

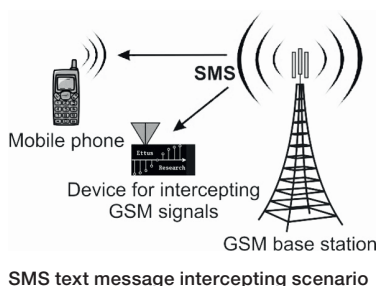
Intercepting SMS with a Software Defined Radio

Mobile Information Society / Thesis advisor: Prof. Dr. Ulrich Fiedler
Expert: Prof. Dr. Torsten Braun, University of Bern

Today SMS messages offer a quick and easy way of almost immediate transfer of information to a mobile phone. Even when a mobile phone is off, an SMS is still able to reach its subscriber once its phone is up and running again. Very often banks employ SMS messages to deliver confidential data to their clients, such as balance statements or one-time passwords. However, the GSM encryption has been broken.

In this project we develop and build an awareness demo to intercept and decrypt SMS messages in GSM networks using only commodity hardware and open source software. Such demo should be used to show that the SMS in GSM networks can be intercepted and decrypted. Hence, we will be able to show that it is an insecure means of communication to transfer confidential data such as banking information (e.g. balance statements) or passwords.

The possible intercepting scenario looks as follows. We send a test SMS message to our phone and use a special device to intercept the radio signal from the base station. We then decode and decrypt captured SMS message.



In our work we describe the concepts and implementation of passively intercepting SMS text messages over GSM's air interface by means of the software defined radio called USRP (Universal Software Radio Peripheral).

We also review major weaknesses of GSM's A5/1 cipher which make it possible to construct Rainbow Tables and to perform known-plaintext attacks to identify the ciphering key and decrypt the ciphered SMS text message.

Our implementation is based on open-source software which represents the GSM radio layer. In order to support GSM channels which employ frequency hopping (i.e. changes of central GSM channel frequency over time), we have extended the existing software with the wide-band capture capability which allows decoding the hopping GSM channel.

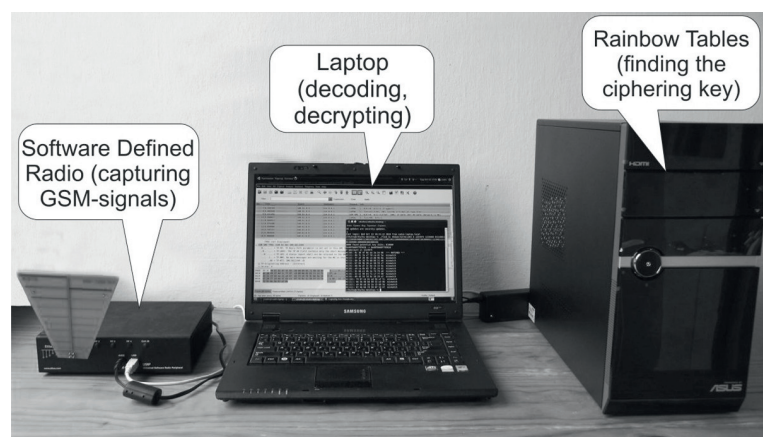
Our demo is based on self-programmed Python scripts which make it easier to perform attacks on the GSM A5/1 cipher in order to find the session key.

As a result, we have built an awareness demo that requires no more than 15 minutes of time to intercept and decrypt an SMS text message in GSM networks. We have employed only commodity hardware and open-source software with self-programmed modifications.

Our awareness demo can be used to show how little effort is needed to intercept an SMS message in GSM networks. It also significantly contributes to raising the awareness on the insecurity of GSM's current 64-bit A5/1 encryption within a broader audience.



Vadym Uvin



Equipment employed in the demo