Privacy of Smart Devices

Group members:

1. Sagar Patadia – spatadia@email.sc.edu
2. Bailey Metz – bmetz@email.sc.edu
3. Jolie Beviss – jbeviss@email.sc.edu
4. Michael Cantwell – mac9@email.sc.edu
5. Michael Afrin – mafrin@email.sc.edu
6. Saipriya Sairam – ssairam@email.sc.edu
7. Adiv Sivakumar – adiv@email.sc.edu
8. Mercy Barigala – mercy@email.sc.edu
9. Rashid Annahas – rannahas@email.sc.edu
10. Russell Burckhalter – burckhar@email.sc.edu

The point of contact will be Sagar Patadia. He can be reached at spatadia@email.sc.edu or (540) 278-0679.

Overall Summary:

After witnessing the massive DDos attack of 2016 in which a network of infected IoT devices were used to take down the Internet's infrastructure in the Mirai BotNet scandal and the news hysteria that followed after geolocation data from the FitBit watches of US soldiers abroad were readily available online for anyone to view and the infamous Jeep Hack in 2015 where IBM reported a vulnerability in Jeep's firmware that allowed remote control over the SUV when connected to the same network, it's no wonder that the security of IoT devices has become a major concern for consumers and developers alike.

Many IT professionals are not readily adopting these new devices because they are well aware of the security risks that they present. In this paper we will explore what kind of advancements are being made in the areas of security and privacy for IoT devices to try and understand where the industry is lacking in these areas and see how far we have come in mitigating the risks and securing the onset of ubiquitous smart devices that are quickly becoming part of our everyday lives.