IoT Security and Privacy

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

11/03/2024

THE UNIVERSITY of EDINBURGH

Overview

- IoT
- Take-home

What is the Internet of Things?

Data-driven agriculture (taken in Madison, Wisconsin during my first PhD research)

Smart city

Fitness tracker

Introducing

echo studio

"Alexa, play the Best of 3D Music

Press the mic off button to disconnect the microphones

"Internet of Things"

- Previously known as:
  - Ubiquitous computing
  - Ambient computing

- Idea is that the computers are embedded into the world around people, effectively pushing computation into the surrounding infrastructure, rather than in devices we carry around.

- Large issues:
  - Privacy
  - Security
  - Trust
  - Battery
  - Computational power

Security and privacy issues in IoT

Hotel ransomed by hackers as guests locked out of rooms

The Local
news.austria@thelocal.com

28 January 2017
10:42 CET+01:00

crime

Share this article

✉ 🐦 f

Photo: CEN

One of Europe's top hotels has admitted they had to pay thousands in Bitcoin ransom to cybercriminals who managed to hack their electronic key system, locking hundreds of guests out of their rooms until the money was paid. (Updated)

Furious hotel managers at the Romantik Seehotel Jaegerwirt, a luxurious 4-star hotel with a beautiful lakeside setting on the Alpine Turracher Hoehe Pass in Austria, said they decided to go public with what happened to warn others of the dangers of cybercrime.

Ring's smart doorbell can leave your house vulnerable to hacks

The $199 Ring Video Doorbell may be "smarter" than your average buzzer, but a major vulnerability can leave your Wi-Fi network wide open to hackers.

Megan Wollerton January 13, 2016 11:50 AM PST

Why don't people protect themselves?

1. People are not **aware** of the risks or protection mechanisms.

2. People cannot **use** the available protection mechanisms.

3. People do not **care** about security and privacy.
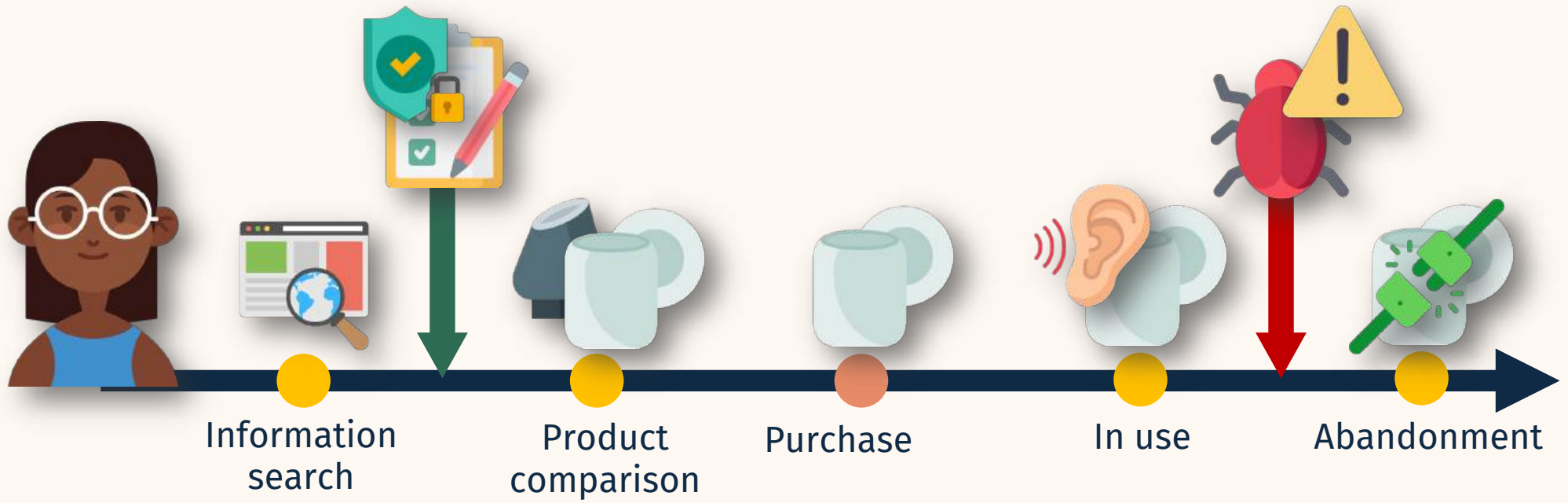
Lemon markets

Security and privacy in IoT is currently a lemon market.

