go2INTERCEPT

GSM Interception ▪ IMSI Catcher and Voice Interception

Part of the product line   go2SIGNALS

go2INTERCEPT passive:
GSM interception –
Passive, massive, of the air.

(page 3-4)

go2INTERCEPT active basic:
IMSI catcher –
Identify, control, locate, 2G, 3G.

(page 5-6)

go2INTERCEPT active extended:
IMSI catcher and voice interception –
Intercept, control, track, 2G, 3G.

(page 7-10)

Part of the product line   go2SIGNALS

go2INTERCEPT passive:
GSM interception –
Passive, massive, of the air.

The go2INTERCEPT passive off the air GSM interception unit is able to intercept the communications between the handset and the BTS.
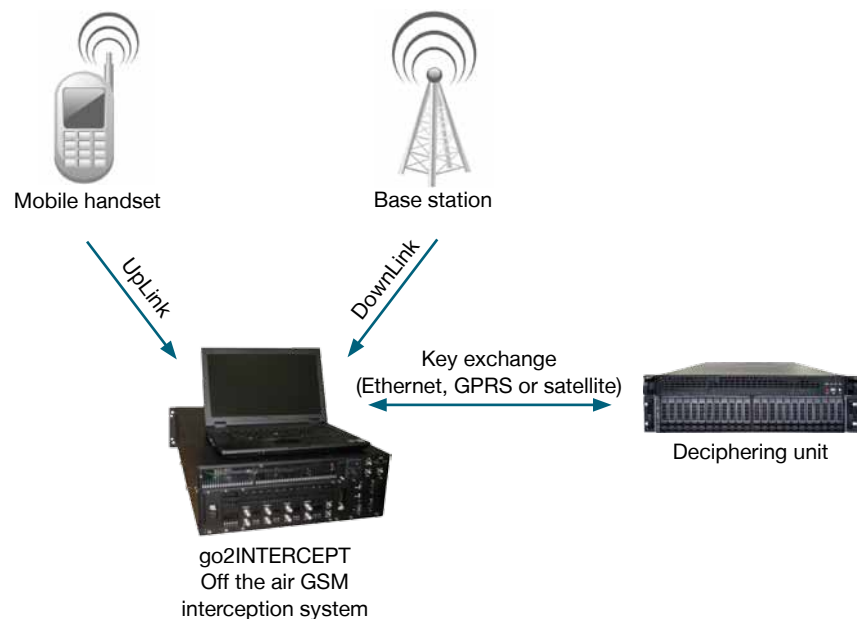
It is a wide band (processing the whole GSM bands) and passive solution, meaning that absolutely nothing is sent to intercept. It makes this solution completely undetectable by the targets or the operators unlike active interception solutions in the markets. Thanks to its dense FPGA architecture, this solution is able to intercept up to 60000 communications per hour, which enables this solution to be suited for massive application (border control for example), the go2INTERCEPT (passive) is able to demodulate and decipher in real time up to 320 duplex communication.

Two versions of go2INTERCEPT (passive) are available either in a 2U format for low cost application (up to 20 full duplex simulta-neous communication) or in a 3U format to get the full power of the systems.

The front end can be connected to the deciphering box (go2DECIPHER) through ethernet connection using either Vsat, 3G or cable links. In the case of a powerful deciphering box, multiple front ends can be connected.

Key features

- 3U 19" rack device

- 2G and 2,5G

- SMS, data and MMS supported

- From 10 to 320 simultaneous voice interceptions

- Up to 60000 intercepted communications per hour

- Simple Ethernet interconnection to the deciphering box

- Can be used as a tactical equipment in vehicles

Mobile handset

Base station

UpLink

DownLink

Key exchange
(Ethernet, GPRS or satellite)

Deciphering unit

go2INTERCEPT
Off the air GSM
interception system

Filtering abilities

Once the intercepted communications are stored in the data base, the user friendly GUI proposes many filtering abilities (operators, services, target ...):

· Provider selection

· Cell selection: power and quality criteria

· Service selection: GSM, GPRS, SMS, In/Out call

· Target selection: TMSI, IMSI, IMEI, MS-ISDN

Passive off the air GSM interception front end

· Passive and wide band solution

· All GSM bands (GSM450, GSM850, EGSM900, DCS1800, PCS1900)

