

**CSCI – Project (Android Packet Sniffer)**

Project Proposal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Group SS18/2A  Soh Yu Xuan Timothy Chin Kenneth Huang Kendric Tan |  | Supervisor  Mr Tian Sion Hui |  | Assessor  Mr Tan Kheng Teck |
|  |  |  |  |  |

**Document Control**

Title: Project Proposal

Document Name: SS182APP.docx

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Owner | Current Version | Last Change on | | Approved by |
| Date | Time |
| Soh Yu Xuan | 0.8 | 17th August | 1138 |  |

**Distribution List**

|  |  |
| --- | --- |
| Name | Title/Role |
| Soh Yu Xuan | Team Leader / Lead Programmer |
| Timothy Chin | Assistant Programmer / Lead UI |
| Kenneth Huang | Assistant Programmer / Lead Tester |
| Kendrick Tan | Project Management |

**Record of Revision**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Revision Date | Description | Section Affected | Changes Made By | Version after Revision |
| 21th April | Filled Executive Summary & Introduction | Executive Summary & Introduction | Soh Yu Xuan | 0.1 |
| 23rd April | Filled Research | Research | Timothy Chin | 0.2 |
| 24th April | Completed Research & Objectives | Research & Objectives | Soh Yu Xuan | 0.3 |
| 26th April | Completed Scope and Limitations | Scope & Problems of Limitation | Kenneth Huang | 0.4 |
| 28th April | Filled Development Method | Development Method | Kendrick Tan | 0.5 |
| 28th April | Updated Research | Research | Soh Yu Xuan | 0.6 |
| 28th April | Completed Timetable | Timetable | Soh Yu Xuan, Timothy Chin, Kenneth Huang | 0.7 |
| 17th August | Format doc & remove outdated info | All | Timothy Chin | 0.8 |

Table of Contents

1. [Executive Summary 3](#_Toc522276187)

[Summary](#_Toc522276188)

[Introduction](#_Toc522276189)

1. [Project Description 3](#_Toc522276190)

[Background](#_Toc522276191)

1. [Project Description 4](#_Toc522276192)

[What is packet sniffing?](#_Toc522276193)

[The Network Interface Controller / Card (NIC)](#_Toc522276194)

[Promiscuous Mode and Monitor Mode](#_Toc522276195)

[IEEE 802.11](#_Toc522276196)

[Layer 2 – Datagrams](#_Toc522276197)

[How Android State Machine Works](#_Toc522276198)

[Android Wifi Architecture](#_Toc522276199)

[Root Access on Android](#_Toc522276200)

[PCAP Library – API for packet capturing](#_Toc522276201)

[Bcmon/Nexmon – Enabling monitor mode on an android device](#_Toc522276202)

1. [Requirements for Packet Sniffing 8](#_Toc522276203)

[About the Device](#_Toc522276204)

[Requirements](#_Toc522276205)

1. [Objectives 9](#_Toc522276206)

[We plan to achieve these functionalities](#_Toc522276207)

[Possible additions of function](#_Toc522276208)

[Scope and Problems with Limitation](#_Toc522276209)

[Choice of language](#_Toc522276210)

[IDE](#_Toc522276211)

1. [Development Method – AGILE 10](#_Toc522276212)

[AGILE Software Development Method](#_Toc522276213)

[AGILE’s Manifesto](#_Toc522276214)

[12 Principles of AGILE Software Development Method](#_Toc522276215)

1. [Timetable 11](#_Toc522276216)
2. [References 12](#_Toc522276217)

# Executive Summary

## Summary

Technology has improved with leaps and bounds, computers used to be large clunky machines which were largely immobile but now, almost everyone if not all has a “computer” with them all the time, a smartphone. One of the jobs of a network administrator requires him/her to monitor the network. This can be done with a computer with either with an external network card or with an internal one, however the computer was something that was needed, adding weight and hassle. What if one could monitor and sniff packets from their device whom they carried with them everywhere? One could simply be in a location, capturing packets in their vicinity for analysis, without having to lug around a laptop right into their mobile device.

