Supporting Tangible Multi-factor Key Exchange in Households

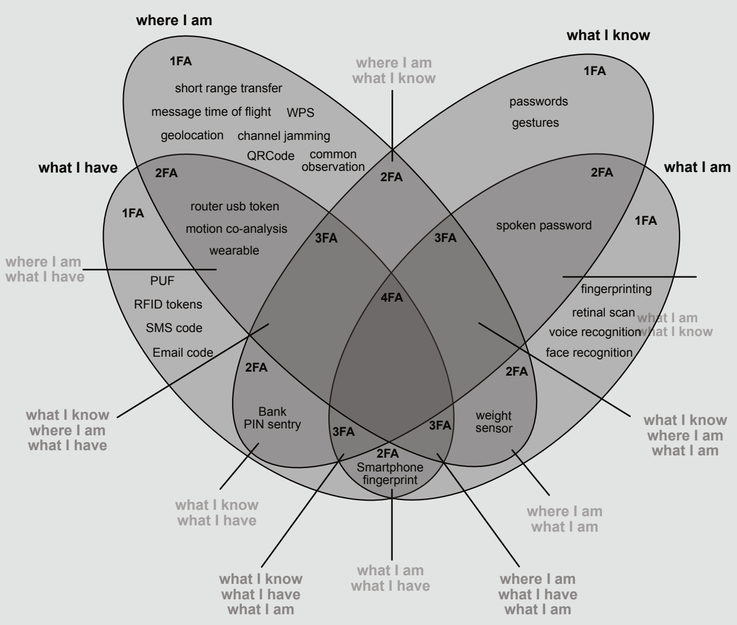
Dr T. Lodge, Horizon Institute, University of Nottingham
Dr Sameh Zakhary, Horizon Institute, University of Nottingham
Prof D.McAuley, Horizon Institute, University of Nottingham

INTRODUCTION

A common approach to securing end-to-end connectivity between devices on the Internet is to use a cloud-based intermediary. A promising new protocol, Wireguard, dispenses with the middleman to provide secure peer to peer communication. Support for the initial key exchange falls outside the protocol's scope. The design of secure and usable key exchange methods is challenging, not least in domestic spaces, as they're often characterised by technically naive users in multi-occupancy environments, making them susceptible to insider and passer-by attacks.

AIM

This research investigates the use of a home's semi-fixed features (i.e lamps, shelves, chairs) to support a multi-factor authentication approach. We undertake a study that explores the merits and limitations of this potential solution space.



WHY

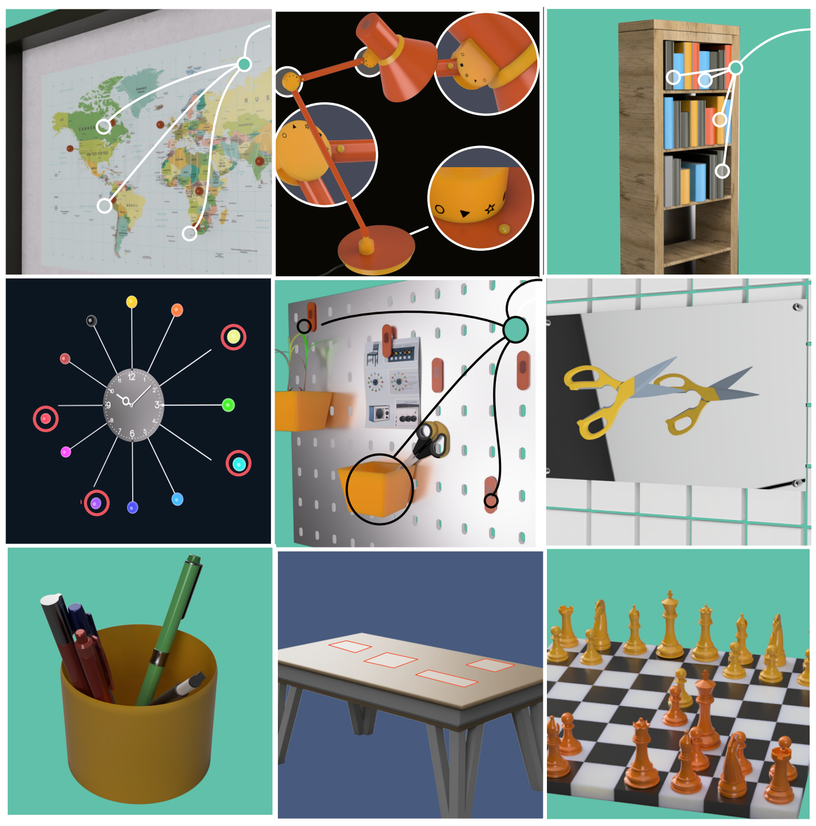
This work is intended to inform the design of new key-exchange solutions that are i. more secure than commonly used naive approaches and ii. desirable for end users.

METHODOLOGY

We adopted a 'sketching and ideation' approach akin to a focus group to gather feedback on nine alternative solutions. For each of the possible solutions we solicited feedback on a variety of characteristics, namely:

- intelligibility: how easy was the design to comprehend?
- desirability: would users actually want/use it?
- interactional complexity - relating to the solution's usability
- perceived security

We asked users to rank each solution and provide (unstructured) feedback on the approach.



Solution Sketches

KEY OUTCOMES

This project provides a set of **11 key observations** that provide a useful contribution to the further exploration and development of a promising approach tangible in-home key exchange mechanisms. These include:

- Perception of security is not the overriding factor in a user's acceptance of a solution.
- Interactional complexity can be offset by playful, personal or independently useful interactions around an object's primary purpose.
- Users prefer solutions where the patterns or combinations of secrets can be aligned to a narrative (such as pins in a map)
- Users care about (and readily anticipate) the influence of other householders on the solution (i.e. accidental or deliberate tampering)
- Users do not like solutions that utilise 'unfixed' items (i.e pens / pegs) as authentication tokens, fearing that their loss or destruction will result in the loss of access.

MAJOR FINDINGS

Our work suggests that physical in-home interactions offer a promising design space for secure, usable key exchange. User acceptance is subject to a set of concerns that extend beyond usability and perceptions of security and include aesthetics, domestic arrangements and personal routines and interests,

ACKNOWLEDGEMENTS

This work has been supported by the PETRAS : EP/S035362/1 National Centre of Excellence for IoT Systems Cybersecurity under the project "Tangible Security" (TanSec)

PUBLICATIONS

T. Lodge, S. Zakhary and D. McAuley, “Supporting tangible multi-factor key exchange in households”, **http://arxiv.org/abs/2203.13540**