Wideband Fully Passive GSM Interception System

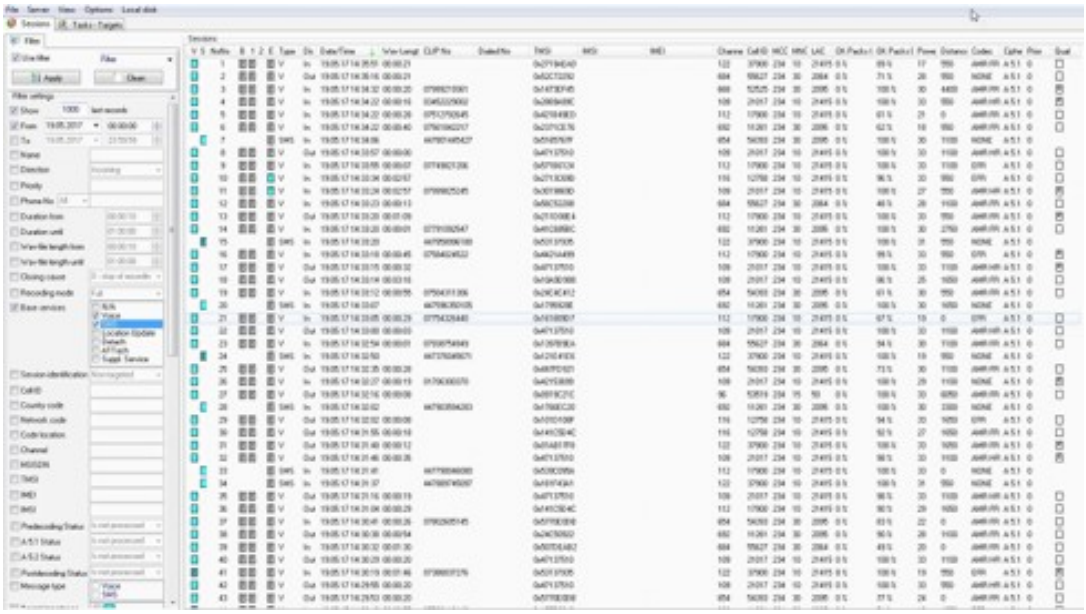
- A convenient solution that enables extensive and loss-free gathering of information.

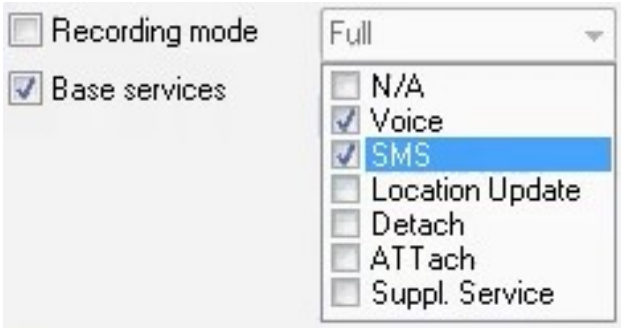
- EGSM-900/GSM-1800 or GSM-850/GSM-1900.
- 600 simultaneous calls using 1096 frequencies receiving system.
- The system continuously analyses all 548 downlink channels and provides identification of BTS control channels.
- Any fake BTS can be detected and shown to the system operator.
- The system is able to receive, decode, store and show Voice and SMS from a GSM-network.

- Distance of interception.
- 2G duplex interception is up to 400 meters line of sight and simplex interception up to 2 km.

- Distance of interception.
- Using optional active subsystem allowing monitoring of 4G/3G target phones in 2G. 100 meters

- The system can also be used as Passive IMSI catcher and provide notification about any new IMSI event inside of the interception area. White and black list of targets IMSIs can be used for filtering of group of subscribers.





WHITESTEPS

Technical Information
Wideband Fully Passive GSM Interception System



WHITESTEPS

TABLE OF CONTENTS

Introduction
1. Passive GSM Interception System
1.1 Passive receiving station
1.2 Laptop/Working station and storage unit
2. Networking of Multiple Stations
3. Specifications
3.1 Technical characteristics
3.2 Functional characteristics
4. System delivery list
5. System components
6. Screen shots

INTRODUCTION

The Global System for Mobile Communications (GSM) is widely used mobile radio network. The GSM standard defines a digital network for voice communications, for circuit-switched and packet- switched data services as well as for short message services (SMS).

The document describes Wideband Fully Passive GSM Interception System. The system is able to show the entire receivable GSM mobile radio traffic from EGSM-900, GSM-1800, GSM-850, and GSM-1900 and to disclose call contents. It is a convenient solution that enables extensive and loss- free gathering of information.

