Security of SMS communication

SMS messaging has a distinct and specific place in the world of mobile communication. It is far less intrusive than a voice call, and often used for exchange of information that must not be contorted – like someone's phone number, place and time of a meeting etc. Many users are used to SMS messaging so much that they prefer it to voice calls.

It is important to realize the fact that SMS messaging – though attractive – introduces security problems for both parties of communication, especially if it is used for exchange of sensitive information, which should not be available to third parties. Let us review some of the risks.

1. Easy interception

Short texts like SMS messages can be intercepted (wiretapped) very easily. Costs of wiretaps are lower than in voice communication. For an operator, it is easy to scan all SMS going through their network for keywords, which is often really done.
Scanning need not be done with consent of the operator. Devices for GSM wiretap can be bought on black market for tens of thousands of euro, which is affordable price for many corporations and people, including private detectives etc.

2. Compromise of text due to users' error

SMS is more persistent than a call. A person entering the room 30 seconds after you have finished a call, can hardly learn anything. On the other hand, if you forget to delete an incoming or outgoing SMS, it will be present in your phone until you delete it finally. Now, if you leave your phone for a few minutes, anyone can look into your SMS list and read the secrets.
This, of course, also concerns situations when your phone is stolen.

3. Long lifetime

SMS are very small in size, and therefore can be stored easily. Currently, when a gigabyte of storage capacity costs less than $1, the possibility of long-term archivation is clear. Some countries already have law requiring storage of SMS for several years; if this spreads on, some people could have access to a long history of your SMS communication.

4. Side channels

For someone interested in your communication, even the contact list in your phone can be interesting. This does not mean only jealous partners searching for suspicions entries; the criminals are sometimes known to check contact lists for interesting names and other details.

5. Danger of message modification

SMS message, going through operator's network in plaintext, can be not only intercepted, but also modified. For example, identity of the sender can be altered, or the text changed. One can never be sure, whether a normal SMS has been received in the same form as it has been sent, and who is the real author. The network acts as a blackbox to both parties of communication.

From the above list it is clear that relying upon standard SMS service is dangerous in case of sensitive data. Users of the network can therefore choose from two possibilities: either use SMS only for exchange of unimportant data, or protect their SMS in some extra way.

Principles of SMS protection

If SMS messages are to be a reliable and secure means of communication, several requiremens must be fulfilled in order to thwart the abovementioned risks.

1. They must be secured against wiretapping (reading) by a third person.
2. They must be secured against modification (any change, even senseless one, must be detected at arrival).
3. Sender of the message must be certain.
4. Saved messages must be protected from reading when the phone falls into adversary's hands.
5. List of contacts must be protected as well.

Thanks to current state-of-the-art in science and technology, such objectives are possible to meet in the world of mobile communication.

Cryptography is a part of mathematical science studying protection of information from unauthorized access. At first, cryptographic results were available only to the military. However, in the 1970s, rapid development of digital communication led to rise in nonmilitary cryptography, which protects data in everyday life. Nowadays, cryptography is widely used in protection of many secrets, including internet banking (transfers of billions of dollars are protected using cryptography every day), access to private databases and personal communication (like PGP).

Practical cryptography

Several standards for data encryption and protection have been created in cryptography. One of them is AES (Advanced Encryption Standard), a very strong symmetric cipher, which is used (among others) by American military and diplomatic corps. Despite many years of scientific research, no real weak points of AES cipher have been found. Other important standard is SHA-2, a hash algorithm, which can be used to protect data integrity (=that no one has changed the data in any way).

A basic rule concerning ciphers is so-called Kerckhoffs principle. By this principle, a detailed knowledge of the cipher must not help the attacker to retrieve the encrypted information; all security must lie in used key. In autumn 2005, both AES and SHA-2 standards respected Kerckhoffs principle.

SMS 007 – a real protection of your messaging

CircleTech Corporation has developed special software for SMS protection – SMS 007 system. It uses standards SHA-2 and AES and fulfills all requirements stated in previous paragraphs.

1. *Security against eavesdropping*

Messages between two SMS 007 users are encrypted using AES and a key derived from a mutually exchanged password (passphrase). An adversary which monitors the communication seems only a senseless sequence of binary data, and is unable to decrypt them without the password. In case of a good password, this would take billions of years.
The keys for communication with other users are saved in the phone as encrypted („the keyring“), and the „main application password“ is used for their encryption. Therefore there is no need to remember the passwords, only the „main application password“. Also, the keys (passwords) can be changed very easily, when the two sides agree upon new ones. This gives the users an opportunity

to alter keys regularly - say, every week.

