ECE750: Usable Security and Privacy

Study Design

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

TULiPS
Technology Usability Lab in Privacy and Security

First, something random…

- First 5 minutes we talk about something interesting, often from recent events
- You will not be tested on the 5 minutes part of lecture
- This part of lecture will sometimes not be recorded
- Why do this?
  1. Some students show up late
  2. Reward students who show up on time
  3. Important to see real world examples

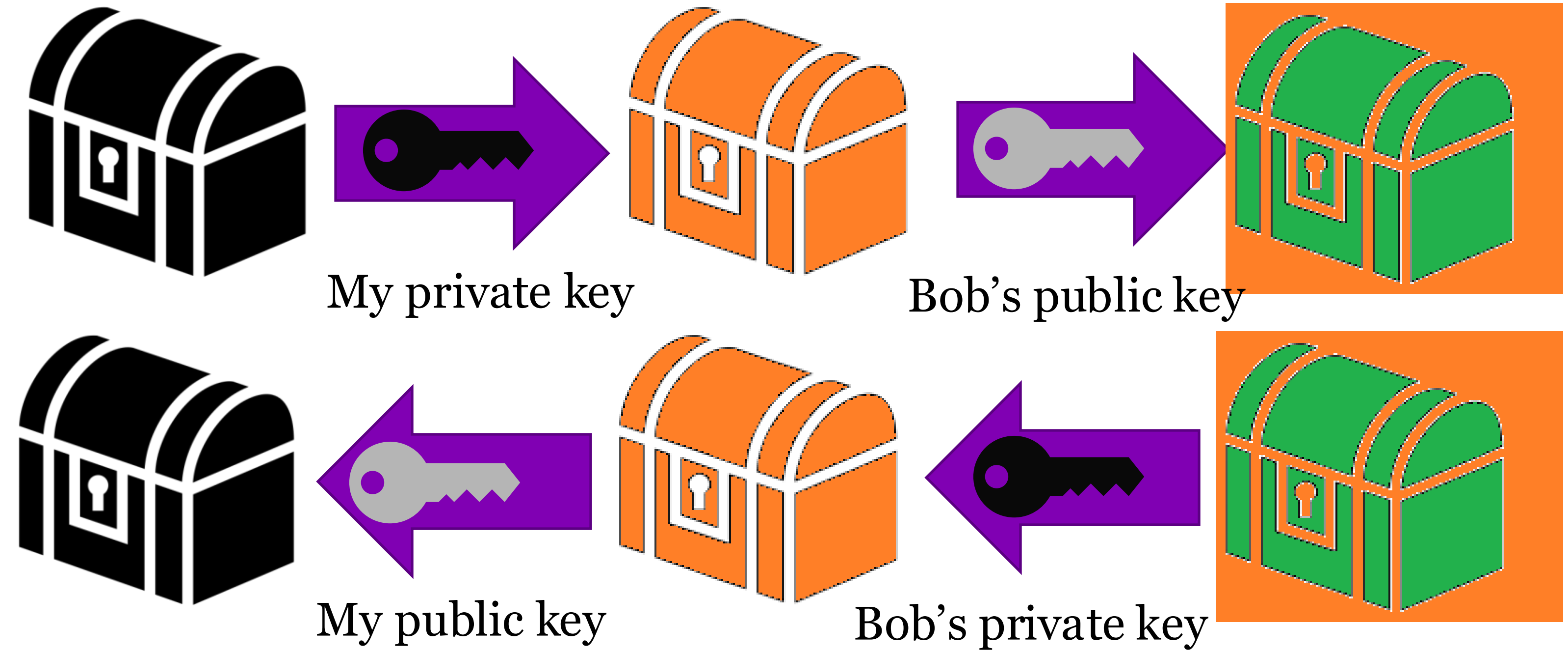
Today…

1. Overview of public/private key encryption
2. Cognitive Walkthrough
3. Deep discussion of the paper: Why Johnny Can't Encrypt

If I do both of those at the same time I can prove that:

1. only I could have sent the message (signature)

2. only Bob can read it (encryption)