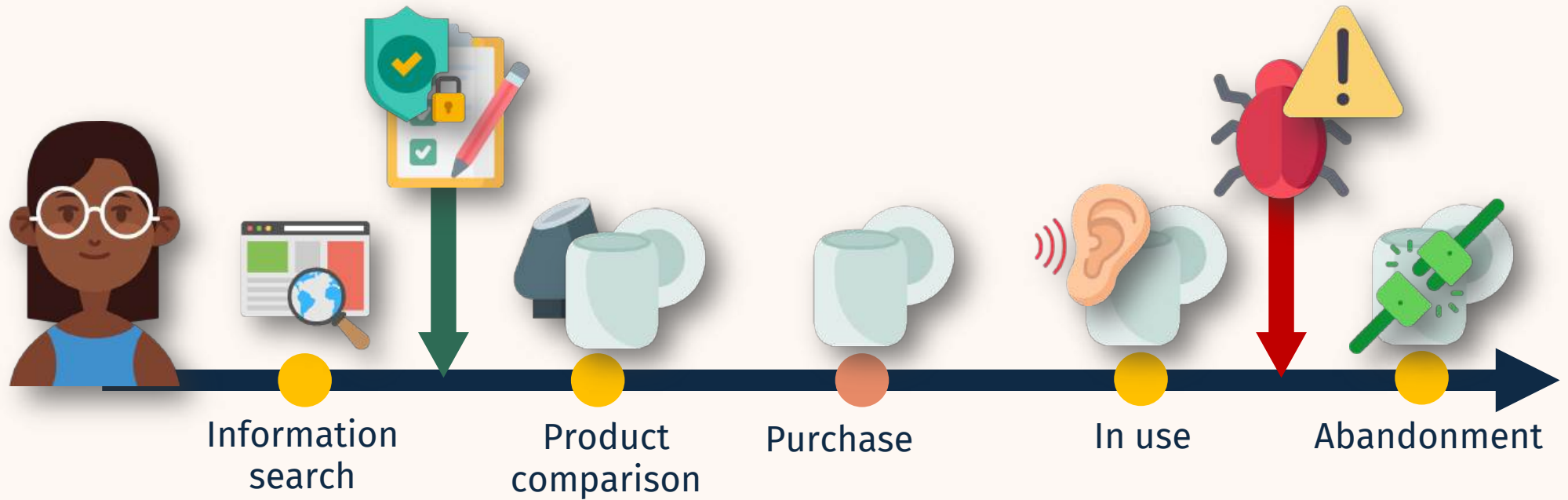People with purchasing power cannot differentiate between a "good" device and a "bad" one

Are the arguments above still valid today?

User awareness == secure behavior?

Information search · Product comparison · Purchase · In use · Abandonment

Information search Product comparison Purchase In use Abandonment

How do users **develop** security and privacy attitudes organically?

Research Questions

How users think of S&P issues (**considerations**)
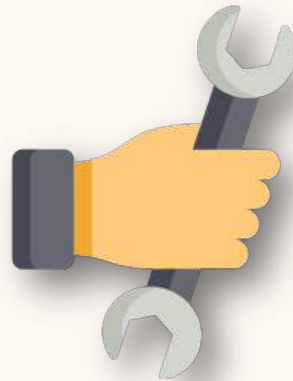
How users react to S&P issues (**attitudes**)

How **online discussion influences** users

NLP-Assisted Data Collection

- Collected **46,637 raw threads** between 2010 and 2021

- Built a **natural language processing classifier** to identify relevant threads, incorporating diverse S&P terminology

- Sampled and coded **180 threads** with 4,957 comments until data saturation from 7,255 candidates

Qualitative Data Analysis

```
/homeautomation subreddit  →  46,637 raw threads  →  Automated thread filter  →  7,255 thread candidates        Open coding

         1,000 labeled sentences  →  Training DeBERTa                          Sampling  →  180 relevant threads
```

