CSE 4820 Fall 2022

Final Exam

Grant Butler

Table of Contents

1. Most Interesting Information

What is the most interesting information (that you think it is) that you have learned in the class throughout the semester? (10p)

Our labs and the hands on experience has been invaluable in learning exactly what it means to break the different protocols that we have learned about. In movies, hacking is never quite shown correctly and having the firsthand experience seeing what happens when a malicious party attempts to gain control of one of the wireless devices that we use on an everyday basis allows me to see the amount of vulnerabilities that are truly present in them. The perspective gained from understanding that helps me see that there is much to be improved upon when it comes to wireless security, and the puzzle of trying to increase reliability and security while optimizing for sub-optimal hardware is something that will continue to be of interest to me.

2. Common Security Vulnerability

What do you think is the common security vulnerability for the wireless/mobile communication protocols that we have covered? Please explain in short. (15p)

The most common security vulnerability in most of the different protocols that we have seen had to be replay attacks specifically because of packets being sent with either very basic encryption or simply plain text. The surprising lack of encryption when it comes to the communication protocols seems to be intrinsic to wireless technologies ease of use.

The convenience factor of being able to connect and disconnect to a wireless router no matter the device being used is an integral part of Wi-Fi or Bluetooth, so packets like de-authentication or the handshake being public allow us to exploit the low security measures being used.

Alongside this, the backwards compatibility of protocols is also a large downfall, seen in Bluetooth or SSL allow us to rollback which version is being used to allow us to attack the devices without dealing with the increased security in later versions. Thus, the intrinsic promise of wireless' convenience is often its downfall.

3. Z-Wave Slave vs. Controller

Let's assume that you have obtained a root access to a Z-Wave slave device. What can you do in the Z-Wave network that the slave is connected to? Instead of Z-Wave slave device, if you were to get access to a Z-Wave controller, what would be the differences and similarities that you can do? Please explain. (20p)

The differences in a Z-Wave Slave and Controller device are as follows:

Controller Device

- portable or static, being battery powered able to relearn network topology or consistent source and connected to other networks to provide services between Z-Wave and IP.

Slave Device

- typically battery powered and wireless.
- requires permission from the controller to be able to join/leave a network
- only really sends data back to the controller.

Z-Wave Authentication

- Inclusion & Exclusion: requires physical access to controller
  - authenticates slave devices with inclusion mode, telling the controller the capabilities of the slave node.
  - uses exclusion mode to remove a node which has to happen before a slave device can leave the network.

With a slave device, not much can be done in the network. A slave node can be routing or non-routing, meaning that the node can either participate in the mesh or vice-versa. With root access to that specific node, though, you could easily send it commands. For instance, if the device is a camera or a door lock, you could tap into the video feed or open the door with your access.

A controller device is different, however. You can access the information from all of the different devices in the network, and send commands to all of them. You could even remove or add a device from the network using Inclusion/Exclusion. Using the controller, you can wreak havoc on the entire network and potentially cause a lot of harm to the devices on it.

4. Zigbee End Device vs. Coordinator

Similarly in the question #4, if it was Zigbee Coordinator instead of Z-Wave, what would be the similarities and differences that you can do. Please elaborate. (15p)

Similarly to to Z-Wave, Zigbee has nodes that are 'end devices' and a 'coordinator', which work similarly to slave and controller nodes. One problem with Zigbee is that each frame sent in the network has a frame counter, which increments and has a maximum number of `0xffffffff - 1`, and once it reaches that, the entire network goes offline and needs to be manually reset.

With access to an end device, you could send nonsensical packets to artificially cause the network to increase the frame counter to the point of no return, essentially disrupting the entire network without the need to access the coordinator. This Denial of Service attack allows you to take the Zigbee network offline with little work.

With a coordinator, you can again access all of the network's nodes and the information being sent back to the coordinator. This could mean unlocking doors, tapping into audiovisual feeds, and much more. Having access to the coordinator/controller node on either Z-Wave or Zigbee allows you to do anything that the owner of the network could do, and much more.

5. LoRaWAN Cellular

Can we do all cellular networks with LoRaWAN instead LTE? Why or why not? If it was possible, would this provide a better security? Why/why not? (20p)

Using LoRaWAN as a cellular network is possible, but with a lot of problems. The nature of LoRa is that it is a long range communication protocol that is ideal for 'small chunks of data with low bit rates.' This intrinsically contrasts with the idea of LTE, where it is built for large amounts of data sent at consistently high bit rates. Not to mention, the narrow bandwidth of the LoRaWAN protocol makes interference between signals very common. This would mean that watching a video over LoRaWAN would be largely impossible, including lots of artifacts due to interference along with long buffering times due to the low bitrate and chunk size of the packets being sent. Even with its low power draw, LoRaWAN isn't ideal for cellular since it cannot keep up with the amount of data being sent over cellular, both in size and frequency of communication.

6. eSIM Cellular

An eSIM is an industry-standard digital SIM that allows you to activate a cellular plan from your carrier without having to use a physical SIM. You can install eight or more eSIMs on an iPhone and use two phone numbers at the same time. What do you think of eSIM and its security benefits? If eSIM was possible within GSM network, would this solve its security problems? If so, how? If not, why not? (20p)

eSIM intrinsically brings more security simply because it is not a physical object that can be stolen from you, along with the convenience of being able to store as many eSIMs as you can on one device. This is ideal for someone who often travels to different parts of the world and wants to have one device to communicate no matter the network that they are near. eSIM also brings security benefits in terms of law enforcement, since it can be instantly traced to a phone by an authority. One problem that is quite prominent with GSM is that you could simply use a stolen SIM card to authenticate with the network and gain access.

eSIM benefits from being separate from GSM, but also its digital nature means that it is accessible from the internet, so having it be decentralized from GSM that an attacker could use it to authenticate without connecting to GSM, and simply hijack the network without physical access to the phone. This puts the eSIM in a poor position as the data can be hijacked without access to the device.

Despite the lack of GSM's central authentication, eSIM still seems to be a more secure implementation of SIM, especially as encryption algorithms grow more and more secure. The bigger problems that I see are if the current implementation is vulnerable and future implementations allow for backwards compatibility, allowing attackers to downgrade the security of eSIM. Hopefully history will not repeat itself in that way.

7. Bonus

What was the research challenge the guest speaker Maryna Veksler talk about and what was their proposed approach? (10p)

Maryna talked about using LoRa and Unmanned Aerial Vehicles (UAVs) to fingerprint communications over the LoRa protocol and check for impersonation and random delay attacks. The implementation of UAVs allows this to happen without any changes in the physical layer due to LoFin's resistance to changes in RF signals and LoRa's parameters and using them to fingerprint communication devices. This makes the future of LoRaWAN more secure as it is used for long distance communication, especially because their test results showed an astounding 100% detection of unknown devices.