IBIS

(In-Between Interception System)

Product Description

Fast and reliable interception, interrogation and jamming of GSM traffic

- Interception for Incoming and Outgoing encrypted GSM communication including A5/1 in real-time and without cooperation with network operators
- Interception for multiple concurrent duplex calls
- Selective jamming capabilities
- Extracting phone identities including IMSI, IMEI and MSISDN
- Making and receiving calls and SMS on behalf of target phones
- Invisible and undetectable operation
- User-friendly operation

Ability Limited

Suite 813, 8/F Hollywood Plaza, 610 Nathan Road, Hong Kong
Tel. (852) 8199 0412, email: sales@ability.hk

Table of Content

Notice

IBIS

(In-Between Interception System)

1. Introduction

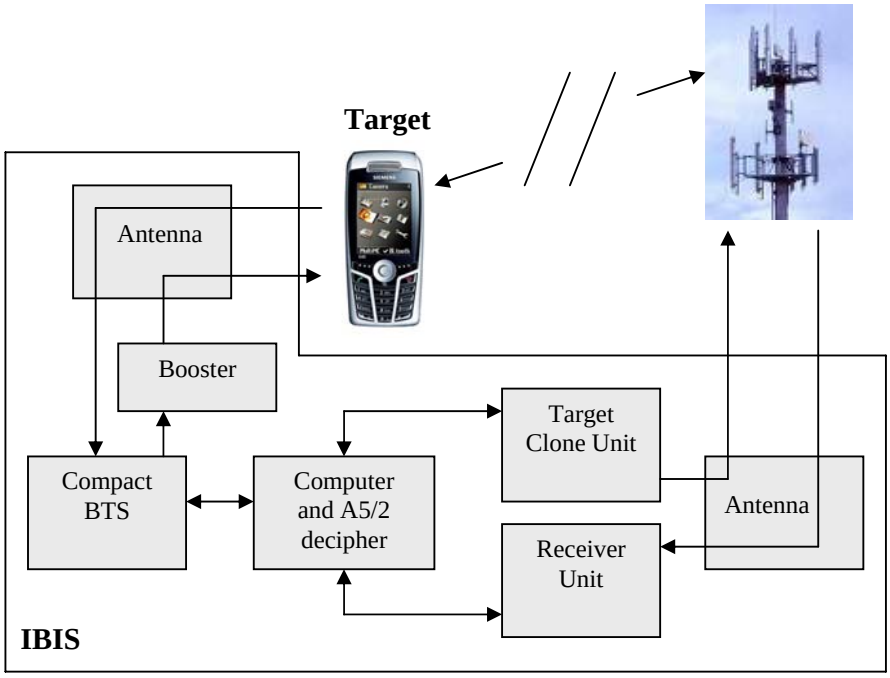
This document provides product description and technical characteristics of IBIS. It generally explains its features, capabilities, operational modes and applications.

2. System overview

IBIS consists of following parts:

1. Compact BTS
2. Target Clone Unit
3. Receiver Unit
4. Notebook computer with A5/2 decipher
5. Booster
6. Two antennas

Functional diagram of IBIS is represented bellow:



3. Operational overview

It is a true Man-In-The-Middle (MitM) attack on GSM communication which is fully implemented in the IBIS.
Compact BTS forces GSM phones in its vicinity to register with it. Using of booster and directional antenna helps to increase operational range of the system. Compact BTS requests mobile phones to introduce themselves, i.e. to send their identities – IMSI and IMEI. During the registration and authentication process compact BTS requests mobile phones to implement encryption A5/2 which they do. Real-time A5/2 decipher decrypts the information exchange and calculates Kc (ciphering Key). From this moment IBIS can fully imitate target's phone and talks with GSM network on its behalf.
So the target communicates with compact BTS which poses to be a real GSM network. The real GSM network talks to clone of the target phone. Computer collects information from the compact BTS and the clone. Such a scheme makes possible interception of incoming and outgoing calls, SMS messages, DTMF tones and all call related information transmitted over the air.