· Full band analysis: Simultaneous acquisition of all channels

· No limit on frequency hopping and real time handover management

· Up to 64 cells can be under surveillance

· Automatic cell detection

· Store telephone conversations on the hard drive

· Ability to listen to conversations in real time

· Optional speaker identification thanks to biometric voiceprint technique

Control and test

· Remote and local control

· Ethernet connection to the deciphering unit

· BITE

Operational / physical / electrical specifications

Technical parameters	2U version	3U version
Connection to deciphering unit	Ethernet (RJ45)	Ethernet (RJ45)
Number of simultaneous calls	20	128, 256 or 320
AC power	115/230 V AC ± 15 % 47-63 Hz	115/230 V AC ± 15 % 47-63 Hz
Consumption	300 VA	400 VA
Size	19" 2U	19" 3U
Weight	< 10 kg	< 27 kg
Operating temperature	0°C to +40°C	0°C to +40°C
Storage temperature	-40°C to +70°C	-40°C to +70°C

go2INTERCEPT active basic:
IMSI catcher –
Identify, control, locate, 2G, 3G.

The go2INTERCEPT active basic is a tactical equipment managing target identification and localization through their IMSI or IMEI on 2G (GSM - DCS) and 3G (UMTS) networks. Designed to be operated by non specialists, it can be used for mobile or fixed operations.
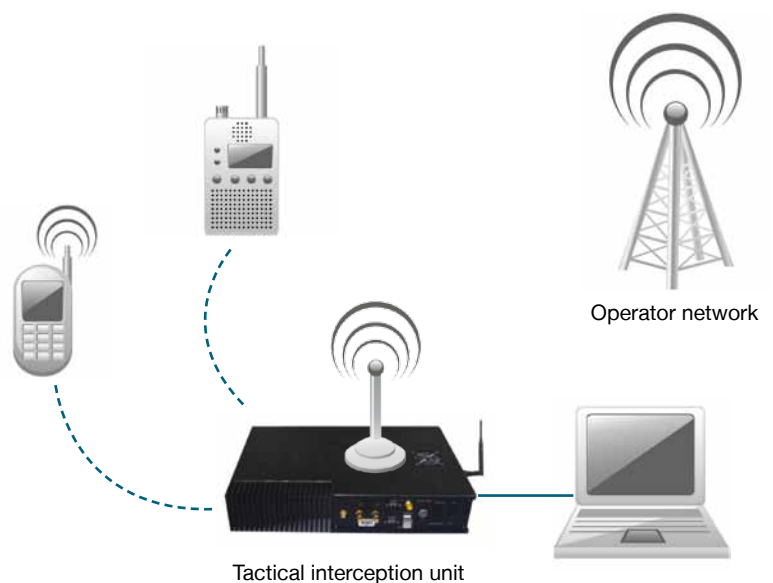

The equipment clones a neighboring cell (BTS or Node-B) with user controlled parameters, forcing the surrounding mobile equipments to identify themselves. Once identified, the mobiles can either be kept within the cloned cell for further intelligence, eavesdrop or send SMS in 2G, ringing the phone, released on the original network, disabling it.

Cell cloning is pursued thanks to an advanced automatic 2G and 3G spectrum scanner.

The front end can be connected to the deciphering box (go2DECIPHER) through ethernet connection using either Vsat, 3G or cable links. In the case of a powerful deciphering box, multiple front ends can be connected.

Key features

- Embedded power amplifier

- Multi-bands and multicells (GSM, DCS and UMTS)

- Fast 2G/3G scanner

- Target identification, target localization, SMS interception, SMS sending, mobile ringing for localization purpose, 3G -> 2G switch, mobile disabling, interception of called numbers, listening of environmental sounds

- Data mining with a on-line and off-line exploitation

Operator network

Tactical interception unit

Technical specifications

Mission Preparation	
Organisation	■ Use of predefined scenarios or manual configuration ■ Off-line & on-line mission creation ■ Automatic generation of scenarios from environment (quick start)
Mission options	■ Power ramp effect ■ Mission scheduler: multi clone start / stop ■ Ability to follow a moving target with continuous adaptation of clones to the environment (roaming)
Tools	■ 2G/3G fast scanning, advanced configuration & cloning tool ■ Clone coverage indicator

