REVELO

Detector of Mobile Phone Interception Systems

REQUEST A DEMO:
- Bring your own interceptor – we'll detect it
- Alternatively we may simulate any interceptor

Swiss Made SWISS MADE Swiss Made

SCG
Security & Counterintelligence Group Ltd.

REVELO

Detector of Mobile Phone Interception Systems

SCG Security & Counterintelligence Group Ltd

APPLICATIONS

- Detect attempts of mobile phone communication interception
- Protect premises and offices against industrial espionage
- Protect governmental premises against military espionage
- Privacy protection anytime & anywhere

INTRODUCTION

REVELO, the state-of-the-art Detector of mobile phone interception systems was designed to counter the extremely wide spread and increasing governmental / industrial espionage activities via passive and active mobile phone interception systems. Tactical mobile phone interception systems are mobile devices which are easily accessible in the security market. A mobile phone interception system is considered to be “active” or “passive”. Both systems are mobile and act in vicinity of the target (from 50 meters up to 1 km).
The active system simulates an operator or BTS (Base Transceiver Station) and takes-over all communication handling, a so called “man-in-the-middle” attack. The interception system transmits on the standard telecom operator frequencies.
The passive system intercepts the mobile phone communication without any transmission.
However, when the target handset is connected to the 3G network, both, the active and passive interception systems need to force the target to switch from the undecipherable 3G network to the decipherable 2G network. In this case, 3G frequency jammers are used to block the 3G mobile phone network, forcing the handset to 2G.

A mobile phone interception system allows to intercept the phone conversation and SMS, to retrieve the identification of the target and to locate the intercepted mobile phone. Furthermore the target’s incoming and outgoing calls may be blocked and the incoming or outgoing SMS may be withheld. The SMS content may be modified and a fake SMS may be sent (spoofing). In addition the target’s environment may be monitored by remotely activating the mobile phone’s microphone.

FUNCTIONS

- Detection of any new appearing or disappearing RF activity.
- Detection of parameter changes: power level, MCC Mobile Country Code, MNC Mobile Network Code, LAC Location Area Code, Cell-ID.
- Detection of 3G jamming activity.
- Detection of signal strength instability of an operator or interceptor (power levels drastically change once an interceptor appears or disappears).
- Detection of active interception systems even if the power levels are increased in extremely small steps in order to catch the target (hand-over from the current base station).
- Detection of LAC changes.
- Recording of all parameters in the history file and automatic comparison with new scans.

REVELO

Detector of Mobile Phone Interception Systems

SCG Security & Counterintelligence Group Ltd

SYSTEM DESCRIPTION

The mobile phone interception Detection System REVELO was designed to detect GSM and UMTS interception systems, IMSI catchers, undesired phone manipulations and fake GSM / UMTS networks.

The system REVELO scans all mobile phone frequency bands and detects any radio transmission activity of active interception systems as well as 3G jamming, a common technique used by active and passive systems.

All detected GSM / operators, including the interceptors are listed with their identification and transmission characteristics. They are compared to the database list of official telecom providers present in the specific geographic region.

The 3-level alarm (alerting by internal log, audio, SMS, email or popup) is configurable depending on the kind of detected activity, or a combination of detected activities. E.g. alarm level 1 would generally be triggered at the detection of a single suspicious activity, whereas level 3 would be triggered at the detection of multiple activities excluding any doubt of the presence of an interception system.
This feature excludes false alarms due to normal telecom operator activities.
All detected data is stored and available in the history for further investigation / analysis.

FEATURES

- **Mobile & permanent application:**
  The system is integrated in an easily transportable pelicase with the dimensions of an attaché case or for camouflaged appearance inside a Samsonite hand-luggage case. The system may be used occasionally during specific conversations / meetings or continuously for permanent espionage awareness.

- **Fast & easy system setup:**
  Within 2 minutes the system is fully operational and the initial scan is completed.

- **100% reliability:**
  The sensitivity of detection corresponds to an interceptor's sensitivity, i.e. the distance of detection is equal to the distance of interception. In other words, if the interceptor is located close enough to the target to intercept the communication or to remotely activate the mobile phone's microphone, - in this case REVELO will detect the interceptor's presence immediately.

- **Highest performance:**
  The system incorporates a state-of-the art technology which is able detect even the most advanced interception system applying smart procedures such as increasing the transmission in low-level power steps in order to stay undetected.

- **Instant alert on mobile phone:**
  As soon as interception activity is discovered the alert will be indicated in the internal log and also by sound. The alert may be transmitted to predefined numbers by SMS or email as well as a popup via Wi-Fi to compatible phones (Android).

