Maejo Int. J. Sci. Technol. **2012**, *6*(03), 514-527

Maejo International
Journal of Science and Technology

ISSN 1905-7873
Available online at www.mijst.mju.ac.th

Full Paper

Ciphering Indicator approaches and user awareness

Iosif Androulidakis [1,*], Dionisios Pylarinos[2] and Gorazd Kandus [3]

[1] Jožef Stefan International Postgraduate School, Jamova 39, Ljubljana SI-1000, Slovenia
[2] Electrical and Computer Engineering Dpt, University Of Patras, 26504, Rio, Patras, Greece
[3] Communication Systems Dpt, Jožef Stefan Institute, Jamova 39, Ljubljana SI-1000, Slovenia
* Corresponding author, e-mail: sandro@noc.uoi.gr

Received: 13 November 2011 / Accepted: 28 December 2012 / Published: 28 December 2012

Abstract: One of the fundamental mobile phone security problems in GSM is the absence of base station authentication, which allows man-in-the-middle attacks. During such attacks, a third party activates a fake base station, which acts as a bypass to the network, thus switching off the encryption and intercepting the user's communications. 3G mobile networks enforce mutual authentication but this can be circumvented if the 3G band is jammed by the attacker, forcing the phone to connect using GSM. GSM and newer standards provide a user alert indicating that the encryption has been switched off, which is called a Ciphering Indicator. In the present paper, different approaches followed by various manufacturers concerning the Ciphering Indicator are investigated. A total of 38 different mobile phones ranging from old to new and from simple to smart-phones that were produced by 13 different manufacturers were intercepted using a GSM testing device in order to document their reactions. Four approaches were identified with some manufacturers choosing not to implement the feature at all. It was also found that in the cases in which the feature was actually implemented, no universal indication was used and it was seldom documented in the phones' manuals. User awareness regarding the Ciphering Indicator and security issues was also investigated via an empirical survey employing more than 7,000 users from 10 countries and was found to be significantly low.

Keywords : Ciphering Indicator, graphical user interface, mobile phone, fake base station

INTRODUCTION

One of the fundamental security problems and a basic shortcoming regarding GSM security planning is the fact that mobile telephone base stations do not have to authenticate themselves to the user [1]. A user wishing to gain access to a provider's GSM mobile telephone network must own the proper SIM card and have it inserted in his or her phone device. The user's authentication is therefore performed by comparing the SIM's credentials with the data stored in the network's database [2]. A base station authentication mechanism, however, is not employed and mobile phones are not capable of assessing the legitimacy of the system they are connecting to, nor certifying whether this system is indeed part of their provider's network. Therefore, a fake base station can easily present itself as a part of the victim provider's network.

Furthermore, mobile phones constantly monitor a special data transmission beacon from the nearby base stations (through the broadcast control channel - BCCH) in order to choose the one offering the strongest signal for their communication [3]. This way, they can achieve better communication quality, economise the amount of energy consumed and increase their autonomy time. Hence, if the attacker installs his or her equipment in a nearby area and starts transmitting, masquerading as a legitimate operator and overlapping the authentic base stations' signals, mobile phones of that specific operator located nearby will choose the fake base station for their communication.

The next stage of the attack would be to neutralise the encryption. GSM uses an A5 algorithm for voice encryption [4]. There exist various versions of this algorithm that offer different levels of security (A5/2, A5/1, A5/3 – listed in strength order from lowest to highest), as well as a version with no encryption at all (A5/0) [5]. Under normal circumstances, the network has stored in its Authentication Centre's (AuC) database a secret key, Ki, which is also stored in the user's SIM card and is never transmitted in the network. These keys are compared by using a signed response (SRES) with the help of algorithm A3 and thus, the mobile phone is authenticated [6]. Finally, using the Ki and other data, the A8 algorithm produces the session encryption key, Kc, which is used in the speech encryption algorithm, A5 [6]. In the case of the fake base station, the basic information of the Ki key is not known to the attacker. Hence, the attack cannot proceed. However, the system planning prioritises usability instead of security in this case. As such, the corresponding protocols allow the negotiation and agreement between the mobile phone and the base station regarding whether they will use an encryption algorithm and which one they will use [6]. Therefore, sending the proper signal, the fake base station may inform the mobile phone that it does not have any encryption capabilities (A5/0) and that communication should take place without the use of encryption.

With encryption switched off, the attacker can act as a man-in-the-middle and intercept the communication of the target phone. Following this, using a simple mobile or fixed telephone, he can relay the call back to the genuine network and to the intended recipient, recording the communication in the process [7]. It is worth noting that 3G mobile networks enforce the mutual authentication scheme [8], which means that an authentication of the base station is required, eliminating fake base station attacks in practice. However, this can be circumvented if the 3G band is jammed by the attacker. Indeed, when a multi-band-capable mobile handset loses 3G signal connectivity, it will try to connect to older networks (2.5G and 2G) present in the area, thanks to backward compatibility. Therefore, even 3G users may fall victim to a fake base station attack. In addition, many users still prefer not to connect to 3G networks because of the increased power consumption and the shorter autonomy time of the handset [9]