Catching	
Capacity	Multi-cells, multi-operators, multi-bands: GSM-900, DCS-1800, UMTS 900 and UMTS- 2100 (other frequency bands on request)
Action and data gathering	■ IMSI and IMEI ■ New contact / previously catched IMSI highlight ■ Multi localization ■ SMS (send / receive) (2G only) ■ Ringing for localization purpose (2G only) ■ Presence management (2G only) ■ Silent call for localization purpose ■ Blocking (2G only) / disabling of the mobile ■ Forcing target from 3G to 2G ■ Interception of called numbers (2G only) ■ Listening of ambient sounds (2G only) ■ Searching of mobile location with display on a map

Administration	
Station	Semi-ruggedized laptop
Post-analysis	■ Inter-case / inter-mission search ■ Multiple catched IMSI and IMEI focus ■ Wild card search ■ Data base export ■ Eavesdropped SMS search / export ■ Display of Vortex-Air location when capturing
Contact identifications	■ IMSI & IMEI full or partial ■ Attributes (photos, notes, friends, enemies and associated actions [block, unblock, disable])
User profile	User restriction or full access

Packages	
Pack 1 - pedestrian: backpack configuration with enhanced battery autonomy	■ 2 omnidirectional antennas and 1 high gain directional antenna ■ 1 hot-swap battery (1.5 hour) with charger ■ Back rack
Pack 2 - vehicle: installation in a vehicle with enhanced autonomy and high coverage	■ 2 omnidirectional antennas and 2 high gain directional antennas ■ Lighter adapter
Pack 3 - fixed: monitoring and site protection	2 omnidirectional antennas and 2 high gain directional antennas

Physical specifications	
Dimnesion	400 x 268 x 80 mm
Weight	5.3 kg
Energy	110/220 V AC (power supply provided) or 9/24 V DC < 140 W

Power	
Amplifier	40W at 900 MHz, 60W at 1800 MHz, 100 W at 2100 MHz
Antenna output	10 W mean in the band, up to 20 W peak

go2INTERCEPT active extended:
IMSI catcher and voice interception – intercept, control, track, 2G, 3G.

The powerful intelligence tool allows effectively track targets activities by monitoring their most used device – their cell phone.

The IMSI catcher and voice interception system of go2INTERCEPT is a state-of-the-art system that was designed to monitor, track, manipulate and control cell phones both in GSM networks and 3G (UMTS) networks.

Key features

- Extract the phone identities – IMSI, IMEI, MSISDN
- Collect the identities (IMSI/IMEI) of all phones in area of interest
- Alert about presence of target phones in the area
- Blocks phone communication – for all phones or selectively
- Intercept multiple calls and SMS simultaneously in random and target mode (inbound and out-bound communication)
- Disconnect designated calls
- Reroute calls and SMS to designated destination

- Change the content of target SMS
- Send fake SMS to target, or on behalf of a target
- Locate phones/target position
- Disable GSM activated explosive devices
- Covers multiple GSM and 3G networks simultaneously
- Handles effectively any network encryption (A5.0, A5.2, A5.1, A5.3)
- Tactical design for intuitive operation, easy transport and fast deployment

Description

go2INTERCEPT (active extended) is designed to perform man-in-the-middle attacks for mobile phones over GSM (2G, 2.5G) and UMTS (3G) networks.

The system emulates a real cell (base station) attempting the surrounding phones to select and register to the fake cell. As a result, the system becomes the serving cell of the surrounding phones (all pho-nes or only designated phones) and consequently controls the phones communication.

As such, the system is used to extract the target identity, to track the target location, to monitor the target communication and to manipulate the target phone in advanced methods.

Typical applications

Calls and SMS interception

go2INTERCEPT (active extended) conducts seamless interception of target inbound and outbound and SMS over GSM networks with-out cooperation or authorization from the GSM operator. The system can monitor as much targets as required and hand-le multiple live calls simulta-neously.

Calls and SMS manipulations

Besides of monitoring the target calls and SMS, the system allows to manipulate the target communication in various ways:

- Block or disconnect specific or all calls and SMS-messages of any target.

- Send fake SMS messages (fake content and fake identity) to the target or on behalf of the target.

- Reroute calls and SMS from/to the target.

- Change SMS content that was sent from/to the target.

