Delay distributions on encrypted real-time traffics

Dirja Nur Ilham¹, S Suherman², G Sihombing³, Yulianta Siregar²

¹Politeknik Aceh Selatan, Indonesia
²Electrical Engineering Department, Universitas Sumatera Utara, Medan-Indonesia
³*suherman@usu.ac.id

Abstract. Real-time streams are common for nowadays communication for both data and video. Real-time data communication such as chat application and telemetry, as well as real-time video communication such as video call, video conference, or monitoring video are prone to the third party attacked. End to end encryption has been considered as the most realistic solution such as applied by WhatsApp so that the transmitted data is difficult to be revealed by the attacker. Since encryption and decryption processes injected additional delay, the algorithm should be fast enough to avoid inconvenience to users. This paper examines delay distribution for encrypted real-time traffics. The simulation shows that the decryption contributed the most to the end to end delay. Decryption delay is about 4.58 times higher than encryption and transmission delay. Although assessment involves only two links, the complex network has relatively lower than the obtained decryption delay. Meanwhile, encryption contributed only about 0.2% to the overall end to end delay.

1. Introduction

Customer premises equipment as the end node of traffic generators in communication systems has been diversely developed, from small distributed sensors, monitoring nodes, smartphones to standalone computers. Mobile phone, for instance, has been the major traffic generator. Meanwhile, real-time traffic, especially real-time messaging has dominated the communication traffics. Whatsapp for instance has almost 2 billion users spread over 180 countries and become the most popular real-time messenger applications [1]. The usage increases public concerns on security matters, especially on identity theft as it has been reported as the most treat on communication systems [2][10][11]. Treats may come from anyone in networks, even the closest person as reported by [3] that 22.5 % of the identity crimes committed by a family member.

End to end encryption provides an effective way to prevent this attack. Encryption is considered as “a gift from God” [3]that although possible to breach but not lessen the contribution and usability. Therefore encryption is worth to be implemented in real-time traffic. However, encrypted data often cause unexpected transmission delay, in some cases, messages were failed to decrypt as the key might be lost. Even dough, the current application has mostly been secured by encryption. This paper examines the distribution of delay on encrypted real-time traffics. Assessment is conducted by using the Rivest-Shamir-Adleman algorithm (RSA) [4] on the simulated network. The distribution of delay is revealed by assessing encryption, transmission, and decryption stages.

RSA is an asymmetric key algorithm that uses mathematical concepts to generate inexpensive fast generation private key and public key pair [5]. RSA uses block encryption [6] which adopted block cipher, where plaintext is chopped into fixed length blocks between 1 to N before being encrypted. values usually
1024 bits with block length is equal to or less than \( \log_2(N) + 1 \). Encryption and decryption function is defined as [6] Equation 1 and 2, where \( C \) is cipher text, \( M \) is message, \( e \) is public key and \( d \) is private key.

\[
C = M^e \mod N \\
M = C^d \mod N
\]

2. Evaluation Method

In order to evaluate delay distribution on real-time encrypted traffic, a two links network is set up by using the NS-2 simulator as shown in Figure 1. Alternatively, for crowded traffic setup may use ad hoc network configuration as in [7]. The encryption stage is performed by using the RSA with varying modulus length from 1000 to 10000. Delay is measured from the time data retrieved by the transmission control protocol (TCP) up to data is reconstructed from cipher text. Delay is distributed into encryption delay starts from plain data reading to cipher text writing, transmission delay starts from cipher text reading in sender node up to cipher text writing on receiving node, and decryption delay start from cipher text reading to plain text revelation.