## Introduction

The scope of the project has its limitations. An android device differs from a personal computer, in a great many ways. Applications such as wireshark or the aircrack suite on a Linux PC are easy to operate and have been around for decades. Such applications, which capture packets, require a Network Interface Card set in Monitor mode. With a large number of drivers easily downloadable and installable on a personal computer, compatibility and configurability between the NIC cards and the OS make it easy and straightforward as compared to on an android device. Android devices themselves differ in a great many ways. The chipsets from different manufacturers are different, resulting in a lack of universal features. Drivers do not work the same as with a personal computer, for an android device, the native drivers are precompiled in the Linux kernel, making compatibility with external WLAN adapters limited at best without a reverse engineer of existing drivers, integration with the kernel and re-flashing to the new OS. These factors, added to the fact that manufacturers do not/are not supporting development with their hardware make this project very limited and experimental. This document will describe in detail the objectives, scope and limitations of the project.

# Project Description

## Background

The idea of having airodump-ng albeit a limited version of it on a phone thrills us. Even though android devices are largely segregated by their manufacturers, and the result from this project will be fairly limited, there might be a way to implement such an application on a wider scale with enough time. As with airodump-ng, the user can only capture packets in their vicinity within the range of the NIC, and what better way than to use an android phone, something that weighs so little and are most likely on person most times.

# Project Description

## What is packet sniffing?

“A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn’t generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of the sniffer, all traffic is hared when the sniffer software commands the **Network Interface Card (NIC)** to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. [1]

## The Network Interface Controller / Card (NIC)

To connect to a network, a computer can use a wired connection via Ethernet or wirelessly, which requires a NIC. It can be built into the motherboard or plugged in via USB with an external WLAN adapter. An android device with OTG capabilities (to act as host) with the relevant drivers will be able to detect and use an external WLAN adapter.

## Promiscuous Mode and Monitor Mode

Monitor mode (RFMON) enables a wireless NIC to capture packets without associating with an access point or ad-hoc network. This is desirable in that you can choose to “monitor” a specific channel, and you never need to transmit any packets. In fact, transmitting is sometimes not possible while in monitor mode (driver dependent). Another aspect of monitor mode it that the NIC does not care whether the CRC values are correct for the packets captures in monitor mode, so some packets that you see may be in fact corrupted. Monitor mode only applies to wireless networks, while promiscuous mode can be used on both wired and wireless networks. Monitor mode is 1 of 6 modes that 802.11 wireless cards can operate in: Master (acting as an AP), Managed (client mode), Ad- hoc, Mesh, Repeater and Monitor mode.

Promiscuous mode allows you to view all wireless packets on a network to which you have to be associated. The need to associate means that you must have some means of authenticating yourself with an access point. In promiscuous mode, you will not see packets until you have associated. Not all wireless drivers support promiscuous mode.

One important difference is Promiscuous mode does tell the card to process all frames (removing 802.11 frame headers) [2]

## IEEE 802.11

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5 and 60 GHz frequency bands. They are the most widely used wireless computer networking standards, used in most home and office networks to allow laptops, printers and smartphones to talk to each other and access the Internet without connecting wires. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAM/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997 and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the marketplace, each revision tends to become its own standard.

## Layer 2 – Datagrams

**Management frames**

* Authentication frame
* Association request frame
* Association response frame
* Beacon frame
* Deauthentication frame
* Disassociation frame
* Probe request frame
* Probe response frame
* Reassociation request frame
* Reassociation response frame

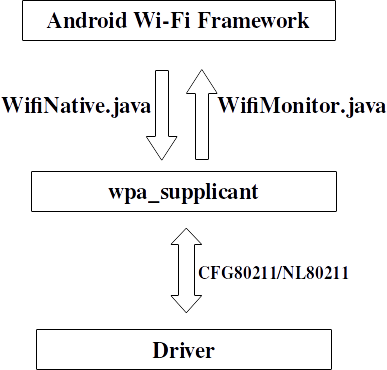
**Control frames**

* Acknowledgement frame (ACK)
* Request to Send frame (RTS)
* Clear to Send frame (CTS)

**Data frames**

Data frames carry packets from web pages, files, etc. within the body. The body begins with an IEEE 802.2 header, with the Destination Service Access Point (DSAP) specifying the protocol, followed by a Subnetwork Access Protocol (SNAP) header if the DSAP is hex AA, with the organizationally unique identifier (OUI) and protocol ID (PID) fields specifying the protocol. If the OUI is all zeroes, the protocol ID field is an EtherType value. Almost all 802.11 data frames use 802.2 and SNAP headers and most use an OUI of 00:00:00 and an EtherType value. [3]

