Study of Mobile SMS Security Issues and Techniques

Nalla Girish

Research Scholar, CMJ University, Shillong, Meghalaya

Abstract: ***The short message service (SMS) is one of the highly used and well-tried mobile services with global availability within all GSM networks. The existing SMS is limited to the transmission of secure plain text between different mobile phone subscribers. SMS does not have any built-in procedure to authenticate the text and offer security for the text transmitted as data, because most of the applications for mobile devices are designed and developed without taking security into consideration. This paper details an overview of the current SMS security aspects and concerns during the SMS transmission. It also chronologically presents the existing mechanisms used to protect the SMS with the goal to provide useful advices for further research. In addition, the security and efficiency of these mechanisms are analysed, considering the limitation on the mobile devices and the security requirements. Finally it suggests the SMS security future direction for generating extra research topics.***

----------♦----------

INTRODUCTION

The use of mobile devices has increased rapidly over the years, particularly, during the last decade. These wireless devices were initially started as devices to store personal information. Short message service (SMS) will play an important role in the future business areas, which are popularly known as m-commerce, mobile banking, governmental use, and daily life communication. Furthermore, SMS has become a popular wireless service throughout the world as it facilitates a user to be in touch with any mobile phone subscriber anywhere in the world, instantaneously and without any hassle (Grillo et al., 2008; Zhang et al., 2005).

SMS SECURITY TECHNIQUES

Unprotected communication channels pose serious security vulnerabilities. Thus, it is importantly pertinent that both the mobile applications and the mobile operators must apply some reliable protective techniques to avoid these assailable vulnerabilities. This used to protect the mobile subscribers from the undesirable communication attacks during the SMS transmission. It can be provided in the network base (transport layer) or in the application base (mobile application) (Tiejun et al., 2008). This section reviews and describes the security mechanisms used for protecting the SMS transmission besides analyzing this mechanisms based on the security requirements comparing with the mobile performance capability. Beside, describes on how this mechanism can be applied to avoid the security concerns. There are two types of techniques that can be applied in different ways as mentioned (application layer and network layer). This paper focuses on the application layer techniques, which are considered as the current SMS research issues since it is under the researchers' control and development.

SECURITY AND PERFORMANCE ANALYSIS

Several challenges have to be over comed for wide deployment in the mobile systems. These challenges include a complexity (difficulty) management of applying PKI mechanisms to the limited devices capability during the deployment process in the large scale heterogeneous mobile system (Seema et al., 2004). As known PKI technology is a kind of asymmetric cryptography techniques, which depends on high intensive computationally of generating keys, and that makes them less suitable for devices of limited size and processing power, such as, mobile phones (Dankers et al., 2002). In simple terms, if the mobile user likes to use the PKI mechanisms, these should have the full support for the PKI features which require a high mobile capability (Cai et al., 2005). Currently, all the mobile devices have limited computational capabilities and a limited power supply since they are depending on batteries, thus, traditional PKI quite unsuitable for these existing devices (Lee et al., 2007). It is obvious that, mobile devices must have the high power capability to implement the PKI functions, beside owns associated capacity. That will provide a huge effort for the authentication process,

and can lead to a significant achievement of higher levels of security. However, due of resources in the mobile devices, the PKI implementation consider as a serious drawback for the mobile devices application. Thus, the relationship between the high security requirements and the mobile performance is inversely proportional, as the PKI provides a high security level for protecting the SMS transmission; however, at the same time it decreases the mobile performance.

