Lab7: Robot Bluetooth Hijacking

Pre-Requisite Knowledge and Skills

1. Understand basic knowledge of Sparki robot.
2. Be able to compile and upload a code.
3. Be able to run Python3

Learning Objective:

1. Understand how Bluetooth works in Sparki.
2. Understand Server and Client application model.
3. Understand the Malware.
4. Understand the usage of sniffing attack
5. Explain the Hijacking attack.

Recommended Running Environment and Software:

1. Computers Running Windows OS, OSX, or Linux
2. Python3
3. SparkiDuino IDE

Instructional Material:

1. Sparki Robot
2. Instructions of this activity
3. Server and Client applications

Video Demonstration:

1. to be developed

Lab Assessment:

1. Exercises
2. Quiz

Lab Instructions

This lab requires two (2) PCs, running Window OS, OS X, or Linux, and one of two PCs should be Bluetooth capable. It also requires Sparki and Bluetooth card included in Sparki package. In addition, Python3 should be installed in both PCs to run the applications.

For the convenience, let's label PCs as PC1 and PC2. PC1 is a Sparki robot user and PC2 is an attacker. Sparki robot user uses Bluetooth connection to controller the robot. For this purpose, Sparki user should create the Bluetooth connection and upload the code. First, we will need to connect PC1 to Sparki using Bluetooth. Bring the Bluetooth card from the box and plug it into the Bluetooth communication pins in the Sparki as shown in Figure 1.

The next step is Python 3 installation. Use following links to install the Python 3 for the corresponding Operating System (OS).

Woidnows 10: https://phoenixnap.com/kb/how-to-install-python-3-windows
Mac OS X: https://docs.python-guide.org/starting/install3/osx/
Linux: https://docs.python-guide.org/starting/install3/linux/

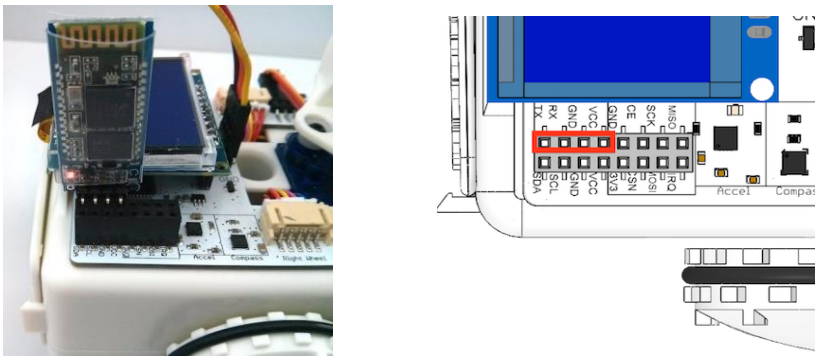


Figure 1. Bluetooth card setup

Now, we need to write a code for Sparki to check if there is any command received on Bluetooth connection and take an action if command is arrived. The structure of code is consisted of two part, read the communication channel and make a move based on reading. Use the code developed from previous lab 6.

Step 1: Compile and upload the code. Then, disconnect the cable and turn the Sparki on.

Now we need to create the Bluetooth connection between Sparki robot and PC1.

Step 2: On PC1, open the Bluetooth setting. "Windows > Setting > Devices > Bluetooth & other devices", then click "Add Bluetooth or other device". Find the device called "ArcBotics" and enter the PIN, "0000" (four zeros) for ArcBotics as shown in Figure 2.
Note: This setup may differ based on OS.

