

-::: Deepquest :::-

his site contains information which could be considered illegal in some countries. It is provided here for educational use only and is not intended to be used for illegal activities.



- [HOME](#)
- [Archives](#)
- [Coming soon](#)
- [Links](#)
- [/dev/null](#)
- [rss feed](#)

2005
04.13

Turning your mobile into a magnetic stripe reader

Category: [Security](#) / Tag: [phreaker](#) / [Add Comment](#)

Exploring my new Siemens MC 60 mobile I discovered an interesting feature. It has the ability to record small pieces of sound with its integrated microphone and store them as WAV files, so that you can use them later as personalized ring tones, etc. This suggests that the MC60 has a builtin ADC just the same as computer soundcards have. In fact every mobile must have an ADC to send voice because transmission is digital, not like in traditional analog cable telephones, but simply the ADC is not accessible to users, it is transparently used during communication.

The recording feature made me think that I might use the mobile as a magnetic stripe reader, just like I did with computers with soundcard. After some tests I had successful results, so here is the process in case you are interested in doing the same. I only did it with the Siemens MC60, but there are a lot of chances that it can be repeated with other mobiles of similar features. In order to use your mobile as a magnetic stripe reader it must comply with certain requisites, but even those might not be sufficient, only experience will tell you. First, the mobile must have the capability to record sound as an option through menu, and store it in a file within the mobile filesystem. Second, it must be able to transfer those files to a computer, and third, it must have a handsfree kit input, that is, an external microphone input. The later requisite is not strictly needed because you might open the phone to access the microphone and create your own mic input. I know you must be dare to do that 😊 but surely it won't be needed because all mobiles I've seen have handsfree kit input. The second requisite won't also be needed if the mobile is capable of running software to decode tracks within the mobile itself. Most often this is achieved with a Java Virtual Machine, that is, with Java enabled mobiles, but those kind of sophisticated devices always have the feature of computer connectivity to transfer games, melodies, etc., so finally the second requisite will be always present in practice.

The reason for the first requisite is obvious, however even without it you might try to modify your mobile hardware to add such a feature, but that process is beyond the scope of this article. The second requisite is needed in order to be able to decode the information of the magnetic track with a computer. If the mobile is Java enabled or has the ability to run software you can write, then sound files might be decoded within the mobile itself. More on that later. The third requisite must be present to be able to connect a magnetic head which will read the magnetic tracks.

Hardware

No much hardware is needed apart from the mobile itself, a computer to decode tracks and the cable to connect

EX1024

both (except if you can establish an IrDA or Bluetooth link). You just need a magnetic head and a connector for the mobile, so that the magnetic head connects with the microphone input of the mobile. Some mechanics to swipe cards will also be helpful. See the page of my soundcard reader for the specifications of the magnetic head and some ideas for the mechanics of the reader.

You need a mobile connector and the mobile pin out to know how to connect the magnetic head. See the page of my mobile interface for pinouts of common mobiles and ideas about how to get a connector. There you can see how to make an interface to connect the mobile with a computer in case you don't have one already.

Once you have the mobile connector and the magnetic head you have to wire them in the following way (exact pinout only valid for the Siemens MC60 and other Siemens mobiles with the same pinout). Both terminals of the magnetic head have to be connected to MC60 pins 11 and 12 respectively. If one of the pins of the magnetic head is connected to its metal case, then connect this pin to pin 11 of the MC60 (MIC_GND) and the other head pin to pin 12 (MIC) of the MC60. You must also shortcircuit MC60 pin 2 (GND) with pin 5 (Z_DATA), and pins 3 (TX) and 4 (RX) with pin 6 (RTS). These two shortcircuits are required to activate automatically the handsfree profile of the mobile when the connector is inserted. Otherwise you won't record the magnetic stripe data, but the ambient sound with the normal mobile microphone.

Capturing data

When you want to read a magnetic stripe card, you just have to navigate through your mobile menu and select the recording option. For example, in the Siemens MC60 this is achieved by selecting the "New ring tone" option in the "Extras" menu of the main menu. When the recording is in progress, swipe the card using the method chosen by you, then stop it and save data in a file. Try to minimize the time between the beginning of the recording and the start of the swipe, and the time between stopping the recording and the end of the swipe, so that recording time is minimum. This will ensure that sound files are as small as possible and you will be able to store more data in the mobile filesystem. For example, with some practice you will be able to record a swipe in around three seconds and even less. This means a file of less than 12 kB in the MC60 WAV format. This mobile has a filesystem capacity of more than 1.8 MB, and nearly all of it can be used to store records by deleting all unused images, melodies, games and applications, this means you can reach an autonomy of more than 150 swipes; but having into account that you can transfer data through SMS or directly to a laptop using a data cable, the autonomy is virtually infinite.

