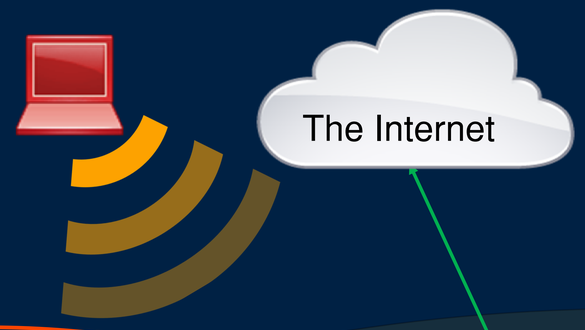
Security of the Internet of Things (IoT)

Tyler Williams | Jordan Frantsvog | Saeed Almalki
Mentor: Dr. Abdulrahman Yarali
Murray State University | Telecommunications System Management

Outside attackers getting in

Nefarious individuals outside of networks have many avenues to gain access without ever stepping inside thanks to common vulnerabilities and poor practices on modern networks. A rogue Access Point could be setup outside and transmit a WiFi signal into the same area as any other network and masquerade as the legitimate network. Since devices connect to the known network with the strongest signal, if the Rogue Access Point can push a signal stronger than the legitimate router, then devices will automatically start to fall into the hands of the enemy and hand over all the information it has about the network. However, if the network is vulnerable for other reason, like weak WiFi encryption, there are other ways to gain ac-



WiFi vulnerabilities and unsafe practices

Wireless networks secured with WPA2 were thought to be secure until October of 2017 when the Key Reinstallation Attack (KRACK) was announced by researchers at KU Leuven, a Belgium University. This method of gaining access to WPA2 traffic was not device specific leaving any wirelessly connected device vulnerable until patches were released. Some device are still vulnerable to this attack if not updated. WPA2 passwords are vulnerable to a series of other attacks if a weak password is used. Any device without a patch, secure password, and, as already known, still on a wireless network using WEP or no encryption is vulnerable.

Antivirus and passwords

The computers on your network must also be secured by keeping your operating system and programs up to date. Every computer should be running antivirus software to prevent malware from damaging your system or ransomware like WannaCry from taking data hostage. A password or passcode should be decided upon without consulting easily identifiable information, such as birthday, social security, hobbies, etc., using this information risks compromising that password as opposed to a randomly generated password. Never write passwords down on paper by your computer, if you have trouble remembering your passwords use a password man-

Dolphin Attacks

A dolphin attack, coined by researchers at Cornell University, is an attack on voice recognition services, like Siri, Amazon Alexa, and Google Assistant, that is named for the inaudible audio that makes it possible. The audio played at frequencies > 20 kHz, which is inaudible to humans but can still be picked up by microphones on these devices, can contain any command that the voice recognition service can normally recognize. These commands can include ordering items online, calling on smartphones, and controlling smart home devices including door locks. Up to this point an inaudible attack is unlikely without specialized speakers, but Bluetooth speakers could send an audible command if

Bluetooth Vulnerability

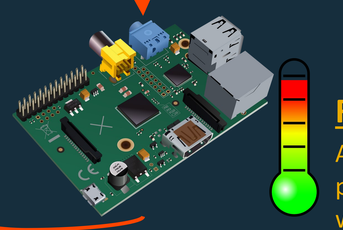
BlueBorne is a set of vulnerabilities that affect Bluetooth devices. Bluetooth has very few security measures, and the security measures that are in place tend to be a simplistic passcode that is used to connect the device to other devices. BlueBorne attacks do not require the target device to be connected to the attackers device or for the target device to be discoverable to gain access. Once the attacker picks out a target, all they have to do is identify the type of device and adjust their attack accordingly. Since Bluetooth has a lot of privileges on devices, that attacker can be granted full control

Smartphone dangers

The mobile operating systems on a smartphone can be compromised just like other systems. iPhone and Android were both vulnerable to the aforementioned KRACK attack which effected WPA2 WiFi encryption discovered in October of 2017. Similar to computers smartphones should always get OS and app updates to keep them secure. You should also avoid connecting to suspicious WiFi networks and leaving your phone unattended. This could potentially lead to unwanted software like a Remote Administration Tool (RAT) to be installed, compromising every part of your phone and privacy. These pieces of malware can record audio from you microphone, take pictures from your camera, and view any content or information on your phone including

Smart lights and smart home

Testing was done with a TP-Link LB-100, so this is not necessarily accurate for all brands and models but some factors will be the same. The initial configuration is broadcast on OSI layer 2 and 3 meaning any device can receive and interpret the configuration. That being said we were unable to gain access to the internal systems on the light bulb remotely meaning it cannot be used to attack other devices on a network, but it is vulnerable to a basic Denial of Service (DoS) attack that can prevent access to the device from the control app. Other smart bulbs might not be vulnerable to the DoS attack, but might be vulnerable to other attacks that could lead to remote access.



Raspberry Pi and DIY IoT

A Raspberry Pi is a single board computer developed by a UK based charity with the goal of creating affordable computers for education. A Raspberry Pi can be used for any variety of needs from a weather station, such as the one created for our project, to turning any TV into a smart tv or even to control robots making a very popular IoT device. The weather station that was created for our project is just an example of the many different DIY IoT devices that one may create at home with a Raspberry Pi. However, if the device is not secured the fun DIY project can turn against you. Nearly every Internet of Things (IoT) device has some form of security measures that can be implemented. If one does not change the default password to a strong password, then an attacker can easily access the device and use it as a door to access or attack the rest of the devices on the network.

Summary

Good security practices are more important than ever with the Internet of Things movement adding millions of new devices to the market every year. Every device on a network increases the attack surface of that network and every unsecured device is a door for nefarious hackers to gain access through. While devices like smart bulbs have limited functionality and customizability making them easy to lock down, a DIY project on a Raspberry Pi that is connected to the internet has so many potential uses that if it is not secured it could be used by a remote hacker to either attack the network or could be enslaved for use in a