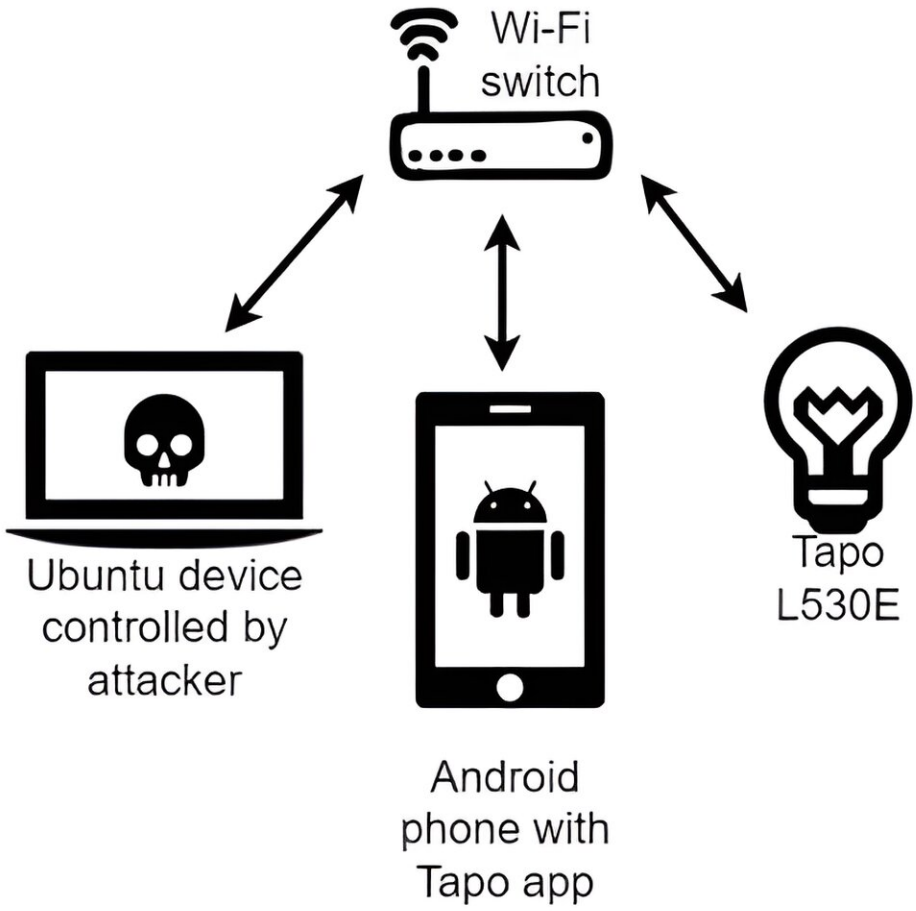
TP-Link's Tapo smart bulb found to be vulnerable to hackers

August 24 2023, by Bob Yirka



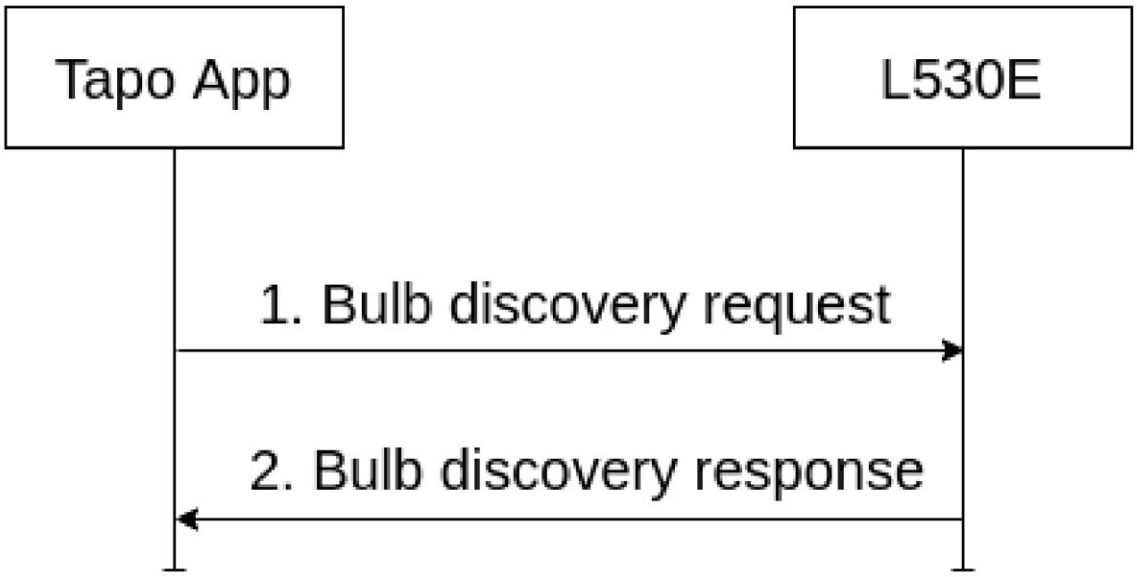
Setup B, network with a configured smart bulb. Credit: *arXiv* (2023). DOI: 10.48550/arxiv.2308.09019

A pair of information security specialists at Universita di Catania, working with a colleague from the University of London, have found four security vulnerabilities in one of TP-Link's most popular smart-bulbs. Davide Bonaventura, Giampaolo Bella and Sergio Esposito have written a paper describing their testing of the smart-bulb and what they found. They have posted it on the *arXiv* preprint server.

Smart lightbulbs like those from TP-Link, allow users to control features of the bulb using a smartphone app. Such features include the ability to chose which color they want the bulb to be, to schedule a timer telling it when to turn on or off, and to monitor their energy usage. The bulbs also can be controlled directly through Wi-Fi, which means they do not require a hub or any other equipment. It is this last feature which the research trio found leaves the bulb vulnerable to hackers.

In testing the most popular Tapo smart bulb, the L530E, the researchers found what they describe as four vulnerabilities. One of those vulnerabilities was described as highly severe—the bulb lacked authorization capabilities between it and the associated app. And that allowed the research team to impersonate the bulb during a testing session, to record the password associated with the bulb, and to control its actions from there.

The second vulnerability, which the team classified as severe, allowed adjacent hackers to authenticate during device discovery to obtain a secret code used for authentication. The third vulnerability was a lack of randomness during encryption that made the scheme predictable, and the fourth vulnerability allowed the team to replay messages sent to and from the bulb.



Tapo (local) Device discovery. Credit: *arXiv* (2023). DOI: 10.48550/arxiv.2308.09019

The research trio noted that the vulnerability related to bulb impersonation allowed for stealing Tapo account information, which indirectly could be used to reveal the Wi-Fi password used by the Wi-Fi system to which the bulb was associated. Once hackers have such a password, they could not only hijack the network for their own use, but conceivably use it to access other devices on the network.

The research team reported what they found to TP-Link and were notified that all the vulnerabilities they had found were being addressed and that fixes were in the works.

More information: Davide Bonaventura et al, Smart Bulbs can be Hacked to Hack into your Household, *arXiv* (2023). DOI: 10.48550/arxiv.2308.09019