3. Observation results

Figure 2 shows the encryption time for various modulus lengths. The encryption time almost linearly increases to modulus length. The magnitude of encryption time is between 0.03 ms and 3.55 ms.

| Modulus length | Encryption Time (s) |
|----------------|--------------------|
| 1000           | 0.00003            |
| 2000           | 0.00025            |
| 3000           | 0.00054            |
| 4000           | 0.0005             |
| 5000           | 0.00095            |
| 6000           | 0.00165            |
| 7000           | 0.00244            |
| 8000           | 0.00249            |
| 9000           | 0.00278            |
| 10000          | 0.00355            |

Figure 2. Encryption time
Meanwhile, transmission in Ethernet and wireless Ethernet link with additional background traffic results in network delay 125 ms and 161 ms (Figure 3). Figure 4 shows decryption time which increases exponentially to modulus length. Decryption time rises from 287 ms to 2140 ms for 10 fold modulus increment.

| Modulus length | Decryption Time (s) |
|----------------|---------------------|
| 1000           | 0.00287             |
| 2000           | 0.02022             |
| 3000           | 0.05954             |
| 4000           | 0.13947             |
| 5000           | 0.2982              |
| 6000           | 0.58383             |
| 7000           | 0.98717             |
| 8000           | 1.23639             |
| 9000           | 1.50199             |
| 10000          | 2.13977             |

(a) Figure 4. Decryption time

Overall, decryption contributed the most for encrypted real-time traffics. Delay due to decryption achieves 83% of the overall delay (Figure 5). In average, total delay becomes 840 ms which is not acceptable for real-time traffics. This delay may decrease significantly if modulus length for encryption and decryption is lower than modulus2000, which exerted total delay less than 150 ms. Decrement also reduces TCP packet length, which avoid losses [8, 9]. For modulus length 2000 enable encryption algorithm to fulfill real-time requirement.

(a) Figure 5. Delay comparison
4. Conclusions
This paper has assessed the delay distribution for the encrypted real-time traffic. Encryption delay and transmission delay increase linearly to modulus length. Decryption delay increases exponentially to modulus length that contribute to 83% of the end to end delay. Meanwhile, encryption and transmission are only 0.2% and 16.8% of the overall delay. In order to satisfy real-time requirement which demands delay less than 150 ms, encryption should use modulus length of 2000. By using this length, end to end delay can be minimized lower than 150 ms.

References
[1] Endeley, R.E. (2018) End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. Journal of Information Security, 9, 95-99.
[2] Bai, S. and Koong, K.S. (2017), "Financial and other frauds in the United States: a panel analysis approach", International Journal of Accounting & Information Management, Vol. 25 No. 4, pp. 413-433. https://doi.org/10.1108/IJAIM-03-2017-0033.
[3] Navarro, J. C., & Higgins, G. E. (2017). Familial identity theft. American Journal of Criminal Justice, 42(1), 218-230.
[4] Ellis, S. R. (2013). Fundamentals of Cryptography. In Computer and Information Security Handbook (pp. 1059-1066). Morgan Kaufmann.
[5] Shankar, K. (2018). An optimal RSA encryption algorithm for secret images. International Journal of Pure and Applied Mathematics, 118(20), 2491-2500.
[6] Iswari, N. M. S. (2016, October). Key generation algorithm design combination of RSA and ElGamal algorithm. In 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE) (pp. 1-5). IEEE.
[7] Al-Akaidi, M. (2017). A review on transport layer protocol performance for delivering video on an adhoc network. MS&E, 237(1), 012018.
[8] Suherman, S., Panjaitan, S. P., & Ginting, A. G. (2019, June). Impact Transport Layer Protocol Performances to the Encrypted Traffics. In Journal of Physics: Conference Series (Vol. 1235, No. 1, p. 012032). IOP Publishing.
[9] Candra, R. A., Ilham, D. N., & Sipahutar, E. (2020, January). Reducing link quality impact to encrypted packets by compressing the transmitted data. In IOP Conference Series: Materials Science and Engineering (Vol. 725, No. 1, p. 012110). IOP Publishing.
[10] Candra, R. A., Ilham, D. N., S Suherman, A Sani and D S Tarigan.(2019, April).The Impact of Buffer Queue Interface Size to The 802.11 Ad Hoc Network Performances. In IOP Conference Series: Materials Science and Engineering (Vol. 506, No. 1, p. 012039). IOP Publishing.
[11] Candra, R. A., Ilham, D. N., & Mubarakah N. (2019, April) Various layer techniques to improve video transmission on 20 GHz radio link in a rainy environment. In IOP Conference Series: Materials Science and Engineering (Vol. 506, No. 1, p. 012044). IOP Publishing.