Data Security Threats On Smart Devices At Home

Giovanny Andrés Piedrahita Solorzano‡, Anderson Flórez Gutiérrez‡, Angie Paola Gordillo‡

‡ Institución Universitaria Politécnico Grancolombiano, Bogotá, Colombia

Corresponding author: Giovanny Andrés Piedrahita Solorzano (gapiedrahita@poligran.edu.co)

Abstract

The Internet of things (IoT) has been trending recently as a new technology for connecting devices to the Internet, from simple sensors or actuators to more powerful components with processing and prediction capabilities. Although home automation is not new, IoT has boosted domotics by allowing remote management of security and energy through mobile phones and providing new (smart) and more natural methods of interaction with home devices (Edu et al. 2019). Along with this trend, information security concerns have also emerged due to the possible security breaches and personal data access by IoT devices, or even unauthorized access to devices and their capabilities to turn on or off electrical appliances.

When mobile app users skip or ignore the terms and conditions proposed by the companies, it shows how little concern exists about the use or exploitation of personal data because there is no choice, because it's difficult to understand the legal terms, or just because the threats or abuses are unknown. Similarly, the users of home automation devices (not necessarily using IoT protocols or standards) are focused on functionality but unaware of security issues due to the device's connection to the home network and the Internet.

The exploration of common vulnerabilities and attacks in home automation devices highlights the need for resilience in the IoT ecosystem. As more devices become connected to the Internet, the risk of security breaches and unauthorized access to personal data increases. Developing effective countermeasures and improving awareness among users are key factors in creating a more resilient IoT infrastructure.

This working paper explores common vulnerabilities and attacks in home automation devices identified in the literature, aiming to establish guides and recommendations for using them more smartly and securely.

For this, we have done a preliminary review based on the results of the search equations shown in Table 1, filtering those titles which address technical issues, thus classifying them and analyzing possible countermeasures to prevent or mitigate the vulnerability at different levels.

The review of the documents has led to a first classification of the results of the threats for the users, regardless of the technical source of the security breach:

- Personal data exploitation: it refers to gathering data related directly to the functions of the device, for example, voice patterns extracted from personal assistants, which may be used for identity supplantation, or routines analysis based on timestamps stored on each interaction with the device (Acar et al. 2018).
- Unauthorized control of devices: it refers to accessing the device to control its outputs (lights, locks, appliances) due to poor authentication mechanisms, communication protocols, or the lack of a secure channel between the user and its device.
- Unauthorized access to network resources and personal data: this is related to sharing network access data with third parties, letting them access other devices on the same network, getting personal data from the user's accounts.

Understanding the roots of the vulnerabilities help us to establish a road to further examination of its challenges and possible solutions, which are not only technical, but also regulatory, or oriented to improve the awareness of the final users. Also, the results also lead to other studies directly with the users and their knowledge and perceptions about the security issues inherent to the smart devices.

Keywords

Internet of things, IoT, home automation, security, smart devices, personal data, security breaches, unauthorized access, mobile apps, communication protocols, secure channel, network resources, awareness, resilience.

Presenting author

Giovanny Andrés Piedrahita Solorzano

Presented at

CABMR 2023 colloquium on Resilience and Cybersecurity, held on March 9, 2023, at Ascencia Business School – Collège de Paris, ISF campus, La Défense, Paris, France.

Conflicts of interest

The authors have declared that no competing interests exist.

References

- Acar A, Fereidooni H, Abera T, Sikder AK, Miettinen M, Aksu H, Conti M, Sadeghi A, Uluagac S (2018) Peek-a-Boo: I see your smart home activities, even encrypted! arXiv https://doi.org/10.48550/arxiv.1808.02741
- Edu J, Such J, Suarez-Tangil G (2019) Smart Home Personal Assistants: A Security and Privacy Review. arXiv https://doi.org/10.48550/arxiv.1903.05593

Table 1.

Titles which address technical issues with classification.

No	Search equation	Results (No. Doc.)	Year filter
	1 TITLE-ABS- KEY (iot AND smart AND home AND appliance)	875	All
2	TITLE-ABS-KEY (iot AND (iot AND home AND automation AND platform AND advantage) AND (LIMIT-TO (PUBYEAR, 2022) OR LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020))	413	2022, 2021, 2020
3	[All: vulnerabilities] AND [All: iot] AND [All: smart home] AND [All: appliance] AND [Publication Date: (01/01/2020 TO 08/30/2022)]	200	2022, 2021, 2020