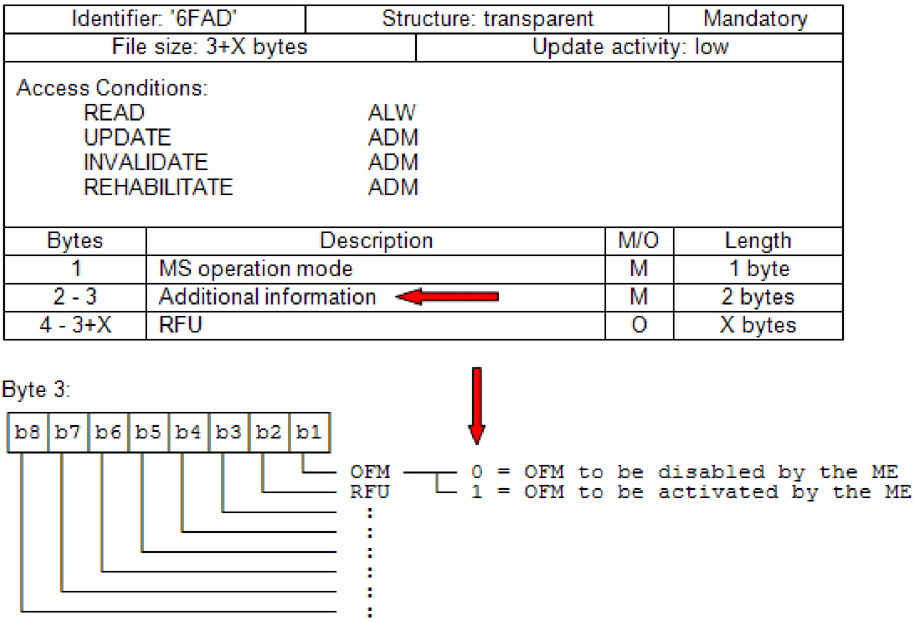
Even though the industry and researchers have shown an active interest in enhancing the mobile phone user experience, offering more and more services and a wealth of applications [10-13], the user notification issue regarding encryption being switched off, as well as user awareness of the matter, has not yet been thoroughly investigated. In this paper, the history of GSM standards regarding this issue, the different approaches followed by manufacturers and user awareness regarding this issue are widely investigated by employing a data set of 38 different models, 13 different manufacturers and 7,172 users.

METHODS

A GSM tester was used to intercept 38 different phones from 13 different manufacturers in order to identify their reaction when under attack (implementing the Ciphering Indicator or not) and also to investigate whether the matter has been documented in their manuals. User awareness was also investigated via a survey of 7,172 university students from 10 different EU countries. To formulate the process, the history of GSM standards regarding this issue was researched.

History of Ciphering Indicator in GSM Standards

It took several years for an alert informing the user of the loss of encryption to be included in the GSM standards. The first notion of this alert for a lack of encryption (albeit not explicitly stated as 'encryption') in the GSM standards was in 1997 [14], when a cryptic operational feature monitor (OFM) bit was mentioned. That bit controlled the OFM attribute, as shown in Figure 1, but the meaning of the term OFM was not explained in the abbreviations or elsewhere in the text.



Identifier: '6FAD'	Structure: transparent	Mandatory
File size: 3+X bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	MS operation mode	M	1 byte
2 - 3	Additional information	M	2 bytes
4 - 3+X	RFU	O	X bytes

Byte 3:

b8	b7	b6	b5	b4	b3	b2	b1

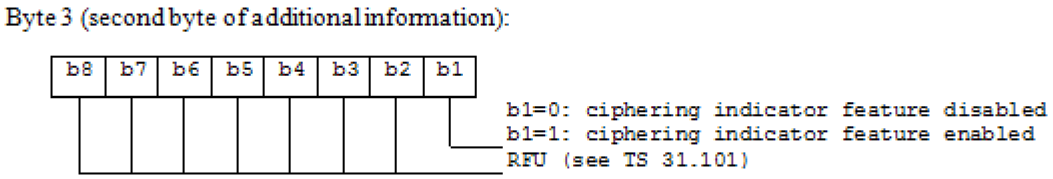
OFM — 0 = OFM to be disabled by the ME
1 = OFM to be activated by the ME
RFU

Figure 1. The first occurrence of the OFM bit in the standards

A Ciphering Indicator was introduced a few months after the first mention of the OFM and it was clearly stated that a notification should show the user the lack of data confidentiality [15]. It was also stated that the Ciphering Indicator feature should be mandatory, enabled by default, and potentially switched off via the respective SIM setting controlled by the network operator [15, 16]. As such, even if a handset has implemented the feature, the operator is able to instruct it not to alert the user in the case of a loss of encryption.

In 1999, the OFM term was described as an Operational Feature Monitor, and it was also explained that the OFM bit is indeed used to turn the Ciphering Indicator on and off [17]. In 2004, the

OFM term was abandoned in favour of the more straightforward Ciphering Indicator term [18], as shown in Figure 2. In 2009, further clarification of the feature was provided, and it was stated that phones with a suitable user interface should offer the user the capability to override Ciphering Indicator setting set by the operator [19]. This standard seems to be the first step towards actually empowering the user to overcome the control of the operator regarding Ciphering Indicator, although such technology has yet to be widely embraced.


Byte 3 (second byte of additional information):

b1=0: ciphering indicator feature disabled
b1=1: ciphering indicator feature enabled
RFU (see TS 31.101)

Figure 2. OFM is officially replaced by the Ciphering Indicator term

Phone Interception

In order to test mobile phones' behaviours with regard to Ciphering Indicator, a professional GSM testing device [20], shown in Figure 3, was used. The GSM tester provides all necessary signalling to the mobile phone in the same way as a base station does, enabling us to perform our tests. The experimental set-up consisted of the GSM tester, properly configured, and an antenna. The required settings for the parameterisation of the GSM tester are mobile country code (MCC), mobile network code (MNC), channel number (ARFCN) on which the broadcast control channel (BCCH) is transmitted and the traffic channel (TCH) on which the actual communication takes place. It should be noted that all MCCs are publicly available information [21]. In order not to interfere with any legitimate networks, a specially designated test-only network was used (a combination of MCC 001 and MNC 01), as shown in Figure 4. The encryption capability was deactivated by choosing algorithm A5/0, and a test call was initiated by the handset in order to test for the presence of an indication. The international mobile equipment identity (IMEI) of the target phone was logged, as shown in Figure 5, in order to deduce the exact phone model.

For every handset tested, two SIM cards from two different providers were used: one with Ciphering Indicator feature enabled and the other with Ciphering Indicator feature disabled. The former was used in order to test the manufacturer's approach regarding the indicator (whether implemented or not) and the latter was used to test whether the operator's setting was actually followed by the handset.