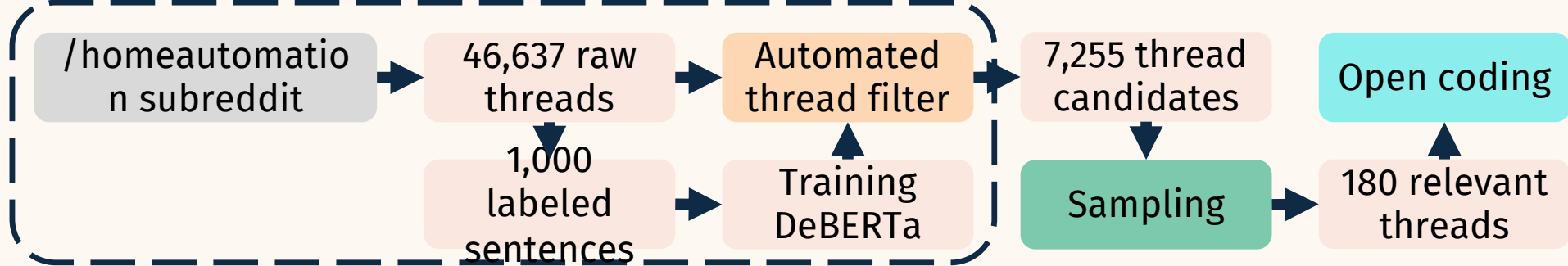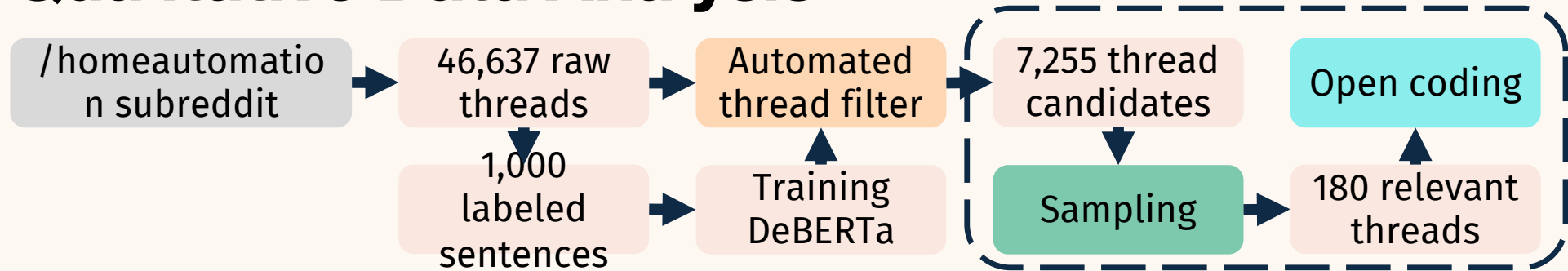- Our team with broad knowledge (S&P, computer science and engineering, information science, psychology, and legal studies) performed **qualitative coding** and **thematic analysis**

- Inter-rater reliability = 0.74 (substantial)

Reddit comments   →   **Themes**   **Codes**
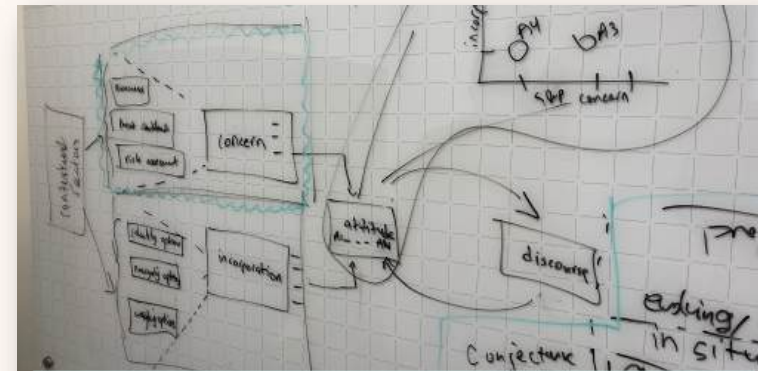
Our framework under construction (2021)

Findings: S&P Considerations

Users develop S&P concerns and protective strategies **overtime and reflectively**

Findings: S&P Concern - S&P Awareness

- **Contextual factors** contribute to awareness

> [MQTT] may expose something on your Internet

- Awareness evolves based on **changing** contextual factors

> Yeah i had gotten a discounted nest thermostat from my power company but after seeing their reluctance to let me access *my own data* i returned it

Findings: S&P Concern – Threat Identification

- Technical expertise affects **vulnerability assessment**

I assume Z-Wave doesn't suffer from this problem due to the certification process? Or are there attack vectors that could be leveraged against that particular tech?

