ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

# Eavesdropping On GSM

Muthu Pavithran. S
Computer Science and Engineering,
Velammal Engineering College,
Chennai, India

***Abstract*—In the nearly 28 years since GSM was deployed, but still its meeting at various security problems have been found both in the protocols and in the original secret. Thither are 3.5 billion subscribers, GSM remains as the de facto standard for cellular communications. Only the security has still weak like at the start of the historic periods. The standard is no longer sufficient to guarantee the protection and concealment of the users. Furthermore fourth generation (4G) cellular technologies have been deployed these networks could never achieve strong security guarantees because the most of the still have using GSM subscribers. This report evaluates the claims and practical possibilities when it adds up to eavesdropping on GSM using relatively cheap hardware and open source software. This paper is extensive experiments with the USRP (Universal Software Radio Peripheral) and software tasks for this hardware.**

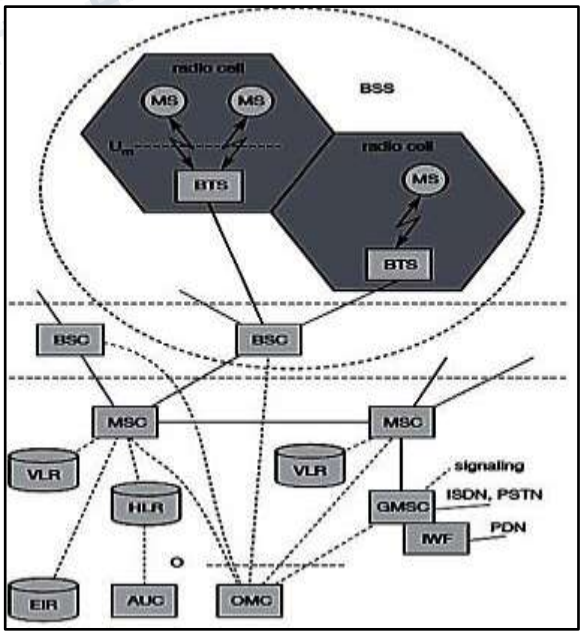
***Keywords*- GSM, USRP, SDR, 2G, 4G**

## I. INTRODUCTION

First cellular communication has developed in between 1960 and 1970 then mid 1990`s the cellular communications industry has witnessed explosive growth there is rapid worldwide increase in cellular telephone subscribers has demonstrated millions of users conclusively that wireless communication is a robust viable voice and data transport mechanism. In end of 2006 30% of world population, it has been increased 40% next year. When garments throughout the world provided increased competition and new radio spectrum licenses for personal communication services (PCS) the 1800-2000MHz (Frequency Band). A study by the international telecommunication union (ITU) shows that by the close of 2009 about 2 billion people in the world use the internet. But there were about 4.1 billion people in the world over 60% who had a mobile subscription while over 90% of the world population lived in a region that at least has access to GSM. The main important GSM specific dose not use to point point encryption between callers. It only encrypts the messages while on the air interface. It will leave the law enforcement to tap into the nucleus of the GSM net.The mobile phone has out of band channel to verify the transaction. Meanwhile, more service has been deployed through GSM network. It will the incentive for criminals to attack on GSM. Based on this paper, research work with a USRP an open source hardware generic radio transceiver and several open source software products which could in theory be used to eavesdrop on GSM.This is potential because of GSM the cell towers do not authenticate themselves to mobile telephones.In which an attacker acts as a genuine cell tower to instruct the cell phone to not utilize encryption and transfers outgoing calls via a VOIP connection

## II. GSM NETWORK ARCHICTURE

- Mobile Stations (MS),
- Base Stations (BS),
- Base Station Controllers (BSC) and
- Mobile Switching Centers (MSC).



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

### A. *Mobile Station*

A Mobile Station can be visualized as a mobile phone with a Subscriber Identification Module (SIM), a removable smart card. Every mobile phone has a unique 15-digit serial number, called International Mobile Equipment Identity (IMEI). In practice, this tin be applied to prevent stolen phones from accessing a web. The designation of the subscriber is effected with the aid of the SIM. It contains the International Mobile Subscriber Identity (IMSI), which is also a 15-digit number.

