



NSS
Rest Assured

Network Security Solutions

By Rajendra Dave, Chief Operating Officer

XMS Technology To Counter SMS Vulnerabilities

We always wonder why banks and other financial institutions have yet to make a big impression with mobile commerce – mainly SMS-Commerce. Text messaging (SMS) has captured widespread interest and has an almost ubiquitous accessibility to mobile consumers, thus presenting enormous business opportunities. However, the roll out of such services is still at its infancy and is yet to make a big impression, be it service from banks, financial investment firms or debit card vendors despite the fact that mobile commerce presents a new and viable revenue stream.

Backed by more in depth research and analysis, the result shows that the mobile commerce idea is put off simply due to the fact that the security flaws inherent within SMS have become an impediment for such services. In order to further examine this topic in greater detail, I will take you through the underlying challenges and vulnerabilities of SMS (text messaging technology) and hope to present to you some known cases based on peer to peer text messaging (SMS from one mobile phone to another) and also peer to server technology (short code driven SMS).

SMS Vulnerabilities

This section offers a detailed description of SMS specifications and their underlying security threats.

About SMS

Mobile communications have been an integral part of the lives of more than 1 billion people worldwide with more than 80% of mobile users not leave home without their mobile phone. Businesses are gradually turning to mobile devices to “get the message across” to their employees anywhere, anytime. Consequently, SMS has become one of the more innovative and cost effective ways with which to enhance the overall productivity of our routine.

So much more to SMS

Some of you might or might not know that SMS travels as plain text and that privacy of the contents during this process is not guaranteed. The privacy issue might not be a matter to some but to those who rely on SMS to transmit confidential data, they are skeptical - hence the slow pick up in mobile commerce.

SMS services that are provided by vendors, banks or other businesses are mostly passive in nature with the SMS not being allowed to cause an active transaction, with the rationale for this being the gaps in security and vulnerabilities inherent in SMS. Gradual change and demand of active SMS based services can be met only by a solution that can address existing SMS security concerns in an end-to-end manner.

There are a multitude of active SMS services that can be brought to users at a personal and business level in the form of SMS messaging. For example:

- Banking: Check balances, transfer funds between accounts, and paying bills using credit cards. VAS is valuable not only for the subscriber but also for financial institutions offering this service.
- Customer service: Charge a customer's credit card right at the table, at any time, instead of going to a fixed POS terminal located by the register.
- Track the location of a moving asset: Interchange small amounts of information in an inexpensive manner, such as the longitude and latitude, current time, and perhaps parameters like temperature or humidity.
- Home security and vehicle security: Alerts and notifications in the event of a break in.

SMS Security issues and vulnerabilities

There are two important points to consider for anyone using consumer technologies such as SMS for business purposes:

- SMS is not a secure environment.
- Breaching security often occurs more easily by concentrating on people (social engineering) rather than on the technology.

The contents of SMS messages are known to the network operator's systems and personnel which makes SMS an inappropriate technology for secure communications. Most users do not realize how easy it is to intercept an SMS. Although it would likely be relatively complex to hack into a telecom provider's systems from an external source to obtain the contents of SMS messages, finding staff privileged to look at the SMS messages and persuading them to reveal the contents proves a much easier proposition to handle. Gartner, for example, has already expressed reservations about security in U.K. trials of SMS voting in local elections held in May 2002. Enterprises, including governments, should not use SMS for any confidential communications. Rather, such enterprises which seek secure communication channels to mobile employees should consider encrypted end-to-end solutions on devices that boast additional security features.

The underlying specifications and technology for SMS transmission leaves many security gaps. These gaps make SMS vulnerable to –

Snooping

On device, at the store and forward network elements

SMS Interception

Over the air, in wired network

Spoofing

Using commercial tools, own SMS gateway

Modification

Using conventional hacking techniques

SMS Security: What is needed?