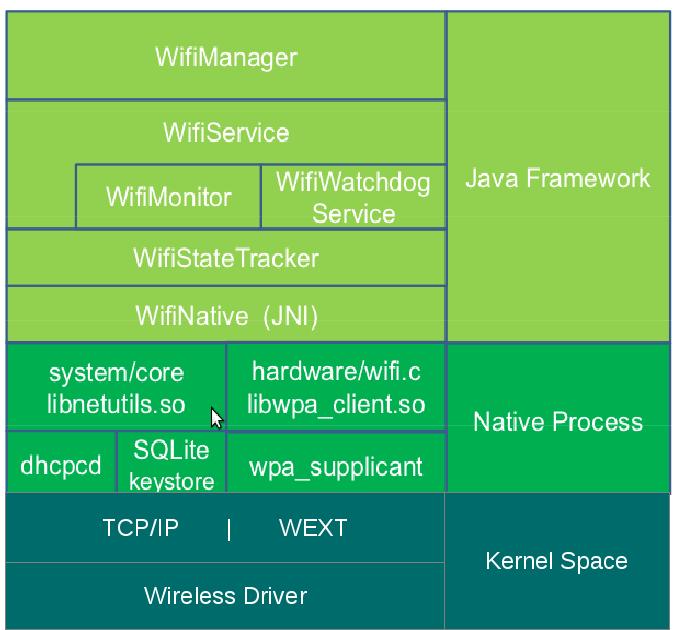
## How Android State Machine Works



Android uses a customized wpa\_supplicant to perform AP authentication and association, and also communicate with the underlying driver. The **WifiNative** class is used to send various commands to wpa\_supplicant and the **WifiMonitor** class is used to monitor wpa\_supplicant status change and notify the Android framework.

Wpa\_supplicant communicates with the underlying driver using new CFG80211/NL80211 interface [4]

## Android Wifi Architecture

****

**[5]**

## Root Access on Android

Root access is not available on a normal android device. Like the sudo command in linux, root access is required to run certain processes in Android. Rooting basically means to give yourself root permissions. However, manufacturers do not support this function at all and by doing so will void the warranty of the device. Rooting of a model of device depends on the community working on it, trying to escalate the default privileges to root. As such, some devices might not have root or exploits available at all.

## PCAP Library – API for packet capturing

The Packet Capture library provides a high-level interface to packet capture systems. All packets on the network, even those destined for other hosts, are accessible through this mechanism. It also supports saving captured packets to a “savefile” and reading packets from a “savefile”. The pcap API is written in C, with wrapper libraries (Libtins – C++, jNetPcap - Java) available.

## Bcmon/Nexmon – Enabling monitor mode on an android device

Android devices have their firmware locked down, development of applications which require special privileges are unsupported. Users have to enable root permissions with third party applications which are often experimental, made by enthusiasts who try to reverse-engineer into the device. Bcmon, succeeded by Nexmon is an open project that requires root, it enables devices with select Broadcomm/Cypress WiFi chipsets to enable monitor mode.

# Requirements for Packet Sniffing

## About the Device

The device we are using: LG NEXUS 5 (with a BCM 4339 NIC)

## Requirements

1. Making sure having a device that has a NIC(Network Interface Card) that supports Monitor/Promiscuous Mode
2. Rooting the device
3. Controlling root privileges(optional, recommended)
4. Modification of Drivers/Kernel to enable Monitor mode

Based on the above research, we have some level of understanding of the context, requirements and limitations of our project. There are two ways to implement packet sniffing with an android device, and both have their limitations. The first way is to connect an external Wifi adapter via an OTG cable (with a device that supports OTG). The limitations to this method is that, depending on the wireless card, specific drivers are required. In android, drivers are precompiled in the Linux kernel, and to update to the required driver, the kernel has to be rewritten with the driver, and the OS has to be re-flashed with the new kernel. This process of reverse engineering of the driver and recompiling of the kernel is extremely difficult and time consuming. Another way is to utilize the in-built NIC of the device. This method is limited by the base device, only a tested device that works will be able to run the sniffer. Both methods require root access to the device, escalating root privileges to the user. Rooting a device is unsupported by the manufacturers and therefore, is highly dependent on open source communities and may differ from model to model. Once a device has a NIC in monitor mode, the application which will be developed, with the help of the PCAP library can then capture packets, save it to a file and possibly provide some sort of an analysis of the data captured.