Software

Once you have recorded the magnetic stripe data in a sound file, you need to decode it. To do that, transfer the file to a PC, there you can use the program I wrote to decode magnetic stripes using the soundcard of a PC. See the reader page to download it and for instructions to use it. Unfortunately WAV files recorded by the MC60 have not the right format, they are IMA ADPCM WAV files but the header is not properly written. There are a couple of fields left empty (values set to zero), but they are needed to be able to decode the sound using the sox utility, which is required by my program. I did a quick & dirty C-shell script to fix the MC60 WAV files (set execution bit after download). It is not the cleanest method and it only works for small files (less than 65 kB, about 15 seconds of sound, which is far more than required to swipe a card), but it does the job.

Summary

Here are the steps to read a magnetic stripe with your mobile:

Check that the mobile is able to record sound, to transfer files to a PC and that it has a external microphone input.

Connect a magnetic head to the mic input of the mobile.

Select record option in menu and swipe a card.

Transfer the sound file to a PC, surely Windows will be required.

Boot the PC in Linux and fix the WAV file, if needed, using my script.

Compile my reader program and use it to decode the sound track.

Here is a sound track I recorded using my MC60 so that you can use it to test the programs and see that you are doing everything well. First you have to fix it using my script:

```
Linux prompt>./fixmc60wav.csh soundtrack.wav
```

and then decode it using my program with a command line like this (output also included):

```
Linux prompt>sox fixed_soundtrack.wav -t dat - | ./soundtrack -t 1 -c 55 -m z
```

Bad or no peak duration parameter, using default: 1
Bad or no stop duration parameter, using default: 500
Reading track 1
Bad or no threshold level parameter, using data...
Noise max./mean/rms amplitude: 0.002/-0.000/0.000
Threshold: 0.003
Recognition error of bit 697, stopping.

Swipe time: 0.553 s
Data max./mean/rms amplitude: 0.111/-0.000/0.022
Bits: 696, individual duration: 0.795 ms
Start sentinel found
%RUEDA, J?
End sentinel found
LRC OK.

Improvements

I know the process described above is somewhat complicated and tedious, but what did you expect for free? 😊
It is very unpleasant to record stripes with the mobile and later to have to transfer them to a PC with Windows and then reboot in Linux (or transfer to a second PC with Linux) to decode data. Then you can realize that some tracks were not correctly recorded and that you have to swipe them again, but you may no longer have the chance; so I advise to record more than one swipe per track.

To overcome these caveats I considered the possibility of writing a program to record and decode the tracks, all in one, within the mobile itself, taking advantage of the MC60 Java feature. You can download for free the Siemens Mobility Toolkit (free registration is required) and the Java Software Development Kit for Windows required by the Siemens kit. When I had a look I realized that the Siemens Java API is rather primitive and limited. There is no API to capture sound from the microphone, so you must use the “New ring tone” capture option anyway. Then you should execute the application that loads and decodes the sound file. But even that is difficult because the MC60 uses the MIDP 1.0 API which lacks the float type!

Yet there is another possibility, though even more complicated. You can attach an standard serial port magnetic stripe reader (or a non standard reader) to the mobile serial port (interface adapter will be required) and read data with a custom application. However I find this option less useful due to power considerations. If you want to avoid an external power supply (surely desired because you are looking for something portable), no much devices are available which might be powered from own (or mobile itself) battery, nevertheless a very small power consumption device might be designed for that purpose. It's up to you!

11 comments so far

[Add Your Comment](#)



1. jiwaniaziz said: 2010.05.13 14:58

Hi,

I have gone through your post. I had one question, how is magnetic swipe card reader powered? Is it powered by the cell phone using the speaker out of the cell phone?

Thanks,
Aziz



2. deepquest said: 2010.05.13 15:03

correct



3. jzting said: 2010.05.29 02:53

hi there, can you post your decode script?



4. Dimitar said: 2010.06.16 12:16

hi can you tell me how can I decode a soundfile already made by a recorder.



5. [Pero](#) said: 2010.12.02 04:34

hi can you send on my email the wav decode software, thank,s.



6. james said: 2011.08.23 18:43

i would like some assistance in deocoding some wav files



7. harri said: 2011.09.20 00:31

Square made billions on your idea!



8. deepquest said: 2011.09.20 01:08

I know Harri, but you can see it was here first.



9. Albert said: 2011.09.29 20:17

hey man , deepquest how can I contact you ? PM with ICQ or any id.



10.

deepquest said: 2011.11.11 03:28

for what?



11.

jon said: 2011.11.20 14:49

man you are a genius pls hit me with a chip idea as a door lock opens a lock the same data transfere must be applicable ?

Your Comment

You must be [logged in](#) to post a comment.

NSA/Echelon/Carnivor Jammer

undernet al-Qa'ida rubella enigma Halliburton dictionary protest harbor Halliburton rail gun counter-intelligence armada radar MD5 teflon bullets

© __-::: Deepquest :::-__. Powered by humans