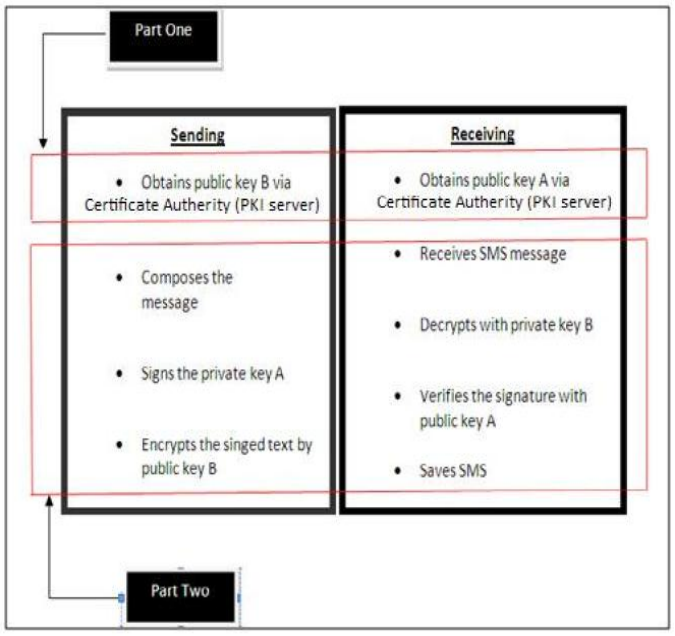

Figure 13. Securing SMS transmission parts.

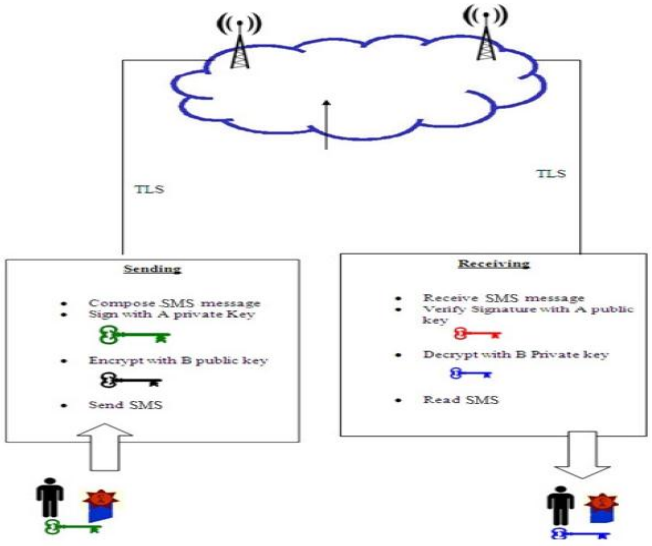

Figure 14. Securing SMS transmission overview.

Transport layer concerns	
Concern	**PKI solution**
All the network concerns mentioned in Table 4.	A public key infrastructure (PKI) provides an end-to-end secure transmission for the SMS content. All the intermediary people during the SMS transmission layer cannot read or modify the SMS content as it has been encrypted and duly signed by using the keys of the communicating parties. Therefore, the SMS content will be encrypted during the OTA, SS7 transmission media, and inside the SMSC and the BS. Even the Network employee's operators cannot read or modify the SMS content.
Application layer concerns	
Concern (Table 5)	**PKI solution**
Identity impersonation.	All The SMSs are signed by using the sender's private key which is unknown to the intermediary people including the network operator employees. Furthermore the PKI achieve the necessary of non-repudiation requirement.
Message forgery and tampering.	In the current PKI application, the message is signed by the sender which means attacker cannot know the private key of the sender, thus, attacker cannot tamper with the message neither can generate a correct signature. It is easy to verify the integrity of the message.
Eavesdropping.	An SMS message is encrypted, and only the sender and receiver know the decryption key (distributed via the certificate authority). Any attacker will need a great deal of effort (years) if he wants to decode the encryption, especially, if a strong encryption algorithm is used.
Unencrypted storage.	It can store the SMS inside the mobile inbox as a cipher text and when the user wants to check it, he can decrypt it by using his private key.
(MITM).	Thus, it can solve the authentication issue on both the communicating parties. The PKI utilizes the X.509 certificate for authenticating the communicating parties.

Moreover, the server architecture mobile security systems user has to get the mobile network operator or the service provider's approval as it still depends on the services of the mobile network operator or the service provider. Furthermore, the overhead cost of communication is increased due to the users' need to access to the servers in many cases, such as, uploading and downloading the cryptographic keys. Researchers do not expect that the mobile operators will provide the security services to the transmitted data through the SMS service for individuals, at least not in the near future. Additionally, in the current mobile systems, some applications based on the PKI have already been installed. They can satisfy the security requirements through the use of the X.509 as the certificate standards.

