



TECHNISCHE
UNIVERSITÄT
DARMSTADT

ANSIAN - ANDROID SIGNAL ANALYZER

DENNIS MANTZ AND MAX ENGELHARDT

SEEMOO Secure Networking Lab

April 28, 2016

Secure Mobile Networking Lab
Department of Computer Science



AnSiAn - Android Signal Analyzer
SEEMOO Secure Networking Lab

Submitted by Dennis Mantz and Max Engelhardt
Date of submission: April 28, 2016

Advisor: Prof. Dr.-Ing. Matthias Hollick
Supervisor: Jiska Classen

Technische Universität Darmstadt
Department of Computer Science
Secure Mobile Networking Lab

CONTENTS

1	INTRODUCTION	1
1.1	Project Definition	1
1.1.1	Features	1
1.1.2	Time Schedule	3

ACRONYMS

AnSiAn Android Signal Analyzer

FM Frequency Modulation

LSB Lower Side Band

MVC Model–View–Controller

RDS Radio Data System

SDR Software-Defined Radio

USB Upper Side Band

INTRODUCTION

Android Signal Analyzer (AnSiAn) is an Android application by the Secure Mobile Network Lab (SEEMOO) at Technische Universität Darmstadt. It features a graphical signal analyzer that can be used with common Software-Defined Radios (SDRs) like the HackRF and the RTL-SDR. The project is based on RF Analyzer, an application by Dennis Mantz. AnSiAn currently extends RF Analyzer by the following features:

- Time Domain Signal Graph (Waveform)
- Morse Decoder
- Scanner
- Codebase structured according to the Model–View–Controller (MVC) pattern

This lab aims to further extend the feature set of AnSiAn while also making the app more stable and refining existing features. The description of the project goals are listed in Section 1.1.

1.1 PROJECT DEFINITION

This section defines the features that will be implemented throughout the project and schedules them into three sprints.

1.1.1 *Features*

The new features can be divided into mandatory features, that will have high priority within this project, and optional features, that will be implemented if time permits. As can be seen in Section 1.1.2, the third sprint is reserved for either optional features or completing mandatory features and the documentation.

1.1.1.1 *Mandatory Features*

The following features are scheduled for implementation during the first and second sprint:

- Radio Data System (RDS) demodulation
If the user selects the existing wide-band Frequency Modulation (FM) demodulation option, the app shall try to detect and

demodulate any existing RDS signal along with the audio demodulation. The extracted information shall be displayed on the screen.

- **PSK₃₁ demodulation**
If the user selects either of the single side band demodulation modes (Upper Side Band (USB) and Lower Side Band (LSB)), he or she shall have the option to enable PSK₃₁ demodulation along with or instead of the audio demodulation. The demodulated text string shall appear and scroll through the analyzer window.
- **Extraction of RDS-, Morse- and PSK₃₁-data to logfiles**
If the user selects to demodulate any digital mode, the demodulated text shall be written to a log file specified by the user.
- **Support for the rad10 badge**
The rad10 badge, which is a modified low-cost replica of the HackRF, shall be supported as a signal source by AnSiAn.
- **Transmission support for HackRF and rad10**
If AnSiAn is used with an SDR capable of transmitting signals, it shall offer options to send signals in the following ways:
 - Replay I/O samples from a file
 - Generate and send Morse code from text
 - FM-modulate and send audio from a file

1.1.1.2 *Optional Features*

The optional features are scheduled in the third and last sprint. However, they will only be added to the feature set if the last sprint is not needed in order to compensate for delays on the mandatory features. The optional features are listed in the order of priority:

- **Walkie-Talkie Mode**
The user shall have the possibility to put AnSiAn into a Walkie-Talkie mode. In this mode, the application will demodulate an FM channel and the user can quickly switch between demodulation and transmission of audio recorded from the internal microphone.
- **Packet Radio demodulation**
A new mode *Packet Radio* shall be added to AnSiAn. Once selected, it shall allow the user to tune to a Packet Radio channel and display information about demodulated packets on the screen. If time permits, it might even be possible to implement a transmission feature for Packet Radio.

1.1.2 *Time Schedule*

The project will have two developers, Dennis Mantz and Max Engelhardt, working in three sprints. There are three milestones corresponding to the sprints, labeled Alpha, Beta and Final Version. They each add an independent and self-contained set of features to the application:

- Sprint 1: Alpha Version (due 09.06.)
 - RDS demodulation
 - PSK₃₁ demodulation
 - Extraction of RDS-, Morse- and PSK₃₁-data to logfiles
- Sprint 2: Beta Version (due 21.07.)
 - Support for the rad10 badge
 - Transmission support for HackRF and rad10
 - * Replay I/O samples from a file
 - * Generate and send Morse code from text
 - * FM-modulate and send audio from a file
- Sprint 3: Final Version (due 25.08.)
 - Complete leftovers from previous sprints
 - Walkie-Talkie Mode (optional)
 - Packet Radio demodulation (optional)

ERKLÄRUNG

Hiermit versichere ich gemäß der Allgemeinen Prüfungsbestimmungen der Technischen Universität Darmstadt (APB) § 23 (7), die vorliegende Masterarbeit ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus den Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, 28. April 2016

Dennis Mantz and Max
Engelhardt