Security Plan

Group 5

Home Automation

The home automation system, as it stands with four use cases implemented, consists of a central server, one or more Bluetooth equipped Android devices, Raspberry Pi Bluetooth beacons, and Raspberry Pi's that are connected to and control their attached light sources. The primary way that we prevent unauthorized access to this system is through the use of a local network. Anyone is able to view Bluetooth beacons. However, these do not store any personal or private data. They broadcast a signal containing a Universally Unique Identifier and no other information. They do not receive information. They are the only publicly visible component of the home automation system. All other components are only accessible through the local network. This local network is produced through the router of the user. By default, access to the router and local network is closed to the internet unless port forwarding is enabled. Therefore, no one can access this network remotely. Accessing the network requires being in range of the wireless router and knowing the password. Communication with the wireless network is also encrypted depending on the security protocol. WIFI access and communication protocols are system dependent but can be extremely secure. WPA-2 is the best protocol to prevent unauthorized access to the local network. As is, unauthorized access to the local network and communicating with the system's devices is impossible to all but the most experienced penetration researchers. No dilettante has the technical expertise to exploit WPA-2.

Another way that we could have made security a cornerstone of our implementation is to make the communication between the Android app, server, and Raspberry Pi light clients uses

HTTPS instead of HTTP. HTTPS uses SSL to encrypt the messages between the different systems. As a result, the broadcasts are not decipherable to anyone who is not already engaged with the local network. The implementation of HTTPS also means that the devices are able to determine whether or not they are communicating with a trusted participant of the network. Devices communicating with HTTPS first use a “handshake” to determine the authenticity of each other. Once this is completed, they are then able to pass securely encrypted messages between each other. Not only are attackers unable to access the local network, they are unable to spoof their authenticity. They cannot access the local network and they cannot fake it. Unfortunately, due to time constraints and “Certification Errors”, we couldn’t get this feature implemented within this iteration.

If we had more time to work on this project, we would also require a password for the Android app and require the successful completion of a handshake process for other clients like the lights. This also adds another layer. While it may not be fundamentally secure or raise the threshold for exploitation a significant amount, it’s one more layer that prevents unauthorized access to the system and one more barrier that an attacker would have to cross through.

The use of a local network that cannot be accessed outside of itself and a wireless authentication system make the Home Automation system relatively secure. The local network prevents attackers from remotely accessing it and adds a wireless authentication protocol that makes unauthorized access unreasonably difficult. Many wireless networks encrypt data and have various protocols to ensure usage by only authorized parties which adds to the application security. HTTP also ensures that each device is communicating with its desired target.