Although the mobile PKI fulfills all the security requirements, it is still unsuccessful to provide heterogeneous PKI standards for other mobile devices (Leung et al., 2003). Furthermore, different certificate standards from different Certificate Authorities (CA), (vendors), are considered as overheads for the mobile applications. Therefore, mobile applications have to proceed with different verification processing functions for different PKI certificate standards. In addition, any modification on the server side must also be made applicable to the user's mobile application. For

example, changing or upgrading the certificate standards means upgrading of the mobile application process. Thus, the mobile application has to deal with any new certificate standards, as the current PKI cannot maintain integrity between the standards.

Methodology	Weaknesses
Developing a new sever to act as a trusted third party or a middleware between the main server and the mobile device (Chanson and Cheung, 2001).	Difficult to develop for practical application because it depends on using two SIM cards.
Describes a simple symmetric key key cryptography and creates a lightweight based identity AKE protocol (Forsberg, 2007).	It is considered as a light protocol because it is based on binding the sender and/or the receiver identities to the key establishment, as it also needs different communication and operation processes with the third trusted server.
Install fixed Internet line because the exiting fixed line had already been developed and evaluated (Kawamoto and Nakamura, 2002).	Devices can use only the x.509 standard as it is considered as a certificate internet standard and it is heavy for verification in the normal mobile standards.
Based on using identify based cryptography and other techniques to overcome memory limitation (Zhao et al., 2008).	Has to deal with the mobile server provider and suitable only for large commercial organizations.
Using approximated one-time pads (Croft, et al., 2005).	Cannot provide a secure communication between two mobile devices.
Combined with a structure called Latin square, and cryptography processing (Hassinen and Markovski, 2003).	Cannot fulfil all the security requirements, such as, integrity, authentication and non-repudiation.
Encryption generated from the one-time password is entered by the user (Chikomo et al., 2006).	Cannot provide the end-to-end security requirements.
Shared a secret password between all the communicating parties (Hassinen, 2005).	Sender and receiver must previously have agreed on the password and PKI mentioned but not used.
Encrypts the plain text to the cipher text by using the existing mobile network to achieve the confidentiality and then signed before sending it to the receiver (Hossain et al., 2008).	Mobile devices have to be compatible with the GSM mobile service provider's network because it provides an encryption scheme.
Uses 10 functions or steps to achieve a reliably total security (Harb et al., 2008).	The system uses a symmetric key cryptography which has a key distribution problem and does not provide an end-to-end security between the two devices.
Using PKI technology (Jumaat et al., 2008).	The mobile device must download the certificate from the M-PKI directly and then stores the certificate inside the mobile device to perform the verification process which incurs high power consumption besides having a memory limitation problem.
Using PKI for exchanging the secret key (Toorani et al., 2008).	Although the public key is used for generating the secret key to reduce the public key complexity, it still needs the SMSC to apply some security techniques.

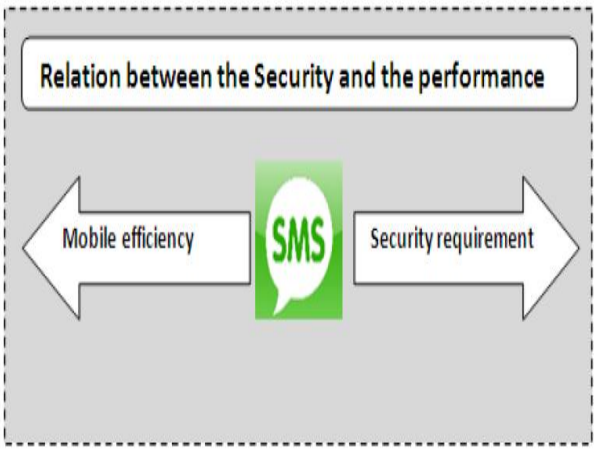

Figure 15. Protecting the SMS transmission.