Insufficient understanding may lead to overestimation or underestimation of the threat

Findings: S&P Concern – Threat Identification

- **Preconceptions** (trust, reputation, reliability, etc.) shape users' views toward products and stakeholders

> Not specifically for Xiaoyi, but it is quite common for low-priced Chinese brands to have embedded backdoors or privacy-invading snooping by the company

Redditors may show differing trust but a predominant distrust toward Chinese stakeholders

Findings: S&P Concern – Threat Identification

- Assumptions regarding stakeholders' behaviors result in **different role assignments** (e.g., potential victim, adversary, and "good Samaritans")

> Well Google records all your data, but they are highly incentivized to keep it safe and not sell it, because having exclusive access to it is their core business

Users assumptions on stakeholders' roles and their dynamics differ

Findings: S&P Concern – Risk Assessment

- Users' assumptions (e.g., resource and technical sophistication) about adversaries drive their **likelihood assessment** of risks (health, finances, physical and digital assets.)

> I can disable the system with a walkie talkie after using an SDR [software defined radio] to find the exact frequency the system is on and just blast it the entire time I'm in your house . . . $20 baofeng [radio] will kill simplisafe since it uses 433[MHz]

Users' assumptions about adversaries are subjective
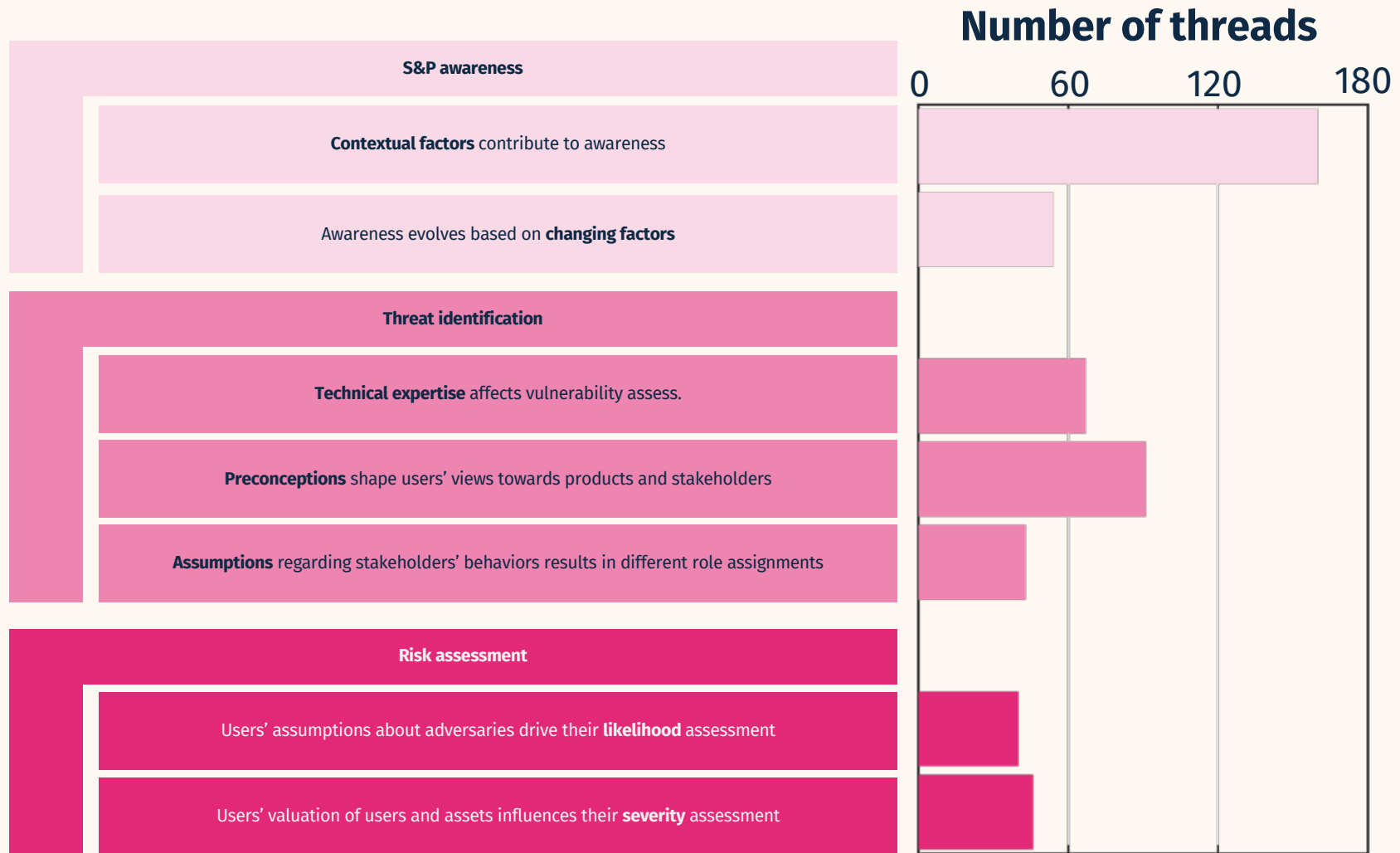
Findings: S&P Concern – Risk Assessment

