Making the 'Internet of Things' configuration more secure and easy-to-use

September 9 2015

With an ever increasing number of everyday objects from our homes, workplaces and even from our wardrobes, getting connected to the Internet, known as the 'Internet of Things' (IoT), researchers from the University of Southampton have identified easy-to-use techniques to configure IoT objects, to make them more secure and hence help protect them from online attacks.

This increased connectivity brings additional risk. Setting personalised and strong passwords when connecting new devices to the Internet, for example through our home Wi-Fi networks, can mitigate such risks. However, many IoT devices have limited interfaces: just a few buttons (if any at all) and light indicators, making it challenging for users to configure them. If secure configuration becomes complicated, users may choose easier, less secure options that leave their devices vulnerable.

Southampton researchers compared four interaction techniques for the configuration of IoT devices, looking for methods that allowed security, but were quick and easy to use. All four techniques used the smartphone touchscreen to let users enter secure passwords.

Two of the techniques used a more 'traditional' approach by connecting the smartphone and the IoT device through a USB or audio cable, via the smartphone's headphone socket. The third technique used a 'Wi-Fi-only approach, where the smartphone creates a special temporary Wi-Fi network, or 'ad-hoc network', to which the IoT device automatically connects before being redirected to the correct permanent network. The

final option was the smartphone and the IoT device exchanging information through light: the smartphone's screen flashed black and white to mean binary 'zero' or 'one'; the IoT device read this light/binary pattern to learn the password from the smartphone.

The results, which are presented at the ACM Ubicomp 2015 conference in Japan this week, found that two of the techniques were noticeably more usable than the others - the audio cable and the Wi-Fi-only interactions.

Study co-author Dr Enrico Costanza, from the Agents, Interaction, Complexity Group in Electronics and Computer Science at the University of Southampton, says: "IoT objects can be attacked and possibly hijacked, putting our privacy, data and safety in question. We believe that our results can help designers and researchers make IoT devices, and especially their configuration, more usable and therefore secure. Moreover, we believe that not enough attention has been placed on how to make the IoT easy to use and to configure, so we hope that our results will motivate others in researching this topic."

Provided by University of Southampton