By adding a mobile handset with monitoring software installed, a second mobile phone, in order to channel the interception communication through it and a PC, the setup could be used to actually intercept communication before relaying it to the original recipient. More details about the experimental set-up and the process can be found in the author's previous paper [7].

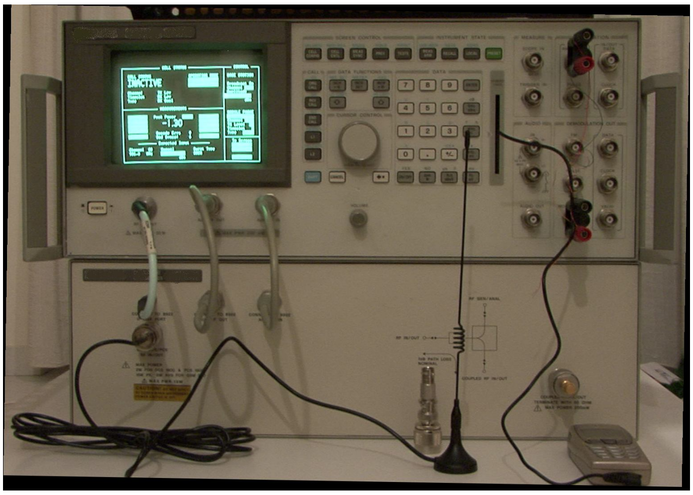
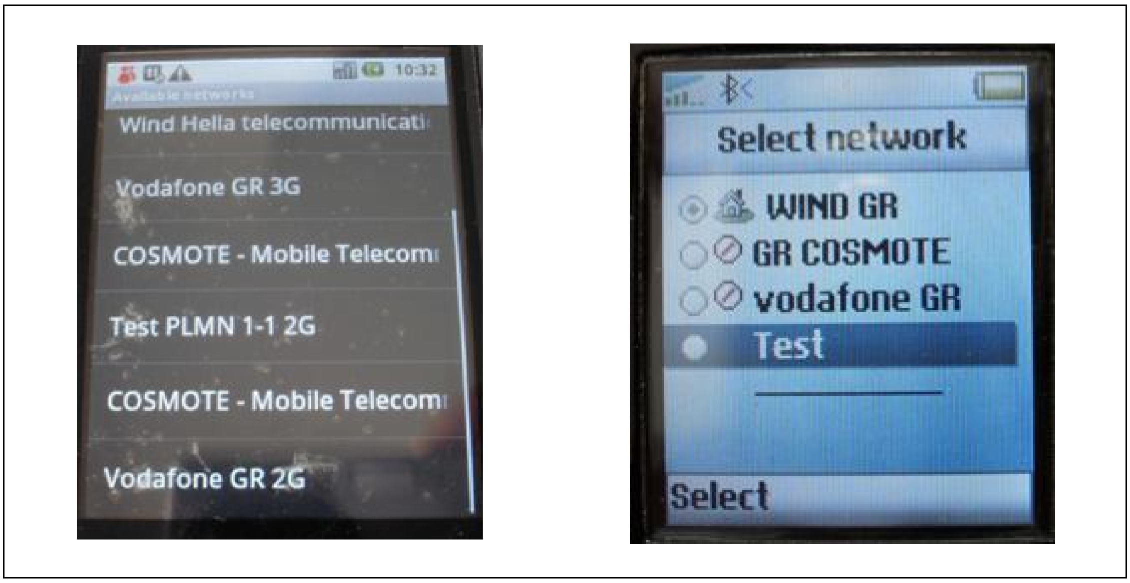


Figure 3. Mobile phone tester



10:32

Available networks

Wind Hella telecommunicati

Vodafone GR 3G

COSMOTE - Mobile Telecom

Test PLMN 1-1 2G

COSMOTE - Mobile Telecom

Vodafone GR 2G

Select network

○ WIND GR

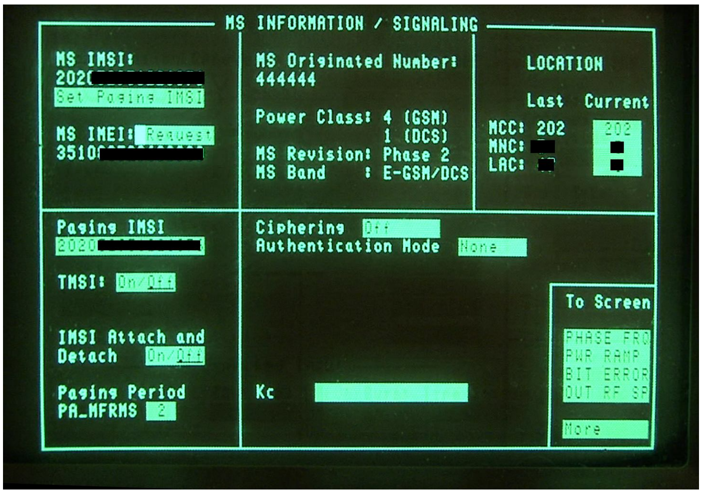
○ GR COSMOTE

○ vodafone GR

● Test

Select

Figure 4. Designated test-only network in the available networks list



```
MS INFORMATION / SIGNALING

MS IMSI:                MS Originated Number:       LOCATION
2020[redacted]          444444
Set Paging IMSI                                     Last  Current
                        Power Class: 4 (GSM)
MS IMEI: Request                     1 (DCS)        MCC: 202   202
3510[redacted]          MS Revision: Phase 2        MNC: [redacted]  [redacted]
                        MS Band    : E-GSM/DCS      LAC: [redacted]  [redacted]

Paging IMSI             Ciphering Off
2020[redacted]          Authentication Mode None

TMSI: On/Off
                                                             To Screen

IMSI Attach and                                              PHASE FRQ
Detach  On/Off                                               PWR RAMP
                                                             BIT ERROR
Paging Period           Kc                                   OUT RF SP
PA_MFRMS 2
                                                             More
```

Figure 5. Fake base station has extracted the mobile subscriber and mobile equipment identification as well as the number that the user intends to call (444444). Ciphering is switched off, as shown.