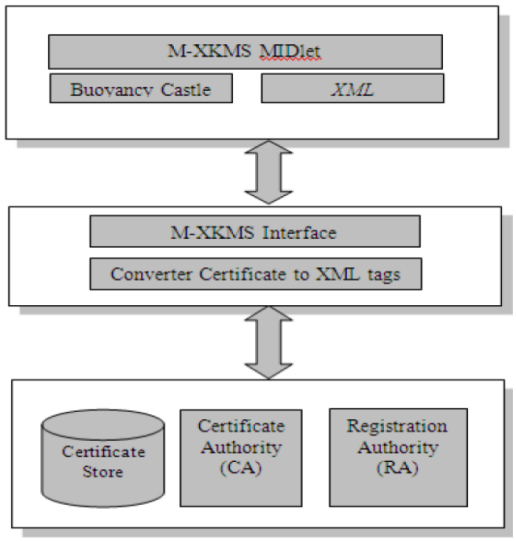

Figure 16. Securing SMS transmission.

LIMITATION

Although this review paper details all security concerns of GSM systems and mobile devices during the SMS transmission, but it does not mention the techniques which could be used to secure GSM architecture. This is because we have already introduced the security techniques in application layer to provide end to end security and protection.

FUTURE DIRECTION

Presently, there are two directions for enhancing the PKI limitations, such as, a high power capability demand as mentioned earlier. Firstly, install the middleware server (with suitable requirement) between the mobile devices and the PKI server. This middleware can shield the mobile devices from the PKI complexities and precedes some on the PKI mobile operation on behalf of the mobile, such as, verifying and storing the mobile certificate to reduce the mobile power consumption. The XML Key Management Specification (XKMS) can be the main structure for that middleware (Inc, 2002; Kangasharju et al., 2005; Nguyen and Ivar, 2008; Weerasinghe et al., 2006). The XKMS can be a good solution for the client's (mobile device) deployment limitation and resolving different vendor's problem in the mobile PKI M-PKI implementation for the security of the end-to-end SMS transmission. Figure 16 demonstrates the installation of the middleware server base on the XKMS technology. Secondly, provide or create a direct communication (No certificate authority) between the mobile devices can be also a solution, as we have mentioned that the main duty of the certificate authority is authenticating the communication user, therefore,

the main challenge is how we can ensure the authentication (Al-bakri et al., 2010).

CONCLUSION

SMS is an integral part of mobile communication and SMS security is undoubtedly useful and interesting but yet a challenging issue to consider. It holds great potential in applications related to businesses, government bodies as well as in military. This paper reviews the SMS security by outlining the different security issues related to SMS systems and the mechanisms used to overcome these issues during the entire SMS transmission circle from the mobile source to the final mobile destination. Based on the author's experience, it is apparent that PKI provides high level security to protect SMS during transmission because it resolve and avoids most of the issues related to SMS security. However, it decreases the mobile performance as it requires high mobile power capability to apply the PKI process. Alternative methods should be offered to improve the mobile PKI usage in a mobile environment.

REFERENCES

- Anuar NB, Kuen LN, Zakaria O, Gani A, Wahab AWA (2008). GSM mobile SMS/MMS using public key infrastructure: m-PKI. WSEAS Trans. Comput., 7: 1219-1229.
- Asokan N, Niemi V,Nyberg K (2005). Man-in-the-middle in tunnelled authentication protocols. pp. 28-41.
- Asvial M, Sirat D, Susatyo B (2008). Design and Analysis of Anti Spamming SMS to Prevent Criminal Deception and Billing Froud: Case TELKOM FLEXI.
- Aziz Q (2006). Payments through Mobile Phone. Emerging Technologies, 2006. ICET '06. International Conference on. pp. 50-52.
- Cai L, Yang X, Chen C (2005). Design and implementation of a serveraided PKI service (SaPKI). pp. 859-864.
- Chanson ST, Cheung TW (2001). Design and implementation of a PKIbased end-to-end secure infrastructure for mobile E-Commerce. World Wide Web. 4: 235-253.
- Chikomo K, Chong MK, Arnab A, Hutchison A (2006). Security of mobile banking. University of Cape Town, South Africa, Tech. Rep., Nov. 1:
- Croft NJ, Olivier MS (2005). Using an approximated one-time pad to secure short messaging service (SMS). pp. 71-76.
- Dankers J, Garefalakis T, Schaffelhofer R, Wright T (2002). Public key infrastructure in mobile systems. Elect. Communi. Eng. J., 14:180- 190.
- De Paula R, Ding X, Dourish P, Nies K, Pillet B, Redmiles D, Ren J,Rode J (2005). Two experiences designing for effective security. p. 34.
- Diffie W, Hellman M (1976). New directions in cryptography. IEEE Transactions on information Theory. 22: 644-654.
- Ekdahl P, Johansson T (2001). Another attack on A5/1 [GSM stream cipher], 49(1): 284-289.
- Forsberg D (2007). Use Cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding. pp. 1-8.
- Garza-Saldana JJ, Daz-Pérez A (2008). A State of Security for SMS on Mobile Devices, Electronics, Robotics and Automotive Mechanics Conference, CERMA '08. 4(5):110-115.
- Grillo A, Lentini A, Me G, Italiano GF (2008). Transaction oriented text messaging with Trusted-SMS. pp. 485-494.
- Guthery S, Kehr R, Posegga J. (2000). How to Turn a GSM SIM into a Web Server. p. 209.
- Gutmann P (2004). Simplifying public key management. Comput., 37: 101-103.
- Hassinen M (2006). Java based public key infrastructure for sms messaging. Information and Communication Technologies, 2006. ICTTA'06. 2nd. 1:
- Hassinen M, Hyppönen K, Haataja K (2006). An open, PKI-based mobile payment system. Emerging Trends in Information and Communication Security, pp. 86-100.
- Inc VS (2002). Trust Assertion XML Infrastructure. p. 45.

