SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Children and Cybersecurity

Cyber Threats and Data Hacking Risks in Smart Toys

MSc. In Cybersecurity, Privacy and Trust

South East
Technological
University
Ireland

Hi, my little bear!
My name is xxx. I'm 5 years old. I'm living in Dublin.
I have two sisters and one pet dog ......

1. Introduction

Network-connected, AI enabled toys ("smart toys") include sophisticated dolls, robots and soft toys with cameras, microphones, speakers, sensors, screens and more. Smart toys use user-sensitive data for a variety of reasons. Smart toys can hold a huge amount of customer data and communicate over the internet. The data obviously needs to stay confidential from the point of child safety protection.

The focus area of this research is to analyse security issues for smart toys for children.

2. Literature Review

Most of the literature covers a few well-known incidents. Those are summarised into the following areas: The impact of cyberattacks on smart toys. • The need for a specific survey. • The need for guidelines for manufacturers of smart toys. • The need for strong privacy policy and supporting technology

Even though smart toys appear like simple playthings, in realty they are sophisticated IoT devices. Smart toys are hackable and children's data is under threat .

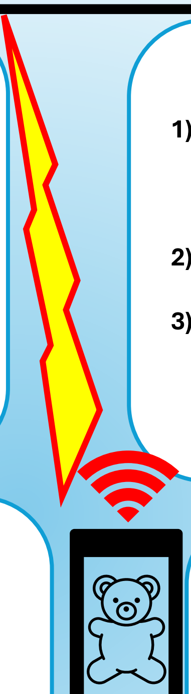
3. Research Questions

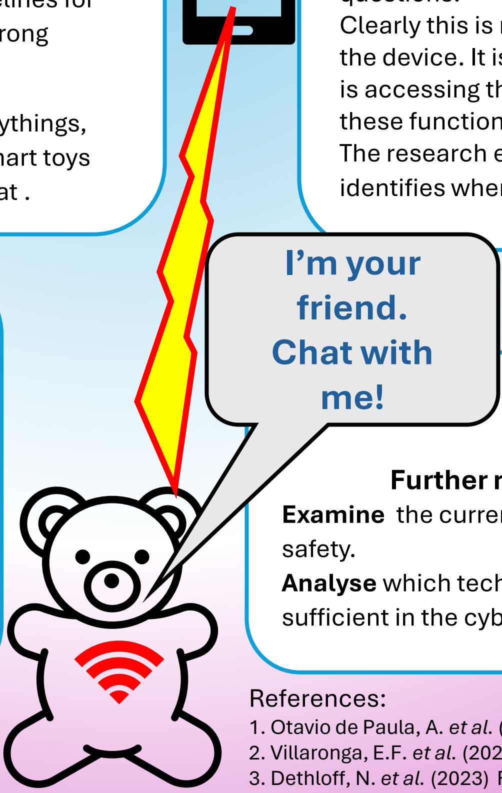
Do smart toys have sufficient cybersafety and data protection? This is broken into 3 sub questions:

RQ1 How is the data stored by the device?

RQ2 Is any data transferred to other countries?

RQ3 Is there the risk of direct data intrusion on the smart toys?





4. Methodology

1) **Data collection and analysis – Passive analysis + Actual analysis** product analysis • security analysis • API security • Network scanning
2) **Testing Products** - Data handling and analyse supporting technology
3) **Risk assessment using tools** – traffic analysis, Bluetooth/Wi-Fi exploitation, Security measuring, Communication analysis by Raspberry Pi and Wireshark.

5. Early Indication

The toy is processing speech recognition and answering any questions.

Clearly this is not all processed inside the device. It is suspected that the toy is accessing the internet to perform these functions.

The research examines the data and identifies where it transfers.

6. Next Steps

Further research areas

Examine the current state of smart toys' safety.

Analyse which technologies are currently sufficient in the cybersecurity environment.

References:
1. Otavio de Paula, A. *et al.* (2020) Privacy in Smart Toys
2. Villaronga, E.F. *et al.* (2021)Toy Story or Children Story?
3. Dethloff, N. *et al.* (2023) Families and New Media
4. Chaudron, S. *et al.* (2019) Testing internet of Toys, P.223- 229
5. Salgado, A. *et al.* (2019) Smart Toy and Children's Privacy

Contact:
Etsuko Michelle Hegarty