User Awareness Survey

To investigate user awareness regarding Ciphering Indicator, a large-scale survey of user security habits and trends was employed. The survey started in 2009 with a small sample of students from the University of Ioannina, Greece [22] and eventually resulted in a large sample of 7,172 university students from 17 different universities located in 10 different European countries, i.e. Hungary, Czech, Estonia, Latvia, Lithuania, Bulgaria, Greece, Romania, Slovakia and Slovenia [23, 24].

Multiple-choice questionnaires were used, employing an in-person delivery technique. Data entry took place using custom optical mark recognition (OMR) software, which enabled the processing of the questionnaires in a very rapid and accurate manner, avoiding human data entry mistakes [25]. Statistical processing took place using the SPSS analysis tool [26]. The aspect of the questionnaire considered in this paper is the awareness of Ciphering Indicator along with the brand used, because different brands follow different approaches.

RESULTS AND DISCUSSION

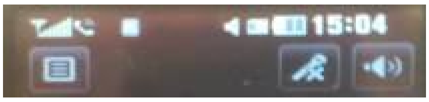
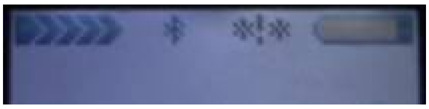
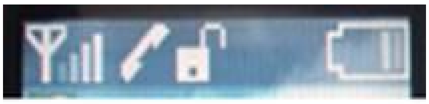
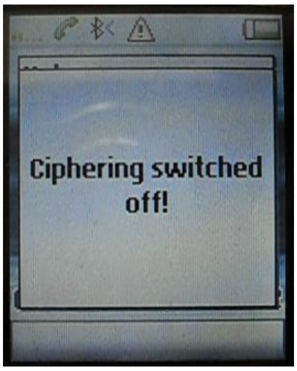
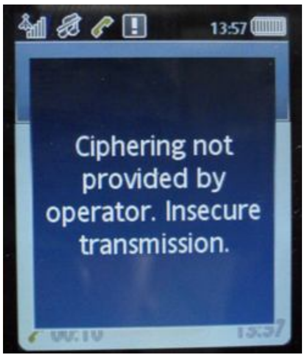
Implementation of Ciphering Indicator in Different Brands

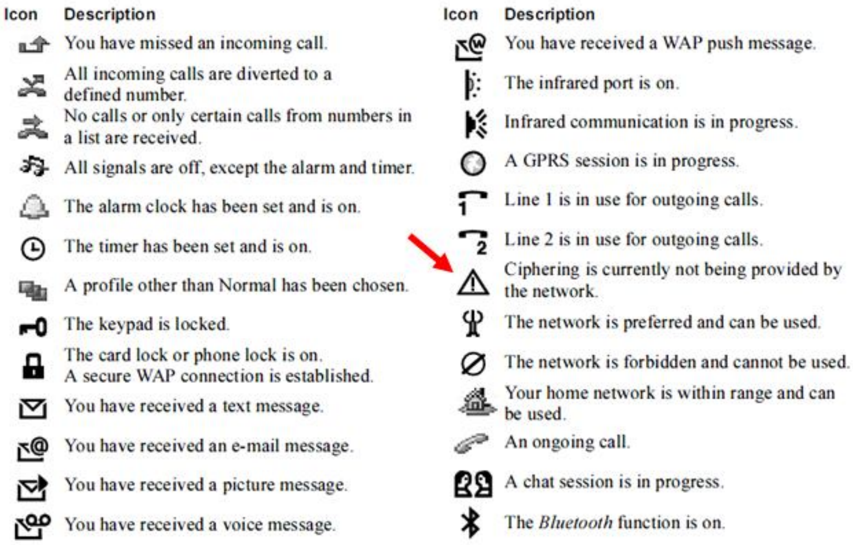
To acquire a wide view of the behaviour of phones during man-in-the-middle attacks, a group of 38 different mobile phones from 13 different manufacturers covering a large time span (from 2002 to 2010) was investigated.

In the case of SIMs with Ciphering Indicator feature enabled, four different approaches followed by the manufacturers were identified and are shown in Table 1. Nine different manufacturers in the considered dataset (Sharp, Samsung, Qtek, HTC, Motorola, LG, Huawei, Chinabuye and Apple) did not employ a Ciphering Indicator, although this is required by the standards, an approach which was identified as “Approach 0”. Furthermore, a universal indication was not employed by the manufacturers that did incorporate a Ciphering Indicator. One manufacturer in the considered dataset (Siemens) used stars and an explanation mark (an approach identified as “Approach 1”). Two others (ZTE and Nokia) used an open-padlock (an approach identified as “Approach 2”). Another manufacturer (Sony Ericsson) used an exclamation mark inside a red triangle or a grey square, along with an explanatory text message, an approach identified as “Approach 3”. Although there is inconsistency regarding the icon used in this approach (triangle or square), the presence of the accompanying text should be able to clear up any confusion. The text itself has been amended in more recent models to be more descriptive, as shown in Table 1. However, this informative message would disappear after a few seconds in eight out of the eleven cases considered, leaving only the icon present for the rest of the call. Only in three of the cases studied did the manufacturer choose to follow a more robust implementation, requiring that the user specifically acknowledge reading the message.