- Islam S, Ajmal F (2009). Developing and implementing encryption algorithm for addressing GSM security issues.Emerging Technologies, 2009. ICET 2009. International Conference. pp. 358-361.
- Jøsang A, Zomai MA, Suriadi S (2007). Usability and privacy in identity management architectures. p. 152.
- Jumaat NB, Zakaria O, Gani A (2008). GSM Mobile SMS/MMS using Public Key Infrastructure: M–PKI. WSEAS Trans. Comput., 7: 1219- 1229.
- Lam KY, Chung SL, Gu M, Sun JG (2003). Lightweight security for mobile commerce transactions. Comput. Commun., 26: 2052-2060.
- Lison KD, Drahanský M (2008). SMS Encryption for Mobile Communication. SECTECH '08 Proceedings of the International Conference on Security Technology, pp. 198-201.
- Lu CC, Tseng SY (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. pp. 277-285.
- Meyer U, Wetzel S (2004b). On the impact of GSM encryption and manin-the-middle attacks on the security of interoperating GSM/UMTS networks. Personal, Indoor and Mobile Radio Communications, 2004.
- PIMRC 2004. 15th IEEE Int. Symposium on. 4: 2876-2883.
- Moore T, Kosloff T, Keller J, Manes G, Shenoi S (2002). Signaling system 7 (SS7) network security, 2(3): 496-499.
- Nah FFH, Siau K, Sheng H (2005). The value of mobile applications: a utility company study. Commun. ACM, 48:90.
- Pesonen L (1999). Gsm interception. lecture notes, Helsinki University of technology, Lauri. Pesonen@ iki. Fi, pp. 1-9.
- Pitoura E,Samaras G (1998). Data management for mobile computing, pp. 1-11.
- Quirke J (2004). Security in the GSM system. AusMobile, May, pp. 1- 26.
- Ratshinanga H, Lo J, Bishop J (2004). A Security Mechanism for Secure SMS Communication. pp. 1-6.
- Schneier B. (2005). Two-factor authentication: too little, too late. Communications of the ACM. 48: 136.
- Sengar H, Wijesekera D, Jajodia S (2005). Authentication and integrity in telecommunication signaling network, pp. 163-170.
- J2ME-enabled mobile devices. Computer and Information Sciences- ISCIS 2004935-944, pp. 935-944.
- Toorani M, Shirazi B, Asghar A (2008). LPKI-a Lightweight Public Key Infrastructure for the mobile environments. pp. 162-166.
- Wilson S (2005). The importance of PKI today. China ommunications. p. 15. Wu S, Tan C (2009).
- High Security Communication Protocol for SMS. pp. 53-56.
- Zhao S, Aggarwal A, Liu S (2008). Building Secure User-to-user Messaging in Mobile Telecommunication Networks. pp. 24-26.