“The Thing Doesn’t Have a Name”: Learning from Emergent Real-World Interventions in Smart Home Security

Brennen Bouwmeester, Elsa Rodríguez, Carlos Gañán,
Michel van Eeten, **Simon Parkin**

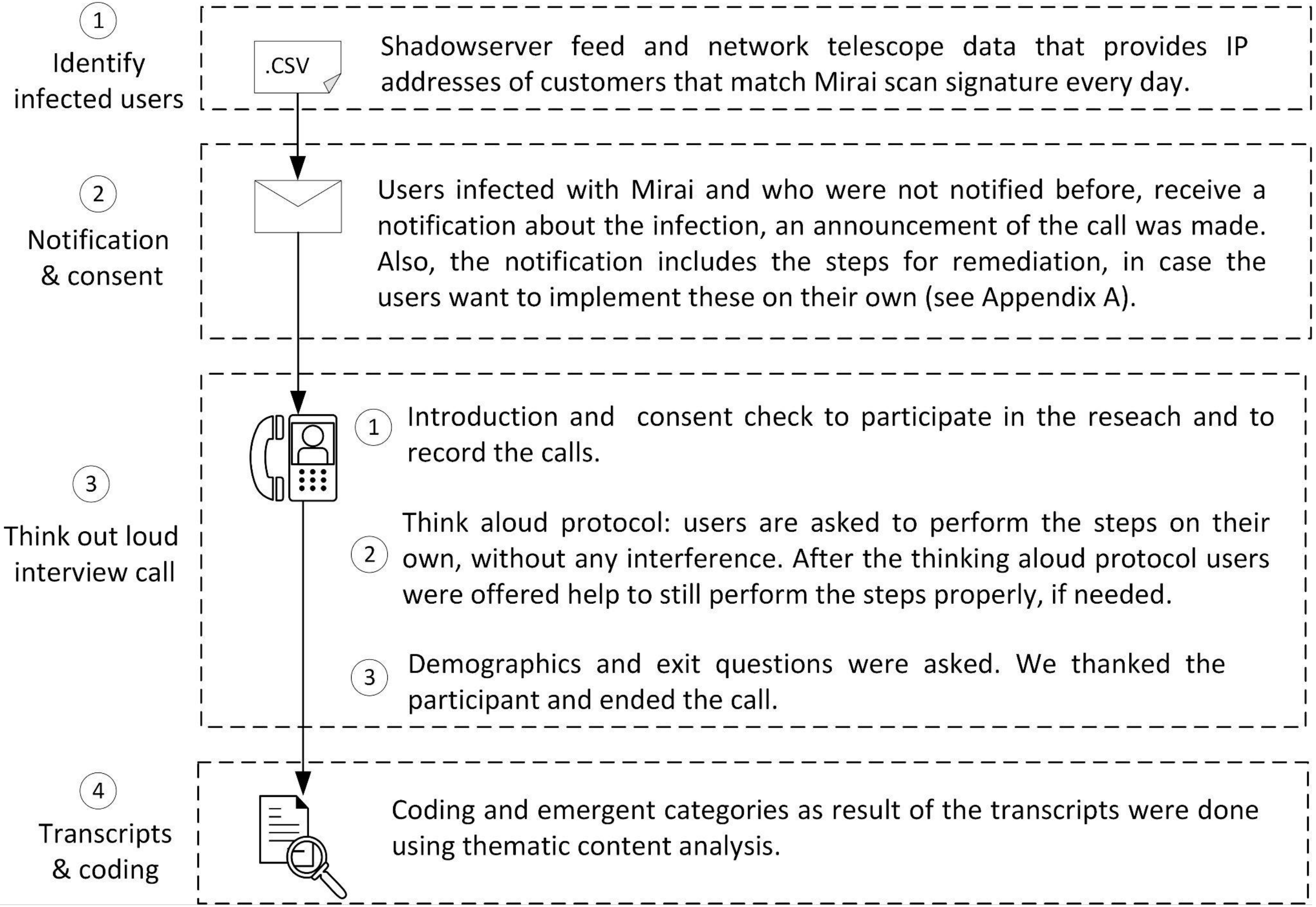
Delft University of Technology

Aims

- It remains that many IoT devices have technical vulnerabilities, or ineffective security configuration options
- These problems expose a range of consumer IoT devices to malware infections
- A typical fix is Internet Service Providers (ISPs) sending clean-up prompts to owners of infected IoT devices
- Little is known about what takes place in end-users’ homes after receiving remediation advice
    - They may not be able to confirm if a device is infected, or prove removal of malware
- We coordinated with an ISP, conducting remote think-aloud observations with 17 customers with an infected device
- Observations focus on the following question:

How do end-users act on remediation advice about their infected Internet of Things device(s)?