### B. *Base Station And Base Station Controller*

The wireless connection of a Mobile Station and a Mobile Switching Centre is realized by a Base Station1. Consequently, the country is split into various cellular networks with one Base Station for each cubicle. The size of the cell depends basically on the geographic features of the region and consequently on the orbit of the stations. But likewise the number of possible calls, that have to be handled simultaneously, has to be seen, since it is determined by the number of usable channels. Hence, in densely populated areas, the cells often have a diameter of just a few hundred meters, whereas in sparsely populated areas several kilometers are common. In subway stations, or large buildings Relais Stations are installed to ensure high connectivity. These Relais Stations act like a Repeater in wired networks. They simply amplify and relay incoming signals to the nearest Base Station. However, Base Stations are not only responsible for the connectivity. They are likewise required for encryption and decryption of communication information. As the epithet entails, on the next higher level the Base Station Controller manages the collaboration of the Base Stations and induces power controlling if necessary. If a Mobile Station moves from single cellular phone to another during a yell, the Base Station Controller accomplishes a handoff. The connection is transferred to the second Base Station to avoid a final result of the yell. The supposition is that both Base Stations are linked with the same Base Station Controller. Otherwise the handoff has to be made out by the Mobile Switching Centre

### C. *Mobile Switching Center*

The Mobile Switching Centre has the function of a mobility management. It is responsible for the authentication, routing, handoffs over different Base Station Controllers, connection to the landline, etc. For this design, there are 4 databases available Home Location Register (HLR) There is only one HLR in one GSM network, which stores personal information's of the contributor, e.g. The IMSI, the phone number3 or the GSM services. Visitor Location Register (VLR): Every MSC has its own VLR. It holds dynamic information's of the contributors that are below the legal power of the respective MSC. The information's are mostly copies of the personal information's, stored in the HLR. Certification Centre (AuC): The AuC holds the access information of every subscriber, particularly the secret key Ki of the SIM.Equipment Identity Register (EIR): As already noted, it is possible to prevent mobile phones from accessing the web.To understand this, the IMEI numbers of banned or stolen phones are held open in the EIR.

## III. SECOND GENERATION

This is the most common technologies in a cellular network. A first generation cellular network that relied on frequency division multiplexing access (FDMA) or frequency division duplexing (FDD). Second generation uses the digital modulation formats like time division multiplexing (TDMA) or frequency division duplexing (FDD) and code division multiplexing access (CDMA). Eight time slot users 200 KHz radio channel and has been grown widely by service provided in Europe and Asia. International standard 136 (IS-136) also known as North American digital cellular (NADC). Which support 3 times slots for each 130KHz. Pacific digital cellular (DDC) used in japan (TDMA). The popular 2G (CDMA) standard 95 code division multiple access (IS-95) also known as CDMA one. It holds up to 64 orthogonally coded and simultaneously transmitted on each 1.25MHz channel. POTS- plain old telephone services

## IV. THIRD GENERATION

it is system gives a unpatrolled wireless access in a way that have never been possible before possible before multi-megabitinternet access, communication using voice over internet protocol (VOIP). Companies producing merchandise that has equipped with 3G.It has power to receive live data from internet activity live web session and deliver simultaneous voice and video and data access with multiple parties at the same time employing a single mobile handset.Theneventually 3G evaluation for CDMA systems leads to CDMA2000. They are established on the fundamental of IS-95 and IS-95B technologies.Then it evolves to IS-136 and PDC system leads to wideband CDMA (W-CDMA). It's also predicted a universal mobile telecommunications service.(UMTS) 3G became most popular communication of the 21st C.Many nations

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

throughout the world are currently finding out new radio spectrum bands to accommodate the 3G networks that will likely be deployed the 2004-2005 time frame.In ITU`s 2000 world radio conference established the 2500-2690MHz, 1710-1885MHz and 806-960MHz bands as candidates for 3G. The third generation W-CDMA air interface standard had been projected for "always-on" packet-based wireless service.So computers, entertainment devices and telephones may all share the same wireless network, and be linked to the internet, anytime, anywhere, W-cdma will support packet data rates up to 2.048Mbps per user, thereby allowing high quality data multimedia, and diffuse-type services to consumers.Future version of W-CDMA will support stationary user data rates in excess of 8Mbps. W-CDMA provides public and private network features all of the small portable device.

## V. EQUIPMENT USED

In parliamentary law to assess the practicality of eavesdropping attacks, we experimented with hardware and software.