The documentation of Ciphering Indicator in manuals of the considered phones was also investigated. It was found that the presence or the meaning of the possible icons used as a Ciphering Indicator was mostly not documented. As shown in Table 1, proper documentation for the Ciphering Indicator was rather rare and only one manufacturer (Sony Ericsson) in the considered data set included it while this was done in only three out of its eleven models in the considered group. Quite interestingly, this manufacturer also used an explanatory message in addition to the icon and therefore it was the one that least needed to include such documentation in the phones’ manuals. Another manufacturer (Nokia) documented, in three different cases, that a closed padlock icon shows that the data services (e.g. WAP and WiFi) use encryption and that the absence of this icon indicates a lack of encryption, but Nokia has provided no documentation regarding the open padlock icon for voice and text communication. As an example, the way the icon of Approach 3 is explained in the respective phone manual is shown in Figure 6.

Table 1. Examples of different implementations of the Ciphering Indicator

Approach	Brand	Ciphering Indicator	Example of phone GUI	Documented
0	Sharp Samsung Qtek HTC LG Motorola Huawei Chinabuye Apple	No indicator		n/a (19 cases)
1	Siemens	Stars and an exclamation mark		0/2 cases
2	ZTE Nokia	Open padlock		0/6 cases
3	Sony Ericsson	Exclamation mark inside a grey square or a red triangle, along with a text message	 Ciphering switched off!  Ciphering not provided by operator. Insecure transmission.	3/11 cases



Icon	Description	Icon	Description
	You have missed an incoming call.		You have received a WAP push message.
	All incoming calls are diverted to a defined number.		The infrared port is on.
	No calls or only certain calls from numbers in a list are received.		Infrared communication is in progress.
	All signals are off, except the alarm and timer.		A GPRS session is in progress.
	The alarm clock has been set and is on.		Line 1 is in use for outgoing calls.
	The timer has been set and is on.		Line 2 is in use for outgoing calls.
	A profile other than Normal has been chosen.	⚠	Ciphering is currently not being provided by the network.
	The keypad is locked.		The network is preferred and can be used.
🔒	The card lock or phone lock is on. A secure WAP connection is established.	⊘	The network is forbidden and cannot be used.
✉	You have received a text message.		Your home network is within range and can be used.
	You have received an e-mail message.		An ongoing call.
	You have received a picture message.		A chat session is in progress.
	You have received a voice message.		The *Bluetooth* function is on.

Figure 6. Examples of the documented Ciphering Indicator (Approach 3)

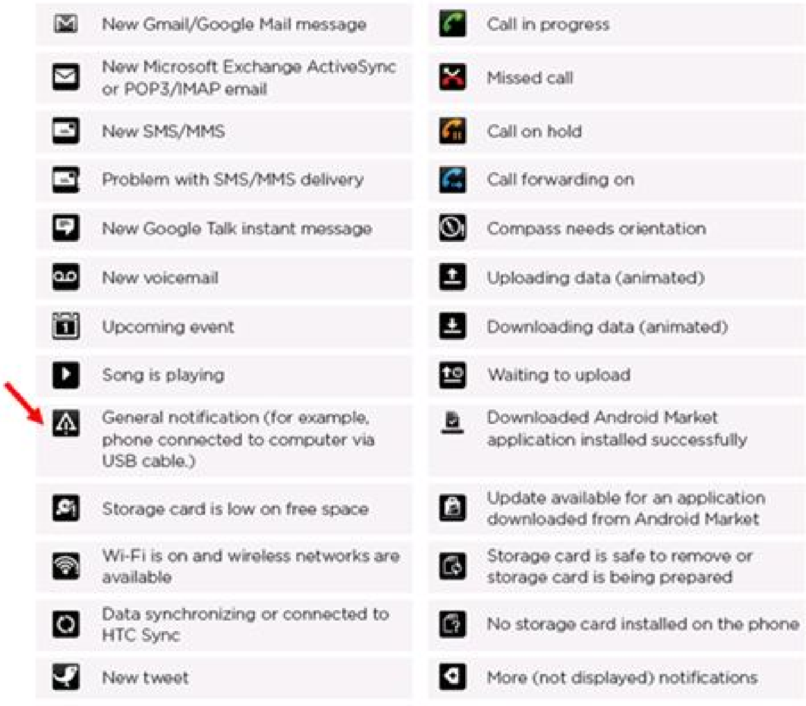
At this point, it is interesting to examine the behaviour of the so-called ‘smartphones’. These phones have advanced operating systems that allow a myriad of applications to be installed, minimising the gap between mobile phones and PCs. Our sample encompassed smartphones with four main operating systems (Android, iOS, Windows Mobile, and Symbian). It was found that only Symbian had implemented a Ciphering Indicator. This could possibly be attributed to the fact that Symbian is closely related to Nokia, a telecom manufacturer that has been using a Ciphering Indicator since its early models, whereas the other advanced operating systems have evolved out of the computer community (i.e. Windows Mobile, Android and iOS). It should also be noted that in the case of Android, a similar icon with the Approach 3 implementation of the Ciphering Indicator (a triangle with an exclamation mark) is used as a general notification icon, as shown in Figure 7, but it is not used to alert the user when the encryption is switched off.

Handsets using a SIM with the Ciphering Indicator feature switched off were also tested. It was found that all phones obeyed the network operator setting, with the exception of one. This occurrence should probably be attributed to a bug and not to a general manufacturer approach, because a later model from the same manufacturer had no such issues. Further, it should be noted that a phone that allowed the user to override the network operator setting for the Ciphering Indicator was not found in the considered group. A detailed report for each phone tested which contained the manufacturer, the model, the IMEI, the manufacturer’s approach and an indication whether the Ciphering Indicator was documented can be found in Table 2.

