GITF333: IoT Security
Spring 2019

Exercise No. 2

Notice that you should *not* submit the paper.

1. Describe ‘raw public key’ and compare it with X.509 certificate
2. Describe the DTLS using authorized public key (APK).
3. Describe briefly the scheme, attribute-based encryption.
4. Briefly describe the ‘RPL’ routing protocol.
5. Describe the ‘Selective forwarding attack’ on sensor network routing or IoT routing
6. Describe the ‘hello flood attack’ on sensor network routing or IoT routing
7. Describe the ‘wormhole attack’ on sensor network routing or IoT routing.