Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Angriffe auf Funknetzwerke

Heiner Perrey

Betreuer: Dirk Westhoff

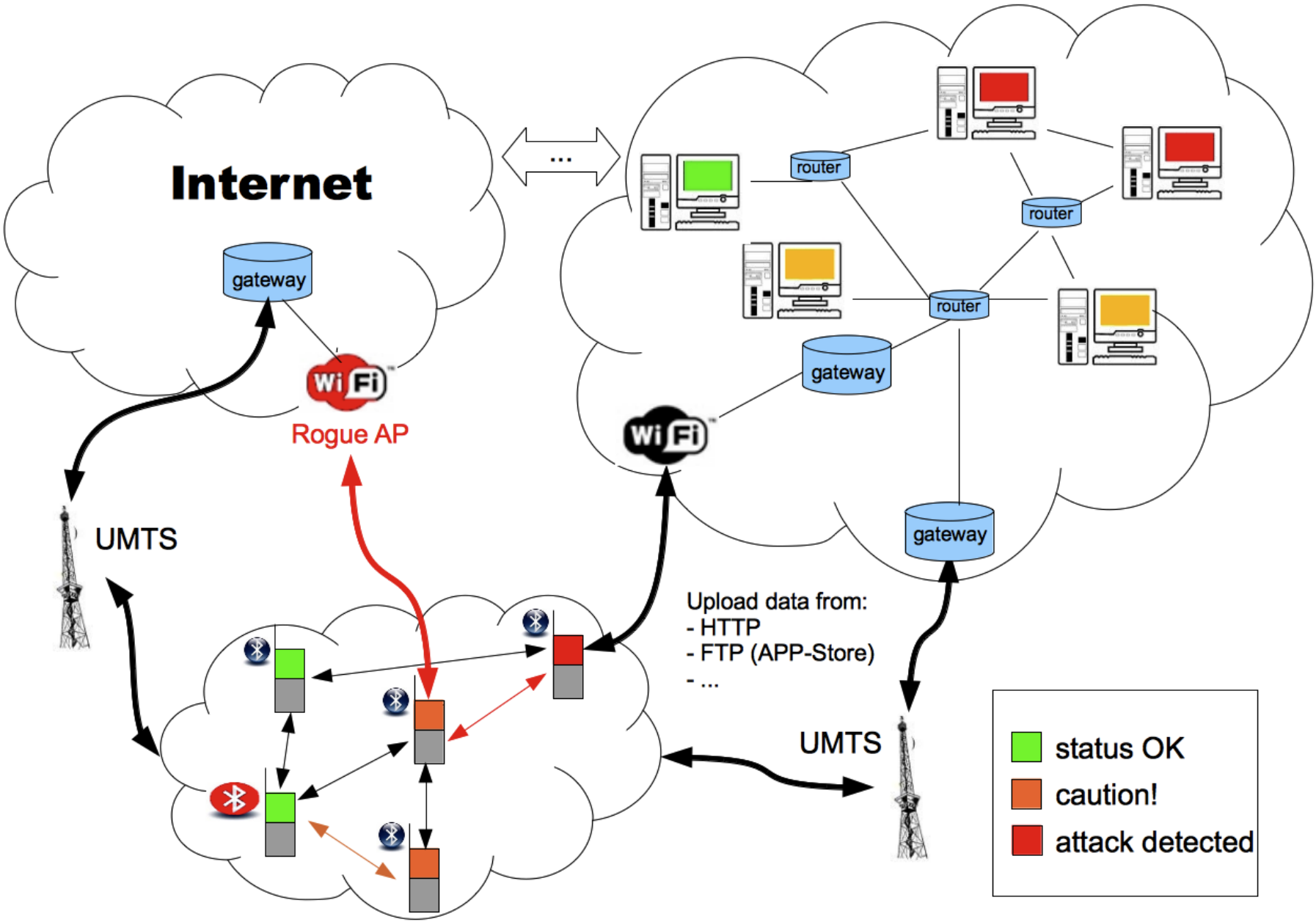
Anwendungen 1,
14. Januar 2011

Overview

Grobe Zielsetzung

- Sicherheitserweiterung für Bluetooth Low Energy (LE)
  - Schutz vor einem passiven Lauscher
  - Teilnahme-Nachweis in SKIMS für micro-payment

SKIMS


Internet
...
gateway
router
router
router
gateway
gateway
Wi Fi
Rogue AP
Wi Fi
UMTS
Upload data from:
- HTTP
- FTP (APP-Store)
- ...
UMTS
status OK
caution!
attack detected

Content

Geschichte

- von Ralph Merkle 1974 vorgestellt [6] [10]
- dient dem sicheren Schlüsselaustausch über einen unsicheren Kanal
- Rechenaufwand kann ggf. zum stärkeren Gerät geschoben werden [1]

Motivation

- Alice möchte sich mit Bob über einen unsicheren Funkkanal unterhalten, doch die Daten sind geheim!
- ein pre-shared secret ist nicht möglich!
- Alice nutzt ein Smartphone mit geringer Leistung
- Bob ggf. ein **noch leistungsschwächeres** Gerät

