GreenLeaf

COMINT

SEMI ACTIVE GSM MONITORING SYSTEM

Surveillance, Interception, Monitoring & Logging System

Technology Introduction:

GSM networks are the most popular and widespread wireless communication media across the world, having a wide customer base in Europe and Asia-Pacific and command more than 50 percent of mobile customers. The advancement of GSM networks increases rapid growth of its users and services. Being an advanced technology it has become favorites for the criminals. These facts have created worldwide market for the analysis and monitoring of GSM network.

The advancement of GSM technology, enhanced technological features and increased complexity, presents competitive environment for Stratign to design and develop solutions to provide total **Off -The-Air** Communication Surveillance system to its various Government and Intelligence Gathering customers.

GSM operates on standards frequency 850MHz, 900MHz, 1800MHZ and 1900MHz bands and offer services such as SMS, MMS, email, advanced video features, dictionaries

Due to the widespread availability of GSM networks, a GSM mobile has the potential to seamlessly roam nationally and internationally.

System Approach:

The system is designed and developed as a Semi Active **OFF-THE-AIR GSM** Monitoring System. The Surveillance of UM interface (b/w BTS and Suspect's mobile) provides total traffic monitoring including SMS and Voice, of the targeted Mobile. System uses state of art technology to on-line deciphering of A5.1 and A5.2 cipher algorithms.

The system comes in a camouflaged case along with Control Laptop and Accessories.

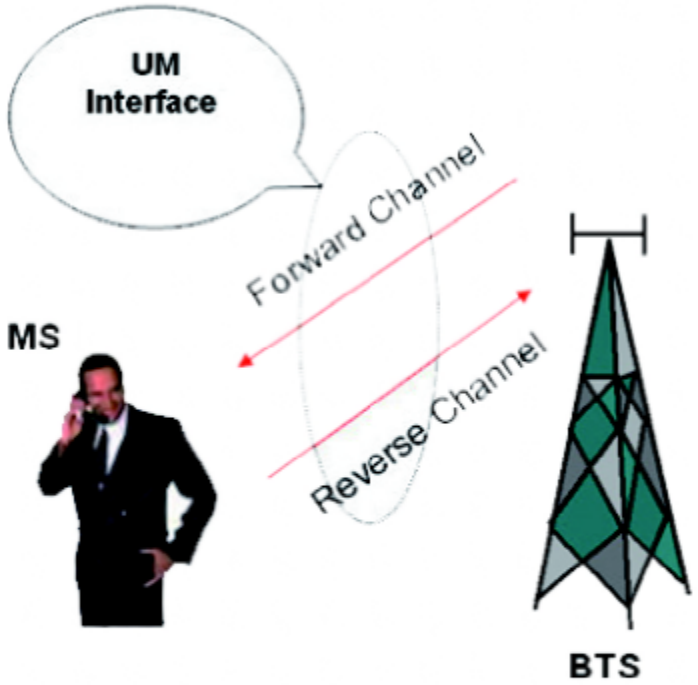

Figure 1 – The **GL-H14** *Intercepts calls from the UM interface between Target and BTS*

System Solution:

The GL-H14 has universal operating capability. This system can be used to intercept communications from any GSM service providers in the world irrespective of the type of encryption being used.

System supports both A5/1 and A5/2 encryption algorithms which are widely deployed on GSM Networks. The system is equipped with a Kc Retriever to obtain the Kc (Ciphering Key) from the network. As soon as the system GL-H14 identifies that the target communication-taking place is using encryption, the Kc retriever in the system becomes active. The Kc retriever automatically acts as a genuine BTS and forces the suspects mobile to register with it, during the periodic location update. The Kc retriever communicates with the suspects mobile using A5/2 encryption, in the process GL-H14 calculates the Kc. The Kc retriever also asks the mobile to authenticate itself with its IMSI, by doing so the system obtains the suspect's IMSI.

Both the Kc and IMSI information is stored in a data base. With the Kc in the database the system can now decipher all communications encrypted using A5/1 or A5/2.

The GL-H14 system does not require the service providers SIM for operation.