4. Operational Applications

- Off-Air Interception
- IMSI/IMEI catching
- Selective jamming of communication
- Presence verification
- Data Analysis
- Direction Finding Support

5. What is in the package?

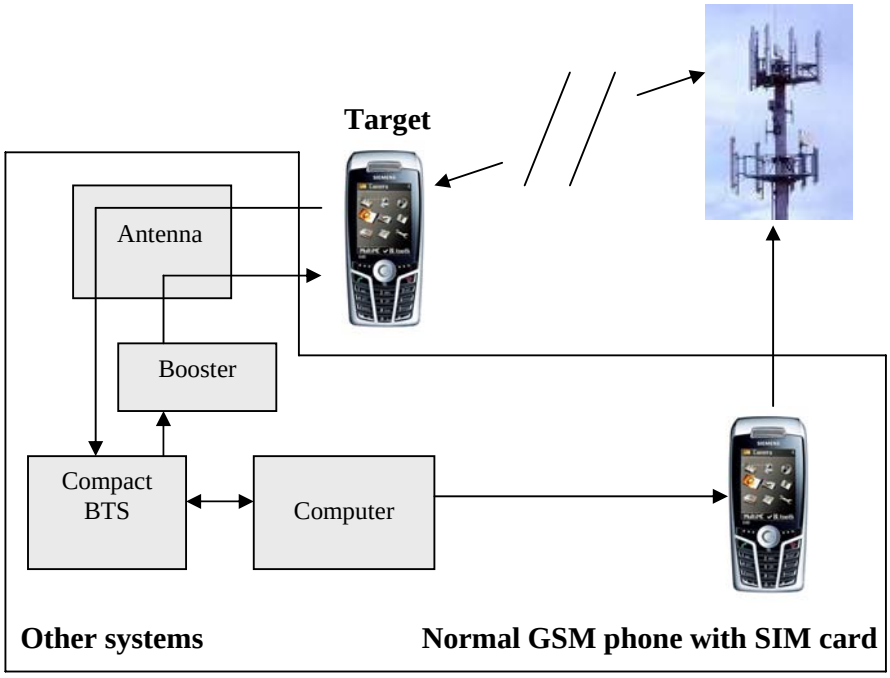
- Receiver Unit
- Notebook Computer with preinstalled interception software and A5/2 decipher
- Target clones Unit
- Booster
- Two planar directional antennas
- Carrying Case
- Special Phone for silent call
- Nokia phone with Net Monitor
- Set of Cables
- User's Manual
- Software Backup

6. Comparison between IBIS and other known active systems in the market

There are two major distinctions making significant difference between IBIS and all other known active systems in the market:

- ability to clone target phone
- using A5/2 decipher for ciphering key calculation

Bellow is functional diagram of all others known active systems.



Not having such features all other active systems are only able to force mobile phones to register with faked BTS and identify themselves. While operating well as IMSI/IMEI catchers they are not able to efficiently intercept communication.
The table bellow compares IBIS with other active systems:

Comparison Table

Features	IBIS	Other active systems
Does the system disconnect mobile phones from real network?	No	Yes There are no incoming calls and SMS at all.
Does the system downgrade GSM encryption?	Yes From A5/1 to A5/2	Yes From A5/1 to A5/0 (i.e. to non encrypted mode)
Does the system relay Caller ID of intercepted phone?	Yes	No
Does the system need SIM card to operate?	No	Yes
Number of simultaneously intercepted calls	Up to 6	1