1. Universal Software Radio Peripheral (USRP)
2. DBSRX daughter board
3. GNU radio
4. Air probe
5. Nokia mobile
6. Gammu software

### *A. Universal Software Radio Peripheral (USRP)*

The Universal Software Radio Peripheral (USRP) is planned as a general purpose hardware subsystem for software defined radio. It is an open-hardware device developed by Matt Ettus and which can be ordered through his company Ettus Research.The first device is USRP Universal Software Radio peripheral it is an open hardware transceiver that can be connected to a data processor via USB.It handles a receiving component of an eavesdropping of an eavesdropping attack.The USRP is connected with the daughter board in order to obtain the correct frequency spectrum, we need to use the DBSRX daughter board for this research which is an 800MHz to 2.4GHz and covering all basic GSM frequency bands. There are presently two types: the USRP1 and the USRP2. Both consist of a motherboard which contains a Field Programmable Gate Array (FPGA), Programmable Gain Amplifier (PGA), ADC(s), DAC(s) and a communication port to connect it to the computer. Daughter boards can be plugged into the USRP motherboard according to the specific frequency bands needed. These daughter boards can be lifted up to appropriate antennas. On the receiving path (RX), a daughterboard captures the required frequency range and sends it through the PGA, possibly amplifying the signal, towards the ADC. The resulting digital signal is drawn along to the FPGA, where it is translated into 16 bits I and Q samples. These are complex samples, with the material part (Q) describing the cosine of the sign, and the imaginary part describing the sine of the signal plus 90 points.One sample is thus 32 bits long and can be transmitted to the host computer through the communication port, for further processing.The FPGA and the host CPU both do more or less processing on the signal, and though the precise class of labor can be changed, standardize the high speed general purpose processing, like down and up conversion, decimation, and interpolation are performed in the FPGA, while waveform-specific processing, such as modulation and demodulation, are done at the host CPU.

### *B. USRP Daughter boards*

Different frequencies require different antennas and sometimes different signal processing, like amplifiers or filtering, to receive or transmit correctly. So in order to keep the USRPs as general as possible the actual receiving and transmissions are handled by daughter boards that can be plugged into the USRP motherboard. These daughter boards are specifically intended for certain frequency bands. Presently there are thirteen daughter boards available, of which there are interesting in relation to GSM signals.

- DBSRX, a 800 MHz to 2.4 GHz Receiver.
- RFX900, 800-1000MHz Transceiver, 200+mW output.
- RFX1800, 1.5-2.1 GHz Transceiver, 100+mW output.

The most used GSM frequencies are GSM900 (890.2-959.8 MHz) and GSM1800 (1710.2-1879.8 MHz) in Europe, and GSM850 (824.0-894.0 MHz) and GSM1900 (1850.0-1990.0 MHz) in America and Canada. The DBSRX board covers all these frequencies, but is only a receiver board. In parliamentary law to actively transmit an RFX board is required.

### *C. GNU Radio*

GNU Radio is a free software toolkit licensed under the GPL for implementing software-defined radios. It was started by Eric Blossom. It plays with various different cases of RF hardware, like sound cards, but it is generally applied in compounding with an USRP. Basically GNU Radio is a library containing dozens of standard signal processing purposes. These roles, usually called blocks, are

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

often divided into three categories: source blocks (USRP drivers, but also file readers and tone generators), sink blocks (USRP drivers, graphical sinks like an oscilloscope and audio card drivers) and processing blocks (like filters, FFT and (de) modulations).These cubes can be tied to each other to form a graph. All the low level blocks are written in C++, while higher level blocks and GNU Radiographs are made in Python. These two languages are glued together using SWIG. This implies that, for performance reasons, the actual computations are done in C++, while at a higher level a more user friendly language is applied to fix a software radio. This also abstracts from implementation details of the processing offices. If I want to see a Fast Fourier Transform (FFT) of a certain frequency onscreen, I just need to instantiate a source block (for instance a USRP source, with a frequency) and a graphical FFT sink and connect these two together. I do not need to recognize or understand how the actual FFT is computed, in parliamentary procedure to utilize it. And at that place are hundreds of implementing blocks inside GNU Radio.GNU Radio, out-of-the-box, does not offer much in terms of GSM sniffing capabilities, although it can be utilized to place the beacon frequencies of GSM masts [12].However, GNU Radio can be used by other software packages, like AirProbe in the following section, to perform the low level functions of GSM sniffing, like reception and demodulation.

