Scientific and Practical Cyber Security Journal (SPCSJ) 3(3): 12 - 15 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

TextFort: An Efficient Hybrid Short Message Service Encryption Scheme for Mobile Devices

Faisal A. Garba
Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria.
Department of Computer Science Education, Sa'adatu Rimi College of Education, Kano, Nigeria.
Cyberforce Pentest Ltd, Kano, Nigeria.

[1]Prof. Afolayan A. Obiniyi and [1,2]Prof. Saleh E. Abdullahi
[1]Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria
[2]Department of Computer Science, Nigeria Turkish Nile University, Abuja, Nigeria

ABSTRACT

Mobile device users prefer to preserve the privacy of their SMS communication from mass government surveillance and other adversaries using mobile device SMS encryption solutions. The mobile devices in use however, are highly constrained in terms of memory, power and computing capability to utilize the current SMS encryption solutions. There is a room for improvement in term of the speed efficiency of the SMS encryption schemes proposed for use on mobile devices. This paper propose an end-to-end SMS encryption scheme ideal for use on mobile devices using a hybrid combination of cryptographic algorithms: Blowfish symmetric encryption algorithm, Elliptic Curve Diffie Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA). The proposed scheme will be implemented using Java programming language to develop SMS encrypting Android application. The time taken for the proposed SMS cryptographic operations will be measured on five different Android mobile devices with varying processor speed and will be compared with a related work to evaluate the proposed scheme's speed. The cryptographic operations to be measured are the time taken for encryption and decryption and key generation.

Keywords: encryption, SMS, Blowfish, ECDH-ECDSA, cryptography, security, privacy.

Introduction

According to Susanto and Godwin (2010), using SMS over voice calls is the choice of majority of mobile users since it is cheap and trivial. Banks use SMS to send one time password (OTP), bank account details, exchange of security codes. However, this sensitive data could easily be hacked on their way to the intended recipient or send to the wrong recipient. Cryptography could be used to secure the transmission of SMS. Cryptography comes in three forms: symmetric key cryptography (secret key cryptography), asymmetric key cryptography (public key cryptography) and cryptographic hash functions. To ensure privacy of data symmetric key cryptography and asymmetric cryptography are used while cryptographic hash functions are used to preserve integrity. Each of these

forms of encryption has it's weakness as well as strength. To eliminate the weakness and gain the strength, the three forms of encryption are joined together to form a hybrid encryption scheme (Kuppuswamy and Al-Khalidi, 2014). These strengths are speed, security and the elimination of the key distribution problem.

Methodology

An efficient end-to-end SMS hybrid encryption scheme using a combination of cryptographic algorithms: Elliptic Curve Diffie Hellman (ECDH) which is a key negotiation algorithm, and also an asymmetric encryption algorithm with Elliptic Curve Digital Signature Algorithm (ECDSA) and Blowfish encryption algorithms which is a symmetric encryption algorithm. The SMS encryption scheme will be implement using Java programming language to develop SMS encrypting Android app. The target Android version is Android 4.0 (Ice Cream Sandwich). The work of Azaim *et al*. (2016) will also be implemented using Java programming language to develop SMS encrypting Android app. The target Android version is also Android 4.0 (Ice Cream Sandwich). The encryption and decryption rate of the proposed scheme will be compared with the work of Azaim *et al*. (2016) against the CPU clock rate of 5 android mobile devices. Figure 1 is the proposed efficient SMS hybrid encryption scheme. In the system architecture we have two entities Aisha and Buhari trying to exchange SMS. Any of the entities can initiate the communication process. ECDH-ECDSA is being used to generate a shared secret which serve as a temporary key. To encrypt and exchange the permanent Blowfish key, the temporary key is used alongside Blowfish encryption algorithm. The permanent Blowfish key, can now be used with the Blowfish encryption algorithm to exchange SMS. Other entities in the architecture are the database which is used in storing the keys as well as the SMS messages and the mobile network operator.

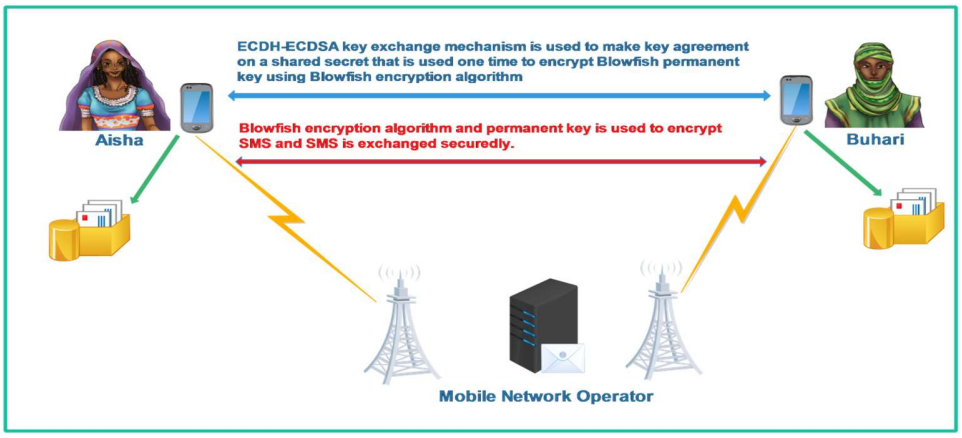

Figure 1: Proposed Efficient SMS Hybrid Encryption Scheme Architecture

Proposed Scheme's Pseudocode

Step 1: Aisha selects an integer X_A to serve as her private key and go on to generate $Y_A = X_A \times G$ to serve as her public key.

Step 2: Aisha sends the public key Y_A to Buhari signed with her ECDSA private key.

Step 3: Buhari verifies that the public key Y_A is from Aisha by using Aisha's ECDSA public key and then picks an integer X_B to be his private key and calculate his public key thus, $Y_B = X_B \times G$.

Step 4: Buhari sends the public key Y_B to Aisha signed with his ECDSA private key.

Step 5: Aisha verifies that the public key Y_B is from Buhari using Buhari's ECDSA public key, Aisha computes her secret shared session key thus $K = X_A \times Y_B$.

Step 6: Buhari also calculates his shared session key thus $K = X_B \times Y_A$.

Step 7: Aisha uses Blowfish encryption algorithm and K to encypt permanent Blowfish key K' and send it to Buhari.

Step 8: Buhari accept the encrypted message and decrypt it with his shared secret key generated in step 1 to recover the permanent Blowfish key.

Step 9: Aisha and Buhari can now exchange SMS encrypted with Blowfish encryption algorithm

Results & Discussion

The result of this research work will be compared with the work of Azaim *et al*. (2016) to evaluate the speed of the proposed efficient end to end SMS encryption scheme.

Conclusion

The result of this research work will be an efficient end-to-end SMS encryption scheme ideal for use on mobile devices which shall advance the state of the art in SMS encryption techniques on mobile devices.

REFERENCES

Azaim, M. H., Sudiharto, D. W., & Jadied, E. M. (2016). Design and Implementation of Encrypted SMS on Android Smartphone Combining ECDSA - ECDH and AES. *The 2016 Asia Pacific Conference on Multimedia and Broadcasting (APMediaCast),* 18-23.

Kuppuswamy, P., & Al-Khalidi, S. Q. (2014). Hybrid Encryption/Decryption Technique Using New Public Key

and Symmetric Key Algorithm. *International Journal of Information and Computer Security, 6*(4), 372-382.

Susanto, T. D., & Goodwin, R. (2010). Factors Influencing Citizen Adoption of SMS-Based e-Government Services. *Electronic Journal of e-Government, 8*(1), 55 - 71.