Team 3016
SDS
Smart Device Security

By: Dhruvjit Singh
Ribhav Verma
Prishaa Talwar
Vidhaant Bhardwaj
Artham Singh Saini

Problems

In the world of smart cities and resilient urban infrastructure, nearly everything is connected to the internet, forming what's known as IoT devices like smart bulbs

These bulbs often lack strong security measures, making them easy targets for hackers.

When compromised, they can jeopardize the entire network they're connected to.

Aim Of The Project

To enhance the overall security of a smart bulb by making a secure OS for them which includes:

- Secure Boot
- Encryption

System that detects unauthorized access on the bulb and shut it off.

Smart bulb security is a growing concern, especially with popular models like TP-Link's Tapo smart bulbs, which have millions of users but often lack robust protection.

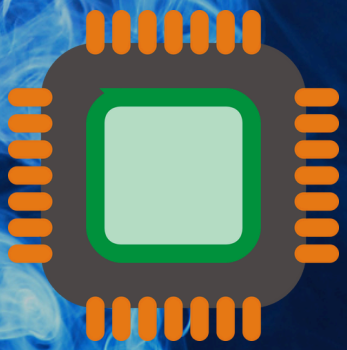
Experts have found vulnerabilities even in these bulbs.

Project Details

The chip acts as a mini-firewall, monitoring traffic between the smart bulb and the user's phone or connected devices via Bluetooth, adding an extra layer of security without direct internet exposure.

It’s a small, adhesive-backed module that can be easily attached to the exterior of the bulbs

Compact and lightweight, the chip is designed to blend in aesthetically and is powered by a battery.



A simple push button allows for easy removal and reattachment

Project Functions

The chip would monitor for unauthorized access attempts.

If any unauthorized access is detected, it would trigger the predefined security responses

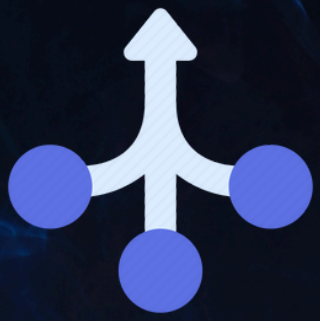
It would automatically shut down the bulb.

A message would be sent to the cybersecurity cell

An alert message would be sent to the user

Advantages

Users can easily move the chip between devices, making it a cost-effective solution for protecting multiple smart bulbs



The attachable/detachable design simplifies the process for non-technical users, who can easily add or remove the chip

Users can choose when and where to activate the chip, giving them full control over their privacy.

Users might attach the chip only when they feel a particular smart bulb is at risk.

For consumers, this detachable chip offers a unique security feature that isn't commonly available in the current market

Drawbacks

Bluetooth typically has a limited range, which might restrict the effectiveness of the chip

The very nature of the chip being detachable and portable means it could easily be misplaced or lost

As the chip is externally attached, it could be physically tampered with or removed by an unauthorized person, defeating its purpose.

The chip might be exposed to environmental factors like heat, moisture, or physical impact, which could affect its performance or lead to failure.