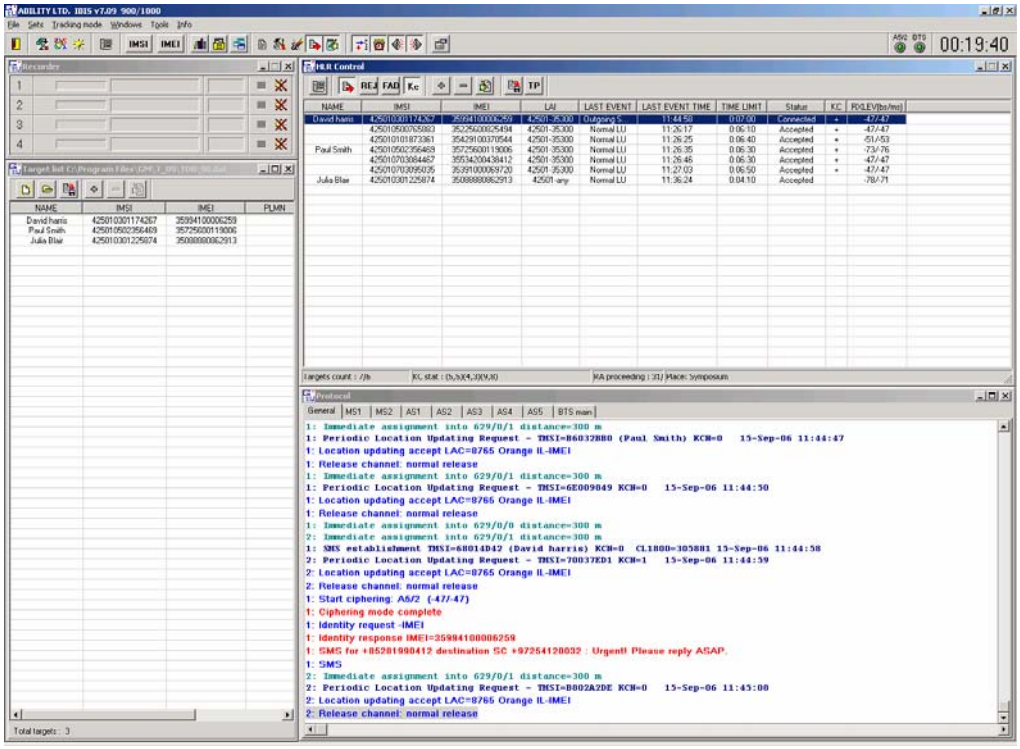
Conclusions

Can the system intercept incoming calls?	**Yes**	**No** Since there is no incoming communication at all
Can mobile phone be intercepted during long period of time?	**Yes**	**No** Target cannot be held without incoming communication for a long period of time
Is the interception undetectable?	**Yes**	**No** 1. Most of the phones alert users when they are working in non encrypted mode 2. Caller ID is never relayed
Can several conversations be intercepted simultaneously?	**Yes**	**No**

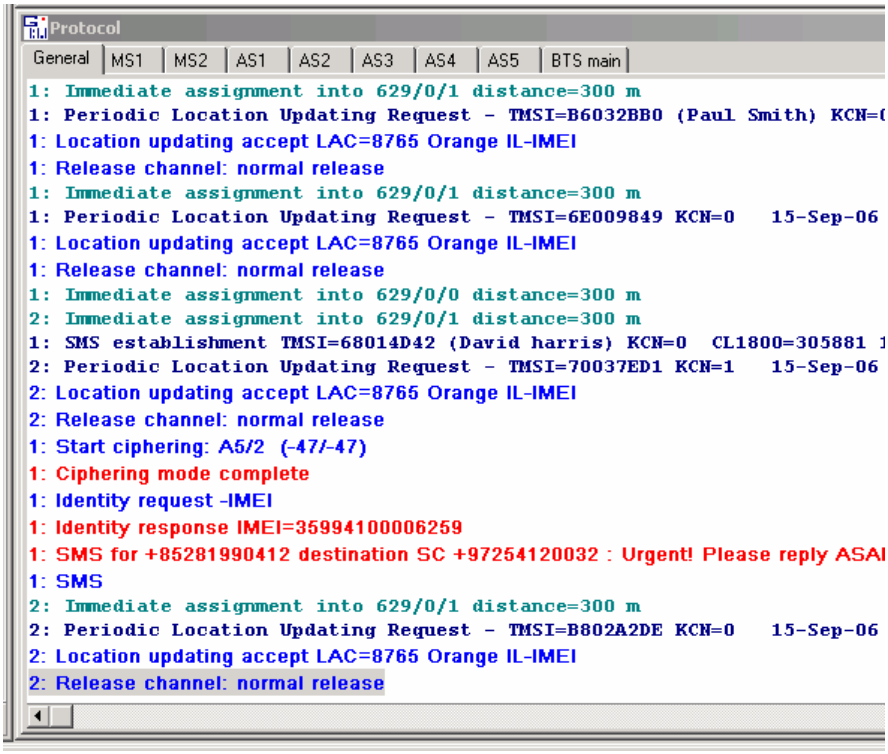
Ability Limited

Suite 813, 8/F Hollywood Plaza, 610 Nathan Road, Hong Kong
Tel. (852) 8199 0412, email: sales@ability.hk