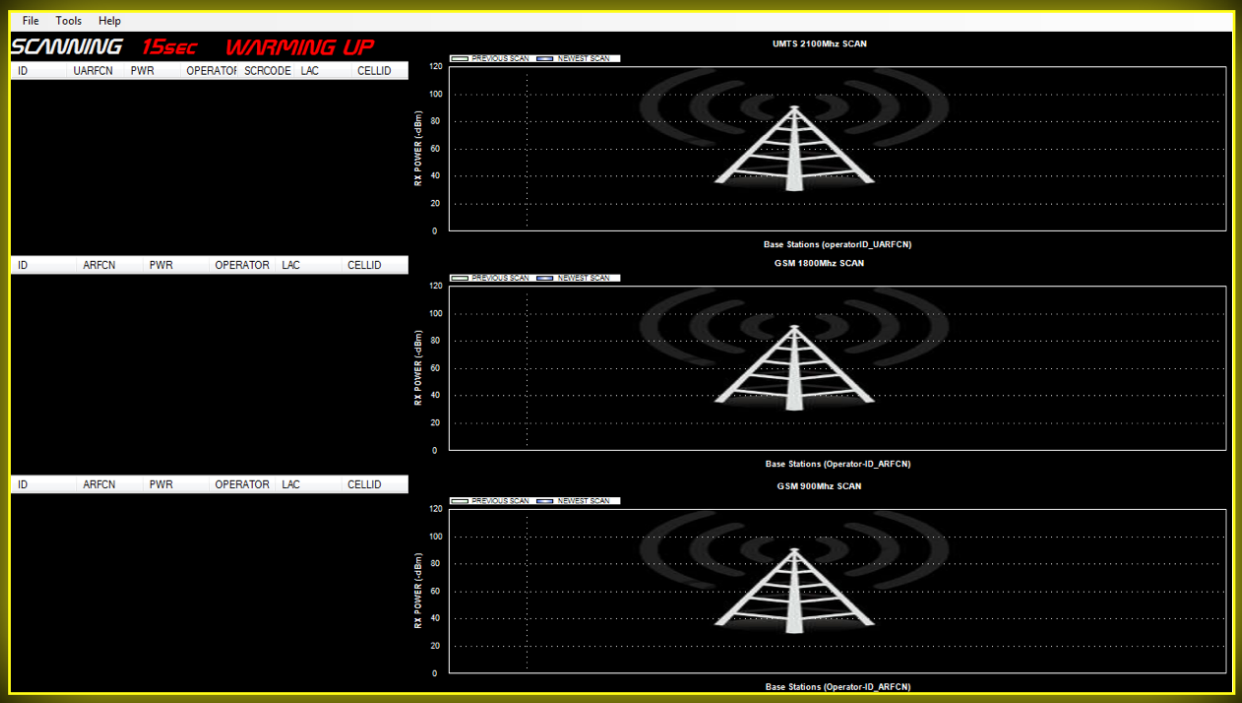
- **Remote controlling / management by AdHoc Wi-Fi network :**
  In order to offer complete discreetness and mobility, REVELO may be controlled via mobile phones running Android / iOS and iPad. REVELO integrates a dual band (2.4 GHz and 5 GHz) Wi-Fi card to establish a secured Wi-Fi network between the mobile device and the REVELO system. The complete User Interface is displayed on the mobile device and all alerts and functions may be controlled at distance.

- **Storing of monitored spectrum:**
  Scanned spectrums are recorded with the specific geographic location (GPS). When returning to the same location the radio frequency spectrum is automatically compared and suspicious changes are immediately recognized.

PROCEDURES

SCANNING

The RF environment of each mobile phone frequency band is permanently scanned and compared to the previous measured values, in order to detect suspicious network activities. All measurements are stored in a database for further analysis and comparison.