Methodology



1 Identify infected users

Shadowserver feed and network telescope data that provides IP addresses of customers that match Mirai scan signature every day.

2 Notification & consent

Users infected with Mirai and who were not notified before, receive a notification about the infection, an announcement of the call was made. Also, the notification includes the steps for remediation, in case the users want to implement these on their own (see Appendix A).

3 Think out loud interview call

1. Introduction and consent check to participate in the reseach and to record the calls.
2. Think aloud protocol: users are asked to perform the steps on their own, without any interference. After the thinking aloud protocol users were offered help to still perform the steps properly, if needed.
3. Demographics and exit questions were asked. We thanked the participant and ended the call.

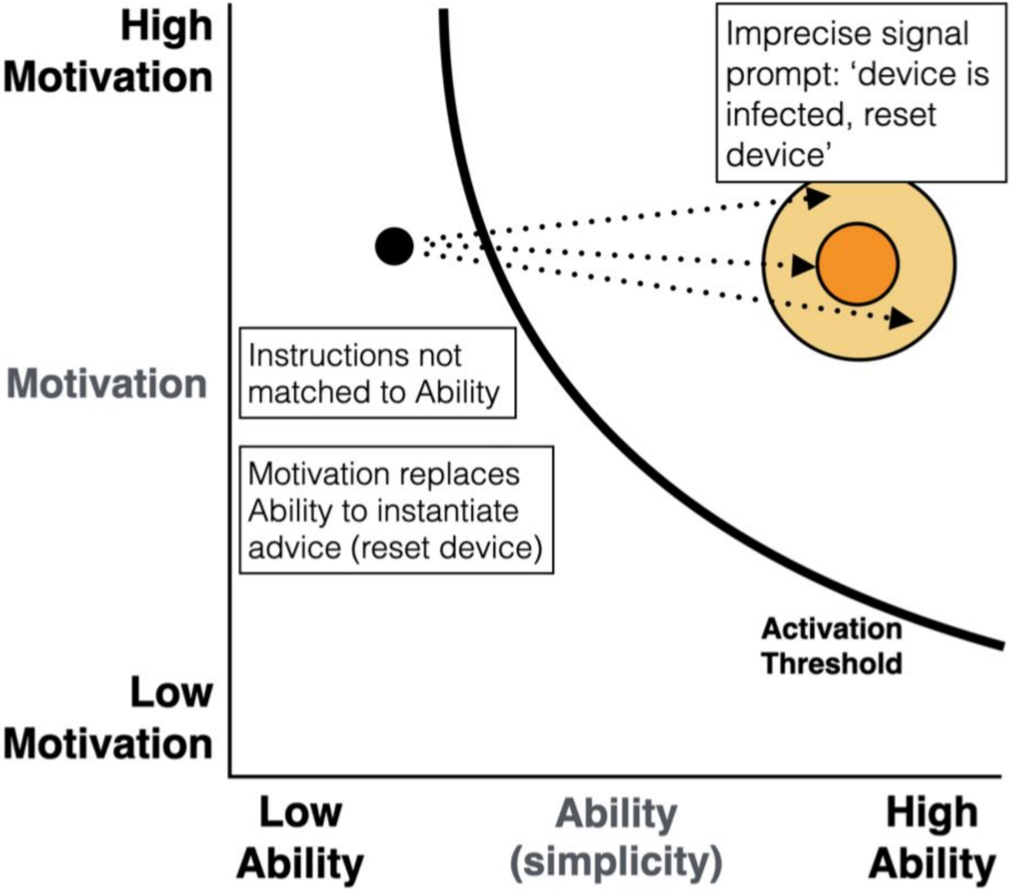
4 Transcripts & coding

Coding and emergent categories as result of the transcripts were done using thematic content analysis.

Outcomes

- Users are motivated BUT advice is constrained in many ways
- Only 4 of 17 participants successfully completed all five remediation steps
- Identifying infection in a home network relies on heuristics
  - Process of elimination, starting with a problematic device, independent searching
- Without a dedicated app or interface (3 participants), dedicated features were sought but hard to find (e.g., password change, reset button)
  - Participants fell back on familiar behaviours
- Cumbersome, non-deterministic remediation process is probabilistically related to desired outcome
  - 3 participants remained infected BUT some who ‘remediated’ had similar (lack of) success
- We saw ‘Action Diffraction’: users not *able to do enough* toward remediation
  - Behaviours had good chance of success, …
  - … but were not definitely going to succeed, or be confirmed as successful

Action Diffraction:



Imprecise signal prompt: ‘device is infected, reset device’

Instructions not matched to Ability

Motivation replaces Ability to instantiate advice (reset device)

Thank you for your attention!

Comments and questions welcome: s.e.parkin@tudelft.nl