Table 2. Manufacturers' approach regarding Ciphering Indicator

	Brand	**Model**	**IMEI**	**Approach**	**Ciphering Indicator documented**	**Year Launched**
1	Nokia	1600	35 89 5801…	2	No	2006
2	Nokia	3510i	35 14 6280…	2	No	2002
3	Nokia	6510	35 11 0510…	2	No	2002
4	Nokia	5000	35 67 9702…	2	No	2008
5	Nokia	E71	35 82 4003	2	No	2008
6	Sony Ericsson	T610	35 12 5300…	3	Yes	2003
7	Sony Ericsson	T200	35 04 0345…	3	Yes	2002
8	Sony Ericsson	K810i	35 94 5101…	3	No	2007
9	Sony Ericsson	W810i	35 94 5701…	3	No	2006
10	Sony Ericsson	K770i	35 61 7902…	3	No	2007
11	Sony Ericsson	K750i	35 93 0200…	3	No	2005
12	Sony Ericsson	W595	3529 6503 …	3*	No	2008
13	Sony Ericsson	W700i	35 52 7101…	3	Yes	2006
14	Sony Ericsson	K630i	35 88 0101…	3*	No	2007
15	Sony Ericsson	W705	35 18 0603…	3	No	2008
16	Sony Ericsson	C902	35 87 9002...	3*	No	2008
17	Sharp	GX17	35 97 9100…	0	n/a	2005
18	Samsung	E1080	35 80 3703…	0	n/a	2010
19	Samsung	SGH-E570	35 49 9201…	0	n/a	2006
20	Samsung	E1310	35 42 3703…	0	n/a	2009
21	Samsung	C3050	35 55 2803…	0	n/a	2009
22	Samsung	SGH-J700	35 26 9302…	0	n/a	2008
23	Samsung	SGH-E250	35 60 7501…	0	n/a	2006
24	Siemens	S55	35 10 8352…	1	No	2002
25	Siemens	S65	35 39 1200…	1	No	2004
26	Qtek (HTC)	S200	35 70 3600…	0	n/a	2006
27	HTC	Wildfire	35 90 2803…	0	n/a	2010
28	Motorola	C115	35 64 9800…	0	n/a	2004
29	Motorola	U9	35 87 9801…	0	n/a	2007
30	LG	KP500 cookie	35 91 3103…	0	n/a	2008
31	LG	KP105	35 79 4002…	0	n/a	2008
32	LG	GB108	35 71 4503…	0	n/a	2009
33	LG	KU990 Viewty	35 90 3603…	0	n/a	2007
34	LG	GU230	35 72 4503…	0	n/a	2010
35	ZTE	340	35 59 2203…	2	No	2009
36	Huawei	Joy 845	35 16 0204…	0	n/a	2010
37	Chinabuye	H969	35 73 6903…	0	n/a	2010
38	Apple	iPhone 3G	01 20 2300…	0	n/a	2008

*Alerting text accompanying Ciphering Indicator should be acknowledged by user



New Gmail/Google Mail message	Call in progress
New Microsoft Exchange ActiveSync or POP3/IMAP email	Missed call
New SMS/MMS	Call on hold
Problem with SMS/MMS delivery	Call forwarding on
New Google Talk instant message	Compass needs orientation
New voicemail	Uploading data (animated)
Upcoming event	Downloading data (animated)
Song is playing	Waiting to upload
General notification (for example, phone connected to computer via USB cable.)	Downloaded Android Market application installed successfully
Storage card is low on free space	Update available for an application downloaded from Android Market
Wi-Fi is on and wireless networks are available	Storage card is safe to remove or storage card is being prepared
Data synchronizing or connected to HTC Sync	No storage card installed on the phone
New tweet	More (not displayed) notifications

Figure 7. Use of a triangle with an exclamation mark as a general notification icon (Android)

User Awareness

Examining the user element, the awareness of the issue was found to be significantly low in the considered sample. This can be attributed to various manufacturers not employing the feature and also to the lack of proper documentation in the case of the manufacturers that do employ it. Since different manufacturers follow different approaches regarding the Ciphering Indicator, the market share of each brand is an important issue in terms of investigating user awareness. As our survey revealed, the two most popular brands (Nokia and Sony Ericsson) in the considered sample, which were used by 64.1% of the students, employ a Ciphering Indicator (Figure 8). However, the user awareness in this sample was significantly low (only 24,9% were aware of the indicator feature). This can be partly attributed to manufacturers not employing this feature and also to the lack of proper documentation by the manufacturers that do employ a Ciphering Indicator, because a large percentage of users that had a Ciphering Indicator feature enabled in their phones were still unaware of the meaning of the icon used.

Our fundamental empirical questions involved whether students are informed about how the options and the technical characteristics of their mobile phones affect their security and how secure they consider communication using mobile phones. Students answered those two questions subjectively. We also used some objective questions in regard to security practices (noting IMEI, using a PIN, using a password-protected screen saver, using antivirus software, and making backups). In this way, we were able to conclude whether their subjective answers were actually aligned with the objective facts.

When answering the question “Are you informed about how the options and technical characteristics of your mobile phone affect its security?”, the majority of students (30.8%) stated that they were ‘moderately’ informed about the security options and characteristics, while 15.8% believed that they were ‘not at all’ informed. We proceeded to weigh the responses with the following weights: Very Much: 4, Much: 3, Moderately: 2, Not much: 1, Not at all: 0. Then, we divided them by the number of occurrences in order to obtain an arithmetic value and better compare the results (Figure 9). It was proved that LG and Samsung users are the most in need of security education because they scored the lowest on the 0-4 scale (1.74 and 1.73 respectively). Nokia (1.85) is around the total mean (1.86). iPhone and Ericsson users are the most informed ones (1.97 and 1.95 respectively).

Continuing with a general question about how 'secure' users felt mobile phone communication is, the majority (36.9%) replied 'moderately' , followed by 'much' at 28.6%. On the other hand, some (21.36%) felt not too much or not at all sure they were safe. Weighting with the same scale (0-4), the results were obtained as shown in Figure 10. It can be seen that iPhone users were the ones that are most 'suspicious' in regard to how safe they consider mobile phone communication to be. Sharp users were more relaxed.