- Users' valuation of users (children, elderly, etc.) and assets (sensitive data) influences their **severity assessment**

> I need to deal with sensitive HR [Human Resources] issues from home, all of which should never be recorded without consent of a third party

Users may have different valuations given the same threat model

S&P Considerations: Concerns

Number of threads

S&P awareness

Contextual factors contribute to awareness

Awareness evolves based on changing factors

Threat identification

Technical expertise affects vulnerability assess.

Preconceptions shape users' views towards products and stakeholders

Assumptions regarding stakeholders' behaviors results in different role assignments

Risk assessment

Users' assumptions about adversaries drive their likelihood assessment

Users' valuation of users and assets influences their severity assessment

0   60   120   180

Findings: Protective Strategies – Strategy Identification

- Users leverage **information sources** (buying guide, online discussion, etc.) to identify protective strategies.
- Contextual factors (e.g., availability of privacy option) **constrain the scope** of strategies

[the control] is buried in the app

Users may not have a complete understanding of the contextual factors

Findings: Protective Strategies – Tradeoff Recognition

- Price and technical effort inform **cost awareness**

- **Benefits of strategies** stand on the security and perceived improvements in use cases

Actually if you know python writing a voice assistant capable of controlling your house and doing other basic functions is a matter of a couple days
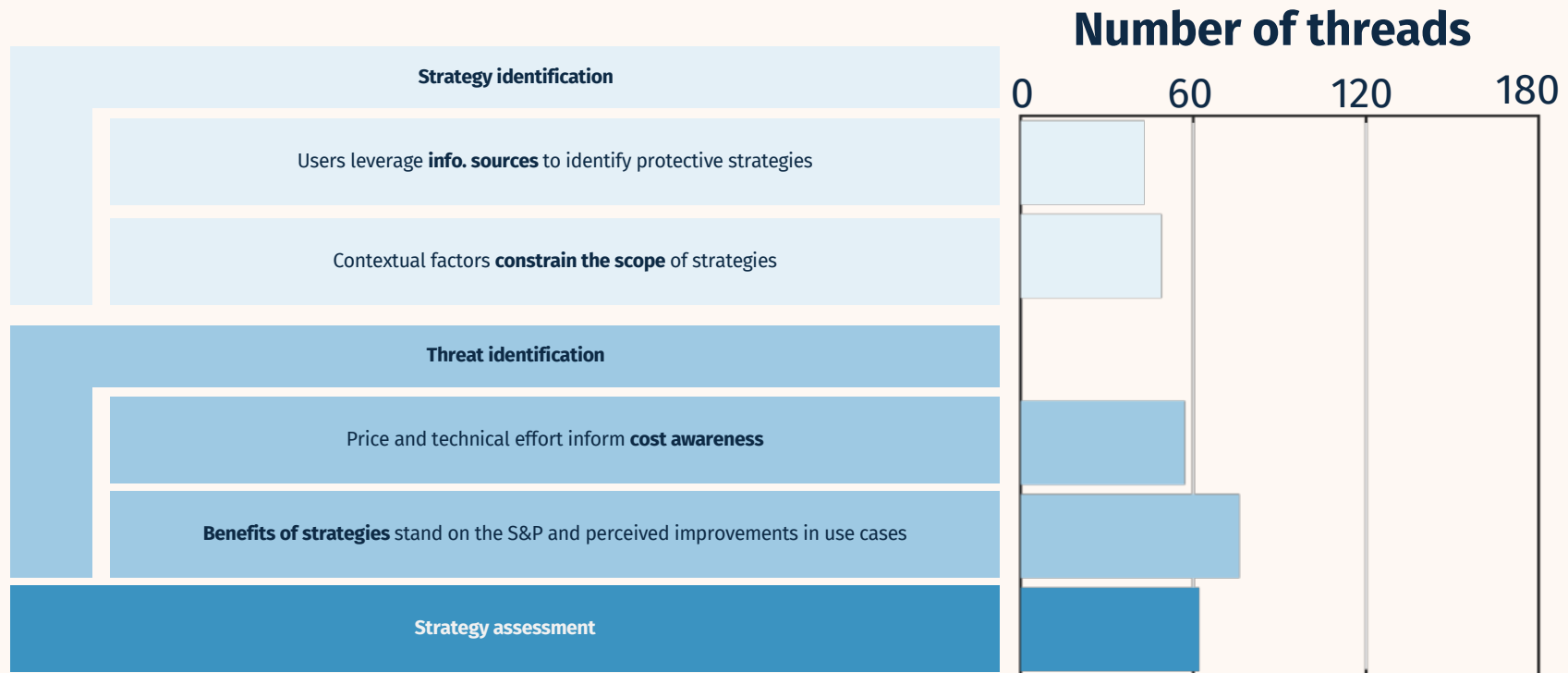
Cost and benefits are subject to personal circumstances

