1. Home
2. Innovations in Bio-Inspired Computing and Applications
3. Conference paper

End-To-End Security in Communication Networks: A Review

- Conference paper
- First Online: 10 April 2021
- pp 492–505
- Cite this conference paper

Innovations in Bio-Inspired Computing and Applications(IBICA 2020)

- Okpe Jonah Bameyi,
- Sanjay Misra,
- Francis Idachaba &
- Jonathan Oluranti

Part of the book series: Advances in Intelligent Systems and Computing ((AISC,volume 1372))
Included in the following conference series:

- International Conference on Innovations in Bio-Inspired Computing and Applications

- **658** Accesses
- **1** Citations

Abstract

Digital communications and e-commerce reshape corporate processes and add new risks to business activities. The recent outbreak of the coronavirus (COVID 19) pandemic, has led to an increase in the demand for instant messaging and videoconferencing. There has been the need to maximize the availability of messaging, and mostly videoconference platforms. These platforms provide end-to-end communications services. Organizations have asked staff to work from home which necessitates work from home as well as meeting up with regular work schedule meetings which are carried out via these platforms mentioned. Communication Networks provide channels for such tasks to be carried out. These networks are used for the transmission for a wide range of valuable and confidential information. As a result, they draw the interest of persons who want to intercept or manipulate data or interrupt or damage the storage or communication of the networks. In this study a review of security as it pertains end-to-end connection is presented, we looked at a brief background of the issues which includes a description of security engineering with attendant examples, made our findings and observations. The paper ends with a brief in the form of a case study of a few ICT firms that provide end-to-end services. Such services fall into the category of instant messaging (IM), videoconferencing and remote management, showing how much they value end-to-end encryption and the impact it could have on their businesses.

Similar content being viewed by others

End to End Security is Not Enough

Chapter © 2017

‘Changing Trend in Network Security Measures: A Review’

Chapter © 2018

End-to-End Security for IoT Communications: A Practical Implementation

Chapter © 2023

References

1. Glissa, G., Meddeb, A.: 6LowPSec: an end-to-end security protocol for 6LoWPAN. Ad Hoc Netw. **82**, 100–112 (2019). https://doi.org/10.1016/j.adhoc.2018.01.013

   Article Google Scholar

2. Ono, K., Tachimoto, S.: SIP signaling security for end-to-end communication. In: APCC 2003 - 9th Asia-Pacific Conference on Communications Conjunction with 6th Malaysia International Conference Communications, MICC 2003, Proceedings, vol. 3, pp. 1042–1046 (2003). https://doi.org/10.1109/APCC.2003.1274257

3. Huang, S.C.H., MacCallum, D., Du, D.Z.: Network security. Netw. Secur. 1–280 (2010). https://doi.org/10.1007/978-0-387-73821-5

4. Ozcelebi, T., Den Hartog, J.: Lecture Notes: Computer Networks and Security (2IC60), vol. 35, p. 197 (2019). https://www.win.tue.nl/~tozceleb/2IC60/lecture_notes.pdf

5. Okpe, Y.J.G.: Computer Network Security, Threats and Mitigation, vol. 14, no. 2 (2016)

   Google Scholar

6. Gondi, V., White, D.L., Gemmill, J., Christopher, W.: Security Vulnerabilities and Challenges in IoT End to End systems and Current Security Implementations, no. April (2016)

   Google Scholar

7. Behrens, R., Ahmed, A.: Internet of things: an end-to-end security layer. In: Proceedings of 2017 20th Conference on Innovations in Clouds, Internet and Networks, ICIN 2017, pp. 146–149 (2017)

   Google Scholar

8. Puthal, D., Nepal, S., Ranjan, R., Chen, J.: A synchronized shared key generation method for maintaining end-to-end security of big data streams. In: Proceedings of 50th Hawaii International Conference on System Sciences, pp. 6011–6020 (2017). https://doi.org/10.24251/hicss.2017.719

9. Choi, J., In, Y., Park, C., Seok, S., Seo, H., Kim, H.: Secure IoT framework and 2D architecture for end-to-end security. J. Supercomput. **74**(8), 3521–3535 (2018). https://doi.org/10.1007/s11227-016-1684-0

