How to Explain Trusted Execution Environments (TEEs)?

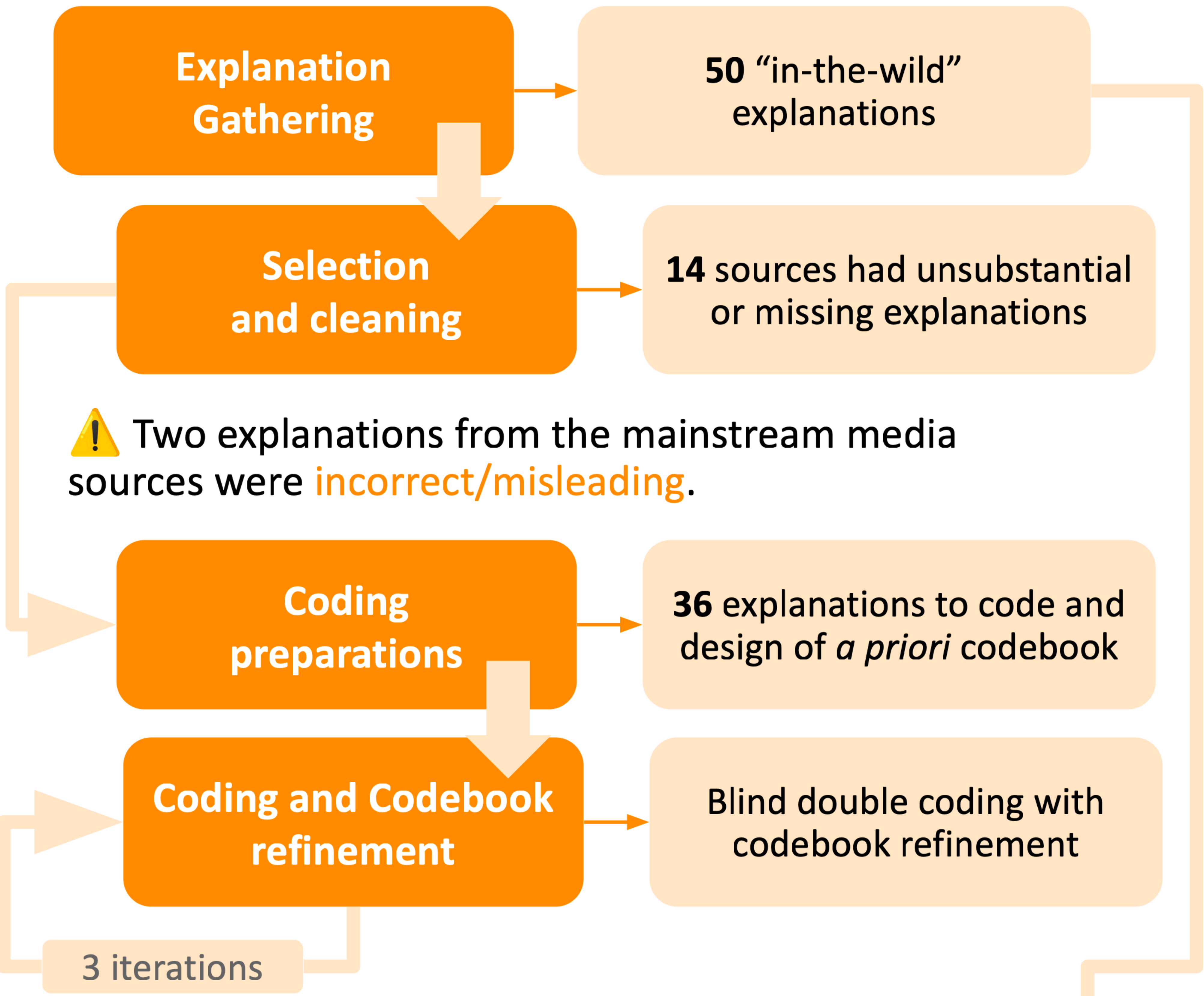
Carolina Carreira[1][2], McKenna McCall[1], Lorrie Faith Cranor[1]

[1]Carnegie Mellon University, [2]IST University of Lisbon and INESC-ID

People don't understand TEEs

TEEs can make people more comfortable sharing data
...*especially if they understand what a TEE is!*
(Musale et al., 2023)

How are TEEs currently been explained?



Explanation Gathering → **50** "in-the-wild" explanations

Selection and cleaning → **14** sources had unsubstantial or missing explanations

⚠️ Two explanations from the mainstream media sources were incorrect/misleading.