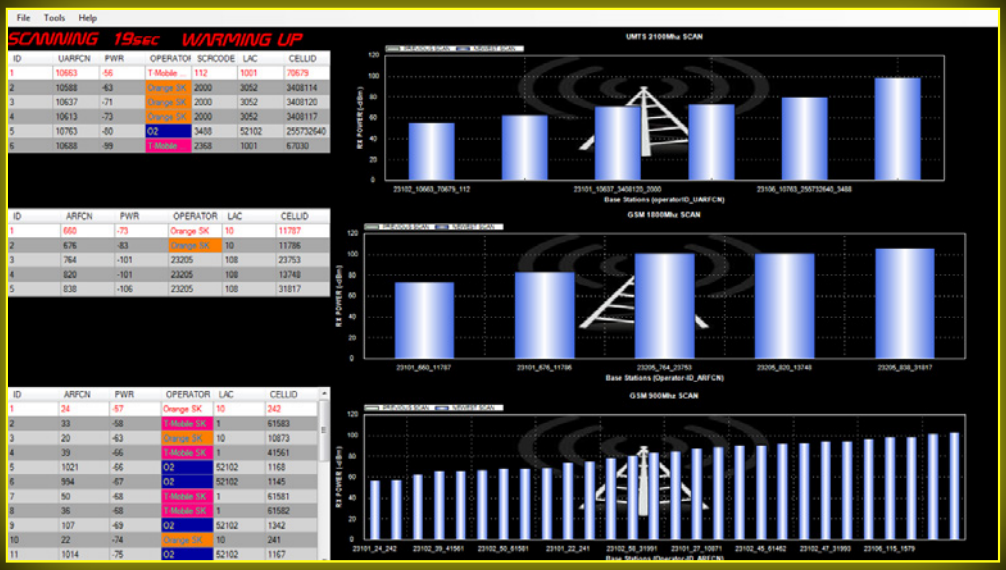
In order to guarantee fast scanning the system integrates two RF scanners, one for the 3G band and one for the 2G bands GSM 900 / GSM 1800 (resp. GSM 850 / DCS 1900).

Due to the larger number of GSM base stations in the 2G bands, compared to the 3G band, the scanning of the 2G bands requires more time.

As shown on the right, the 3G band indicates all detected operators, whereas the 2G bands are still being scanned.

IDENTIFICATION OF DETECTED OPERATORS

Within 2 minutes all operators in the detected range are listed with their identification and parameters such as UARFCN, resp. ARFCN (Ultra / Absolute Radio Frequency Channel Number), PWR (Power Level), OPERATOR, SCRCODE (Scrambling Code), LAC (Location Area Code) and the CELL-ID.



In this case the operator with the MCC (Mobile Country Code) and MNC (Mobile Network Code) 232 05 is not yet identified.

The internal database is used to identify each operator.

In this case the operator 23205 belongs to Orange Austria which will be identified and indicated during the next scan.

MONITORING OF ALARM EVENTS

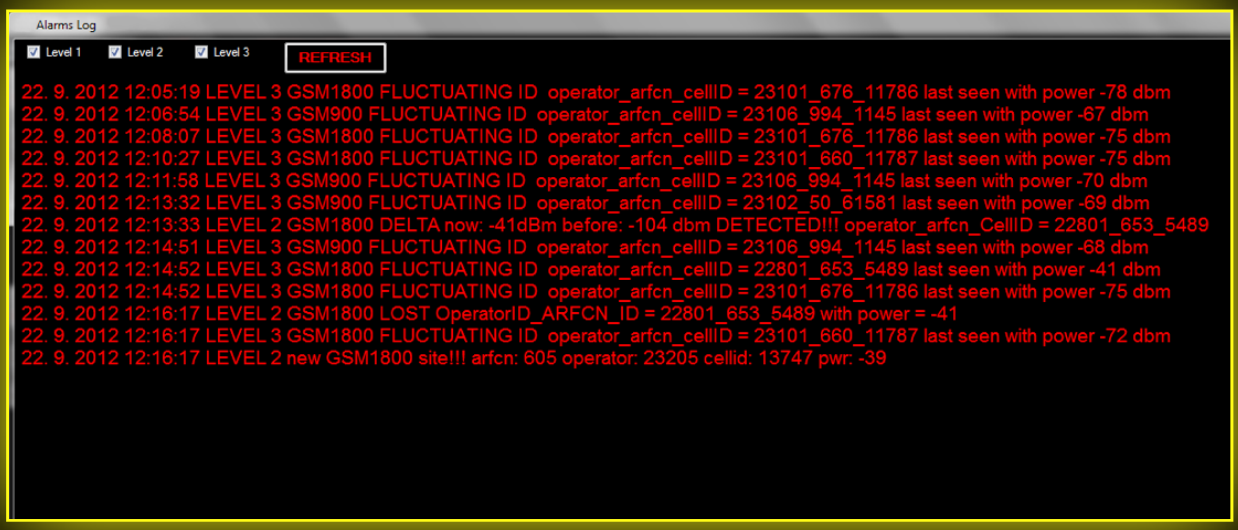
The system is analysing any operators / BTSs that appear and disappear.

Visible in the internal log, the detection of appearing or disappearing operators will trigger the Alarm Level 2 (alarm levels depending on detected activities are customised to the user's requirements).

The screen below indicates the appearance of the operator identified as ARFCN 605 MCC MNC 23205 and the disappearance of the operator identified as ARFCN 653 MCC MNC 22801.

