MISS
Mac-based Identification and Signaling Service

Fabian Schwab (fabian.schwab@uni-ulm.de)

23. September 2014

Kapitel 1

Einleitung

Der *mac-based identification and signaling service* ist ein für Android geschriebener Hintergrunddienst, welcher es ermöglicht mobile oder stationäre WLAN Geräte zu erkennen. Der Service unterscheidet zwischen mobilen Geräten, die hier als *Clients* bezeichnet werden und Stationen den sogenannten *Stations*. Hierbei sind die *Clients* Geräte die sich mit einem WLANs verbinden und *Stations* Geräte, die solch ein Netzwerk aufspannen. Je nach Typ werden verschiedene Informationen gesammelt und zurückgegeben, welche in Kapitel 2.1.1 genauer erläutert werden.
Sobald sich eines der gesuchten Geräte in der Nähe befindet und erkannt wird, wird eine Benachrichtigung über dessen Fund ausgelöst.

Kapitel 2

Grundlagen

Um die Funktionsweise des Service genauer verstehen zu können, sollten zunächst einige Grundlagen erklärt werden. In diesem Abschnitt werden die vom Service genutzten Technologien kurz beschrieben. Da dies keine vollständige Beschreibung darstellt, sollten die Technologien in ihren Grundzügen bekannt sein.

2.1 Kabellose Kommunikation

Die Anzahl der Geräte die mithilfe von WLAN kommunizieren nehmen ständig zu. Bei einem Großteil dieser Geräte wird das *WNIC*, manchmal trotz limitierter Ressourcen, nicht abgeschaltet. Trotz verschlüsselter Verbindungen werden definiert durch den *IEEE 802.11* Standard einige Daten in Klartext übertragen. Diese Daten werden von MISS genutzt um Geräte in der Nähe zu erkennen und bekannte zu identifizieren.
Durch den *IEEE 802.11* Standard werden auf der Sicherungsschicht des *OSI-Modell* Datagramme, sogenannte *Frames* definiert welche in spezielle Teile unterteilt sind. Jeder *Frame* enthält ein *MAC header* Feld, in dem die Absender MAC-Adresse im Klartext dargestellt ist. Durch belauschen der umliegenden Kommunikation kann so nach einer bestimmten MAC-Adresse gesucht werden. Aber nicht nur Geräte die im Moment Daten austauschen können erkannt werden, sonder auch Geräte die inaktiv sind. Jedes WLAN fähige Gerät senden abhängig von der Implementierung des *WNIC* Treibers periodische Pakete aus. Diese Pakete gehören zu der Gruppe der *Managementframes*.
Bei den *probe request frames* handelt es sich um Pakete die von *Clients* gesendet werden um Informationen über Netzwerke zu sammeln. Durch die Angabe einer *SSID* kann im Kommunikationsbereich des Gerätes nach bestimmten Netzwerken gesucht werden oder durch Angabe der *boradcast SSID* kann nach allen Netzwerken gesucht werden die dieses Paket empfangen und darauf Antworten. Diese Pakete werden periodisch versendet egal ob das Gerät bereits mit einem Netzwerk verbunden ist oder nicht.
Stations senden sogenannte *beacon frames* aus. Damit geben sie periodisch ihre

Präsenz, *SSID* und andere Parameter bekannt.
Im Standard Betriebsmodus eines *WNIC* ist es nicht vorgesehen, dass Pakete, die an andere MAC-Adressen gerichtet sind an höhere Schichten weitergeleitet werden. Diese Pakete werden bereits auf der zweiten Schicht dem *Data Link Layer* verworfen. Damit aber auch diese Pakete weitergeleitet werden, ist es notwendig den Betriebsmodus des *WNIC* auf den sogenannten *Monitormode* zu setzten. Dieser Mode wird über den Treiber des *WNIC* eingestellt um muss dort auch implementiert sein.

2.1.1 Airodump-ng

Airodump-ng ist ein Kommandozeilenprogramm welches für das erfassen von *IEEE 802.11 frames* genutzt wird. Mit diesem Programm lassen sich Log-Dateien erstellen welche Informationen über alle erfassten *Stations* und *Clients* enthalten. Eine Auszug von solch einer Log-Datei ist in Abbildung TODO zusehen. Die nachfolgenden Auflistungen beschreiben stichpunktartig die erfassbaren Daten für *Stations* und *Clients*.