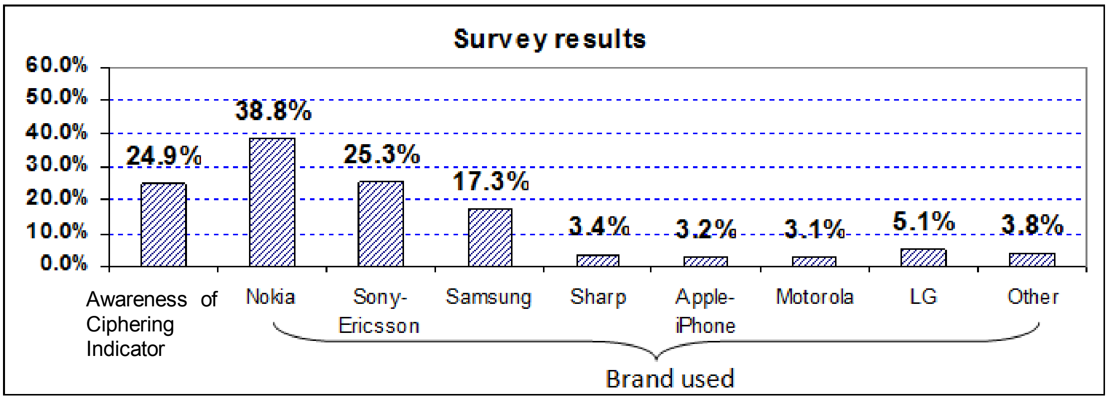


Figure 8. User awareness and percentages of the brands used in the considered samples

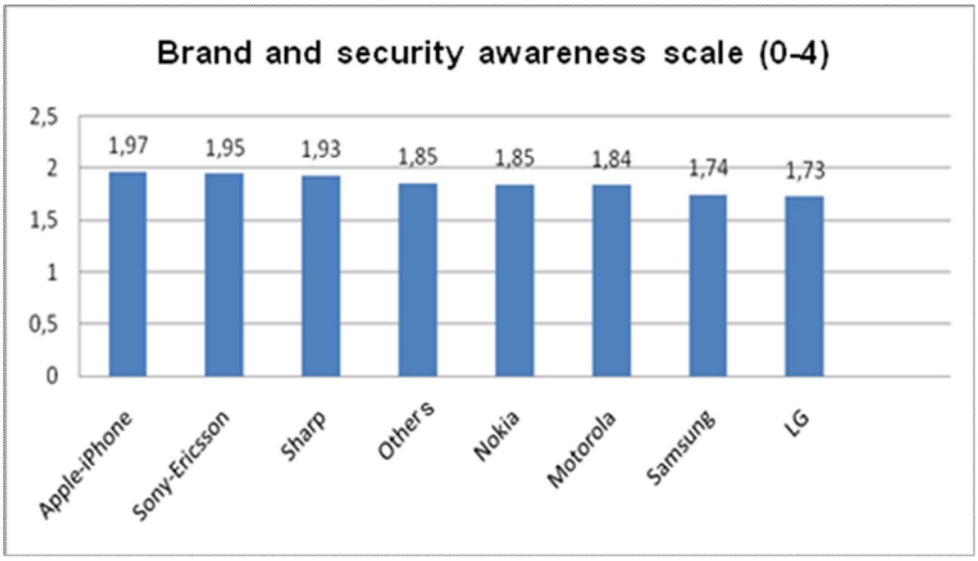


Figure 9. Brand and security awareness

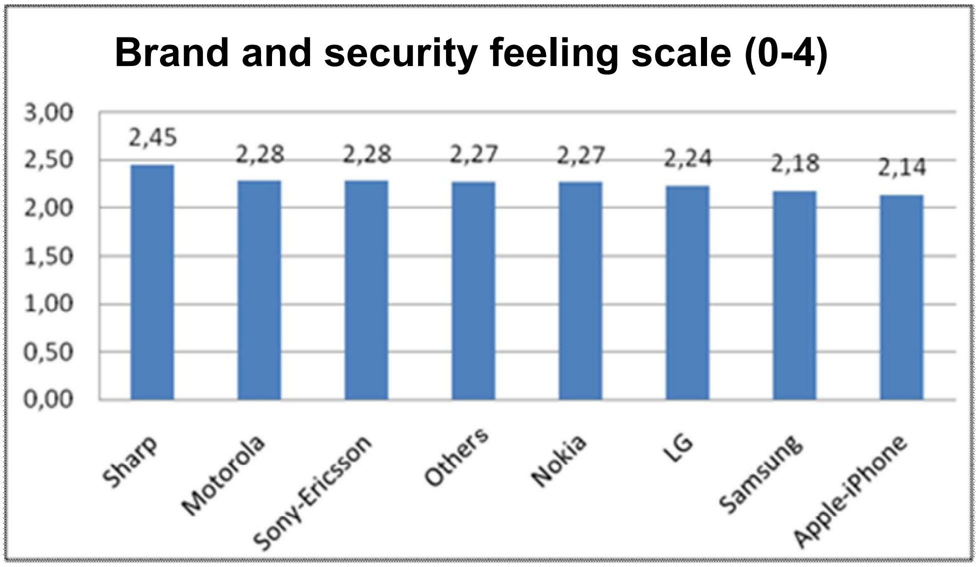


Figure 10. Brand and security feeling

CONCLUSIONS

In this paper, 38 different mobile phone models from 13 different manufacturers were intercepted in order to investigate the implementation of the Ciphering Indicator feature, which aims to alert users of switched-off encryption and possible interceptions. The documentation of the feature (or the absence of it) in various phones' manuals was also examined. In addition, user awareness regarding this feature and other security issues was surveyed by using the results of an empirical study employing a sample of 7,172 university students from 10 European countries.

Four approaches were followed by the manufacturers in the considered group regarding the Ciphering Indicator feature, ranging from no feature implementation to use of icons and an explanatory message. In the case of smartphones, phones with four different operating systems were tested and only one of them was found to implement the Ciphering Indicator feature. In general, the approach of each manufacturer seemed not to change over time, although one minor inconsistency was reported. The documentation of Ciphering Indicator in the considered phones' manuals was also investigated. It was found that the presence or the meaning of the icons used as a Ciphering Indicator was rarely documented. Finally, when examining the user element, awareness of the issue was found to be significantly low in the considered sample.