### *D. AIRPROBE*

Airprobe is an open-source project trying to construct an air-interface analysis tool for the GSM (and possible later 3G) mobile telephone standard.This project came forward out of the GSM-sniffer project.When you currently clone the git repository, you will start out almost ten projects.More or less of these function as libraries for the other projects (e.g.Gsmstack), some of these have more or less the same purpose (e.g.gsm-receiver and T-void) and some of these don't even compile anymore (e.g. T-void). The most interesting part of AirProbe is the gem-receiver project. It is, at this minute, the best working capture tool for GSM.It occurs with two simple shell scripts that address all the necessary functions for saving the signals on a frequency to a file and for translating the signals in this file. Calling capture. Sh<Freq> [duration==10] [decim==112] [gain==52] with a frequency will capture the signals on that frequency to a file. The duration, decimation and gain are optional arguments with default values. A file will be created called capture_<Freq>_<decimal>. File, containing the captured IQ samples. These can then be rendered by calling: gosh <file. cfile> [decim==112].The file name has to be supplied, but the decimation is again optional, though you should utilize the same decimation value that was used during capturing.The gosh script runs a python file that defines a software radio, which performs all the processing required to obtain the information bits out of the samples.This effects in a series of hex values that represent the data as transmitted by the GSM net.The gosh script uses a UNIX pipe method to have these hex-codes interpreted by gsmdecode - one of the other tasks in the Air Probe repository.You could as well attempt to convert these hex codes to a.Pcap file, which can be read by the Wireshark program [15].Currently the gsm-receiver project will simply decode the downlink (GSMnetwork to mobile telephone set).

### *E. OpenBTS / OpenBSC*

It is useful to know that a Base Transceiver Station (BTS) is a GSM cell tower, and a Base Station Controller (BSC) is a command center for several BTSs. Both of these systems possess an open-source implementation: Open BTS [16] and Open BSC respectively. This does not imply that both organizations function in concert. In fact they are different approaches to the same trouble. Open BTS, founded by David Burgess, offers a BTS implementation using the USRP and turning it into a BTS. Some of the logic normally present in a BSC is placed inside Open BTS. Open BSC, developed by Harald Welte, on the other hand implements most of the BSC functions and currently includes support for two BTS types (nanoBTS and the Siemens BS-11 microBTS). It does not support an OpenBTS driven USRP. Both systems give you the opportunity to run your own GSM network, though this requires a license in most countries. This can be really useful for testing purposes, but another big function is their implementation of the GSM protocol stacks.These open source systems offer an extra means to understand the GSM protocol through their implementation, and these implementations can be utilized to create GSM analyzers.

### *F. NOKIA GSM MOBILE PHONE*

The extensive use of a nokia GSM mobile phone tied to the computer and also extending the open source tool games via USB.This will enable us to hightail it the nokia in a debug mode that transparently log all the packets sent to and from the telephone set.The games and nokia mobile is the best combination for a better response than the USRP and air probe, the mobile is specifically prepared to take in these signals thought the phone we can insure the message from and to on that phone we can't modify the behavior of the phone to see the all the network messages.Thus better to ferment with the USRP and then we can tune it to grasp of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

the GSM protocol and fine tune the USRP.Only it has the looks of versatility to be utilitarian in an eavesdropping attack.

## VI. EAVESDROPPING ON GSM IN THEORY

Eavesdropping in any communication system for that affair can be collapsed down into three phases.

- Capturing the signals
- Decoding the signals
- Interpreting the signals

### *A. CAPTURING THE SIGNALS*

The first state of the approach is the capturing the GSM signals it has been a major obstacle for many years and hackers. Specialized equipment to get the GSM signals is also expensive to buy from the common masses.The GSM can be applied on various frequency bands, but commonly used GSM-900 and GSM-1800 bands, then frequency is separated into channels 200 KHz wide each.In more common in conversation, it need two of these channels will be used at whatever given time for a mobile to transmit with the cell tower one channel for the each direction and then these channels has been divided by the constant offset.In a GSM network 20ms of speech data is carried in a four packet is called bursts in GSM network.These bursts are modulated radio waves transmitted in the time slot of 576.9musec most of the GSM network uses in "channel hopping".This is employed to assess the transmission to change over to a new channel after every single explosion.The challenge of capturing GSM signals lies in picking up the bursts on time and in demodulating them correctly.