The system provides interception of up to 600 simultaneous calls without loss of data using 1096 frequencies receiving system approach when all 548 GSM duplex-channels are analyzed. It continuously analyses GSM networks parameters and controls all channels of radio-available BTSs in parallel with calls interception. The wide-band system architecture guaranties that all BTSs with their hopping mode and handover procedure will be processed in any cases. Any other system architecture cannot guaranty successful interception of all radio-available BTSs and subscribers in case of GSM network parameters changing, offline processing or delay in A5.1 deciphering during system operation. Easy use without operator intervention is a strong benefits this system.



HIGHLIGHTS

- All GSM bands in the interception range can be evaluated.
- All eight time-slots in all receivable channels are intercepted.
- Frequency hopping in the GSM band takes place without loss of data.
- Handovers in the receive range are intercepted and evaluated.
- The receiving station has 548 duplex-channels in total. Each channel is divided into 8 x slots (full rate) or 16 x slots (half rate). Maximum capacity of one receiver station is 548 x 8 communications in case of full rate or 548 x 16 communications in half rate.
- Data evaluation does not require any knowledge of IMSI, IMEI, TMSI or phone number (MSISDN).
- The system does not require any Ki information.
- All the data that is intercepted is stored on the server.
- The system is modular. The system components can be used at different locations. This requires just a TCP/IP link.

1. PASSIVE GSM INTERCEPTION SYSTEM

The system has been developed to intercept data from 548 duplex GSM channels that means of 1096 simplex channels in total. The system satisfies the highest of requirements by analyzing and representing all receivable data. It can monitor all 548 channels and all its time-slots simultaneously and moreover keep track of all frequency and time-slot changes within 548 channels. The wide-band approach makes it possible to evaluate the entire useful data traffic on the air interface without losing any information.

The GSM-Interception-System consists of the following parts:

- Directional and Omni-directional antennas set
- Passive receiver station
- Laptop/working-station and storage unit
- Decryption unit. It is third-party product with 2 up to 80 real-life session key recoveries per second

The system is able to receive, decode, store and show Voice and SMS from a GSM-network. It is possible to intercept A5.0, A5.2 and A5.1-communication. The system can intercept uplink and downlink-channels. If the uplink-channel is not available (due to physical reasons), the simplex- communication is recorded (only downlink channel).

The configuration of the system mainly depends on the user requirements as well as on the network infrastructure that exists in the monitoring area.

The receiver station receives the bands to be monitored and checks them for GSM bursts by means of fast GSM decoding. The channel information received is transmitted to the server where it is processed.

The receiver station now makes the received data available to the user and initiates the calculation of the necessary Kc. A separate calculating unit, the Decryption Unit, is required for Kc calculating.

The server stores all the data while the Kc is being calculated. This capability makes sure that no data is lost and that always the entire call content is available.

1.1 PASSIVE RECEIVING STATION

The passive receiving station consists of a RF-front-end to receive GSM up and downlink in 900/1800 MHz-range including EGSM (or 850/1900 MHz-range). It is high sensitivity and a wide dynamic range of the radio receiving station. The received signals are demodulated and stored in a FIFO-buffer. If a start of a communication is detected, the data are forwarded to the decryption unit to archive the Kc (session key for the actual communication). After receiving the Kc from the decryption unit, the receiving station performs decrypting of the intercepted data and forwards this data to the storage system.

The receiving station has 548 duplex-channels in total. Each channel is divided into 8 x slots (full rate) or 16 x slots (half rate). Maximum capacity of one receiver station is 548 x 8 communications in case of full rate or 548 x 16 communications in half rate.

The receiving unit demodulates all time-slots on the 548 channels. As long as the decryption unit needs to calculate the Kc, the receive data are stored temporary in a first-in-first-out-buffer. The capacity of the FIFO-memory is 100 GB.

1.2 LAPTOP/WORKSTATION AND STORAGE UNIT

This is the user-interface to control the system and evaluate the data. The workstation can handle different receiver-units to be combined to one encryption unit. All decrypted information will be stored in a database.

Recording capacities:

Number of duplex GSM channels	Data rate	Recording capacity	Recording time
548 (100% traffic activity)	30 MByte/s	2 TByte	20 hours
Due to frequency reusing principle in GSM network Real environment around the system location contains approx. no more that 200 duplex channels			
200 with 100% Network Utilization	11 MByte/s	2 TByte	52 hours
200 with 30% Network Utilization	3.3 MByte/s	2 TByte	176 hours

The recorded data can be exported to a remote Monitoring Center

This capacity calculation is based on the assumption that the standard hard disks. This operating mode provides higher reliability. Should the memory space nevertheless be insufficient, it is possible to equip the system with additional hard disks.

These flexible memory management options allow the system to be adapted to specific user requirements.

