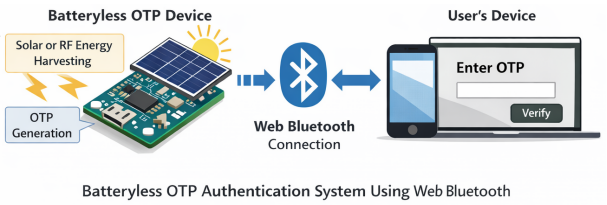
Master Thesis Idea

Title: Batteryless OTP Authentication System Using Low-Power Embedded Devices

Internet of Things (IoT) is pushing authentication mechanisms beyond conventional PCs and smartphones toward distributed, low-power devices. In many smart-building and industrial deployments, users need secure, quick, and frequent access to services (e.g., commissioning, maintenance, local dashboards), often in environments where installing or maintaining batteries is undesirable. One-time passwords (OTP) remain a widely used building block for two-factor authentication, but typical OTP tokens and gateways are not optimized for energy-autonomous operation or seamless browser-based interaction.



Batteryless OTP Authentication System Using Web Bluetooth

Batteryless embedded authentication tokens can reduce maintenance and improve scalability, but they introduce strict constraints on energy budget, compute, and communication. Achieving secure OTP generation (or challenge–response OTP) under intermittent power requires lightweight cryptography, careful key handling, and robust protocol design to mitigate replay and man-in-the-middle risks. In parallel, Web Bluetooth enables direct interaction between a browser and nearby BLE devices, offering an attractive path to deploy authentication flows without dedicated mobile apps.

This thesis aims to design and prototype a lightweight, batteryless OTP authentication architecture based on a low-power embedded device and Web Bluetooth. The student will explore energy harvesting and power management, implement a lightweight security algorithm suitable for constrained hardware, and demonstrate an end-to-end authentication flow between a batteryless token, a web application, and a verification backend.

Goals:

- Design and implementation of a low-power, lightweight OTP (or challenge–response) scheme on an embedded device, including secure key provisioning/storage.
- Development of a batteryless prototype with energy harvesting and power management, and characterization of energy, latency, and reliability under intermittent power.
- Implementation of a Web Bluetooth demo (browser UI) and backend verification service, followed by experimental validation and basic security analysis (e.g., replay/MITM considerations).

Contact:

- Juan Felipe Gutiérrez Gómez (juan-felipe.gutierrez-gomez@tu-braunschweig.de)