### *B. DECRYPTING THE SIGNALS*

The following step is the decrypting the captured beasts there are the three common encryption defined for GSM A5/1 and A5/2, both stream ciphers and A5/3 is the block cipher.From these three A5/2 is the far weak and easy to develop in less second with the personal data processor with only a few dozen milliseconds of cipher text.A5/3 is one considered as the strongest encryption of the leash.It accepts the theoretical break this attack required 226 chosen plain text messages encrypted under related keys.From this treatment does not lead to a practical attack on A5/3 though it is cause for concern since this weakness does not exist in MISTY. The most common used algorithm in the westerncountries is A5/1. It is a stream cipher with three registers that clock irregularly and combined with the size of 64bits and its also size of the session key. The SIM card will compute the session key and in the providers of a home network from a random challenge and a secret key by an undisclosed proprietary algorithm. An algorithm is used by the most of the providers is called COMP128, it has been reverse engineered in 1998 by "Briceno et. Al. At once it showed that COMP128 is actually handing over a 54 bit session key with ten appended zeros.It is still unknown which algorithm are used by the providers to generate the session key and if the session keys still weakened. The A5/1 is the first encryption used in the GSM net.It was kept hidden by the GSM manufacturers under NDA.In 1999 Marc Briceno reverse engineered the design of both A5/1 and A5/2 from a GSM telephone.Since then various types of attack against A5/1 has been issued.But recently brute force time memory trade off against A5/1 was announced which is will be discussed in future, it is an improvised attack in GSM network.

### *C. INTERPRETING THE DECRYPTED SIGNALS*

After the signal has been captured and deciphered they still require to be translated. And then the payload of the bursts needs to be reordered and can be marked for transmission errors. Besides the cryptography all the specifications of GSM are public so this does not call for any reverse engineering.

## VII. COUNTERMEASURES

The GSM is almost as old as the GSM system itself. So the GSM industry has received plentiful time to get up for the practical implementations of these approaches.In that respect are several countermeasures against these attacks, we will discuss the effectiveness about three of these countermeasures here.

A. ENCRYPT CONTENT USING A5/3
B. USE RANDOM PADDING IN GSM PACKETS
C. USE UMTS

### *A. ENCRYPT CONTENT USING A5/3*

The pure eavesdropping will no longer be possible when using A5/3however, it will not improve GSM's security much. This is imputable to the fact that regardless of the option of encryption algorithm, the session key used will be the same.Basically the session key is produced based on the secret key, known simply to the SIM card and the home network, and a challenge transmitted by the cellular phone tower.This challenge is transmitted in the clear, then an attacker could simply put down the challenge and an

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

A5/3 en- scripted conversation, then at any later time pretend to be a base station to the user and retransmit the challenge.These forces the user's SIM to compute the same session key, which could be developed in an A5/2 connection set up by the fake cell tower, and employed to decrypt the conversation.As well, this will not militate against MITM attacks.Finally the GSMA (GSM Association) has suggested the use of A5/3 by providers since 2004, but it seems only a single small provider world-wide has ever caused this conversion

### *B. USE RANDOM PADDING IN GSM PACKETS*

These padding bits can thus be randomized, and that is exactly what specified by the ETSI. This would remove a large source of known plaintext for an attacker. Without knowing plaintext there are no known key stream samples which can be looked up in the Kraken tables. It is questionable how fast this change will be carried out, yet.All the low level GSM processing is managed with closed source GSM stacks, so it is unknown whether this change would affect the already deployed equipment. All the mobile handsets in the field cannot be updated, so this modification can only be established in new phones. Besides this change will not totally remove any known plain text from the organization. Some messages can still be guessed, such as system information messages, still feasible for longer conversations.

### *C. USE UMTS*

This is kind of a cop-out, but a method that is at least currently avail- able to quite some users. The successors of GSM. the 3G systems, mostly UMTS offer much better security. Specifically it has mutual authentic between cell tower and mobile phone preventing MITM attacks and offers stronger encryption, that has seen academic scrutiny. Otherwise an attacker could force a phone to use GSM, by jamming the UMTS frequencies. Of course the usability of this resolution will depend on the handiness of a UMTS network to the specific user, and might have additional data costs.