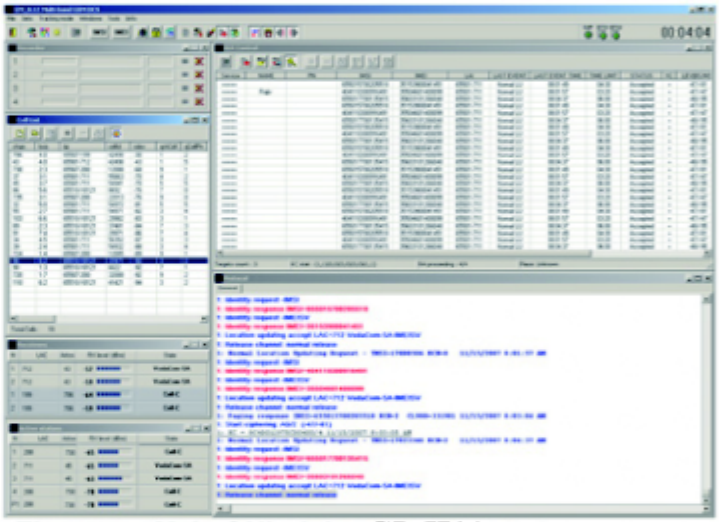

Figure 2 – Main GUI of the GL-H14

Unlike the other active system where the monitoring agency is billed for the forwarding of target's calls, which can raise suspicion for the target due to reduced bill amount (since the call charges are borne by the monitoring agency). The GL-H14 system deciphers A5/1 and A5/2 ciphering algorithms online.

The number of channels, being received and recorded by the system, can be from 4,6,12 for one control computer.

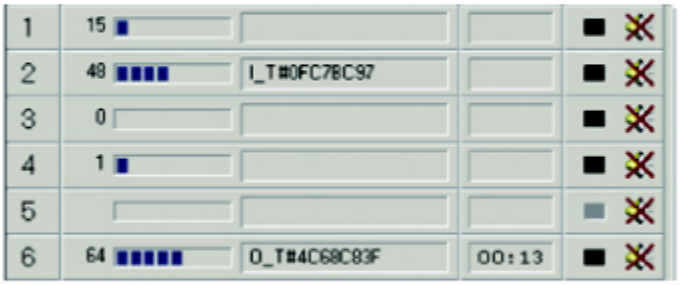

Figure 3 – Recorder Window

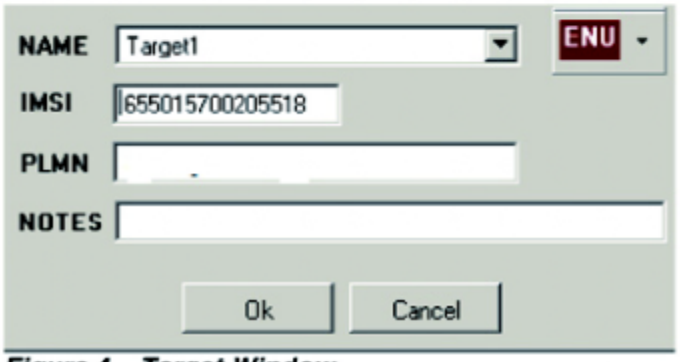

Figure 4 – Target Window

Features:

- Real-time monitoring of GSM communications encrypted using A5/1 and A5/2 Ciphering algorithms.
- Universal Operating Capability – The system can be used to intercept communications from any GSM service providers in the world.
- 100% target call monitor rate: The system can monitor all communications of the target (SMS and Voice) till he/she is within its coverage range.
- The system is capable of extracting the Suspect's actual Mobile Number from the network without any help from the service provider.
- The system can be configured to ignore certain subscribers from being intercepted. This is particularly useful in case of ignoring the operator's cell phone during an operation.
- The system features a selective jamming capability, using which the operator can disable certain services of the suspect like Outgoing Call, Incoming Call, SMS, SS etc. can be jammed.
- The system does not require the service providers SIM for operation
- System provides flexibility for the system operator to modify the ID of selected targets for both incoming and outgoing calls.
- System provides flexibility to the system operator to Make fake call (or send Fake SMS) to target.
- System allows to the system operator to make call (or send the SMS) using target identity
- Inbuilt automatic paging to obtain suspect related information
- No limit on the number of suspects that can be added to the target list.
- Target list can be created using PLMN, IMSI or Suspects Mobile Number.

- On line monitoring up to 12 duplex channels.
- Interception Monitoring and logging of GSM-850/900/1800/1900 communication standards in stationary or in mobile environments.
- Can Handle Latest Non-Supporting A5.2 phones including iPhone, Blackberry etc. with the latest A5.1 Decryptor.
- Can Intercept Voice and SMS communications form a 3G network by forcing 3G mobiles to communicate using 2.5G
- Monitoring of both forward and reverse channels (duplex conversation).
- Direction Finding Equipment can be integrated with the system.
- On-Line listing of the intercepted Cell phone calls.
- Possibility of round-the-clock operation in an auto mode without the operator involvement.
- Provision of reliable reception of the information from channels of cellular communication systems with possibilities of noise-resistant coding.
- The called party or the suspect will not see any change in caller ID (CLI).
- The system can monitor both Incoming and Outgoing calls.
- The system maintains the encryption being used by the network.
- The system is transparent to the suspect and the Service Provider.
- Simplicity of maintenance, which does not require a deep knowledge, either in the field of computers, or in the field of cellular communication systems.
- Several GL-H14 systems can be configured in a LAN environment.