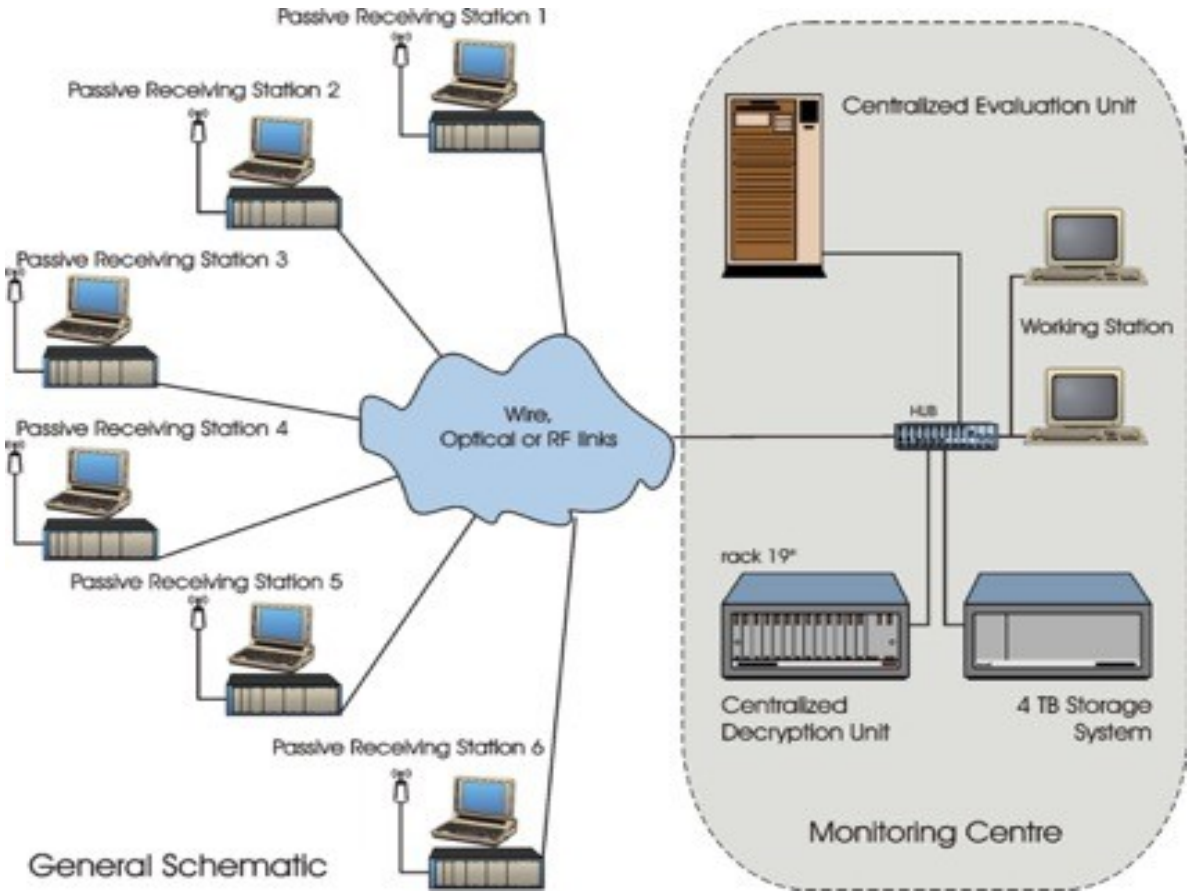
2. MULTIPLE STATION NETWORKING

The full flexibility of the system can be utilized if systems are coupled. It is also feasible to operate multiple systems at different locations. The information that has been collected does not have to be evaluated at the location where it has been recorded.

The individual receiving stations and the server communicate by means of wire line. A wide area network (WAN) can be implemented by applying different technologies.

A realistic scenario would be the positioning of the receiving systems along a border. In this case, the data can be evaluated not only at the place of recording but also at a remote location. An optional decrypting unit for decrypting the Kc at a central location can also be provided.

Appropriate wire line technologies for connecting the subsystems are DSL and LAN. Appropriate wireless technologies for connecting the subsystems are UMTS, HSPA or WLAN.



