A brief discussion about security issues in the SMS world

by

Daniel Lundeen

Abbrevations and definitions

SMS – Short Message System, messages of various types sent within the mobile telephony systems
SMSC – Short Message System Center, the operator gateway for sending and receiving SMS
ESME – External Short Message Entities, the service provider's gateway for sending and receiving SMS
SMPP – Short Message Peer-to-Peer Protocol, the protocol used when sending SMS

Introduction

This document covers some security issues regarding SMS – Simple Message System in mobile telephony. It is interesting because these issues are not very often covered when discussing security in our every day life. It is not a full coverage of the SMPP-protocol, but instead focus on how the protocol is used and what kind of attacks are possible to perform. In the end some security issues about the cell phone itself are discussed.

What is SMS?

SMS is the widely used messaging system when to send messages between mobile phones. Almost everyone is familiar with the small text messages that can be sent to each other. SMS is also used by the mobile net operators when they need to communicate different kind of information to their customers, e.g voice mail alerts. Lately, the SMS market has grown enormously and one can find SMS applications in almost every kind of market segment in the commercial industry.

Examples of implementaion areas are information services such as a subscription application which provides instant stock market changes in "real time", or perhaps weather changes in the swedish arctic. Other popular areas are gaming, lotteries, chat or payment for services not provided by the SMS itself.

SMS is also the carrier of downloadable items to the handheld phone unit, such as ring tones, logos and games. The list of possible areas for using SMS services is limited only by the imagination of man.

What is SMPP?

SMPP is an open standard protocol, designed to provide a flexible data communications interface for the transfer of short messages data. The protocol is used when delivering SMS to handheld telephony devices, e.g. cell phones and also between various kinds of message centers, which in turn, provide those number of different services mentioned above.

The protocol supports all market leading cellular technologies and the vendors of mobile units implements their operating systems according to the SMPP specifications.

SMPP is the protocol used between the mobile phone and the message center, as already said, but the focus of this paper is on the communication between an ESME (External Short Message Entity), such as a Service Provider distributing e.g. mobile banking and a SMSC (Short Message Service Center), which is provided by an operator, such as Telia or Tele2.

Technical

The protocol is based on an application layer tcp/ip connection between the two communication parties. When a connection is made, usually on tcp/ip port 2775, the ESME has to bind himself to the SMSC, using i.e a password.

Communication is asynchronous and the reason for this lies in the use of SMSCs; the SMSC supports a lot of different commercial service providers, and through the asynchronous behavior, it can provide a the same virtual quality of service to them all. Also, if one implements the protocol in a synchronous way, one loose a lot of valuable time, waiting for the other party to respond. There is no parity checking, CRC or other corrupt detetction, but this is left to the transport layer to handle.

A Protocol Data Unit is a central item when using this protocol. The PDU is built by a number of octets which specify the type of action the sender wants to make, for example send a message, to what destination. The PDU consists of a header and a body and may be of variable length.

The SMSC may risk congestion if too many PDUs are to be processed at the same time. SMPP has functions for telling the sending party information about a possible congestion situation. It lies in the hands of the ESME to take care of this according to the operators demands.

Security

There is no security mechanisms defined in the SMPP at all. The exchanged content is sent in clear text and may be intercepted or impersonalised if sent over an open medium such as Internet. However, Internet is most often used in the real world.

A way to avoid this is of course to secure the communication line in which the content is sent. This can be done by some leased line solution. This is often a fairly expensive solution and not always possible to implement, because of the operator providing the SMSC. And even though the solution removes the communiaction from the Internet, it is still sending messages in clear text.

An better way so solve confidentiality and authenticty is to use Secure Socket Layer, SSL/TLS. SSL is commonly used, e.g. in E-commerce solutions, and provides a secure connection between peers, by using encryption and authentication certificates. There are a lot of possible ways to adapt the secure transport layers into the application, some open source libraries and, of course, infinite number of commercial ones. In practice, the secure connection would be established, before the SMPP commences.