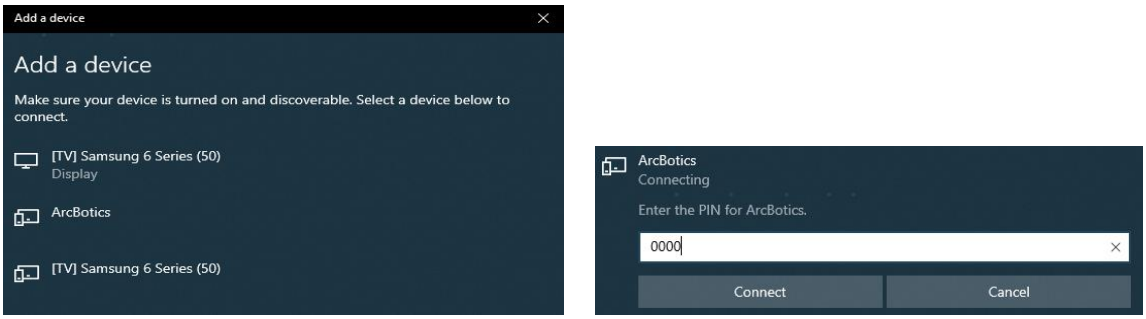
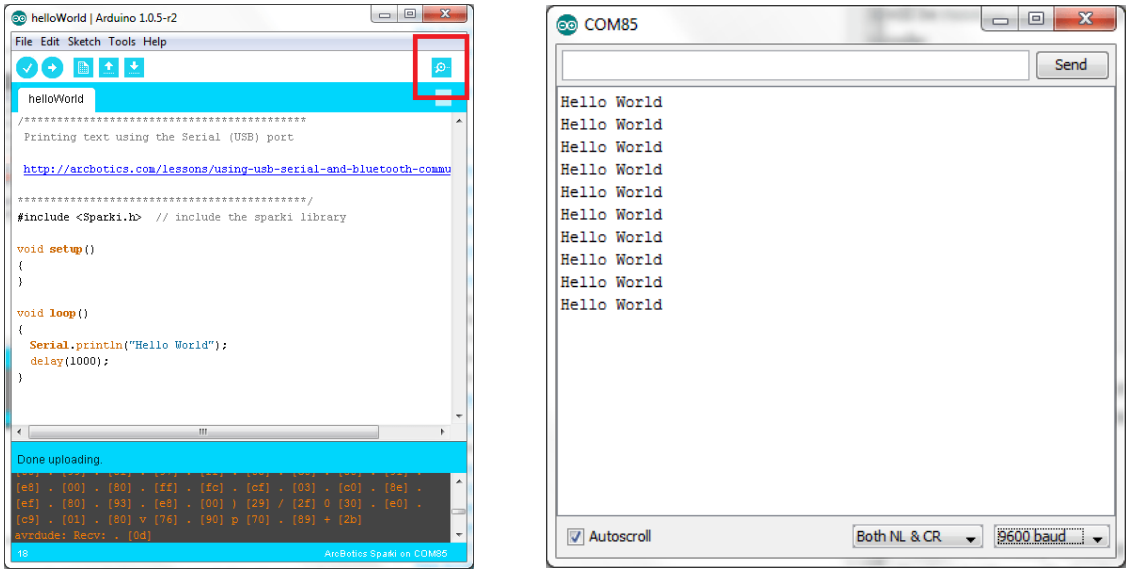


Figure 2. Bluetooth setup in Windows 10

Step 3: Once the Sparki is connected through Bluetooth, Sparki receives a command using serial port. Open serial monitor by selecting "Tools > Serial Monitor" or clicking icon on the top right corner of the IDE as shown in Figure 3.



(a) Serial monitor icon. (b) Serial monitor

Figure 3. Serial monitor

Once the serial monitor is open, send a command to move Sparki.

Step4: In this step, we will run a Malware on PC1 to find the Sparki commands. Use following scenario for the rest of activities.

Scenario: PC1 is a controller unit of the Sparki using Bluetooth and PC2 is a sniffer to find the Sparki commands and hijacking the robot. PC1 and PC2 should be in the same network. If wireless router is available, connect PC1 and PC2 to wireless router in wired or wireless. Assuming that DHCP server is running on the router. If wireless router is not available, use switch to connect PCs. Connect PCs to the switch and assign IP address to each PCs. Go to "Window > Setting > Network & Internet > Change adapter options". Right click on "Ethernet" and click Properties and select "Internet Protocol Version 4 (TCP/IP4)" and click "Properties". Then, select "User the following IP address" and assign IP address and subnet mask properly. Use following information to assign IP address and subnet mask.

PC1: IP address: 192.168.10.5 Subnet mask: 255.255.255.0
PC2: IP address: 192.168.10.10 Subnet mask: 255.255.255.0

Then, click OK and click OK on "Ethernet Properties" window to make it effective. You may need to check if IP address is effective using Command Prompt. Press "window button + R" together and type "cmd" and click "OK". And type "ipconfig" to check if they are all assigned correctly.
Run the Malware "server.py" on PC1. Once it is running, it will display server IP address and searching running devices on PC1. Select the number with ArcBotics and enter. Then, server is ready. As shown in Figure 4 and 5.