Although the Ciphering Indicator is a simple and efficient tool to alert users of possible communication interceptions, it seems to be neglected by both the industry and users. The results described in this paper emphasise the issue and can be employed to enhance awareness in both parties, considering the fact that security in mobile communications is an issue of growing concern.

REFERENCES

1. N. Jefferies, "Security in third-generation mobile systems", IEE Colloquium on Security in Networks (Digest No. 1995/024), **1995,** London, UK, pp.8/1-8/5.
2. R. J. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", 1st Edn., John Wiley and Sons, New York, **2001,** pp.354-358

3. L. Harte, R. Levine and G. Livingston, “GSM Superphones: Technologies and Services”, 1st Edn., McGraw-Hill Professional, New York, **1998**, pp.121-152
4. E. Biham and O. Dunkelman, “Cryptanalysis of the A5/1 GSM stream cipher”, *Lect. Notes Comput. Sci.*, **2000**, *1977*, 43-51.
5. E. Barkan, E. Biham and N. Keller, “Instant ciphertext-only cryptanalysis of GSM encrypted communication”, *Lect. Notes Comput. Sci.*, **2003**, *2729*, 600-616.
6. Technical Specification: “Digital cellular telecommunications system (Phase 2+), Security related network functions (GSM 03.20)”, European Telecommunications Standards Institute, France, **2000**.
7. I. Androulidakis, “Intercepting mobile phone calls and short messages using a GSM tester”, *Commun. Comput. Inform. Sci.*, **2011**, *160*, 281-288.
8. Technical Specification: “3rd Generation partnership project, technical specification group services and system aspects, 3G security, security architecture, V11.0.0”, 3GPP Organizational Partners, Sophia Antipolis, Valbonne, France, **2011**, p.63.
9. K. Pentikoysis, “In search of energy-efficient mobile networking”, *IEEE Commun. Magaz.*, **2010**, *48*, 95-103.
10. P. Baudisch, “My new PC is a mobile phone – techniques and technology for the new smallness”, Proceedings of 12th International Conference on Human Computer Interaction with Mobile Devices and Services, **2010**, Lisbon, Portugal, pp.1-2.
11. K. A. Li, P. Baudisch and K. Hinckley, “Blindsight: Eyes-free access to mobile phones”, Proceedings of 26th Annual SIGCHI Conference on Human Factors in Computing Systems, **2008**, Florence, Italy, pp.1389-1398.
12. V. Balakrishnan, S. F. Guan and R. G. Raj, “A one-mode-for-all predictor for text messaging”, *Maejo Int. J. Sci. Technol.*, **2011**, *5*, 266-278.
13. D. Wagner, G. Reitmayr, A. Mulloni, T. Drummond and D. Schmalstieg, "Real-time detection and tracking for augmented reality on mobile phones," *IEEE Trans. Visualiz. Comput. Graphics*, **2010**, *16*, 355-368.
14. Technical Specification: “Digital cellular telecommunications system (Phase2+), Specification of the subscriber identity module - mobile equipment (SIM - ME) interface, (GSM 11.11 V.5.5.0)”, European Telecommunications Standards Institute, Sophia Antipolis, Valbonne, France, **1998**, p. 61.
15. Technical Specification: “European digital cellular telecommunications system (Phase 2), Security aspects, (GSM 02.09 V.4.4.0)”, European Telecommunications Standards Institute, Sophia Antipolis, Valbonne, France, **1994**, p.12.
16. Technical Specification: “Digital cellular telecommunications system (Phase 2), Mobile Stations (MS) features, (GSM 02.07 V.4.8.2)”, European Telecommunications Standards Institute, Sophia Antipolis, Valbonne, France, **1998**, p.20.
17. Technical Specification, “Digital cellular telecommunications system (Phase 2+), Specification of the subscriber identity module - mobile equipment (SIM-ME) interface”, European Telecommunications Standards Institute, Sophia Antipolis Cedex, France, **2005**, p.175.

18. Technical Specification: "3rd Generation partnership project, Technical specification group terminals, Characteristics of the USIM Application (V6.5.0)", 3GPP Organizational Partners, Sophia Antipolis, Valbonne, France, **2004**, p.94.
19. Technical Specification: "3rd Generation partnership project, Technical specification group services and system aspects service aspects, Service principles (Release 8, V8.11.0)", European Telecommunications Standards Institute*,* Sophia Antipolis, Valbonne, France**,** **2008**, p.54.
20. User Guide: "8922M/S GSM Test Set", Agilent Part No. 08922-90211, Agilent Technologies Inc., South Queensferry (UK), **1998**, p.293.
21. Technical Specification: "The international identification plan for mobile terminals and mobile users", International Telecommunication Union, Geneva, Switzerland, **1998**, p.16.
22. I. Androulidakis, V. Christou, N. G. Bardis and I. Stilios, "Surveying users' practices regarding mobile phones' security features", Proceedings of 3rd International Conference on European Computing, **2009**, Tbilisi, Georgia, pp.25-30.
23. I. Androulidakis and G. Kandus, "A survey on saving personal data in the mobile phone", Proceedings of 6th International Conference on Availability, Reliability and Security, **2011**, Vienna, Austria, pp.633-638.
24. I. Androulidakis and G. Kandus, "Mobile phone brand categorization vs. users' security practices", *Eng. Technol. Appl. Sci. Res.*, **2011**, *1*, 30-35.
25. I. Androulidakis, "On a versatile and costless OMR system", *WSEAS Trans. Comput.*, **2005**, *2*, 160-165.
26. SPSS Technical, "SPSS for Windows, Rel. 16.0.2", SPSS Inc, Chicago, **2008**.