A third way is set up some kind of virtual private network, VPN. Typically, this is often used when for example two branch officies of a company is set up to be able to secure communication between them. The encryption is usually made in the data or packet layers, and an insecure session gets a secure channel. Neither ESME or SMSC need encryption themselves if VPN is used.

Possible attacks of SMPP

Even though this paper shows some ways of preventing possible different attacks, the reality shows that very few precautions are made. This goes for Sweden anyway, which is the scope of this document. Having this said, there are a number of various attacks with somewhat different types of implications.

Interception of messages

Because of the unsecure nature of the protocol, interception attacks are very much an issue. One could argue that the SMS itself is not worth protecting, but then one is overlooking at least a couple of confidential aspects.

The obvious commercial aspect gives that information might very valuable. Stolen information is probably expensive to those who try to commersialise e.g. refined data. The integrity aspect is another matter, and more serious. Intercepted messages might reveal information about how the SMSC and ESME are implemented, and perhaps provide the attacker with the nessecary tool for some other type of attack. One could perhaps even argue that privacy is an apsect as well. A SMS sender, perhaps you or me, doesn't want anyone to know what kind of services we are using.

Integrity

If an attacker gets hold of the information in the way described, one can be sure that the attacker would like to have som fun in replacing or modifying the sent messages. A possible example: An end user, a mobile phone, sends a SMS to a service provider as a payment for an advert placed in a newspaper. The message holds the code which identifies the ad. The message might be intercepted and modified, replacing the code with the attacker's code. Perhaps far fetched, but hopefully the reader gets the idea.

Denial of Service attack

Now, let's say the attacker has intercepted some PDUs and therefore knows a lot, for example the IP address to the SMSC and the password needed to access. This information might be enough for a DoS attack on the SMSC. One way is to combine the attack with the spoofing, and be able to flood the SMSC with messages, thus blocking the unhostile messages sent from a service provider.

Spoofing attacks

Because the SMPP travels over TCP and no security is provided, it is possible, under the right circumstances, to spoof IP addresses. The SMPP is as secure as TCP, i.e. insecure.

Fraud – sending "free" SMS

If an attacker succeeds in breaking the communication setup, by one or more of the attacks described above, it would be possible to act as the ESME, instead of the real ESME, and thus be able to send whatever kinds of messages to whatever kind of destination with whatever kind of type of message. This is of course dependending on how the SMSC is implemented.

Final words

Obviously, the distribution of SMS is not secure at all. This doesn't seem to bother most people though, as they don't consider SMS to be worth protecting. But as I have tried to show in this document, there are several cases of SMS services that involves real money, intellectual rights or origin property rights. And this should definitly be worth protecting.

The SMS service providers, and the operators who provide the infrastructure, obviously uses the mentality of an ostrich. They just hope there are no evil guys out there. But we know better after this course, anyway. And this is quite interesting, as it's quite simple to provide a secure implementation.

The future…?

In mid 2004 there where an alert from the creator of the widely vendor-used mobile phone operating system, Symbian, about a Trojan horse infecting mobile phones when downloading a cracked game, Mosquitos. The game contained a hidden feature which made the game, when played, send out messages to premium rated numbers in Germany, Netherlands, Switzerland and UK. In this case, the game was not downloaded via SMS, but surely could have been.

Another example of compromising the hand held device was performed by the virus/worm Cabir. It uses the Bluetooth functionality when searching for other devices to spread itself to. No real harm is done to the phone, other than draining the battery, as the searching for other devices goes on and on and on…

It is probably fair to claim that mobile phones in general will become more of a target of crackers because of the new 3G mobile system. The 3G-devices are getting more powerful by means of memory and functions, and operating vendors are having more third party software applications with them. Once we belong to the 3G world, we will basically have a broadband online connection and phones will be closer to PCs in terms of functionality. History has shown that having that kind of connectivity leads to the spread of viruses.

References

SMS Forum – Short Message Peer-to-Peer Protocol Specification
http://www.symbian.com/press-office/2004/pr040810.html
Dieter Gollman – Computer Security
Unnamed source, working in one of the largest mobile operators in Sweden