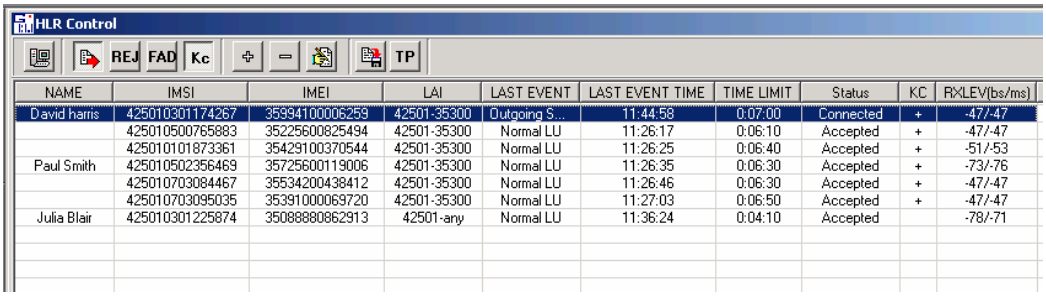
7. Screen shots



Main screen

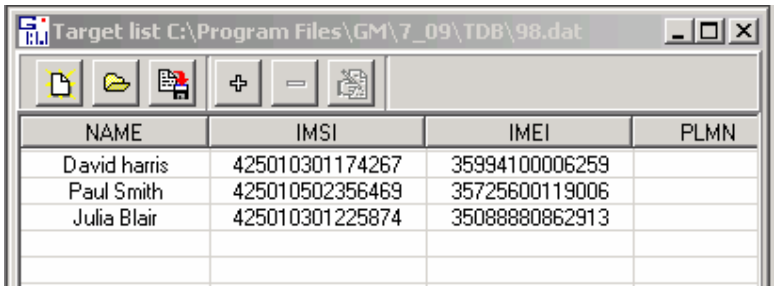


Protocol screen



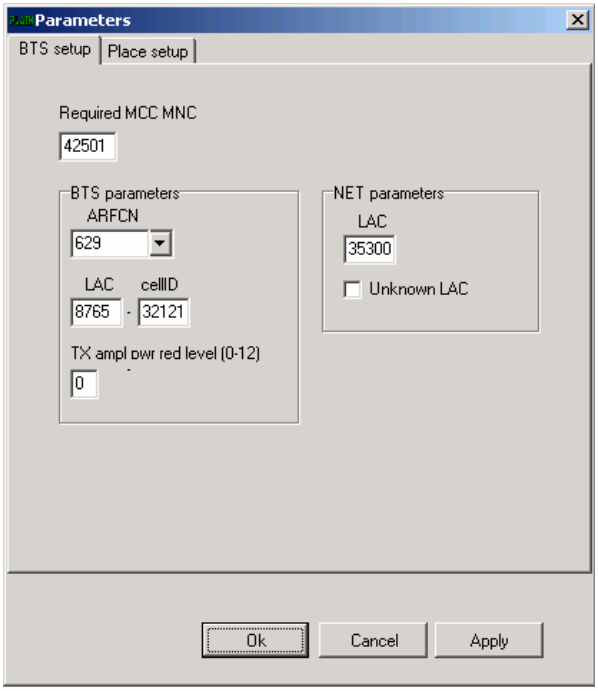
NAME	IMSI	IMEI	LAI	LAST EVENT	LAST EVENT TIME	TIME LIMIT	Status	KC	RXLEV(bs/ms)
David harris	425010301174267	35994100006259	42501-35300	Outgoing S...	11:44:58	0:07:00	Connected	+	-47/-47
	425010500765883	35225600825494	42501-35300	Normal LU	11:26:17	0:06:10	Accepted	+	-47/-47
	425010101873361	35429100370544	42501-35300	Normal LU	11:26:25	0:06:40	Accepted	+	-51/-53
Paul Smith	425010502356469	35725600119006	42501-35300	Normal LU	11:26:35	0:06:30	Accepted	+	-73/-76
	425010703084467	35534200438412	42501-35300	Normal LU	11:26:46	0:06:30	Accepted	+	-47/-47
	425010703095035	35391000069720	42501-35300	Normal LU	11:27:03	0:06:50	Accepted	+	-47/-47
Julia Blair	425010301225874	35088880862913	42501-any	Normal LU	11:36:24	0:04:10	Accepted		-78/-71