Article Google Scholar

10. Dinur, I., Dolev, S., Lodha, S.: Cyber Security Cryptography and Machine Learning, vol. 10879. Springer, Cham (2018)

Google Scholar

11. Rosler, P., Mainka, C., Schwenk, J.: More is less: on the end-to-end security of group chats in signal, WhatsApp, and Threema. In: Proceedings - 3rd IEEE European Symposium on Security and Privacy, EURO S&P 2018, pp. 415–429 (2018). https://doi.org/10.1109/EuroSP.2018.00036

12. Bhardwaj, K., Shih, M.W., Gavrilovska, A., Kim, T., Song, C.: SPX: preserving end-to-end security for edge computing, arXiv (2018)

Google Scholar

13. Cui, J., Shao, L., Zhong, H., Xu, Y., Liu, L.: Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks. Peer-to-Peer Netw. Appl. **11**(5), 1022–1037 (2018)

Article Google Scholar

14. Tanaka, H., Suzuki, H., Watanabe, A., Naito, K.: Evaluation of a secure end-to-end remote control system for smart home appliances. In: 2018 IEEE International Conference on Consumer Electronics, ICCE 2018, vol. 2018-January, pp. 1–2 (2018)

Google Scholar

15. Mukherjee, B., et al.: Flexible IoT security middleware for end-to-end cloud–fog communication. Futur. Gener. Comput. Syst. **87**, 688–703 (2018). https://doi.org/10.1016/j.future.2017.12.031

Article Google Scholar

16. Jan, M.A., Zhang, W., Usman, M., Tan, Z., Khan, F., Luo, E.: SmartEdge: An end-to-end encryption framework for an edge-enabled

smart city application. J. Netw. Comput. Appl. **137**, 10 (2019). https://doi.org/10.1016/j.jnca.2019.02.023

Article Google Scholar

17. Petroulakis, N.E., et al.: SEMIoTICS architectural framework: end-to-end security, connectivity and interoperability for industrial IoT. In: Global IoT Summit, GIoTS 2019 - Proceedings (2019)

Google Scholar

18. Sengupta, J., Ruj, S., Das Bit, S.: End to end secure anonymous communication for secure directed diffusion in IoT. In: ACM International Conference on Proceeding Series, pp. 445–450 (2019). https://doi.org/10.1145/3288599.3295577

19. Li, M., Nazir, S., Khan, H.U., Shahzad, S., Amin, R.: Modelling Features-Based Birthmarks for Security of End-to-End Communication System, vol. 2020 (2020)

Google Scholar

20. Maillet-Contoz, L., Michel, E., Nava, M.D., Brun, P.-E., Lepretre, K., Massot, G.: End-to-end security validation of IoT systems based on digital twins of end-devices, pp. 1–6 (2020). https://doi.org/10.1109/giots49054.2020.9119570

21. Odusami, M., Misra, S., Abayomi-Alli, O., Abayomi-Alli, A., Fernandez-Sanz, L.: A survey and meta-analysis of application-layer distributed denial-of-service attack. Int. J. Commun. Syst. **33**(18), e4603 (2020)

Google Scholar

22. Azeez, N.A., Salaudeen, B.B., Misra, S., Damaševičius, R., Maskeliūnas, R.: Identifying phishing attacks in communication networks using URL consistency features. Int. J. Electron. Secur. Digit. Forensics **12**(2), 200–213 (2020)

Article Google Scholar

23. Arogundade, O.T., Abioye, T.E., Sanjay, M.: An ontological approach to threats pattern collection and classification: a preliminary

study to security management. Int. J. Electron. Secur. Digit. Forensics **12**(3), 323–335 (2020)

Article Google Scholar

24. Osho, O., Musa, F.A., Misra, S., Uduimoh, A.A., Adewunmi, A., Ahuja, R.: AbsoluteSecure: a tri-layered data security system. In: International Conference on Information and Software Technologies, pp. 243–255. Springer, Cham, October 2019

Google Scholar

25. Jambhekar, N.D., Misra, S., Dhawale, C.A.: Cloud computing security with collaborating encryption. Indian J. Sci. Technol. **9**(21), 1–7 (2016)