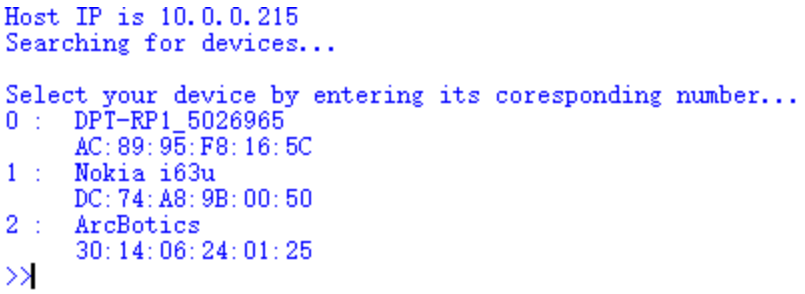


Figure 4. Device selection at server

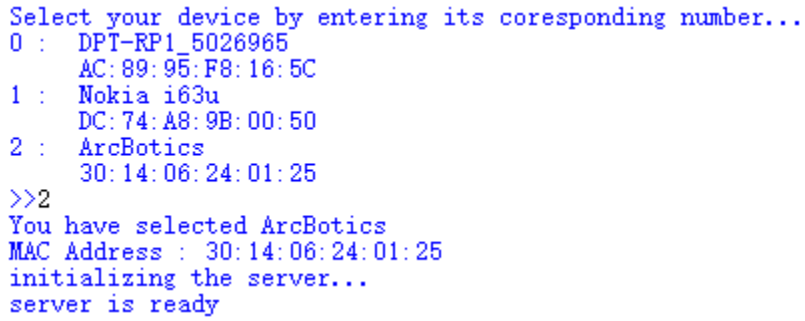


Figure 5. Display when server is ready

Step 5: Now we need to run "client.py" on PC2. Once you run it, all the command form PC1 to Sparki can be seen at PC2. Sniff the commands and take over the robot.

Step 6: Two students can be grouped in one team. One student writes a new code to move Sparki and hide the commands from the other team member. While student moves Sparki, the other team member is spying the PC1 and find the commands for Sparki moves. Then, hijack the robot by sending a command.

Discussion

- **Discuss the differences between passive and active attack. What are the examples of them?**

  Passive attack sneaks into the system and extract the information only. It does not harm or change the system but read or steal the information from the system. Active attack modifies the system or affect the system operation. Examples of passive attack are tapping, scanning, and traffic analysis. Tapping is monitoring the telephone communications. Scanning scans the open ports or a weak operating system version. Traffic analysis monitors the internet traffic and gather the useful information. Examples of active attack are virus, password cracking, denial of service, and etc.

- **Compare sniffing and hijacking attacks in terms of passive and active attacks.**

  Sniffing attack is passive attack and hijacking attack uses both passive and active attacks.

- **Comparing passive and active attacks, which one is more harmful and difficult to detect? What security strategy should be used for each attack type?**

Active attack makes it harmful to the system while passive attack steals the information only. Since active attack modifies the system, it can be easily notified. However, passive attack does not actively show its existence but stays quiet and steals the critical information. In terms of detection, passive attack is more difficult. For the security strategy, active attack uses detection while passive uses prevention.

Appendix

Bluetooth code for Sparki

```
#include <Sparki.h> // include the sparki library

String inputString; //make an empty String called inputString
boolean returnFlag; //flag to check for carriage return
char commArray [10]; //array to store communication
int arrayCounter = 0; //integer to count through commArray

void setup()
{
 Serial1.begin(9600);
}

void loop()
{
 readComm();
 makeMove();
}

void makeMove()
{
 for(int i = 0; i <= 9; i++)
  {
  if(commArray[i] == 'f')
   {
   sparki.moveForward();
   delay(1000);
   sparki.moveStop();
   }
   else if (commArray[i] == 'r')
   {
   sparki.moveRight(90);
   }
   else if (commArray[i] == 'l')
   {
   sparki.moveLeft(90);
   }
   else if (commArray[i] == 's')
   {
   sparki.moveStop();
   delay(1000);
   }
```

```
   else if (commArray[i] != 0) //in case it's a character sparki doesn't know
   {
   Serial1.print("I'm sorry, I didn't understand the command- ");
   Serial1.println(commArray[i]); //send the character back
   }
 }
 memset(commArray, 0, sizeof(commArray)); //clear out commArray
}

void readComm()
{
 while (Serial1.available())
 {
 int inByte = Serial1.read();
 if ((char)inByte == 'n')
   {
   returnFlag = true;
   arrayCounter = 0;
   }
   else
   {
   if(inByte == 32) //if it's a blank space
   {
   arrayCounter ++; //increment array counter to store in new array space
   }
   else
   {
   //add the character to the arrayCounter space in commArray
   commArray[arrayCounter] = (char)inByte;
   }
  }
 }
}
```