Both operators are identified as fake base stations (interceptors) as regular telecom operators do not appear and disappear suddenly (especially a sudden appearance with a strong transmission power level of -39 dBm or a sudden disappearance with a previously strong power level of -41 dBm).

Both detected activities are triggering Alarm Level 2 (selectable).



REVELO

Detector of Mobile Phone Interception Systems

SCG Security & Counterintelligence Group Ltd

DETECTION OF CHANGE OF LAC AND POWER LEVEL

The alarm log lists the alarm “level 1” due to a change of the LAC “DELTA LAC” and the alarm “level 2” due to an abnormal change of the power level “DELTA POWER”.

DETECTION OF INTERCEPTOR FAKING IDENTITY

The interceptor’s attempt to fake the operator or BTS (Base Transceiver Station) with the MCC MNA 232 05 and ARFCN 807 (Orange Austria) is immediately detected.

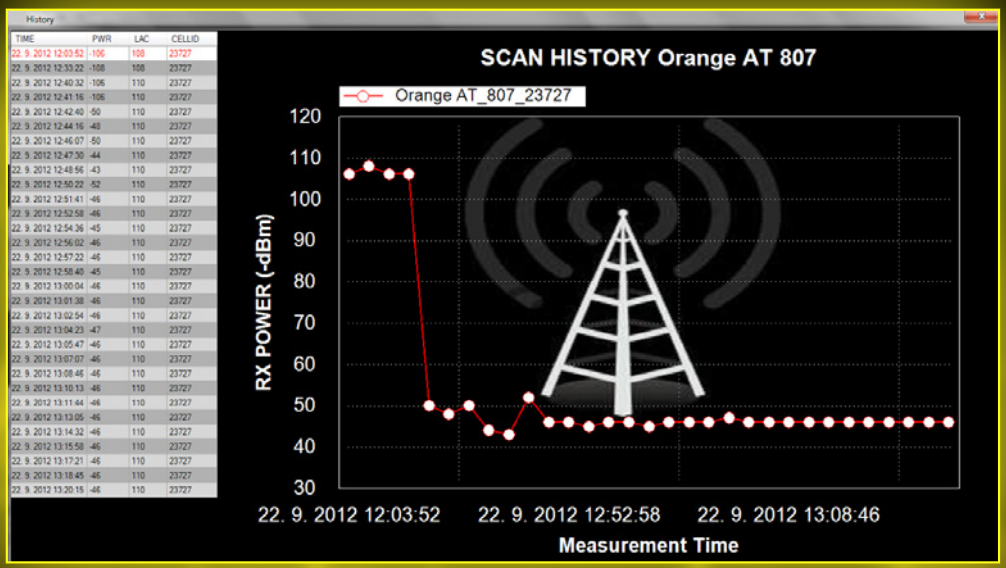
This “faking” operation requests the change of the LAC (Location Area Code) which is instantaneously discovered and indicated by REVELO.

SUMMARY OF INTERCEPTOR ACTIVITY

Following the alert all characteristics of the interceptor are summarized.

The diagram below shows how the original power level increased from -106 dBm (of Orange Austria) to -46 dBm once the interceptor faked the telecom provider’s identity.

