Impact three pass protocol modifications to key transmission performance

A Badawi, M Zarlis, S Suherman
Universitas Sumatera Utara, Medan 20155, Indonesia
suherman@usu.ac.id

Abstract. Key exchange is important to ensure cryptography works as expected. The three pass protocol (TPP) is the popular key exchange protocol. Modifications have been research interest for security improvement. This paper reports experiments to show modification impact to processing time. As modifications applied to 1, 2 and 3 links, the TPP processing time increases exponentially from 79 ms to 511 ms. The modification increases TPP processing time significantly. But modifications have minor impact to encryption and decryption times.

1. Introduction
Information exchange is part of human communication. Currently, information exchange occurs in many forms with almost unrestricted space and time. Information may be secret or not, but other listeners are exist. For secrecy, information exchange though the communication network is protected by cryptography through encryption and decryption processes. Many methods have been proposed and used. The most important part on cryptography is that the key should be exchange in order the intended user to be able to decrypt the information. Some techniques may integrate key exchange with the encryption algorithm [1], other technique requires separate transmission [2].

Figure 1. Three pass protocol
The three pass protocol (TPP) was developed by Adi Shamir in 1980 [2], in the key exchange procedure that involves three way handshakes messages. The messages are encrypted by using two keys, one sender key and other receiver key. The transmitted message is ensured unreadable for the third party (Figure 1).

The TPP modifications have been interests for many researchers as its role position in cryptography. Among them are outlined as follows. Boni and Andysah [3] added TPP within Caesar Cipher Classic Cryptography while a no-key-exchange to secure image sharing using TPP and Fourier transform was proposed by [4]. The TPP can also be implemented by using additional encryption scheme as in [2], [5], [6] where Vigenere with key stream generator modification, H-Rabin, RSA and ElGamal algorithms were inserted. This modification is intended to increase three pass protocol securities so that Eavesdropping may failed.

However, such modifications may induce longer encryption process as key should be sent over the network. This may interrupt communication such in real-time application. For instance, WhatsApp messages are often failed to be decrypted. This article discusses the TPP modification impact to key transmission. The methodology to evaluate the impact and the evaluation results are presented in next sections.

2. Methodology

In order to evaluate the modification impact, the steps as outline in Figure 2 are taken. Initially, the TPP is implemented using java socket programming where AES [7] key should be sent by using this protocol. The El-Gamal algorithm [8] is used to modify the TPP. Modification is performed for 1 link, 2 link and 3 link. The TPP, encryption and decryption processing times are analysed. The experiments are conducted by using an ad hoc 802.11 network.

![Figure 2. Research step](image)

The 1 link modification is performed by using one time pad (OTP) and El-Gamal encryptions. The public El-Gamal key is sent at first place. The modification steps are shown in Figure 3a. There is no change within the second and third messages. The 2 link modification (Figure 3b) requires additional encryption in both parties as well as in 3 link modification (Figure 3c).
Figure 3. The TPP link modifications
3. Results and discussions
As experiments were repeated for 1000 iteration, a sample of results is shown in Figure 4, where the TPP processing time is much higher than encryption and decryption times. The sparking times on Figure 4 may be exerted by the second layer of 802.11 where interferences with the co-existence networks result collisions and retransmissions [9].

Figure 4. Iteration variation for unmodified TPP

As the same experiments conducted to TPP modifications, the average TPP processing time as well as encryption and decryption processing times are show in Figure 5.

Figure 5. Process comparisons
In all conditions, TPP takes much longer to complete than the other processes. TPP processing time reaches about 31 times of encryption or decryption time. It shows that TPP holds the crucial impact to the encrypted information exchange. Meanwhile, the delay tends to increase for modification applied longer. As shown in Figure 6, The processing time of TPP increases exponentially from 79 ms without modification, to 511 ms with 3 link modification. The increment achieves 546.8%. This proofs that modification causes significant increment on processing time.

TPP modification does not only influence the TPP processing time, it also increases encryption and decryption times in small degree. Encryption time slowly moves from 15.65 ms to 15.79 ms. The same pattern applies for decryption, moves from 15.66 ms to 15.78 ms. This shows that TPP modification impacts to encryption and decryption are insignificant.

Figure 6. Average processing time
4. Conclusion
The paper has examined impact of three pass protocol modification to protocol, encryption and decryption processing times. Experiments on 802.11 ad hoc network using java socket programming have been conducted. The result show that the modification influences the TPP significantly with processing time increases up to 546.8%. Meanwhile, encryption and decryption increments are not significant, although increments are exponential.

References
[1] D. Stebila and M. Mosca, “Post-quantum Key Exchange for the Internet and the Open Quantum Safe Project,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10532 LNCS, pp. 14–37, 2017.
[2] A. Subandi, R. Meiyantri, C. Lika, M. Sandy, and R. W. Sembiring, “Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification,” Adv. Sci. Technol. Eng. Syst. J., vol. 2, no. 5, pp. 1–5, 2017.
[3] B. Oktaviana and A. P. Utama Siahaan, “Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography,” IOSR J. Comput. Eng., vol. 18, no. 4, pp. 26–29, 2016.
[4] J. Lang, “A no-key-exchange secure image sharing scheme based on Shamir’s three-pass cryptography protocol and the multiple-parameter fractional Fourier transform,” Opt. Express, vol. 20, no. 3, p. 2386, 2012.
[5] A. P. Sidik, S. Efendi, and S. Suherman, “Improving One-Time Pad Algorithm on Shamir â€” s Three-Pass Protocol Scheme by Using RSA and ElGamal Algorithms.”
[6] D. Rachmawati and M. A. Budiman, “An Implementation of the H-Rabin Algorithm in the Shamir Three-Pass Protocol,” pp. 28–33, 2017.
[7] E. B. P. Manurung, O. S. Sitompul, and Suherman, “Applying transpose matrix on advanced encryption standard (AES) for database content,” in Journal of Physics: Conference Series, 2018, vol. 978, no. 1.
[8] R. Singh and S. Kumar, “Elgamal ’ s Algorithm in Cryptography,” vol. 3, no. 12, pp. 3–6, 2012.
[9] Suherman, A. T. W. Hutasuhut, K. Badra, and M. Al-Akaidi, “Impact of window decrement rate on TCP performance in an adhoc network,” in IOP Conference Series: Materials Science and Engineering, 2017, vol. 237, no. 1.