Computer Science, Florida Tech Dr. Abdullah Aydeger

CSE 4820 – Fall 2022

Quiz #4

Due: 10/27/2022 10:45AM

You are welcome to use any figure/text that you find online. However, you MUST provide your reference (i.e., website link, slide number, book chapter, etc.).

Please answer what is being asked only and provide any justification/assumptions you make.

1. What is SDR and what can we do with them? Using SDR, can you do replay attack? Why or why not (what is your assumption)? Explain in short. (60p)

Software Defined Radios (SDR) are software radio frequency communication used to send and receive data over radio, and they are used commonly to transmit data wirelessly over short or long distances. Good examples include car keys, gate/garage keys, and car radio. Using software, we can record or play these signals to devices. A replay attack is possible if the signal is recorded and sent between the same type of device, assuming that the type of modulation (AM, FM, etc.), the encoding, and the protocol that the device is using is the same as the data that was recorded. If not, a replay attack will not work.

Even then, lots of devices use extra security protocols on top of that, such as a sliding scale in cars, so when the clicker is used to unlock the car, the register of keys being used by the car and transmitter is shifted, so a replay attack is not possible unless you jam the signal to the car, capture the fob's signal, and replay without the user unlocking with that particular set of keys. In short, SDR *can* be used to do a replay attack, but understanding the devices, their protocols, and the radio signals being sent are very important to make a replay work properly, or else replay attacks are not very viable/effective.

2. Why do we need Zigbee as wireless protocol? (10p)

Zigbee is needed because it fulfills requirements that other protocols can't, namely low power usage, persistent power, and simple data stack. Because it has such a simple stack and low power draw, devices with Zigbee can be consistently and reliably on for years at a time without external power sources, making it ideal in environments where WiFi or other standards aren't able to work.

3. Zigbee uses AES 128-bit key, and AES is claimed to be secure cryptographic algorithm. Yet, we discussed it may still not be secure for Zigbee. Why is that? Please provide an example to explain. (30p)

Despite using AES, Zigbee simply sends network and link keys in plaintext without encryption, so it is very easy to intercept those keys for attacks, especially because authentication isn't mutual in many cases, so it is easy to spoof a network to attack a device with those keys. Keeping the keys on as many as thousands of Zigbee devices secure by generating, changing, and revoking keys is quite the challenge.