Design Thought Process Notes

– Foxers Team

1. Empathize

1.1 Research methods used:

- 5 short interviews with:
    - 2 smart-home owners
    - 2 tech-savvy users who have experience with their own setups
- Online mini-survey on Facebook page related to Smart Homes (≈15 responses) about:
    - Devices in use
    - Security awareness
    - Security incidents / worries

1.2 Pain points:

- People have little knowledge about devices security
- Onboarding new devices is often trial and error
- No passwords are usually set when pairing devices
- Tech-savvy users distrust “black box” vendor clouds; they want local control

1.3 Needs:

- Peace of mind: not having to think constantly about security.
- Transparency from devices - where they are connected and how

- Simple steps to pair a device
- Feel in control of the home.

2. Problem Statement

Smart-home users currently lack a simple, trustworthy, and unified way to securely connect and manage IoT devices in their home. Security is fragmented across many vendors, mostly invisible to users, and often based on weak or opaque mechanisms. As a result, personal data and household privacy are at risk, and users cannot be confident that their smart home is safe from unauthorized access.

3. Ideate

3.1 “How Might We” Questions

- HMW make smart-home security feel as simple as plugging in a lamp?
- HMW give users one place to see and control all device connections?
- HMW make strong cryptography and per-device keys invisible to non-experts but transparent to experts?
- HMW notify users about suspicious behaviour in an understandable way?

3.2 Brainstorming

1. **Personal Smart-Home Security Hub**
    - Local server
    - Stores unique cryptographic keys for each device
    - Acts as single gateway for all device communication
2. **Secure Onboarding Phone App**
    - Smartphone app that guides the user through adding a device via QR code
    - Automatically exchanges cryptographic keys with the new device
    - Shows simple messages for users
3. **Live Device Map**
    - Dashboard showing all devices as icons
    - Lines indicate which devices communicate with which services
    - Suspicious activity highlighted
4. **Security Health Score**
    - Simple score (0–100) of home security
    - Factors: default passwords, update status, strange traffic, unencrypted connections
    - Offers plain-language recommendations

3.3 Chosen Concept

Phone App with a Privacy-Tuned Smart Device Protocol to ensure users can easily and safely add devices to their smart home network.

4. Key User Flows

Flow 1: First Setup

1. User unwraps a new device and installs the app
2. App displays possible networks for the user to connect
3. User chooses a network
4. App displays confirmation

Flow 2: Adding a New Device

1. User taps “Add Device” in the app.
2. App asks: *“Scan the QR code on your device”*.
3. After scanning, the hub and device perform secure key exchange
4. App displays confirmation

Flow 3: Checking device status

1. User opens app.
2. User clicks “Connected Devices”
3. App displays currently connected devices with their status

5. Open Questions

- How will users react to the new protocol and way of device pairing?
- What is the best business model (paid app, subscription, license to manufacturers)?
- How can we integrate with existing ecosystems?