HLR screen

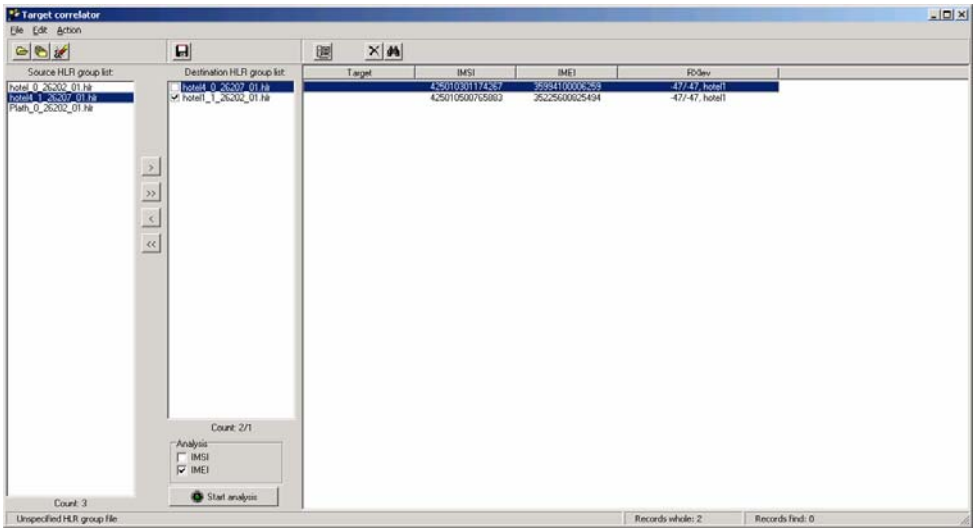


NAME	IMSI	IMEI	PLMN
David harris	425010301174267	35994100006259	
Paul Smith	425010502356469	35725600119006	
Julia Blair	425010301225874	35088880862913	

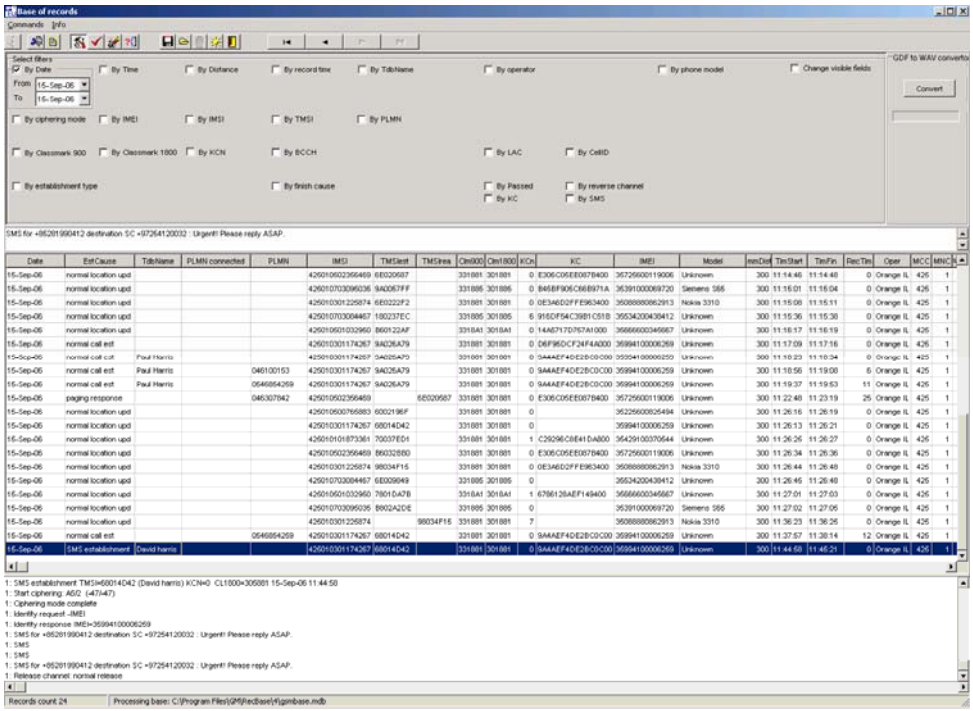
Target list screen



Parameters screen



Cross-compare screen



Data Base Screen

8. System features, Technical and Operational Characteristics

System Features:

Number of simultaneously monitored duplex channels	Up to 6
Voice and data recording on hard disk	Yes
Identities which can be interrogated	IMSI, IMEI, MSISDN
Voice codec types	LPT-RPE, FR, EFR, HR, AMR
Outgoing call number determination	Yes
Incoming call number determination	Yes
SMS messages interception	Yes
DTMF tones interception	Yes
Encryption types	A5.1, A5.2 , A5.3
Ability to interrupt ongoing calls	Yes
Ability to selectively prevent calls	Yes
Support Direction Finding devices	Yes
Making and receiving calls and SMS on behalf of target phone	Yes

Technical Characteristics

Working frequency bands	900/1800 MHz
Frequency stability of each receiver	±0.03 ppm
Sensitivity of each receiver	not worse than -103 dBm (signal/noise =20dB)
AGC – dynamic range	25 dB
Measurement of signal level – dynamic range	75 dB
Synchronization	Adaptive
Demodulator	GMSK
Error correction	Viterbi decoder
P_{out} of Compact BTS	200 mW (1800 MHz) 100 mW (900 MHz)
Booster parameters	18 dB, Max out +44dBm
Impedance of antenna input/output	50 Ohm

Ability Limited

Suite 813, 8/F Hollywood Plaza, 610 Nathan Road, Hong Kong
Tel. (852) 8199 0412, email: sales@ability.hk