Documents

Paris, I.L.B.M.[a] , Habaebi, M.H.[a] , Zyoud, A.M.[b]

Implementation of SSL/TLS Security with MQTT Protocol in IoT Environment
(2023) *Wireless Personal Communications*, 132 (1), pp. 163-182. Cited 1 time.

DOI: 10.1007/s11277-023-10605-y

[a] Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[b] Department of Electrical and Computer Engineering, Birzeit University, Birzeit, Ramallah, Palestine

Abstract

Internet of Things (IoT) is the interconnection of devices with the internet to deliver its tasks. Nowadays, security is the main concern relating to these devices. Low in power storage, low in processing capabilities and low in data storage make it hard to provide a strong set of security protocols to protect the vulnerable devices “things”. Having internet as its backbone, allows the devices to communicate seamlessly. However, without any form of protection, it would open the door for hackers or middleman to hijack the connection, steal data and sabotage the information. In this paper, Secure Socket Layer and Transport Layer Security (SSL/TLS) protocol is implemented on top of Message Queuing Telemetry Transport (MQTT) IoT application protocol and the performance of the network is evaluated and analyzed in a typical IoT testbed comprising Raspberry Pi4 and ESP32 nodes. This work focuses on energy consumption, generated overhead, system complexity and required data storage resources. Experimental results of stress testing the system indicates that SSL/TLS encryption, operating with MQTT Quality of Service (QoS) level 2, while increasing the traffic rate 3.5 orders of magnitude yields more than two thousand times the amount of overhead generated and results in 73.25 J of consumed energy. Whereas operating without the SSL/TLS encryption under the same stress testing conditions yields only 140 times the amount of overhead generated and results in a mere 18.76 J of consumed energy. This difference of 4 folds on consumed energy indicates that the SSL/TLS -enabled node battery can only last a quarter of the lifespan of the TLS-free node and concluding the SSL/TLS encryption is not a viable solution for battery-operated IoT nodes.

Author Keywords
Energy harvesting; IoT; MQTT; Performance analysis; Protocols; Security; TLS/SSL

Index Keywords
Cryptography, Digital storage, Electric batteries, Energy utilization, Internet of things, Network protocols, Network security, Personal computing, Quality of service; Consumed energy, Data storage, Message queuing telemetry transport, Performances analysis, Secure sockets layers, Security, Stress Testing, TLS/SSL, Transport layer security, Transport protocols; Energy harvesting

References

- Canedo, J., Skjellum, A.
  Using machine learning to secure IoT systems
  (2016) *2016 14Th Annual Conference on Privacy, Security and Trust (PST)*, pp. 219-222.
  IEEE

- (2022) *Number of Iot Connected Devices Worldwide 2019–2021, with Forecasts to 2030*, 22 November

- Kasinathan, P., Pastrone, C., Spirito, M.A., Vinkovits, M.
  Denial-of-service detection in 6LoWPAN based internet of things
  (2013) *2013 IEEE 9Th International Conference on Wireless and Mobile Computing, Networking and Communications (Wimob)*, pp. 600-607.
  IEEE

- Ali, I., Sabir, S., Ullah, Z.
  Internet of things security, device authentication and access control: a review
  (2016) *International Journal of Computer Science and Information Security IJCSIS*, 14 (8), pp. 456-466.

- Dineva, K., Atanasova, T.
  Security in iot systems

(2019) *19Th International Multidisciplinary Scientific Geoconference SGEM 2019*, 2 (1), pp. 569-578.

- Tandale, U., Momin, B., Seetharam, D.P.
  An empirical study of application layer protocols for IoT
  (2017) *. in 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing*, pp. 2447-2451.

- Sethi, P., Sarangi, S.R.
  Internet of things: Architectures, protocols, and applications
  (2017) *Journal of Electrical and Computer Engineering.*,

- Tiburski, R.T., Amaral, L.A., De Matos, E., De Azevedo, D.F., Hessel, F.
  The role of lightweight approaches towards the standardization of a security architecture for IoT middleware systems
  (2016) *IEEE Communications Magazine*, 54 (12), pp. 56-62.

- Jokela, P., Moskowitz, R., Nikander, P.
  (2008) *Using the encapsulating security payload (ESP) transport format with the host identity protocol (HIP*,
  . RFC5202l

- Bensalah, F., El Kamoun, N., Bahnasse, A.
  Evaluation of tunnel layer impact on VOIP performances (IP-MPLS-MPLS VPN-MPLS VPN IPsec)
  (2017) *International Journal of Computer Science and Network Security (IJCSNS)*, 17 (3), p. 87.