Confidentiality

Through key based encryption

Integrity

Messages are tamper proof

Non Repudiation

Signed & Secure messages

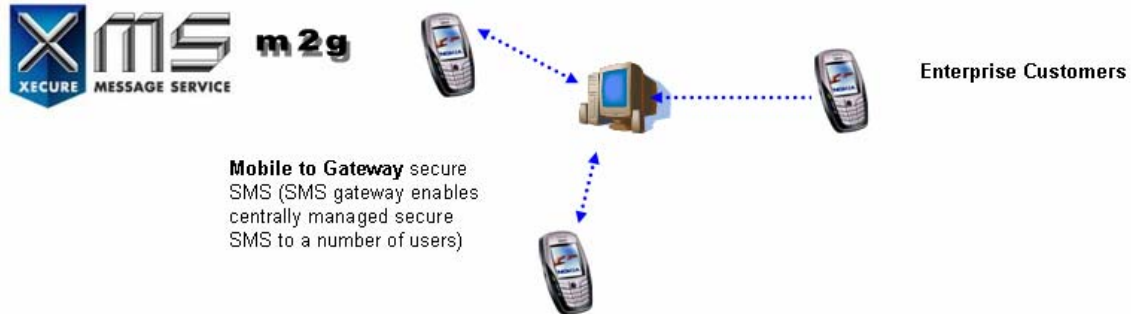
An end-to-end key based encryption technology for SMS plugs the gaps in the transit security of SMS whilst authentication added for resident SMS security access coupled with encryption, addresses the 'Confidentiality' issue of SMS technology. In addition to this, adding features for the validation of message integrity and the digital signing of SMS solve the problem of providing 'Integrity' and 'Non Repudiation' for SMS technology. By having the above features integrated into the SME (smart message entities), be it mobile phones or application servers originating and/or receiving SMS messages, users can be completely assured of the security and authenticity of SMS and the transactions that they involve.

XMS Technology from NSS

XMS as a technology platform from Network Security Solutions (NSS MSC SDN BHD), addresses for the first time ever an end-to-end total security solution to all security vulnerabilities inherent to SMS technology in a peer to peer environment.



In addition to this, the 'XMS' product suite also provides a complete security solution for 'peer to server' SMS applications with the 'XMS Business (Plus)' product extending the end-to-end security solution for SMS driven business solutions.



XMS Technology: Specifications

XMS Cryptography standards

XMS technology adopts Public Key (PK) encryption standards for ciphering and digital signing. This consists of: a 'key pair generation' algorithm, a 'ciphering/deciphering' algorithm and 'hashing' algorithm.

Key pair generation

XMS technology uses Elliptical Curve Cryptography (ECC) for key pair generation which is an approach to public-key cryptography based on the mathematics of elliptic curves. The main benefit of ECC is that under certain situations it uses smaller keys than other methods — such as RSA — while providing an equivalent or higher level of security. The ECC approach to key pair generation is best suited to mobile and smart computing devices.

Encryption

XMS technology uses AES (Advanced Encryption Standard), a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. While the terms AES and Rijndael are used interchangeably, there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits with a minimum of 128-bits and a maximum of 256-bits.

XMS Mobile optionally allows users to select the size of the key for encryption. Provided as 'Low', 'Medium' and 'High', an XMS Mobile user may choose their key length for ciphering as 128, 192 or 256-bits if the downloaded copy of XMS Mobile allows them to do so.

Digital Signing and verification

XMS technology uses Elliptic Curve DSA (ECDSA) for signing and verification purposes, which is a variant of the Digital Signature Algorithm (DSA) operating on elliptic curve groups. Superior efficiency is one reason this algorithm is preferred over DSA. DSA requires that $p > 2512$ in order to be secure against a number field sieve attack and $q > 2160$ in order to be secure against a baby-step giant-step attack.

Hashing

XMS technology uses the Secure Hash Algorithm, SHA-1 for computing a condensed representation of a message or a data file. When a message of any length $< 2^{64}$ bits is input, the SHA-1 produces a 160-bit output called a message digest. The message digest can then, for example, be input to a signature algorithm which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature. Any changes to the message in transit will, with a very high level of probability, result in a different message digest, that the signature will fail to verify.

About NSS – Network Security Solutions

NSS is Asia's leading information security consultancy, solutions and products provider for organizations of all sizes. NSS offers comprehensive information security consultancy services, products and solutions, which excel at delivering business value for its customers. When customers exercise choice, their choice is NSS. For further information, please visit www.mynetsec.com or email at enquiryMY@mynetse.com