GSM Übung 02 - SMS Versand und Empfang mitschneiden

7. Mai 2012

Das Ziel der folgenden Übung ist es den Versand und den Empfang einer SMS mit OsmocomBB und Wireshark mitzuschneiden. Wir gehen davon aus, dass die mobile-App erfolgreich gestartet und mit Telnet verbunden ist (apps-starten.txt). Auch Wireshark sollte schon laufen und eine SIM-Karte in das Telefon eingelegt sein.

1 Einleitung

Die mobile-App entspricht der Implementierung eines Mobiltelefons. Funktionen wie das verschicken von SMS oder das Anrufen können hier über die Konsole erledigt werden (Telnet).

2 SMS versenden

Folgende Schritte müssen durchgeführt werden, um eine SMS zu verschicken (in der Telnet-Session der mobile-App). Die einzugebenden Befehle stehen in Klammern.

1. Den erweiteren Befehlssatz aktivieren (enable).
2. Die MS anzeigen lassen (show ms). Hier steht nur eine.
3. Die SIM-Karte mit dem PIN freischalten (sim pin 1 PIN). "1" steht für die vorher angezeigte MS, PIN für die PIN der SIM-Karte. ACHTUNG! Die PIN wird im Klartext angezeigt!
4. Die aktuelle IMSI und TMSI anzeigen lassen (show subscriber). Diese Daten aufschreiben.
5. SMS versenden: (sms 1 NUMMER ZEICHEN KETTE). "1" steht hier für die MS, NUMMER für die Mobilfunknummer des Empfängers und ZEICHEN KETTE für den Text der SMS.
6. SMS versendet? Es erscheint eine entsprechende Meldung in der Telnet-Session.
7. MS abmelden (off). Einige Sekunden warten, bis der IMSI DETACH durchgelaufen und in Wireshark angekommen ist
8. Die in Wireshark empfangenen Pakete abspeichern.

3 SMS empfangen

Der Empfang einer SMS läuft entsprechend dem Versand ab (bis auf den Schritt "SMS versenden", natürlich). Empfängt die mobile-App eine SMS wird der Inhalt der SMS in der Telnet-Session angezeigt.

4 Fragen

1. Warum und in welchen Situationen wird eine TMSI-Reallocation in den Aufzeichnungen durchgeführt? Vergleicht die Ergebnisse mit anderen Gruppen. Gibt es Operatoren, die öfter / seltener eine TMSI-Reallocation durchführen?
2. Auf welchem Channel wird die SMS verschickt? Wird dieser Verschlüsselt?
3. Welche Channel waren während dem Einbuchen, SMS empfangen, und abmelden beteiligt?
4. Wurde beim Einbuchen vom Operator nach der IMSI / IMEI gefragt?