PRIVACY LABELS FOR HOME INT DEVICES

K M. Ramokapane, M. Sameen, Z. Dkaidek, E. Woodward

University of Bristol, University of Bath

REPHRAIN SHOWCASE LONDON 2023

Motivation and Background

The use of home IoT devices is becoming more prevalent daily. While these devices bring about new services, increase convenience, and improve efficiency, they also bring privacy and security risks.







Concept of Labels





To keep safe, consumers are usually expected to research the products they desire to own and the data practices of the companies that produce them. However, there is often little to no information for them to make informed decisions on what product to purchase or what security and privacy attributes they should look for when considering owning an IoT device.

Iron * Percent Daily Values are based on a 2,000 calorie diet Your Daily Values may be higher or lower depending on your calorie needs: Calories: 2,000 2,500 Total Fat 65g Less than 80g Sat Fat Less than 20g 25g Cholesterol 300mg 300mg Less than Sodium 2,400mg 2,400mg Less than Total Carbohydrate 300g 375g Dietary Fiber 25g 30g



Data Linked to You

The Current State of the Art

Prior efforts have proposed privacy labels for IoT devices to address this gap. Privacy labels draw from food nutrition labelling systems aimed to improve the communication of privacy policies to users. Instead of just text, the types of data collected and the providers' data sharing and processing practices are communicated to the user using icons and symbols to users. However, unlike the mobile application space, research focusing on security and privacy labels for IoT devices is still new and presents new challenges. For instance, device heterogeneity, multiple vendors are involved, labels may need to include more than just data practices, and providing accurate and up-todate info is convoluted.

Aims and Objectives

Existing Privacy Labels for IoT Devices



<	<u> </u>	Certificates	Unknown
	۲	Secure boot	Not supported
	\mathbb{C}	Firmware update	Manual
	d ::	Password	Default password User-updateable
	2	Authentication	Password
	₿	Remote access	Yes 🌔
	2	Encryption	No 🌔
		Internet access	Yes 🌔
	ဗို	Talk to other devices	No
	0	Personal information	Unknown
	0	Telemetry data	Unknown
		Data storage	Local storage
-∿»)	Ĵ	Audio	Yes
	23	Video	Yes
	Ŀ)	Motion	No
	9	Location	No
	0.		

Our overarching aim is to build on existing work and cocreate a security and privacy label framework for IoT devices with consumers and experts. Our key objectives are:

- identify features, and content that should be • To considered and included in IoT security and privacy label framework.
- Propose and evaluate a security and privacy label framework for IoT devices.



