UNTRACEABLE PHONE

Nokia 5000d-2 / RM-362

DISCOVERY telecom

What Does the Phone Include?

- Ability to operate as a standard mobile phone
- Firmware modification that enables the phone to become untraceable
- Set of built-in commands for modifying and viewing interception related parameters
- Phone interception alerts
- Automatic or Manual phone IMEI (International Mobile Equipment Identity) change
- CrypToGo application for end-to-end encrypted SMS communication

Terms and Definitions

MITM:

A man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them.

IMEI:

A 15 digit number (14+1) number, usually unique, that is used to identify valid 3GPP (as GSM) mobile phones that is sent by the phone to the network.

C2:

A cell-reselection criterion (-99 to 99 dBm).

Active equipment attack with C2 > 100.

BTS:

A base transceiver station is a piece of equipment that facilitates wireless communication between user equipment (UE) and a network.

C2 Value

The C2 (reselection criterion) value is used to determine if a new cell should be selected to camp-on. If the transmitted C2 value of a neighbor-cell is higher than the serving-cell for a period longer than 5 seconds, the phone will camp on the new cell (handover).

Active equipment, as the IMEI/IMSI catcher and GSM Interceptors, attack the C2.

- The nominal range of C2 is usually between -99 to 99 dBm.
- Active equipment C2 value is usually >100 (to force camping on).
- The untraceable (UT) phone has a C2 default value of 80; alerting if a larger C2 value is detected.

Ciphering

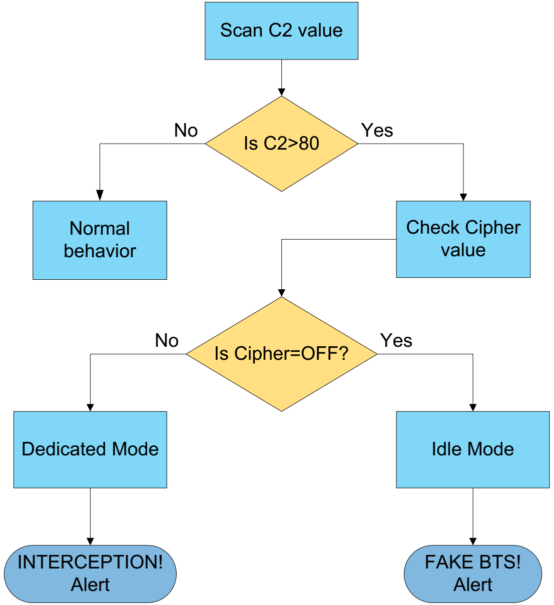
Ciphering algorithm for circuit-switched connection can be either A53, A52, A51 or “OFF”. This value is only set when the phone is communicating with the network (on a TCH).

Cipher value and conditions:

The UT phone uses a cipher value to determine weather in active call (Dedicated Mode) or if in Idle Mode.

- Phone is in Idle Mode when Cipher = OFF.
- Phone is in Dedicated Mode when Cipher = A50/A51/A52/A53.

Workflow



Scan C2 value

Is C2>80

No

Normal behavior

Yes

Check Cipher value

Is Cipher=OFF?

No

Dedicated Mode

INTERCEPTION! Alert

Yes

Idle Mode

FAKE BTS! Alert

MITM Attack – Alerts and Function:

FAKE BTS! Alert function:

Phone is connected to a fake network and there is NO call activity.

- Visual: FAKE BTS!
- Vibration: Constant

INTERCEPTION! Alert function:

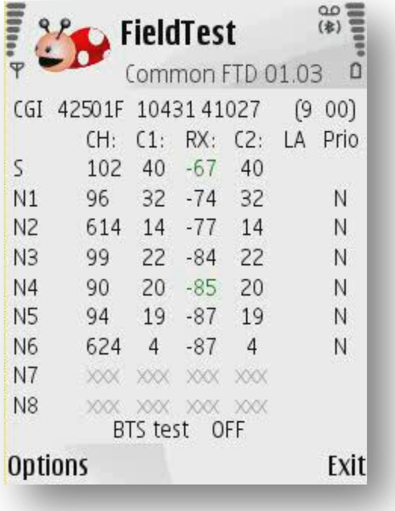
Phone is connected to Active equipment AND there is a call activity.

- Visual: INTERCEPTION!
- Vibration: Intermittent

DISCOVERY telecom

Neighbor-Cells and Measurements:

Detailed information about the Serving-Cell and its 8 Neighbor-Cells is presented in the following example-screen taken from a phone FieldTest (NetMonitor) application.



