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

ABSTRACT

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

ZUSAMMENFASSUNG

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LISTINGS

ACRONYMS

AnSiAn	Android Signal Analyzer
FM	frequency modulation
LSB	lower side band
RDS	Radio Data System
SDR	software-defined radio
USB	upper side band

Part I

PROJECT REPORT

1 INTRODUCTION

Android Signal Analyzer (AnSiAn) is a project of the Secure Mobile Network Lab (SEEMOO) at the Technical University in Darmstadt. The Android applications 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 adds the following features on top of the set of RF Analyzer:

- Time Domain Signal Graph (Waveform)
- Morse Decoder
- Scanner
- Codebase structured according to the 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

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

1.1.1 *Features*

The new features are sorted into must-have and nice-to-have. As can be seen in section 1.1.2, the third sprint has time reserved for either the nice-to-have features or for further working on the must-have features and the documentation.

1.1.1.1 *Must-Have*

The following features are planned to be implemented in the first and second sprint in respecting order:

- Radio Data System (RDS)
  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 (channel name and time) shall be printed on the screen.

- PSK31
  If the user selects either of the single side band demodulation modes (upper side band (USB) and lower side band (LSB)) he shall have the option to also enable PSK31 demodulation along with or instead of the audio demodulation. The demodulated text string should appear and scroll through the analyzer window.

- Extract RDS-, Morse and PSK31-Text to file
  If the user selects to demodulate any digital mode, the demodulated text shall be written to a user configured log file.

- rad1o support (for receiving)
  The rad1o badge, which is a modified low-cost replica of the HackRF shall be supported as signal source by AnSiAn.

- sending with HackRF and rad1o
  If the user connects a SDR with transmission capabilities to his Android device, he shall have the possibility to transmit signals:
  - Replay I/O samples from a file
  - Generate and send Morse code from text
  - FM audio modulation from a file

1.1.1.2 *Nice-to-Have*

The nice-to-have 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 delays on the must-have features. The 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 analyzer will demodulate an FM channel and the user can quickly switch between demodulation and transmission of audio from the internal microphone.

- Packet Radio
  A new mode *Packet Radio* shall be added to the existing demodulation modes of AnSiAn. Once selected it will allow the user to tune to a Packet Radio channel and see 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, Max Engelhardt and Dennis Mantz, working in three sprints. There are three milestones corre-

sponding with the sprints, labeled alpha, beta and final version. Although the milestones are labeled according to the SEEMOO lab requirements, they each add independent and self-contained features to the application:

- Sprint 1: alpha version (due 09.06.)
  - RDS
  - PSK31
  - Extract RDS-, Morse and PSK31-Text to file
- Sprint 2: beta version (due 21.07.)
  - rad1o support (for receiving)
  - Transmission support for HackRF and rad1o
    - replay I/O samples
    - generate and send Morse code from text
    - FM audio modulation
- Sprint 3: final version (due 25.08.)
  - Complete leftovers from previous sprints
  - Walkie-Talkie Mode (optional)
  - Packet Radio (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