Findings: Protective Strategies – Strategy Assessment

- Whether the benefits overweigh the cost?

> I agree that Homeseer's interface is not the prettiest one around, but so far it does far and away more, is stable, and exposes the "nerd knobs" needed to do darn near anything including secure z-wave

S&P Considerations: Protective Strategies

Number of threads

Strategy identification

Users leverage **info. sources** to identify protective strategies

Contextual factors **constrain the scope** of strategies

Threat identification

Price and technical effort inform **cost awareness**

Benefits of strategies stand on the S&P and perceived improvements in use cases

Strategy assessment

Findings: S&P Attitudes

So far I've decompiled the app and found that it uses Ayla Networks IoT platform. Oh and the Cipher Suite for added security

Exploration/Devotion

the last thing I want to do on the weekend is fiddle with Raspberry Pi

Pragmatism with high tech competence

Users' attitudes are contextual and evolve, despite preconception
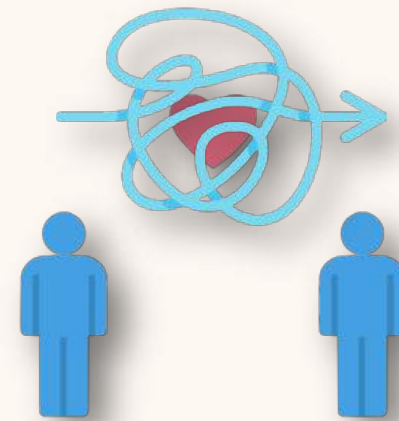
Findings: Resolving Ambiguity

- Collaborative exploration through elaboration

- Transfer of personal experience to a new context

- Supplementary information as evidence

> In my TPLink router, I have an option to block internal IP addresses from accessing the internet. Would it still work at all if it had NO connection

Users helped each other through iterations of discussion

Findings: Developing Attitudes

- The discourse affects S&P concerns

- The discourse informs alternative strategies

Edit: You're right, I wasn't scammed, but if it is a scam, someone else could easily fall for this

UPDATE: I took a hybrid approach. I setup a gmail account for the house and moved all accounts to it. I removed one of my Wink Relays...