Das Verfahren: Sender-Seite

1. Alice erzeugt n geheime Schlüssel key_{weak} und key_{strong} und erstellt daraus n Puzzel
2. ein Puzzel besteht aus: $P(E_{key_{weak}}\{puzzle_{ID}, key_{strong}\})$
3. Alice verschickt alle n Puzzel über den unsicheren Kanal

Das Verfahren: Empfänger-Seite

1. Bob empfängt alle Puzzel und sucht sich zufällig eines heraus.
2. durch eine vollständige Schlüsselraumsuche „knackt“ er key_{weak} des Puzzels.
3. jetzt kennt er den key_{strong} des entsprechenden Puzzels und sendet die $puzzle_{ID}$ zurück an Alice

Stärke des Verfahren

- ein passiver Angreifer kennt alle Puzzel und die Puzzel ID des ausgesuchten Puzzels
  - Eve müsste solange die Puzzel knacken, bis sie die richtige $puzzle_{ID}$ gefunden hat.
  - im Schnitt sind das eine Menge von $\frac{n}{2}$ Puzzel
  - der Mehraufwand für Eve hängt also von der Menge der Puzzel ab
- es geht also nicht darum ob, sondern wann Eve erfolgreich ist!

Content

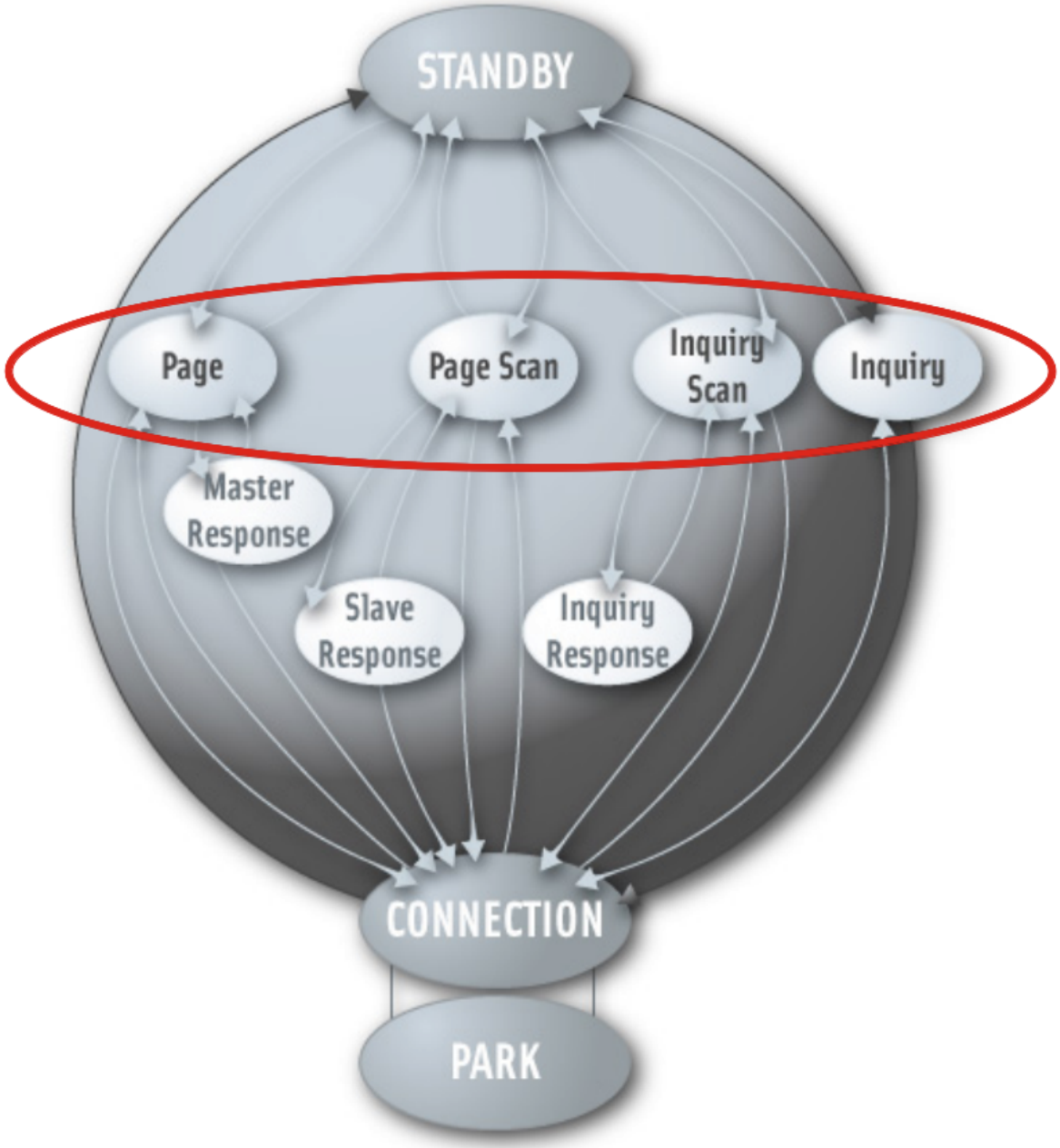
Was ist Bluetooth (LE)?

