MSc in Cybersecurity: Privacy and Trust

Is Home-Based IoT prevalence an Untapped Hacking Attack Surface? A Threat Modelling Study

Stephen Leahy
Supervisor: Paul Barry

Introduction

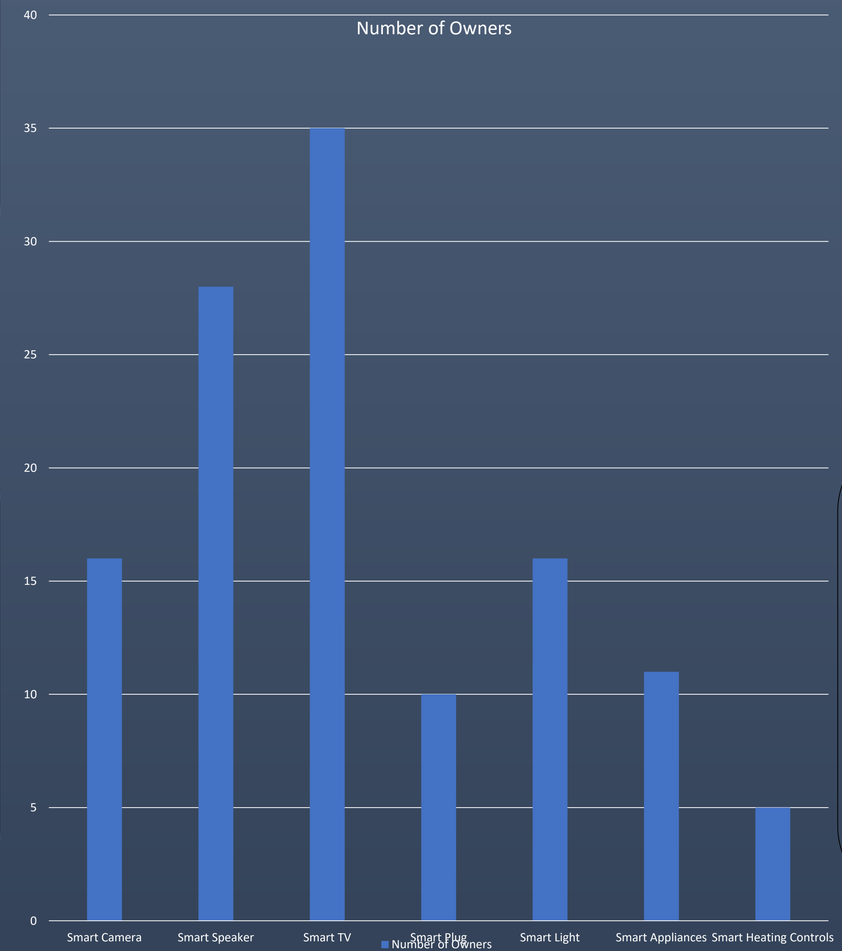
IoT devices have exploded in popularity and have become embedded in modern homes. Many of these devices are interconnected to each other, continually online, creating small networks amongst themselves.

As the number of IoT devices increases in a home network, so does the potential attack surface. Due to outdated software, user behaviour and manufacturer support windows.

This study seeks to investigate whether the influx of IoT devices in modern homes has created an attack surface using surveys and threat modelling techniques

Research Questions

1. What IoT devices are most commonly found in homes?
2. Do older or low-cost devices pose more of a risk to home network?
3. Does brand affect your IoT device's security?
4. Do certain Categories of IoT devices present greater security risks?
5. How long are IoT devices typically supported for?
6. To what extent does User behaviour influence device security?



Literature Review

- There has been a huge increase in IoT device adoption with numbers to grow again from 77.6% in 2025 to 92.5% by 2029. Statista (2026)
- User behaviour introduces a huge security risk, with many ignoring updates and not changing default credentials on IoT devices. Emami-Naeini et al. (2019)
- The type of device influences risk. Cameras and smart speakers can collect high risk data. Lower risk devices can be exploited for lateral movement in a home network. Acar et al. (2020); Sivanathan et al. (2019)
- Older and low-cost devices introduce more security risks due to outdated software, poor hardware and security patch distribution. Ryan & Rozier (2024); Sivanathan et al. (2019)

Methodology and Technology

- Research will be conducted via a mixed methods approach, combining a user survey with threat modelling.
- The survey will collect information from users about their IoT devices and security habits via Google forms and the data will be displayed through Google sheets.
- Threat modelling will be conducted with STRIDE and the use of Attack trees.

Early Indications and Next Steps

- Survey data is showing a high IoT adoption rate among households. Many survey users have reported using devices in the 3-5 years old bracket.
- Apply threat modelling to identify and categorise threats.
- Build attack trees to map potential attack paths for high risk IoT devices.
-

Stephen Leahy, C00193857@setu.ie