My private key

Bob’s public key

My public key

Bob’s private key

My public key

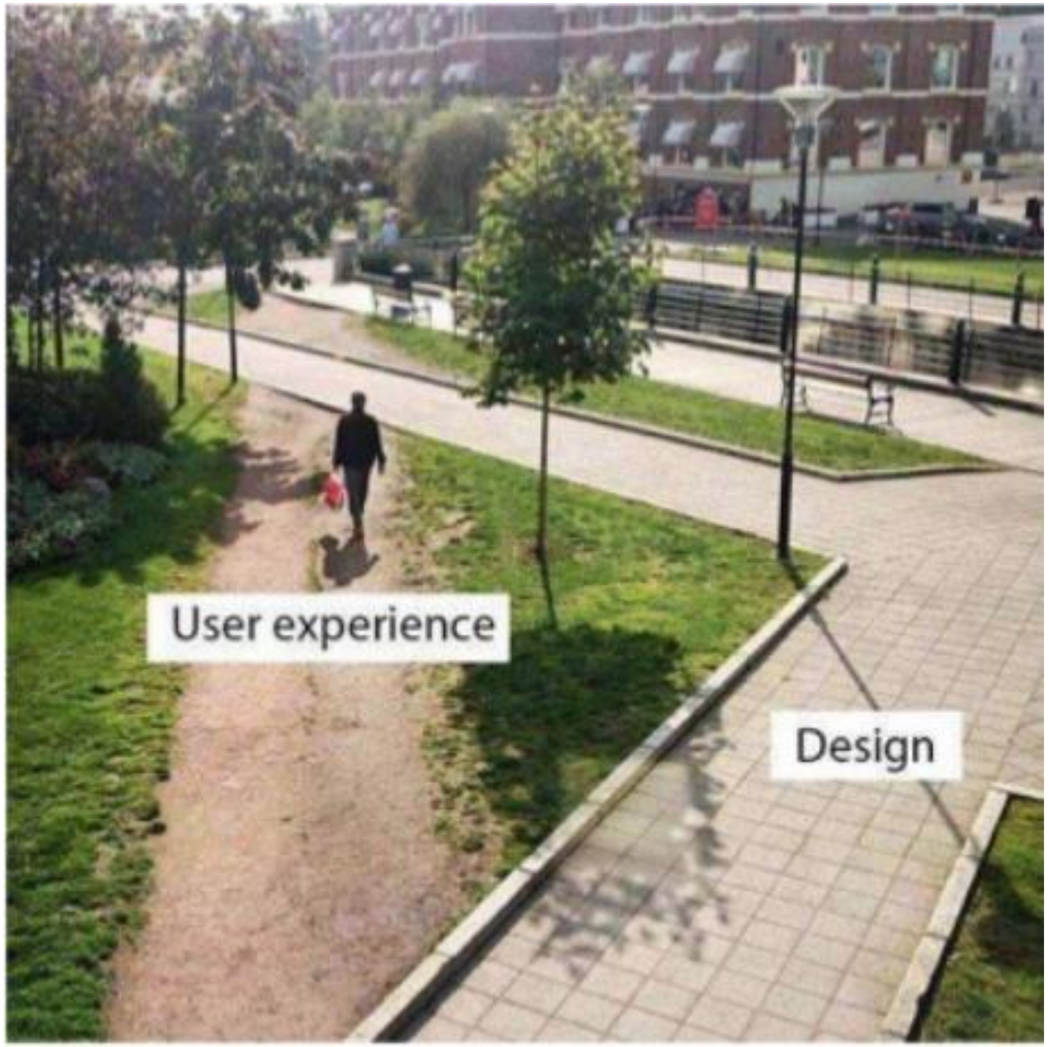
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozHejfV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnqoCplgXcN2GJxfEHHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxdMQkgb2H2xw28RYfYkdDouteIkOrFLrCy9ZF9KdMhA1eBH94KnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAG0IkthbWkgVmFuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIACkFAlYKYvECGyMFCQlmAYAHCwkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIjI2b+Q75/5t+EgXOHpRoPIxfG
lZ6zOEpf6A18iFXx3JgQZdwPDojtBiWNpOyMeBGTgIvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNQhQDPcToODgbRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQkJ7uQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrxuJ8YfHWSohEScNOcYC2P8q2olJwwE26T
lpdtrwCqtB1LYW1pIFZhbmllYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIb
IwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dl9JJAIAIWorxrlYsrmKS6CbW8MgTxxTDOXaCt1b7FoWoQZHskIUQhEcE+a
XBYib1A5uHaatLfyjeXaD3qMEoZnQHoYMGEoGKuoowWsbhfoQzHPgwzRLkD1i75M
BIbawwoKWoVB9e4AkMakXJCnF5BXeo6AHRL2v15V205DikVnlCRXocKtu8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDJpo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+KOdwPM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAlTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJDf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUuIrwezY1NebWNCRQHzQvRv/VJwjbTUx+Q3HsjIkKlHbE7iCiQXXtTRkoEny