IMSI and IMEI extraction

The system allows to extract the identity of any phone in the area and also to alert about the presence of specific phones or targets in a certain area.

Denial-of-service

The system can block the communication of all phones in a certain area or to block the communication of only specific phones.

Find a target

The system force the phone to transmit a seamless signal. The phone signal is tracked by a dedicated receiver and allows getting closer to the target till final resolution of its position.

3G (UMTS) handling

Since interception is not possible over 3G networks, the 3G module generates a signal to the 3G phones that cause them to move to the GSM network.

Once the phone moves to the GSM network, the GSM module takes over and conducts the interception of the target as well as all other actions that are described above.

Main modules of the system

GSM modules

Each GSM module works on a specific band (e.g. 850, 900, 1800, 1900 MHz) and can emulate one GSM network at a time. It is possible to change the emulated network on the fly. If there is a need to work on several networks in parallel or the networks are using different bands, then several GSM modules are required in the system.

3G (UMTS) module

Each 3G module works on a specific band (e.g. 850, 1900, 2100 MHz) and can emulate one 3G network at a time. It is possible to change the emulated network on the fly. If there is a need to work on several networks in parallel or the networks are using different bands and/or multiple UMTS channels, then several UMTS modules are required in the system.

Routing modems

The modems in the system are used to reroute the calls of the target to the real GSM network and vice versa, in order to conduct full and seamless interception of the targets' inbound and outbound calls and SMS.

Software application and UI (User Interface)

Installed on a standard laptop, the software (SW) management application allows conducting all tasks related to the system, to monitor in real time the intercepted calls and to record all calls and interrogated information. The SW application includes also a back-office that presents all logged data and conduct applicable queries on the collected data.

Internal power amplifiers

To boost the transmission signal of the system, the system includes 4W integrated power amplifiers per each GSM module and 25W integrated power amplifiers per each 3G module.

Additional peripheral equipment that may be used with the system

go2DECIPHER

Most GSM networks are using A5.1 or A5.2 encryption protocol to enhance the privacy measures for its subscribers calls.

Yet, some networks allow calls to be conducted with no encryption (AKA A5.0) when the phone does not support the encryption protocol.

When A5.0 is allowed in the network, go2INTERCEPT (active extended) reduces all intercepted calls to A5.0 and does not need any external breaker, however, in cases were the network does not allow to reduce to A5.0, it will be mandatory to connect the system to an A5.1/A5.2 breaker that breaks in real time the encrypted key (AKA Kc) in order to allow the interception of the call or SMS.

The breaker can be located next to the system unit or remotely with any TCP/IP connection (i.e. LAN, WIFI, UMTS connection).

External GSM power amplifier

In certain cases when more transmission power is required to extend the effective range of the system, it is possible to connect 25W external GSM power amplifier.

External antennas

Various types of antennas can be deployed and used for the system operation. The selection of antennas depends on the operation scenario and the system setup such as magnetic omni-antennas when patrolling with a vehicle in and urban area or hi-gain directional antenna installed on a tripod or mast in a long-range operation.

System specifications

Technical parameters	Value
GSM frequency bands	850, 900, 1800, 1900 MHz
3G frequency bands	850, 1900, 2100 MHz
Simultaneous duplex channels	4, 6 or more
Simultaneous GSM BTS	2 or more
Simultaneous 3G BaseStations	2 or more
Interception of outbound calls	Yes
Interception of inbound calls	Yes
Interception of outbound SMS	Yes
Interception of inbound SMS	Yes

Technical parameters	Value
Detected identities	IMSI, IMEI, MSISDN
Voice codec types	LPT-RPE, FR, EFR, HR, AMR
Random & Target Mode	Yes
DTMF tones interception	Yes
Ability to handle 3G phones	Yes
Ability to locate target phones	Yes
Ability to change SMS content	Yes
Ability to interrupt calls	Yes
Ability to prevent calls	Yes

go2SIGNALS

... monitoring a connected world

go2DECODE

go2MONITOR

go2ANALYSE

go2RECORD

go2INTERCEPT

go2DECIPHER

PLATH AG

Stauffacherstrasse 65

3014 Bern

Switzerland

Tel: +41 31 311 6446

Fax: +41 31 311 6447

Email: info@go2signals.ch

Further information on www.go2signals.ch