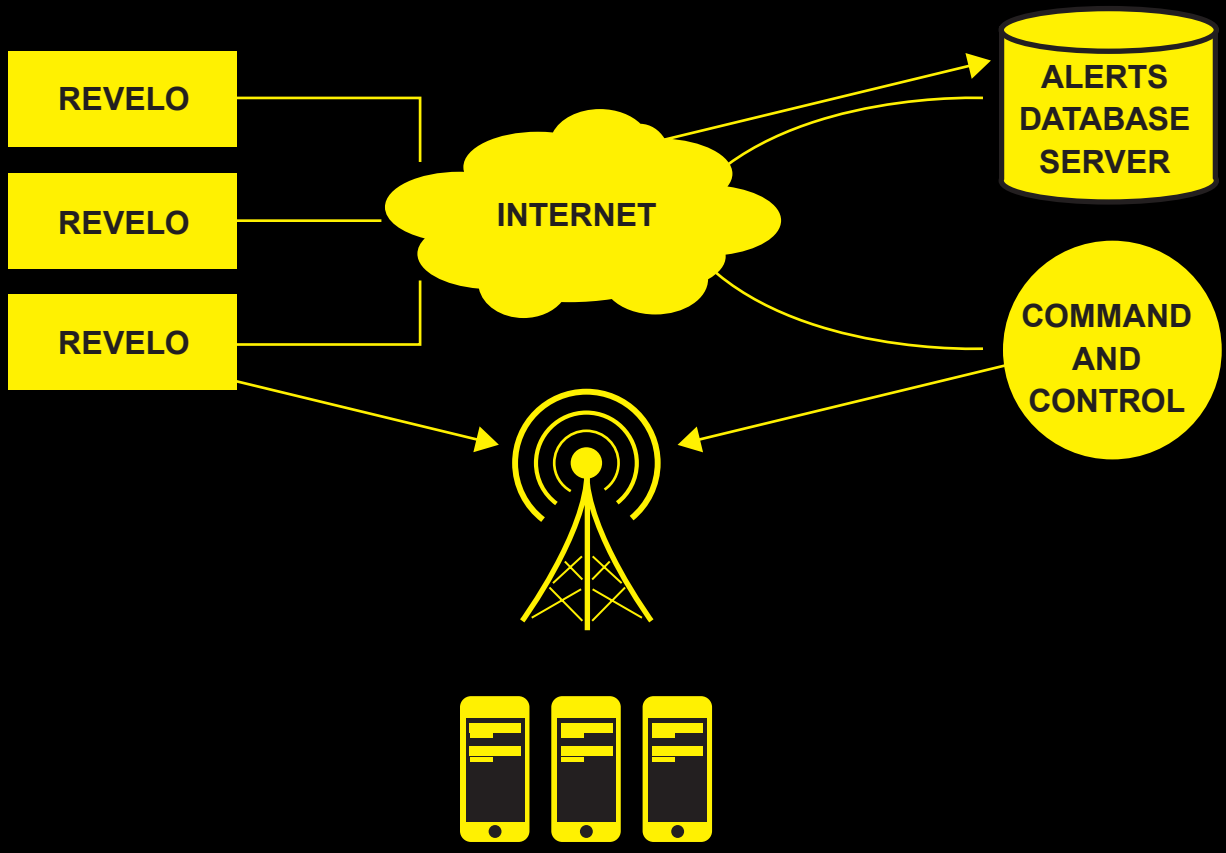
The table also shows the change of the LAC.



COMMAND & CONTROL CENTRE (OPTIONAL)

Applying multiple REVELO detectors, the source of the interception attack may be located and indicated on a map.

All scanned and detected activities of the multiple detectors may be centralized on a server and accessed by Internet via a secured VPN tunnel.



COMPONENTS:

- Central server
- REVELO Detection Systems with integrated GPS
- Network Router with LAN, 3G and 4G transmission

TECHNICAL SPECIFICATIONS

Power supply: 230 VAC / 12 VDC, including cigarette lighter connector
Autonomy: 8 h with internal rechargeable batteries
Operation temperatures: -10°C to +55°C
Dimensions: 40 x 34 x 23 cm
Casing: water / shock proof pelicase or Samsonite hand luggage
Wi-Fi: 2.4 GHz / 5 GHz dual band

Antennas:
VSWR GSM / UMTS antennas:

- 900 MHz: ~ 1.55
- 1800 MHz: ~ 1.66
- 2100 MHz: ~ 1.37

GSM / WCDMA antenna gain: 2.2 dBi
GSM / WCDMA antenna connector: SMA male
GPS antenna gain (optional): 26 dBi at 3V, 28 dBi at 5V
GPS antenna connector (optional): SMA Male
GPS frequency (optional): 1575.42 MHz

Data service (optional):

- HSDPA UL 384 Kbps, DL 7.2 Mbps
- WCDMA UL/DL 384 Kbps
- EDGE UL/DL 236.8 Kbps
- GPRS UL/DL 85.6 Kbps, CSD 9.6 Kbps

Notebook Lenovo X121e:

- 6 cell battery
- 11.1“ display
- MS Windows 7 pro (64bit)
- 4 GB RAM
- Intel i3 processor
- F5521 mobile broadband modem
- Intel HD graphics

OPERATIONAL BANDS

System	Band	Uplink (MHz)	Downlink (MHz)	Channel number
GSM-850	850	824.2–849.2	869.2–894.2	128–251
P-GSM-900	900	890.0–915.0	935.0–960.0	1–124
E-GSM-900	900	880.0–915.0	925.0–960.0	975–1023, 0-124
R-GSM-900	900	876.0–915.0	921.0–960.0	955–1023, 0-124
DCS-1800	1800	1710.2–1784.8	1805.2–1879.8	512–885
PCS-1900	1900	1850.2–1909.8	1930.2–1989.8	512–810
WCDMA-2100	2100	1920–1980	2110–2170	9612 – 9888, 10562 - 10838