Users benefit from the online discussion in making decisions
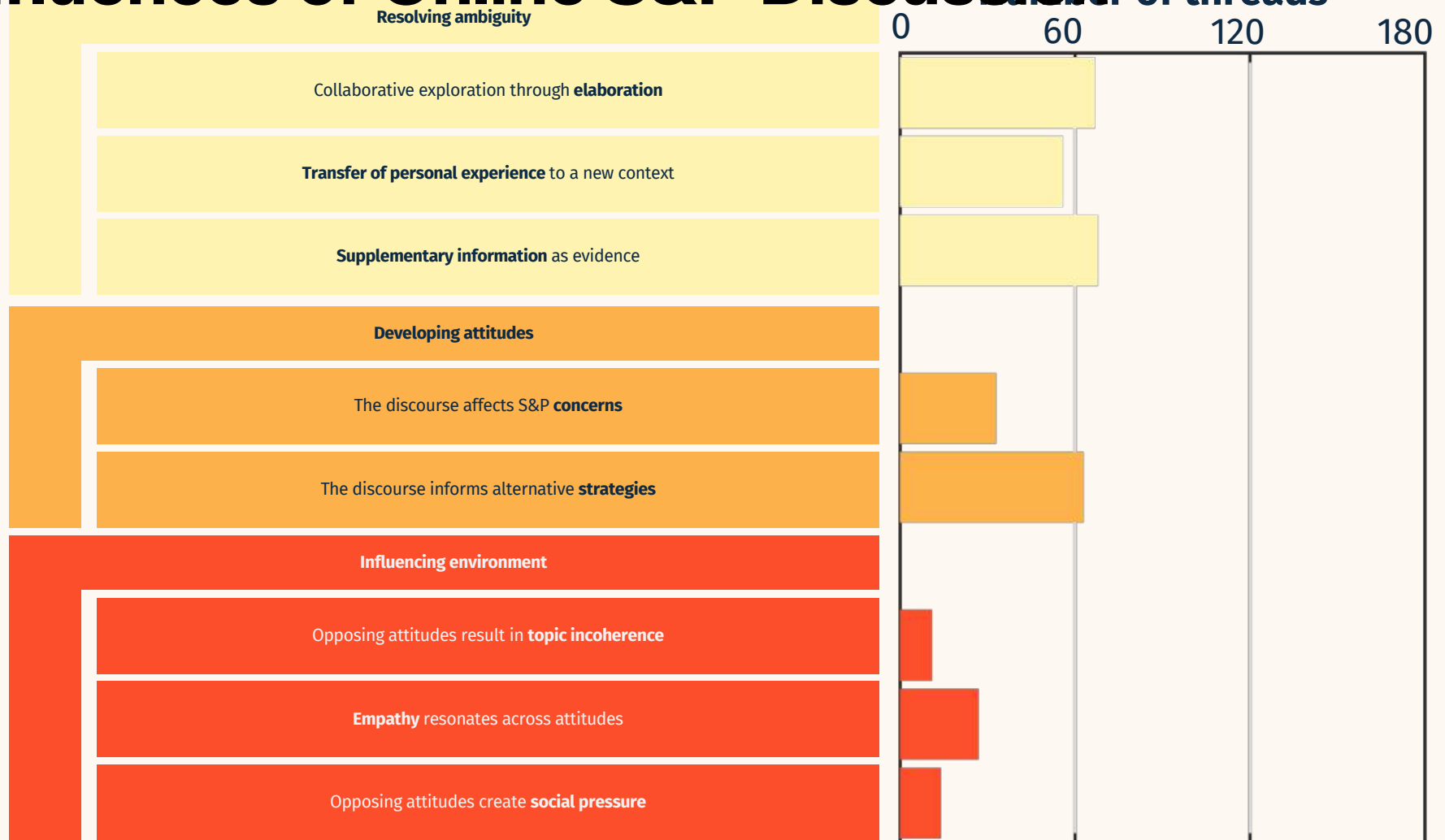
Findings: Influencing Environment

- Opposing attitudes result in topic incoherence

- Empathy resonates across attitudes

- Opposing attitudes create social pressure

… our son managed to get the Google Home Mini to recognize his 'HEY GOOGLE!!' this morning. People with small children and voice recognition Help

Am I weird for thinking it's weird that someone would potentially have access to control many things in my home through that echo?