## VIII. CONCLUSION

The first capturing the GSM signals from the air remains the bottleneck. Especially the channel hopping used in GSM networks which are not even a security measure prevents the correct capture of GSM packets. With the current state-of-the-art, the best way to capture GSM data from the air proved the use of an old Nokia phone (3310), which can be put in a debug mode, logging all the GSM bursts it receives. Nevertheless, this will never reveal bursts that are not intended for this specific phone, and can therefore never be used for eavesdropping. The compounding of the USRP, with Gnu Radio and Air Probe currently does not present the possibilities needed for eavesdropping. The liberation of the rainbow tables and the Kraken tool has pulled in the breaking of the A5/1 encryption much more comfortable. Nevertheless, this plan of attack does have a few downsides: besides the hard disk size this method also requires perfect samples, putting additional stress on the capturing process and of course the tables will never give a 100% chance of finding the key.However, the current coverage of 22% of the key space should be workable given enough samples.Frequency hopping might not be used by a specific cell tower, or the cellphone tower is transmitted on only a few frequencies that lie near together. In fact a cell tower might not even use encryption. In those cases, many attacks become a lot more comfortable, only we do not know if and how many cell towers have such a configuration. During this research all observed cell towers used both frequency hopping and encryption. The countermeasures that are frequently referred to by the GSM industry when downplaying the news reports, the most effective one is essential to by-pass GSM all together and use solely UMTS instead.

## REFERENCES

1. Chris Tryhorn. Nice talking to you ... mobile phone use passes milestone. The Guardian, 2009. Tuesday 3 March http://www.guardian.co.uk/technology/ 2009/mar/03/mobile-phones1.

2. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems, chapter 17. Wiley Computer Publishing, 2001. ISBN: 0471389226.

3. February 2010. http://www.ing.nl/particulier/internetbankieren/ internetbankieren/wijzigingen-in-voorwaarden-mijn-ing/.

4. January 2010. https://svn.berlin.ccc.de/projects/airprobe/wiki/tracelog and http://www.gammu.org/.

5. Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of gsm encrypted communication. In Advances in Cryptology - CRYPTO 2003, volume 2729/2003, pages 600–616. Springer Berlin / Heidelberg, 2003.

6. Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time attack on the a5/3 cryptosystem used in third generation gsm telephony. 2010. http://eprint. iacr.org/.

7. Marc Briceno, Ian Goldberg, and David Wagner. A pedagogical implementation of the gsm a5/1 and a5/2 "voice privacy" encryption algorithms, 1999. http: //cryptome.org/gsm-a512.htm (originally on www.scard.org).

8. Jovan Golic. Cryptanalysis of Alleged A5 Stream Cipher, page 23955. 1997. http: //jya.com/a5-hack.htm.

9. Elad Barkan and Eli Biham. Conditional Estimators: An Effective Attack on A5/1, page 119. 2005.

10. August 2010. http://www.global-security-solutions.com/GSAudioSurv.html.

11. January 2010. http://www.ettus.com/.

12. September 2009. http://gnuradio.org/trac.

13. January 2010. https://svn.berlin.ccc.de/projects/airprobe/wiki.

14. January 2010. http://www.reflextor.com/trac/a51.

15. Steve Muller and David Hulton. The a5 cracking project. In Chaos Com- munication Camp 2007, 2007. http://video.google.com/videoplay?docid=8955054591690672567.

16. January 2010. http://reflextor.com/torrents/.

17. Erguler, Imran, Anarim, and Emin. A new cryptanalytic time-memory trade-off for stream ciphers. In Computer and Information Sciences - ISCIS 2005, volume 3733 of Lecture Notes in Computer Science, pages 215–223. Springer Berlin / Heidelberg, 2005.

18. Jin Hong, Kyung Jeong, Eun Kwon, In-Sok Lee, and Daegun Ma. Variants of the distinguished point method for cryptanalytic time memory trade-offs. In Informa- tion Security Practice and Experience, volume 4991 of Lecture Notes in Computer Science, pages 131–145. Springer Berlin / Heidelberg, 2008.

19. September 2009. http://openbts.sourceforge.net/.

20. September 2009. http://bs11-abis.gnumonks.org/trac/wiki/OpenBSC.

21. Karsten Nohl and Chris Paget. Gsm - srsly? presented at 26C3 in Berlin, http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_ 26C3.Karsten.Nohl.GSM.pdf, December 2009.

22. European Telecommunications Standards Institute, France. Digital cellular telecommunications system (Phase 2);Mobile Station - Base Stations System (MS - BSS) interface Data Link (DL) layer specification, 2010. TS 44.006 v9.1.0.

23.Eavesdropping on GSM: state-of-affairs,Fabian van den Broek, Radboud University, Nijmegen Institute for Computing and Information Sciences (iCIS).