2. *Protection of integrity of messages*

Any encrypted message exchanged between two SMS 007 users includes a special security code (MAC) based on SHA-2 standard. This code prevents anyone in the network from altering contents of the message. If a single bit is changed, the message's code will not match anymore and the receiving user will be notified about decryption failure.

3. *Prevention of impersonation attacks*

Successful decryption of a received message is also a proof of the fact that the sending person has the correct key. Without knowledge of the key, the adversary is unable to generate a message which would decrypt into correct text on the receiving side. Therefore, the fact that a message has been really sent by its author, is ensured.

4. *Protection of saved messages from reading*

All received and sent messages of SMS 007 systém, which are saved into the phone, are protected by encryption, with use of SHA-2 and AES standards, and a key derived from the „main application password“, selected by the user. At each start, SMS 007 asks for the „main application password“. Without it, it cannot decrypt the data correctly. Any adversary which gets access to your saved data will need to guess the correct „main application password“ as well. In case of a good password, checking of all possibilities will také billions of years.

5. *Protection of contact list*

SMS 007 has its own contact list, independent of the main contact list in the phone. This contact list is also protected from reading, in the same way as the saved messages are – with use of SHA-2, AES and „main application password“.
Therefore, if a SMS 007 – enabled phone falls into hands of an adversary, this adversary will not be able to find even with *whom* the messages have been exchanged. This is especially important if you want to hide the very fact that you communicate with someone.

Additional functionality for users

SMS 007 systém does not limit itself to a mere handling of encrypted messages. The authors have made an effort to ensure maximum comfortability and user-friendliness. Additional functionality has been added.

- *sort contacts to groups*

The user can create up to 60 groups in the contact list, using them to sort their contacts. The groups can be opened and closed.

- *support of various languages*

The system supports communication in various languages, using UTF-8. Eastern European, Arabic, Hebrew or Chinese characters can be used in messages and contact list.
The system itself can be translated on-demand to any language version (Spanish, French …). Current versions are Czech and English.

- *extended list of contacts*

At each contact list entry, e-mail and long note (up to 150 characters) can be saved along with name and phone number.

- *easy sending of contacts to other people*

Any user of SMS 007 can send an entry from his contact list to another user via a special SMS (which can be encrypted, of course). The sent entry will contain name, telephone number, e-mail and note, and the receiving side can save it easily. Therefore, no tedious retyping of phone numbers is needed.

- *long messages*

Maximum message length is 200 characters.

- *sort messages into groups*

As well as contacts, saved messages can be sorted to up to 60 user-defined groups.

- *distinction of messages by colored icons*

Received, sent and template messages are denoted in the list of messages by various colored icons. Templates are white, successfully sent messages green, received and unread messages orange, received and read messages blue, and failed messages (which could not be sent) red. This intuitive color scheme helps the user in work with messages.

- *„top secret" messages*

Messages can be marked as „top secret". Such messages are not saved into the list of messages. As soon as such message is succesfully sent, it is removed from the sender's list of messages. When it arrives to its destination, it is saved to the list only until the addressee opens it and reads it. Immediately after being read, a „top secret" message is removed from the received list as well.

- *intelligent menus*

SMS 007 alters commands in menus by status of the message. For example, a received message has an option „Reply", failed message has an option „Resend" etc.

- *automatic deletion of old messages*

An automatic deletion machine for removal of old messages is included in SMS 007. User can turn it off or on; if it is turned on, any non-archived messages older than given time will be removed automatically, thus saving the phone's memory. The period of deletion can be set as 1 day, 3 days, a week, 14 days or a month.
Any message can be protected from automatic deletion by setting it as „Archived".

- *instant changing of passwords*

You can change the „main application password" at any time, provided that you know the old one. All saved data will be re-encrypted with the new key.
The passwords for communication with other users can be changed easily as well.

- *list of memory use*

SMS 007 will tell you how much space do your data occupy and how much free space is left on your phone.

- *sending of group messages*

With SMS 007 the user can send group messages to whole groups in his contact list easily. The message will then be encrypted with respective keys of the group's members.

- *batch deletion of messages*

Besides automatic deletion, SMS 007 allows the user to delete messages manually and in batches. The user can with one click remove all but most recent 3,5,7 or 10 messages from his list of messages.