S&P information in discussion can be difficult to access and assess

Influences of Online S&P Discussion

Number of threads

Resolving ambiguity

Collaborative exploration through **elaboration**

Transfer of personal experience to a new context

Supplementary information as evidence

Developing attitudes

The discourse affects S&P **concerns**

The discourse informs alternative **strategies**

Influencing environment

Opposing attitudes result in **topic incoherence**

Empathy resonates across attitudes

Opposing attitudes create **social pressure**

0   60   120   180
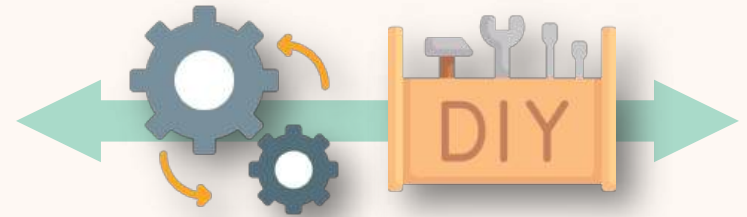
Recommendations: Design and Practice

1 Incorporate users' **diverse considerations**

2 Support **attitude development** in real life

3 Improve access to **credible S&P info.** online
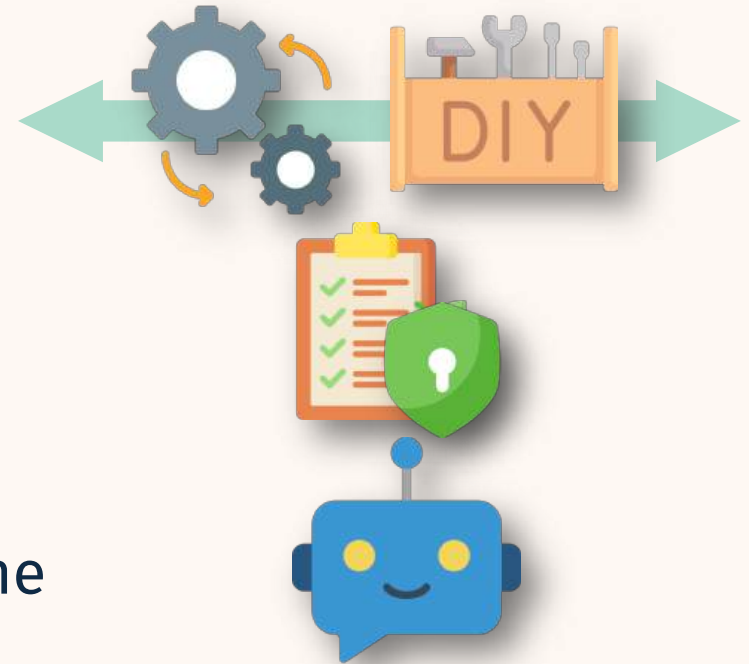
Recommendations: Design and Practice

1 Incorporate users' **diverse considerations**

- Inform users about smart home operations and practices in a transparent and understandable manner

- Make S&P protective strategies available and flexible for products

- Accommodate considerations of different users, e.g., tech-savvy vs. novice, for specific use cases (e.g., by tech caregiving)

Recommendations: Design and Practice

**2** Support **attitude development** in real life

- Nudge users' S&P attitudes with physical metaphors (privacy labels and more?)

- Deploy S&P nudges at scale through automated assessment of smart home products.

Recommendations: Design and Practice

3 Improve access to **credible S&P info.** online

- Highlight the access to credible S&P information and sources (e.g., Wiki and security advice)

- Help mediate S&P discussion by detecting misinformation and moderation
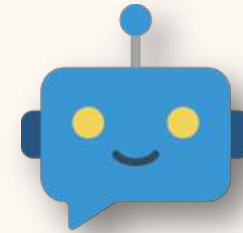
Recommendations: Research Direction

1. Study users' dynamic and context-dependent S&P **attitudes across domains**

2. Study users' attitudes **longitudinally at a community level**

3. Investigate the underlying **geopolitical and cultural influences** on S&P attitudes

4. Understand how different S&P **information sources online** impact users

I don't think smart home will take off for us to concern about.

7 years ago…

The Chinese state overlord may put a backdoor in my device.

Take-home

- **(Blog)** Vetrivel, S., Bouwmeester, B., van Eeten, M. and Gañán, C.H., 2024. {IoT} Market Dynamics: An Analysis of Device Sales, Security and Privacy Signals, and their Interactions. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 7031-7048).

- **(Blog)** Do, Y., Arora, N., Mirzazadeh, A., Moon, I., Xu, E., Zhang, Z., Abowd, G.D. and Das, S., 2023. Powering for privacy: improving user trust in smart speaker microphones with intentional powering and perceptible assurance. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 2473-2490).