3. SPECIFICATIONS

3.1 TECHNICAL CHARACTERISTICS

Parameter	Description
GSM900/1800 Version	
GSM900 channels	0…124, 975…1023 880…915MHz (uplink) 925…960MHz (downlink)
GSM1800 channels	512…885 1710…1785MHz (uplink) 1805…1880MHz (downlink)
Number of RF channels for each RX (duplex)	548 (1096 simplex in total)
Number of traffic channels for each RX (duplex)	4384 (FR) / 8768 (HR)
GSM850/1900 Version	
GSM850 channels	128…251 824…849MHz (uplink) 869…894MHz (downlink)
GSM1900 channels	512…810 1850…1910MHz (uplink) 1930…1990MHz (downlink)
Number of RF channels for each RX (duplex)	423 (846 simplex in total)
Number of traffic channels for each RX (duplex)	3384 (FR) / 6768 (HR)
Both versions	
Specification of FIFO for each RX	100 GB
Call per minute	up to 600
Scalability with add. RX units	Secure
Housing	19" housing
Dimensions for Passive Receiver Station	19", 4U

3.2 FUNCTIONAL CHARACTERISTICS

- Searching and identification of BTS control channels in full GSM900/1800 (or GSM850/1900) frequency;
- Collecting and displaying of technical and statistical information about networks with detailed indication of BTS parameters;
- Displaying of radio frequency environment at the point of system location;
- Tasks assignment for all the receiving channels automatically or manually;
- Operation in scanning mode & data collection mode in parallel;
- Operational evaluation of received signal strength and quality at all the receiving channels;
- Saving and fast loading of the system configuration parameters;
- Support of SDCCH/8 and SDCCH/4 signaling channels formats;
- Session key calculation for A5.1 and A5.2 encryption algorithms;
- Several receiving stations can use the same decryption unit located remotely. Its can be connected with the unit by wired or wireless communication channels.
- Support of HR, FR, EFR, AMR-FR, AMR-HR speech codecs;
- Support of Hopping mode;
- Processing of traffic channels Handover between BTSs;
- Registration and storage all intercepted information in database;
- Registration and storage SMS messages in database (it is supported all languages used in Windows operation system);
- Voice session storage in WAV format;
- Playback of Voice sessions in real time;
- Displaying of dialed during the call DTMF symbols;
- IMSI/TMSI identifying by known MSISDN number (silent call or hush SMS);
- Selection of targets using IMSI, IMEI, IMEISV, TMSI and MSISDN identifiers;
- Support of receiving channels and targets priorities;
- User authorization access to the system;
- The system software is working on Windows 7/10 x64;
- Geographic positioning of the interesting call on the Google map. It uses open Google service with Cell information and gives only supposed location of the BTS. If information about selected call (with appropriate cell ID) is absent in the Google database then no cell icon appears on the map. Internet connection is required for this.

4. SYSTEM DELIVERY LIST

NN	Description	Q-ty	Notes
1	Passive GSM Interception System comprising:	1	
1.1	Passive Receiver, 19" 4U 430x176x546mm v.1) Input: IN1 880-915 MHz, 1710-1785 MHz, IN2 925-960 MHz, 1805-1880 MHz. v.2) Input: IN1 824-849 MHz, 1850-1910 MHz, IN2 869-894 MHz, 1930-1990 MHz. Output: Two Gigabit LAN 10/100/1000 Mbit/s Power: 100-240 Vac, 50-60 Hz, 800W Storage capacity: (2) SSD: 120GB (system) + 2TB (data) SW: Specialized SW with License USB Dongle	1	
1.2	GSM-modem with magnetic antenna and interface cable	1	
1.3	Cargo case for the Receiver, 702x397x686mm	1	
2	Accessories comprising:		
2.1	Accessories case, 619x492x223mm	1	
2.2	Workstation, HP ProBook 450 G2 Notebook PC with Power supply and power cable OS: Windows 7/10 Professional 64 (English) CPU: Intel® Core™ i5-4210U LED: 15.6" (1366 x 768) RAM: 8 GB DDR3 SSD: 128 GB SW: Specialized SW with License	1	
2.3	KVM Console to USB 2.0 Portable Adapter NOTECONS01 with Logan DVI Plug - VGA Socket	1	
2.4	11dBi Omni Antenna + RG 174U 5 m	2	
2.5	Headphones Sennheiser HD 205 II	1	
2.6	Cat 5E UTP Network Cable (5m)	2	
2.7	European standard power supply plug cable 1.8 m	1	
3	A5.1 Deciphering Unit	1	Optional

5. SYSTEM COMPONENTS



(1pcs.) Cargo case for the Receiver, 702x397x686mm, 16kg



(1pcs.) Accessories case, 619 x 492 x 223mm, 10kg





(1pcs.) Receiver, 19" 4U 430x176x546mm, 25kg



(1pcs.) GSM-modem with magnetic antenna and interface cable

Accessory case



(1pcs.) Laptop



(2pcs.) 11dBi Omni Antennas



(1pcs.) Power supply + power cable



(1pcs.) Headphones



(1pcs.) KVM Console to USB 2.0 Portable Adapter + DVI-VGA adapter



(2pcs.) Ethernet cable



(1pcs.) Power cable

6. SCREENSHOTS