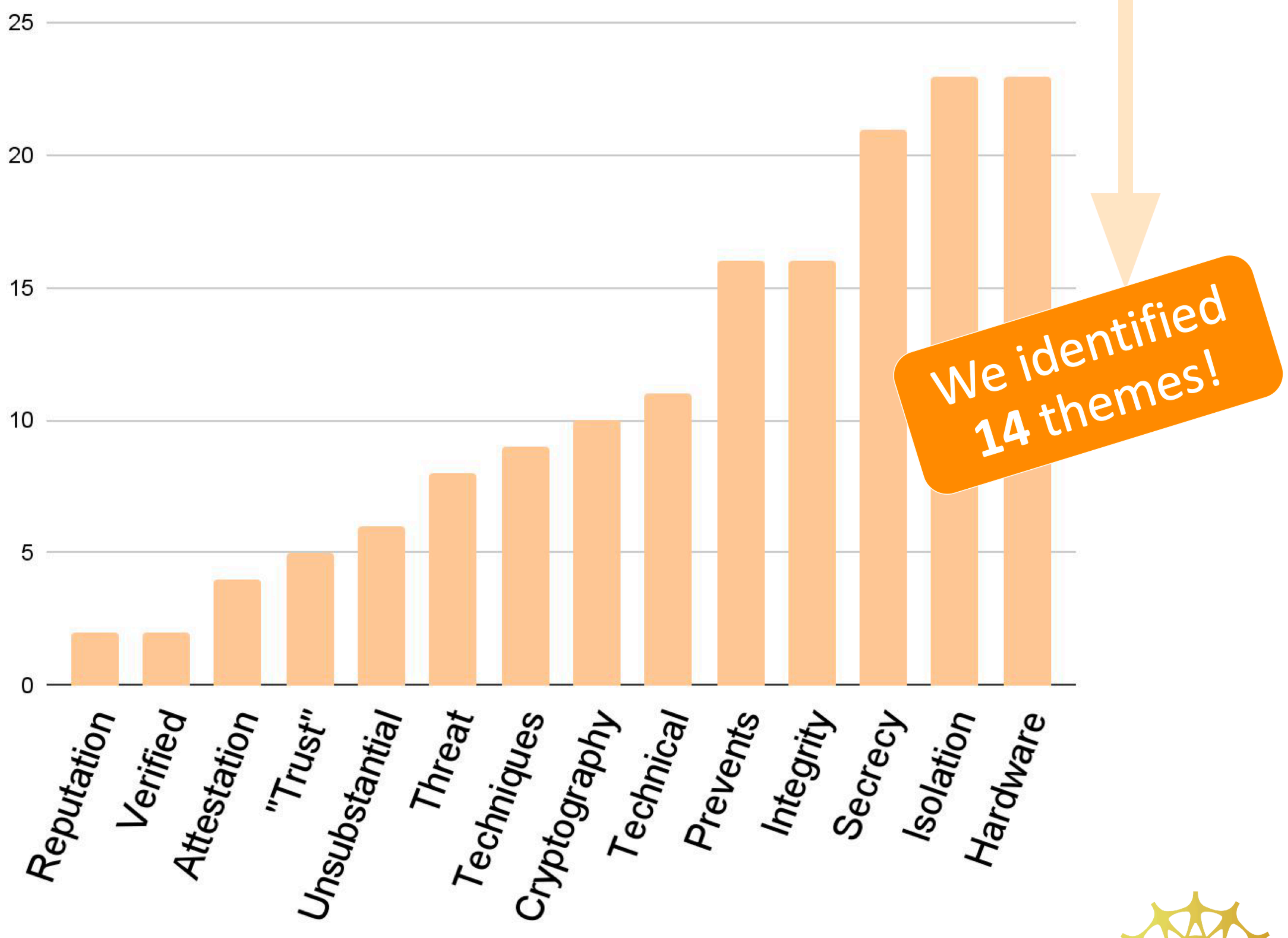
Coding preparations → **36** explanations to code and design of *a priori* codebook

Coding and Codebook refinement → Blind double coding with codebook refinement

3 iterations

Which themes should we include in our experiments?