Article Google Scholar

26. Dhawale, C.A., Misra, S., Jambhekar, N.D., Thakur, S.U.: Mobile computing security threats and solution. Int. J. Pharm. Technol. **8**, 23075–23086 (2016)

Google Scholar

27. Odun-Ayo, I., Ajayi, O., Misra, S.: Cloud computing security: issues and developments. Lecture Notes in Engineering and Computer Science, vol. 2235 (2018)

Google Scholar

28. Granjal, J., Monteiro, E., Silva, J.S.: On the effectiveness of end-to-end security for internet-integrated sensing applications. In: Proceedings - 2012 IEEE International Conference on Green Computing and Communications, GreenCom 2012, Conference on Internet Things, iThings 2012 Conference Cyber, Phys. Soc. Comput. CPSCom 2012, pp. 87–93 (2012). https://doi.org/10.1109/GreenCom.2012.23

29. TeamViewer: End-to-End Network and Data Security for Remote Access | TeamViewer (2020). https://www.teamviewer.com/en/features/end-to-end-security/%0ADownload. Accessed 15 July 2020

30. Lee, J., Kim, S., Kim, K.: Security analysis of end-to-end encryption in telegram. TThe Inst. Electron. Inf. Commun. Eng. 1–6 (2017)

Google Scholar

31. WhatsApp Inc., “WhatsApp Encryption Overview - Technical white paper (2017). https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

32. Yuan, E.: Zoom Acquires Keybase and Announces Goal of Developing the Most Broadly Used Enterprise End-to-End Encryption Offering - Zoom Blog. Zoom (2020). https://blog.zoom.us/wordpress/2020/05/07/zoom-acquires-keybase-and-announces-goal-of-developing-the-most-broadly-used-enterprise-end-to-end-encryption-offering/. Accessed 15 July 2020

33. Lerman, B.R.: Zoom works to make service more secure, even for free users (2020). https://www.washingtonpost.com/technology/2020/06/17/zoom-encryption-all-users/. Accessed 15 July 2020

Download references

Author information

Authors and Affiliations

1. **Covenant University, Ota, Nigeria**
   Okpe Jonah Bameyi, Sanjay Misra, Francis Idachaba & Jonathan Oluranti

Corresponding author

Correspondence to Sanjay Misra .

Editor information

Editors and Affiliations

1. **Scientific Network for Innovation and Research Excellence, Machine Intelligence Research Labs (MIR Labs), Auburn, WA, USA**
   Ajith Abraham

2. **National Institute of Information and Communications Technology (NICT), Koganei, Tokyo, Japan**
   Hideyasu Sasaki
3. **Universidade Federal da Bahia, Salvador, Brazil**
   Ricardo Rios
4. **Scientific Network for Innovation and Research Excellence, Machine Intelligence Research Labs (MIR Labs), Auburn, WA, USA**
   Niketa Gandhi
5. **Institute of Technology and Science, Ghaziabad, Uttar Pradesh, India**
   Umang Singh
6. **School of Information Science and Engineering, University of Jinan, Jinan, Shandong, China**
   Kun Ma

Rights and permissions

Reprints and permissions

Copyright information

About this paper

Cite this paper

Bameyi, O.J., Misra, S., Idachaba, F., Oluranti, J. (2021). End-To-End Security in Communication Networks: A Review. In: Abraham, A., Sasaki, H., Rios, R., Gandhi, N., Singh, U., Ma, K. (eds) Innovations in Bio-Inspired Computing and Applications. IBICA 2020. Advances in Intelligent Systems and Computing, vol 1372. Springer, Cham. https://doi.org/10.1007/978-3-030-73603-3_46

Download citation

- .RIS
- .ENW
- .BIB

- DOIhttps://doi.org/10.1007/978-3-030-73603-3_46

- Published10 April 2021
- Publisher NameSpringer, Cham
- Print ISBN978-3-030-73602-6
- Online ISBN978-3-030-73603-3
- eBook PackagesIntelligent Technologies and RoboticsIntelligent Technologies and Robotics (R0)