# Objectives

## We plan to achieve these functionalities

* GUI
* Capture packets with filtering options
* Manipulate data captured, display data
* Save all captured packets to a file for analysis on PC

## Possible additions of function

* Cracking WEP, requires packet injection
* Driver reverse engineering and implementation on the application itself instead of re-flashing an updated kernel, allows for usage of external NICs

## Scope and Problems with Limitation

* Device MUST have a chipset that allows NIC in monitor mode
* Device MUST be rooted
* Bcmon/Nexmon to enable monitor mode

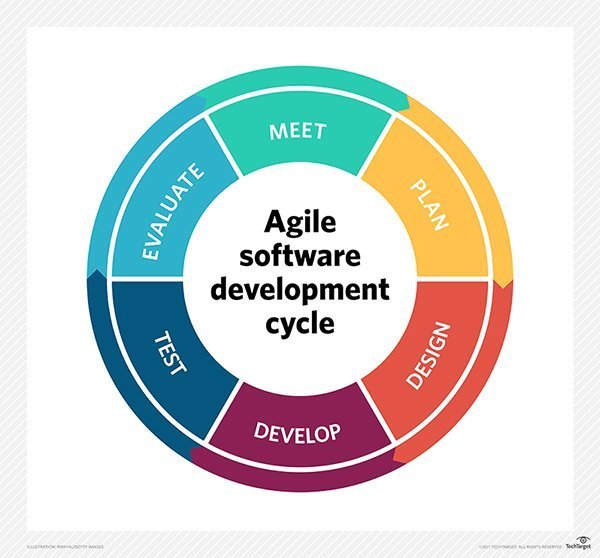
## Choice of language

* Java / C++

## IDE

* Android Studio

# Development Method – AGILE



## AGILE Software Development Method

* Provides the ability to create and respond to change to succeed in an uncertain and turbulent environment
* We feel that AGILE is the most applicable due to the unpredictability of the project, rooting and enabling monitor mode on specific onboard WLAN cards of chosen devices are experimental and untested.
* There are no true examples on the Google Play Store, true packet sniffing requires root and monitor mode on the onboard NIC, which is unsupported.

## AGILE’s Manifesto

* Individuals & interactions > Processes & Tools
* Working Software > Comprehensive Documentation
* Customer Collaboration > Contract Negotiation
* Responding to change > Following a plan

## 12 Principles of AGILE Software Development Method

* Customer satisfaction by early and continuous delivery of valuable software
* Welcome changing requirements, even in late development
* Working software delivered frequently
* Close, daily cooperation between clients and developers
* Projects are built around motivated individuals, who should be trusted
* Face-to-face conversation is the best form of communication (co-location)
* Working software is the primary measure of progress
* Sustainable development, able to maintain a constant pace
* Continuous attention to technical excellence and good design
* Simplicity – the art of maximizing the amount of work not done is essential
* Best architectures, requirements and designs emerge from self-organizing teams
* Reflect on how to become more effective and adjust accordingly

# Timetable

|  |  |
| --- | --- |
| * 29th April | * Overall use case |
| * 6th May | * 1st Prototype (Simple GUI) + Documentation (Usecase + Class) (Hello World) |
| * 13th May | * Set up test devices with monitor mode * Understanding PCAP API and relevant libraries |
| * 20th May | * Understanding PCAP API and relevant libraries * Start of 2nd Prototype |
| * 27th May | * Continuation of 2nd Prototype |
| * 3rd June | * End of 2nd Prototype + Documentation (Displaying of raw frames) |
| * 10th June | * Start of 3rd Prototype |
| * 17th June | * Continuation of 3rd Prototype |
| * 24th June | * End of 3rd Prototype (Displaying of packets) + Documentation, Planning of test cases |
| * 31st June | * Debugging, testing for conformity to test cases |
| * 7th July | * Working 3rd Prototype |

# References

1. <https://www.techopedia.com/definition/4113/sniffer>
2. <http://lazysolutions.blogspot.sg/2008/10/difference-promiscuous-vs-monitor-mode.html>
3. https://en.wikipedia.org/wiki/IEEE\_802.11
4. <http://jhshi.me/2014/04/25/how-android-wifi-state-machine-works/index.html#.WuQSE4gRUwo>
5. <https://mitulmodi.wordpress.com/2012/03/21/android-wifi-architecture-wext/>