Can You Trust Your Smart Home? Investigating the Security of Belkin WeMo Home Automation Systems

Haoyu Liu, Tom Spink, and Paul Patras
The University of Edinburgh

Home automation products are rapidly gaining popularity in a market that is forecast to be worth $80 billion by 2022. Up until recently, smart home systems were typically proprietary installations, with closed, wired, and centralized control, specified only for bespoke new-build homes. As the cost of wireless, sending, and cloud computing technologies plummets and numerous 'maker' communities emerge, Internet-connected home automation products are reaching all consumers, regardless of their housing type and technical knowledge.

Smart home products typically utilize already existing wireless infrastructure (e.g. home Wi-Fi), connect to a cloud-based service, and enable their users to control various appliances, such as interior lighting, mains plug sockets, and ancillary systems (burglar alarms, door bells, etc.). Unfortunately, in a rush to release products that provide new functionality and more convenience, coupled with a lack of rigorous understanding of embedded systems and network protocols, security privacy are overlooked. Poor implementations not only allow malicious actors to compromise the operation of the 'things', but also facilitate side-channel attacks that leak private information, exposing the users' networks and data to further risks.

In this walk, we will present the findings of our in depth security analysis of the Belkin range of WeMo smart home devices. Belkin WeMo has become a market leader that commercializes smart sockets, light bulbs, video cameras, etc., which can be controlled with smartphone apps, or via personal assistants such as Amazon Alexa. We will reveal that shortsightedness in the design of the pairing procedure these implement can lead to the leakage of a user's home network authentication credentials. In particular, we will discuss our WeMo smartphone app reverse engineering efforts, by which we uncovered an exploit that enables to disclose the Wi-Fi passphrase that guards the communication secrecy. In addition, we will show that issues in the design of the mobile app can lead to phishing attacks underpinned by simple software we craft to emulate a WeMo device. This permits cross-site scripting and access to user account credentials. Finally, we discuss a number of technical solutions proposed to mitigate the vulnerabilities found in the Belkin WeMo (but equally applicable to other vendors), which following disclosure, the company is considering for official patches scheduled for release.

[1] H. Liu, T. Spink, P. Patras, "Uncovering Security Vulnerabilities in the Belkin WeMo Home Automation Ecosystem", in Proceedings of IEEE Pervasive Computing (PerCom) Workshops, Mar. 2019.