Erfassbare *Station* Daten	Beschreibung
BSSID	MAC-Adresse der *Station*
First time seen	Datum und Uhrzeit der ersten Kontakts
Last time seen	Datum und Uhrzeit des letzten Kontakts
channel	Kanal auf der die *Station* sendet
Speed	Übertragungsgeschwindigkeit in MBit/s
Privacy	Privatsphäreneinstellungen
Cipher	Art der Verschlüsselung
Authentication	Genutztes Authentifizierungsprotokoll
Power	Signalstärke
# beacons	Anzahl der Empfangenen *beacon frames*
# IV	Anzahl der Erkannten Initialisierungsvektoren
LAN IP	IP Adresse
ID-length	Länge der ESSID
ESSID	Netzwerkname
Key	Netzwerkschlüssel falls bekannt (genutzt mit aircrack-ng)

Erfassbare *Client* Daten	Beschreibung
Station MAC	MAC-Adresse *Clients*
First time seen	Datum und Uhrzeit der ersten Kontakts
Last time seen	Datum und Uhrzeit der letzten Kontakts
Power	Signalstärke
# packets	Anzahl der Empfangenen *frames*
BSSID	BSSID mit dem der *Client* verbunden ist
Probed ESSIDs	ESSID die der *Client* sucht

2.2 Android

Bevor der eigentliche Hintergrunddienst installiert werden kann und funktionsfähig ist, müssen einige Vorbereitungen getroffen werden. Da Google in seinem offenen Betriebssystem Android keine Möglichkeit bietet einen *Monitor Mode* zu aktivieren, implementieren die meisten Hersteller diesen auch nicht für ihre WLAN Module.
Aktuell gibt es kein Android Gerät welches einen *WNIC* besitzt, für den es einem vom Hersteller implementierten *Monitor Mode* gibt. Für bestimmte Chipsätze des Herstellers Broadcom gibt es eine kleine Gruppe von Programmierer, die für die Chipsätze *BCM4330* und *BCM4329* eine neue Firmware geschrieben haben um eben diesen Modus zu aktivieren. Momentan werden folgende Geräte mit diesem Chipsatz unterstützt:

- Samsung Galaxy GS1 mit Cyanogen 7
- Samsung Galaxy GS2 mit Cyanogen 9 oder Cynaogen 10
- HTC Nexus One mit Cyanogen 7
- Asus Nexus 7 mit Cyanogen 7

2.2.1 Cyanogen

Alle zuvor ausgelisteten Geräte nutzen Cyanogen. Cyanogen ist eine erweiterte *open source* Firmware Distribution für Smartphones und Tablets welche auf den Android Betriebssystem basiert. Diese bietet Eigenschaften und Erweiterungen die es in der offiziellen oder in der des Herstellers ausgelieferten Firmware nicht gibt.
Um Cyanogen auf einem Unterstützten Gerät zu installieren, muss es zuvor *gerootet* werden. Diese bedeutet, das man alle Rechte erlangt was normalerweise auch aus Sicherheitsgründen so nicht vorgesehen ist.

2.2.2 bcmon.apk

Nachdem das Gerät gerootet wurde und Cyanogen installiert wurde. Wird das kleine Programm bcmon installiert. Mithilfe dieses Programms, welches die neue Firmware für den *WNIC* enthält, kann der *Monitor Mode* aktiviert werden. Anschließend ist das Gerät für die Verwendung des MISS Hintergrunddienstes vorbeireitet.

Kapitel 3

Architektur und Implementierung

3.1 Architektur

3.2 Implementierung

Für die Implementierung der voran gezeigten Architektur wurde das Eclipse ADT verwendet. Als Zielgerät wurde das Samsung Galaxy GS1 mit Cyanogen 7 gewählt. Hierbei war zu beachten, das bei der Programmierung nur Eigenschaften bis API Level 10 zu Nutzen sind. Die liegt an der geringen Android Version 2.3.3 welche dem Cyanogen 7 Mod zu grunde liegt.

Anwendungsprogramm PAR

Kapitel 4

Benutzung