Prof. Dr. Berna Örs Yalçın Due Date: June 19, 2022

BLG520E Cryptography
3rd Project

We will implement a secure authentication, key exchange and data encryption protocol for IoT which is called Transport Layer Security (TLS) in this project.

1. Give a brief description of the protocol.
2. Implement the protocol by using your choice of programming language.
3. Prove that your implementation works correctly.
4. Give the programme memory, run time memory used for your implementation. Also give the speed properties of your implementation.

As an example the slides for simple station-to-station (StoS) protocol can be accessed from Ninova course sources. Some references about Security Protocols for Internet of Things (IoT) are given below.

References

1. Erich Styger, IoT Security and the Transport Security Layer, https://dzone.com/articles/iot-and-the-transport-security-layer
2. Larry Loeb, A Security Protocol for the Internet of Things, https://securityintelligence.com/a-security-protocol-for-the-internet-of-things/
3. Göran Selander, Application Layer security protocols for the IoT
4. Snehal Deshmukh, S. S. Sonavane, D. Y. Patil, Security Protocols for Internet of Things: A Survey, 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2)
5. IoT Standards and Protocols, https://www.postscapes.com/internet-of-things-protocols/#protocols
6. Mohamed Hammi, Erwan Livolant, Patrick Bellot, Ahmed Serhrouchni, Pascale Minet, A Lightweight IoT Security Protocol, HAL Id: hal-01640510
7. Ahmed Mohammed Ibrahim Alkuhlani, Dr S.B. Thorat, Internet of Things (IOT) Standards, Protocols and Security Issues, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 11, November 2015
8. Nathalie Mitton, Hakima Chaouchi, Thomas Noel, Thomas Watteyne, Alban Gabillon, Patrick Capolsini, Interoperability, Safety and Security in IoT, Second International Conference, InterIoT 2016 and Third International Conference, SaSeIoT 2016, Paris, France, October 26-27, 2016, Revised Selected Papers
9. Victor Chang, Gang Sun, Jin Li, Security and Privacy for Multimedia in the Internet of Things (IoT), in Multimedia Tools and Applications (2018)
10. Sandip Ray, Yier Jin, Security Challenges in the IoT Regime, in Journal of Hardware and Systems Security (2017)
11. Jongseok Choi, Youngjin In, Changjun Park, Seonhee Seok, Secure IoT framework and 2D architecture for End-To-End security, in The Journal of Supercomputing (2018)
12. Luciano Barreto, Antonio Celesti, Security and IoT Cloud Federation: Design of Authentication Schemes, in Internet of Things. IoT Infrastructures (2016)
13. Shruti Jaiswal, Daya Gupta, Security Requirements for Internet of Things (IoT), in Proceedings of International Conference on… (2017)