- ursprünglich als Wibree von Nokia entwickelt [11] - ergänzt heute die Bluetooth Spezifikation (Version 4.0) [8]
- ist eine sehr energiesparende Technologie (relativ zu Bluetooth Classic)
- auf einige Sicherheitsmechanismen wurde verzichtet (Elliptic Curve Diffie-Hellman)

Was ist Bluetooth (LE)?

- maximale Übertragungsrate: 1 Mbit/s (BT Classic: 1 - 3 Mbit/s [2])
- maximale Reichweite: bis 100 Meter (BT Classic: 1 - 100 Meter [3])
- weitere energiesparende Maßnamen (z.B. effizieter idle-mode)
- LE ist mit BT Classic nicht direkt kompatibel (dual-mode Radio nötig) [4]

Zustände in Bluetooth [5]



Frequency Hopping

- um Kollisionen zu vermeiden, „hüpfen“ Sender und Empfänger über bis zu 79 Frequenzen
- die Hopping Frequenz wird vor dem Datenaustausch festgelegt.
- je nach Zustand des Senders und Empfängers ist das Hopping-Muster unterschiedlich

Frequency Hopping: Page/Inquiry

- das Hopping-Muster ist hier asynchron
- der Sender schickt auf allen Frequenzen, um den Empfänger möglichst zu erreichen
- erst beim Verbindungsaufbau ist beiden das gleiche Hopping-Muster bekannt

Content

Problemstellung

- Bluetooth Low Energy bietet keinen Schutz vor passiven Angreifern (Kopplungs-Phase)
- Bluetooth (LE) sieht nicht vor, mehrere Empfänger gleichzeitig zu erreichen.
- Bluetooth LE ist stark energie-beschränkt (ECDH zu rechen-intensiv)
- Rechenleistung der Kommunikationspartner ist ggf. unausgeglichen

Zielsetzung

- konzeptioneller Zusammenschluss von Bluetooth LE und Merkle's Puzzle
- bestehende Konzepte sollen nach Möglichkeit übernommen werden.
- Analyse von Merkle's Puzzle in Bezug auf verschiedene Anwendungsfälle (bietet Merkle's Puzzle ausreichendes Verhältnis aus Performance und Sicherheit?)

Ansatzpunkt für Merkle's Puzzle in der BT-Spezifikation

- Merkle's Puzzle sollte in Paging/Inquiry State umgesetzt werden (Schlüsselaustausch von BT vor Connection-State)
- asynchrones Frequency Hopping zum Verteilen der Puzzel an mehrere Empfänger
- Schutz vor passivem Lauscher

Content

offene Fragen und Probleme

- skaliert das Verfahren für viele Empfänger? (z.B. in puncto Sicherheit oder Sende-Last)
- wie leistungsstark muss ein Gerät mindestens sein? Ggf. nicht günstig für WSN?
- Analysen: Angreifermodel, Anwendungsfälle, Grenzen durch Übertragungsrate etc.
- inwieweit muss die Bluetooth Spezifikation angepasst werden?


F. Armknecht and D. Westhoff.
Using Merkle's Puzzle for Key agreement with Low-end Devices.
Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on, pages 858–864, December 2009.


http://www.bluetooth.com/.
Webseite.
http://www.bluetooth.com/English/Technology/Works/Pages/Architecture__Radio.aspx Abruf: 12.01.2011.


http://www.bluetooth.com/.
Webseite.
http://www.bluetooth.com/English/Technology/Pages/Basics.aspx#5 Abruf: 12.01.2011.


http://www.bluetooth.com/.
Webseite.
http://www.bluetooth.com/SiteCollectionDocuments/Low_Energy_FAQ_External_General_Public.pdf Abruf: 12.01.2011.


http://www.bluetooth.com/.

Webseite.
http://www.bluetooth.com/English/Technology/Works/Pages/Architecture__Baseband.aspx Abruf: 12.01.2011.


R. Merkle.
Secure Communications Over Insecure Channels.
Communications of the ACM, pages 294–299, April 1978.


http://www.merkle.com/.
Webseite.
Abruf: 12.01.2011.


Bluetooth SIG.
BLUETOOTH SPECIFICATION Version 4.0.
June 2010.
https://www.bluetooth.org.


Kontakt zu Mitarbeiter von Nokia, January 2011.


http://www.itas.fzk.de/mahp/weber/merkle.htm.
Webseite.
Abruf: 09.01.2011.


http://www.electronicsweekly.com/.
Webseite.
http://www.electronicsweekly.com/Articles/2007/06/12/41582/Wibree-becomes-ULP-Bluetooth.htm Abruf: 09.01.2011.