- Thomas, S.
  (2000) *SSL and TLS essentials, securing the web*, p. 3.
  John Wiley and Sons

- Chen, X.
  (2014) *Constrained application protocol for internet of things. URL*,

- Prantl, T., Iffländer, L., Herrnleben, S., Engel, S., Kounev, S., Krupitzer, C.
  Performance impact analysis of securing mqtt using tls
  (2021) *In Proceedings of the ACM/SPEC International Conference on Performance Engineering*, pp. 241-248.

- Baranauskas, E., Toldinas, J., Lozinskis, B.
  Evaluation of the impact on energy consumption of MQTT protocol over TLS
  (2019) *CEUR Workshop Proceedings: IVUS 2019 International Conference on Information Technologies: Proceedings of the International Conference on Information Technologies, Kaunas, Lithuania, April 25, 2019*, 2470, pp. 56-60.
  CEUR-WS

- Shapsough, S., Aloul, F., Zualkernan, I.A.
  Securing low-resource edge devices for IoT systems
  (2018) *In 2018 International Symposium in Sensing and Instrumentation in Iot Era (ISSI), IEEE.*, pp. 1-4.

- Laaroussi, Z., Novo, O.
  A performance analysis of the security communication in CoAP and MQTT
  (2021) *. in 2021 IEEE 18Th Annual Consumer Communications & Networking Conference (CCNC), IEEE.*, pp. 1-6.

- Silva, C., Toasa, R., Martinez, H.D., Veloz, J., Gallardo, C.
  (2017) *Secure push notification service based on MQTT protocol for mobile platforms*, pp. 69-84.

In XII Jornadas Iberoamericanas de Ingeniería de Software e Ingeniería del Conocimiento y Congreso Ecuatoriano en Ingeniería de Software

- Alghamdi, K., Alqazzaz, A., Liu, A., Ming, H.
Iotverif: An automated tool to verify ssl/tls certificate validation in android mqtt client applications
(2018) *In Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, pp. 95-102.

- Saverimoutou, A., Mathieu, B., Vaton, S.
Which secure transport protocol for a reliable HTTP/2-based web service: TLS or QUIC
(2017) *?. in 2017 IEEE Symposium on Computers and Communications (ISCC), IEEE.*, pp. 879-884.

- Seufert, M., Schatz, R., Wehner, N., Gardlo, B., Casas, P.
Is QUIC becoming the new TCP? On the potential impact of a new protocol on networked multimedia QoE
(2019) *In 2019 Eleventh International Conference on Quality of Multimedia Experience (Qomex), IEEE*, pp. 1-6.

- Lampkin, V., Leong, W.T., Olivera, L., Rawat, S., Subrahmanyam, N., Xiang, R., Locke, D.
(2012) *Building smarter planet solutions with mqtt and ibm websphere mq telemetry*,
IBM Redbooks

- Wukkadada, B., Wankhede, K., Nambiar, R., Nair, A.
Comparison with HTTP and MQTT in internet of things (IoT)
(2018) *In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), IEEE*, pp. 249-253.

- Habaebi, M.H., Al-Haddad, A., Zyoud, A., Hijazi, G.
Micro search engine for IoT: An IoT search engine prototype for private networks
(2018) *Recent Advances in Electrical and Electronic Engineering*, 11 (2), pp. 123-131.

- Hijazi, G., Hadi Habaebi, M., Al-Haddad, A., Zyoud, A.M.
Stress testing MQTT server for private IOT networks
(2021) *International Journal of Electronics and Telecommunications*, 67 (2), pp. 229-234.

- Carlsson, F., Eriksson, K.-G.
(2018) *Comparison of security level and current consumption of security implementations for MQTT (Master Dissertation)*,
Retrieved from

- Yassein, M.B., Shatnawi, M.Q., Aljwarneh, S., Al-Hatmi, R.
Internet of things: Survey and open issues of MQTT protocol
(2017) *In 2017 International Conference on Engineering & MIS (ICEMIS), IEEE*, pp. 1-6.

- Rodríguez, C., Baez, M., Daniel, F., Casati, F., Trabucco, J.C., Canali, L., Percannella, G.
REST APIs: A large-scale analysis of compliance with principles and best practices
(2016) *. in International Conference on Web Engineering*, pp. 21-39.
Springer, Cham

- Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T.
(1999) *Hypertext Transfer protocol–HTTP/1.1*,

- ESP 32 Series Datasheet (2018)

Correspondence Address
Habaebi M.H.; Department of Electrical and Computer Engineering, Malaysia; email: habaebi@iium.edu.my

Publisher: Springer

ISSN: 09296212
CODEN: WPCOF
Language of Original Document: English
Abbreviated Source Title: Wireless Pers Commun
2-s2.0-85165684814
Document Type: Article
Publication Stage: Final
Source: Scopus