➤ Some themes are more common than others

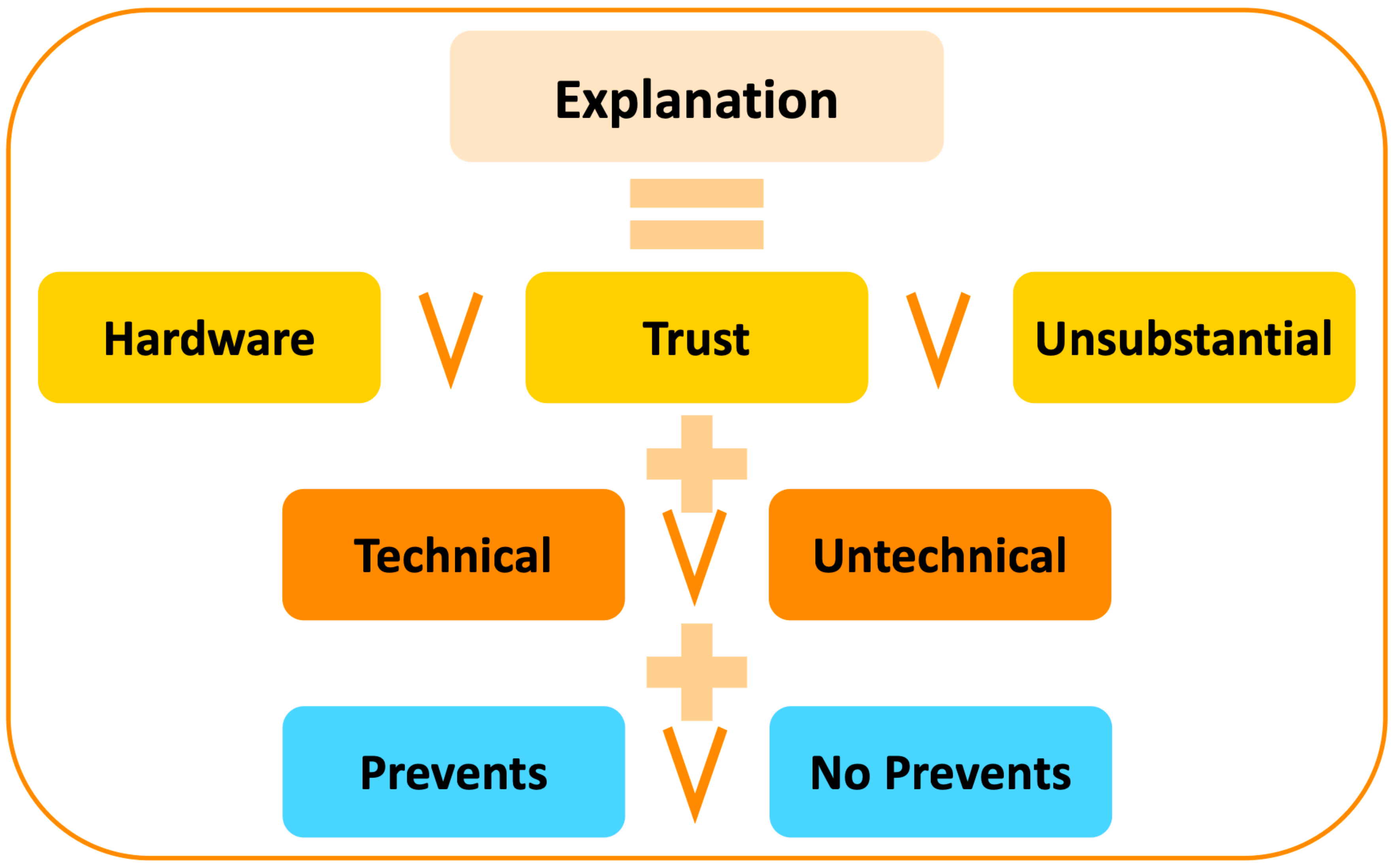


We identified **14** themes!

New explanations with the themes identified "in-the-wild"

➤ Designed in collaboration with the CDCC

➤ Each explanation could have up to 3 different ingredients – some of which may be toggled off.



For example Hardware + Technical + Prevents =

A Trusted Execution Environment (TEE) is a technique for running programs and interacting with data securely using a protected area of the physical computer. A program running in a TEE is isolated from the rest of the computer to protect the confidentiality and integrity of the program and data. The TEE protects the program and data even when other software on the computer is behaving maliciously.

We evaluated 12 explanations with 469 participants…

➤ We measured **understanding** through 10 True/False questions and **trust** by rating **perceptions** of safety and **willingness** to use TEE enhanced technology

➤ Different explanations **can** have an effect on comprehension…

…But little effect on trust

‼️ And people **still have questions** about TEEs which our explanations do not answer!

For future work we will further investigate trust issues, develop an FAQ, and compare explanation vs. no explanation

Musale, P., & Lee, A. (2023). Trust TEE?: Exploring the Impact of Trusted Execution Environments on Smart Home Privacy Norms. *Proceedings on Privacy Enhancing Technologies*.

CDCC
CyLab
Carnegie Mellon University Security and Privacy Institute