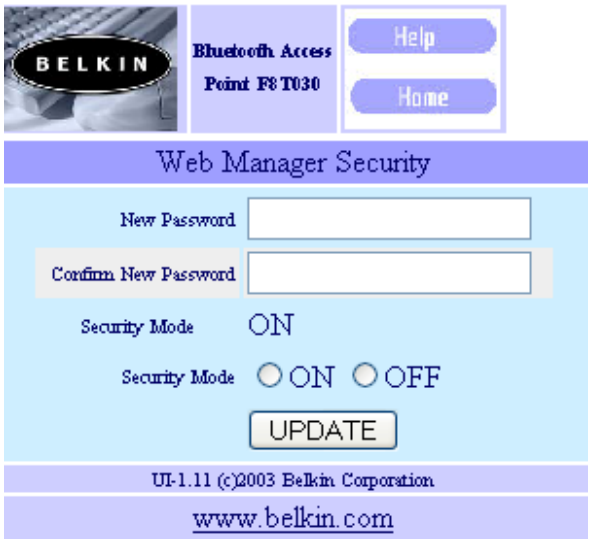

Bild 1-6: Sicherheitsmanager

2.2.5 Utilities:

Unter Utilities befinden sich Systemfunktionen und Statusinformation wie

- Upgrade
  - Einspielen einer neuen Firmware *(siehe Bild 7: Upgrade)*
- Reboot
  - Router Neustarten
- Factory Reset
  - Zurücksetzen auf Werkseinstellung
- Net test ping
  - Anpingen einzelner Hosts *(siehe Bild 8: Ping)*

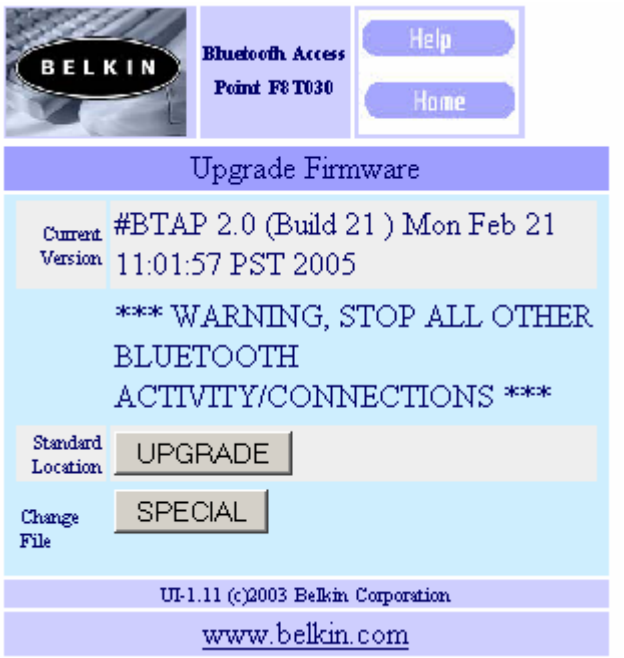

Bild 1-7: Upgrade

Bild 1-8: Ping

3. Aufgetretene Probleme:

Unser erstes Problem war es an passende Bluetooth Hardware zu kommen. Es hat den Anschein das Bluetooth Access-Points zum Verbinden ins Netzwerk am Aussterben sind. Es gab im Grunde nur zwei Hersteller die noch AP herstellten. Selbst diese Geräte waren so gut wie nicht zu bekommen. Mit Glück konnten wir bei eBay den Belkin Access-Point im 4er Paket günstig ersteigern.

Die Standardfirmware die bei Auslieferung installiert war unterstützte nur das LAP Profil. Mit diesem Profil kamen die meisten Geräte gar nicht oder nur mit Problemen zu recht. Als Beispiel sei hier auf zwei fast baugleiche Notebooks (IBM T60 und T60p) verwiesen. Mann konnte zwar mit beiden Notebooks auf den Access Point zugreifen, eine Verbindung zum Netzwerk konnte aber nur von einem Notebook aufgebaut werden.
Nach Recherche im Internet haben wir herausgefunden das das LAP Profil veraltet ist und es bereits einen Nachfolge Profil gibt. Das PAN Profil. Da, wie bereits erwähnt, der Belkin mit der Standardfirmware nur das LAP Profil unterstützt, musste ein Firmware update durchgeführt werden. Die neue Firmware brachte eine neue Unterstützung für das PAN Profil mit. Nun konnten alle Geräte die das PAN Profil unterstützten eine Verbindung aufbauen. Allerdings ist es nicht gelungen unter Windows Vista eine Verbindung herzustellen.

Ein weiteres Problem das aufgetreten ist, ist dass es bei einigen Geräten des öfteren zu Verbindungsabrüchen kam. Der Grund konnte nicht ermittelt werden.

Allgemein trat im FOO-Pool öfters das Problem auf, dass der Belkin per DHCP keine IP Adresse beziehen konnte.

4. Ausblick / Endstatus:

Verbindung zum Internet konnte hergestellt werden. Jedoch wurde noch nicht getestet, wie es mit der VPN Verbindung über Bluetooth aussieht. Dies konnte noch nicht getestet werden da wir die Verbindungsprobleme erst zum Ende des Praktikums lösen konnten.
In Anbetracht der Tatsache das der für uns in Betracht kommende OpenVPN Client für PocketPCs sich im Entwicklungsstadium befindet und immer mehr Handhelds auch WLAN Unterstützung anbieten, ist zu überlegen ob es sinnvoll ist VPN für PocketPCs über Bluetooth anzubieten.

5. Quellen:

http://www.belkin.com/

http://www.wikipedia.de

http://www.google.de

http://www.heise.de/mobil/bluetooth/db/

http://german.bluetooth.com/

http://www.avm.de/de/Service/TechnikLexikon/B/Bluetooth_Profile_Uebersicht.html