A 5.1 Decryptor:

Why A5.1 Decryptor? As mentioned earlier, the system communicates with the suspect's mobile using A5/2 encryption. This is irrespective of whether the network uses A5/1 or A5/2 encryption. Once the ciphering key is calculated, the same key is used by the system to decrypt the communication taking place between the suspect's handset and the network. There are certain mobiles in the market today that does not allow communication using A5/2 encryption. If the mobile does not support A5/2 the system will not be able to calculate the ciphering key and hence we will not be able to intercept the calls. This is true with certain latest model of handsets in the market today. These handsets include all the Latest Versions of Nokia,

Samsung, Motorola, Iphone, Blackberry etc.

To intercept such type of mobiles we need an additional A5/1 decryptor that can communicate with these mobile and calculate their ciphering key.

Figure 5 – A5.1 Decryptor

How does it work? GSM Interception System sends to A5/1 decipher encrypted bit stream – usually one Encrypted burst derived from forward (down link) channel. A5/1 decipher calculates ciphering key Kc and sends it back to the GSM interceptor. GSM interceptor implements Kc and decrypts communication which with known Kc is almost immediate process. GSM Interceptor and A5/1 Decipher can be connected either directly by USB cable or wirelessly using any available communication means (GPRS, UMTS, satellite link, etc.).

A5/1 decipher can serve more than one GSM Interception Systems. It is a typical server-client appilcation. Usually A5/1 decipher is located in a head quarter connected to Internet with static IP address while GSM Interception system can be located virtually in any place of the world.

The use of the A5.1 decryptor will ensure that the system supports latest handsets including all the Latest Versions of Nokia, Samsung, Motorola, Iphone, Blackberry etc.

Features:

- Option for connecting multiple GSM monitoring systems (up to 5) with one decryptor
- Average deciphering time: 2.88 sec (Real-Time option also available)
- Max deciphering time: 5.76 sec
- Probability of deciphering: 100% with BER=0
- Connection to GSM Interception System: USB or wirelessly
- Operating Temperature Range: +50^0 C to +35^0 C
- Storage Temperature Range: 20^0 C to +60^0 C
- Humidity: +40^0 C at 95% humidity
- **Power Supply:110/230 V AC+10%**
- **Power Consumption:230W**
- **Dimensions:350X310X60 mm**
- **Weight:4.5kg**

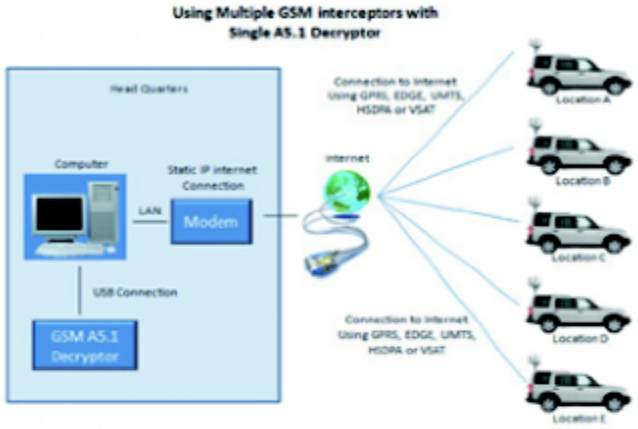

Figure 5 – Using Multiple GSM Systems with Single A5.1 Decryptor

Figure 6 – IMSI Analysis Software.

IMSI Analysis Software

IMSI Analysis – IMSI database contains all the existing service providers in the world. This database contains information like Country Code, MCC, MNC, Operator Name, Operator Region, Network Name, technology (GSM 850/900/1800/1900). Based on the first 5 Digits of the IMSI this software will tell you which country and which service provider does the SIM belongs to. This is very useful when you are monitoring suspects who are visiting your network from foreign networks. By analyzing his IMSI you will be able to know his home network.

Advance Database Management Software

Module for Passive GSM Monitoring System

The Advanced Database Management Software offers verity of features, which will enable the operators to efficiently use the intercepted data.

Features:

Customized Search: Extensive search feature enabling the users to search call database based on different call parameters that they are available off the air. Search based on – Dialed number, Received Number, IMSI, TMSI, IMEI, Called date, IN/OUT, BCCH, encryption, Class Mark (Mobile Mode) etc.