FieldTest

Common FTD 01.03

CGI 42501F 10431 41027 (9 00)

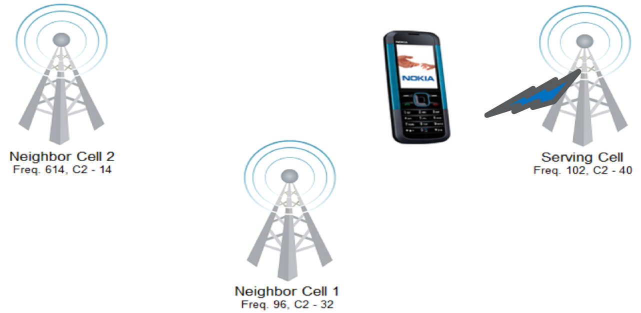
	CH:	C1:	RX:	C2:	LA	Prio
S	102	40	-67	40		
N1	96	32	-74	32		N
N2	614	14	-77	14		N
N3	99	22	-84	22		N
N4	90	20	-85	20		N
N5	94	19	-87	19		N
N6	624	4	-87	4		N
N7	xxx	xxx	xxx	xxx		
N8	xxx	xxx	xxx	xxx		

BTS test OFF

DISCOVERY telecom

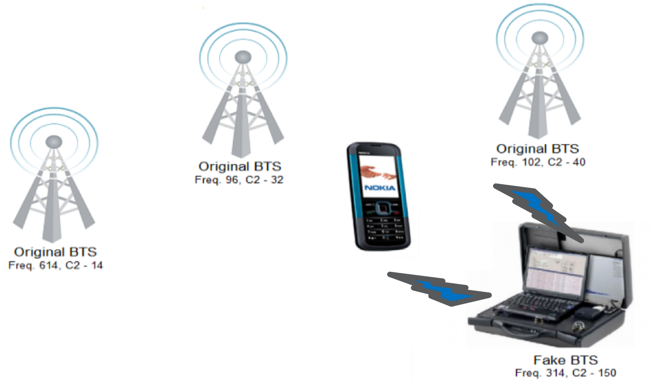
Network Behavior Illustrations

Normal condition



The handset is camped on channel 102 as it has the highest C2 value. The phone switches to a neighbor-cell when its C2 is higher than the Serving-cell.

Active GSM interceptor running its BTS



An active GSM interceptor is running its BTS, transmitting a C2 value of 150 and forcing the phone to camp on it. The phone will switch to fake-BTS with the highest C2.

DISCOVERY telecom

Type of Commands

The phone can receive two types of commands:

- View value command: *** # (CMD) #**
- Modify value command: *** # (CMD) * (NEW VALUE) #**

Giving the phone a command is performed by clicking the phone keypad according to the key letter and/or number (e.g. C2 is created by clicking 22).

List of Commands

The **CMD** can receive one of the following values:

<u>C2 (22):</u>

Get or modify the C2 value that the phone is set to (default is 80). Identifying a higher value than the set value will trigger the interception alert.

<u>C2NW (2269):</u>

Get the C2 value of the current cell.

<u>DEMO (3366):</u>

Manual call to the FAKE-BTS! INTERCEPTION! alert functions.

<u>MITM (6486):</u>

Display log information about the last MITM attack, including the elapsed time.

<u>MODE (6633):</u>

Display the current mode: IDLE/FAKE–BTS/INTERCEPTION

<u>IMEI (4634):</u>

Manually modify the IMEI number (14 digits). The phone will reboot once the command is acknowledged.

DISCOVERY telecom

CrypToGo Application

The CrypToGo application provides an end-to-end encryption solution for SMS communications between two UT phones.

The CrypToGo is a J2ME application.

- Encryption is carried out using AES in CFB mode with a random IV.
- The application is PIN protected, thereby preventing someone with short-term physical access to a user’s phone from opening the application and reading the encrypted SMS messages.

Unique Features and Capabilities

This untraceable (UT) phone provides a 3-layer protection, along with unique features.

- Alert in case of connection to active equipment
- Automatic and Manual phone IMEI change
- Option to set the C2 to any value, preventing vendors from trying to fool the UT phone by transmitting a C2 value that is lower than the set one.
- Ability to view a log of all previous attacks and the elapsed time
- Preinstalled CrypToGo application for end-to-end encrypted SMS communication