Keyword Spotting in SMS: The system has the capability of sporting keywords within the received SMS messages. For example if you want to list all the SMS that has the word "MONEY". You can create a query and the system will list all the SMS that has that

particular word.

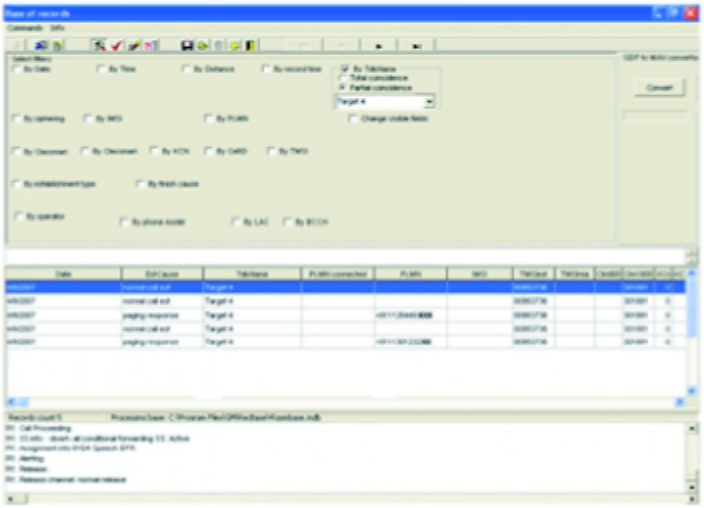

Figure 7 – Advanced Analysis Package

Optional Accessories

Power Amplifier:

Specially designed software controlled power amplifier which will work in conjunction with the BTS to increase the range of the system. The amplifier is suitable for single and Multi-Channel GSM base station. Amplifier utilizes linear LDMOS power devices that provide excellent Linearity and low distortions, high gain, and wide dynamic range. Exceptional performance, long term reliability, and high efficiency are achieved by employing advanced matching networks and combining techniques, EMI/RFI filters, machined housing, and qualified components.

Features

- Max. Power Output : 40Watts
- Solid-State linear design
- 50 Ohm Input / Output impedance
- Weight: 12Kg
- Dimension: 19" x 3.5" x 18"
- High reliability and ruggedness

Figure 8 – Power Amplifier.

High Gain Antenna:

We provide specially designed high gain directional sector antenna's to our customers in different size depending upon the gain and application.

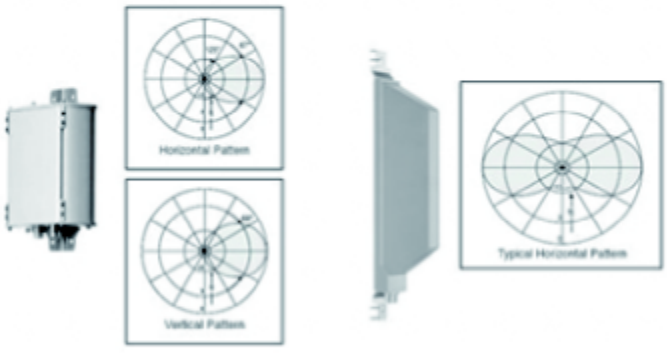

Figure 9 – Typical High Gain Antennas.

Car Kit:

For the deployment of the system in mobile application it's very important to integrate the supplied equipment in car. Improper integration may lead to unstable operation and the desired results cannot be achieved. To overcome from the above situation we have designed special car kit containing the following items.

Shock Proof 19" Rack

Specially designed for vehicular use, the 19" shock proof rack has a unique and integral suspension system. The rack is specially tested for vehicles that are required to operate on rugged terrains.

Small Camouflaged Antenna Bumper Antenna

These are receiver antennas mounted on the front and back bumper of the car. These antennas designed to achieve optimum efficiency even though they are hidden away.

Power Accessories

The power accessories include Inverter (1500 VA)/Battery **Charger, Battery Combiner, Battery Monitor, Circuit Protector etc. Developed for professional duty,the inverters is suitable for the widest range of applications.** The design criteria have been to produce a true sine wave inverter with optimized efficiency but without compromise in performance. Employing hybrid HF technology, the result is a top quality product with compact dimensions, light in weight and capable of supplying power, problem-free, to any load.

Figure 10 – Car Power Accessories.

Special RF Shielding

Special RF shielding cloths are installed in the vehicle to protect the operators from any potential health hazard that might occur due to prolonged exposure to high power electromagnetic radiation.

Figure 10- *Typical Example of System Installed in a Car.*