2nudcjGI2vo3C3B2JCucEw6esF1x79PI/lPv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhohcHdF9oZem1eMeiDEeVkH63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuycVKonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZIarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fVVMhydiRJv8WsoUs6
INfVU3nxH+ZYthPbYoT86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNorir3GIpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFPooJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSSo5x1RdXHqpEbgap8dtuHhVvJw9QYDQBJroK4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTDJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdF
5yu5oJyRSf2fqRND6P/2eHNXejDUtdvhUXIUt8h9MuUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/NAc5TIuVHRHNOWNplcIJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPOdbCZf
2Tozd7h9MXtGJDlPKJ8eLG8ogcMAEQEAAYkBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdsxl9/HZfS+hB/9BJqSmIgcoHFXnb1PVIKxekzL8+WVm5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4ioodwJGw5/daTWRrTzcnKd8YqoP+DUot96HZDSu3m
mCzE9NVAQYboFbVmGOxoeo627UBSvFqaXvAxBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGlZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD831Syvdv
llOBx83/Rogg7hUkI6F2vzXicWmUwFSXRrggCSbLosHsP6isBWwvlHeRmna/aQab
YKG3gbV9iyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
=x5FK
-----END PGP PUBLIC KEY BLOCK-----
```

Usability

A design is not usable or unusable *per se*

- its **features**, together with the **users**, **what the users want** to do with it, and the **users' environment** in performing tasks, determine its level of usability



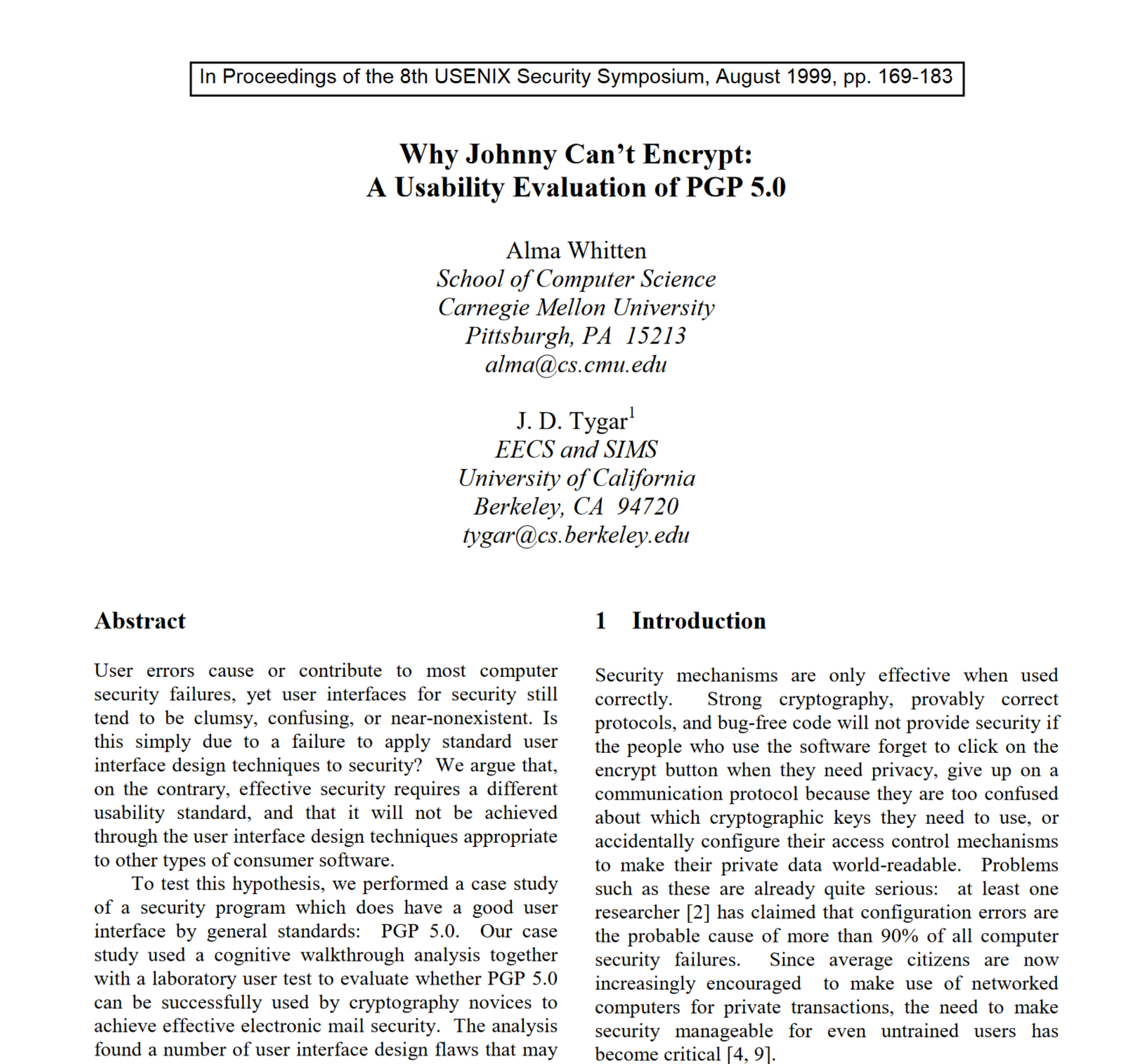
Usability

A design is not usable or unusable *per se*

- its **features**, together with the **users**, **what the users want** to do with it, and the **users' environment** in performing tasks, determine its level of usability

STRUCTURING RESEARCH

Why Johnny Can’t Encrypt



In Proceedings of the 8th USENIX Security Symposium, August 1999, pp. 169-183

Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

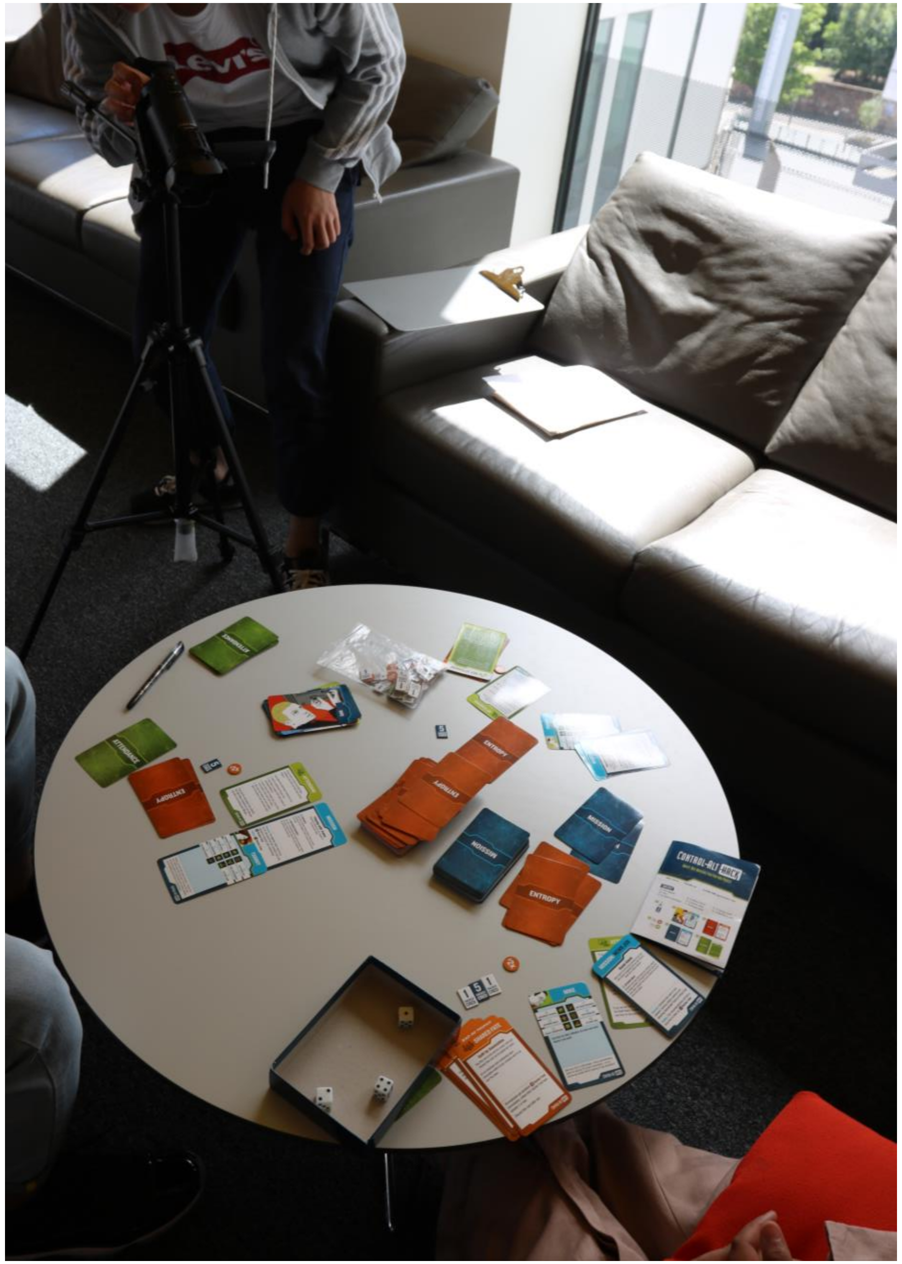
To test this hypothesis, we performed a case study of a security program which does have a good user interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world-readable. Problems such as these are already quite serious: at least one researcher [2] has claimed that configuration errors are the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical [4, 9].

Structuring Research

- Research question or goal
- Literature review (what have others learned or done)
- Methods planned to answer question or achieve goal
- Evaluate outcome
- Contextualize findings
- Writeup



Research Question or Goal

Research Questions

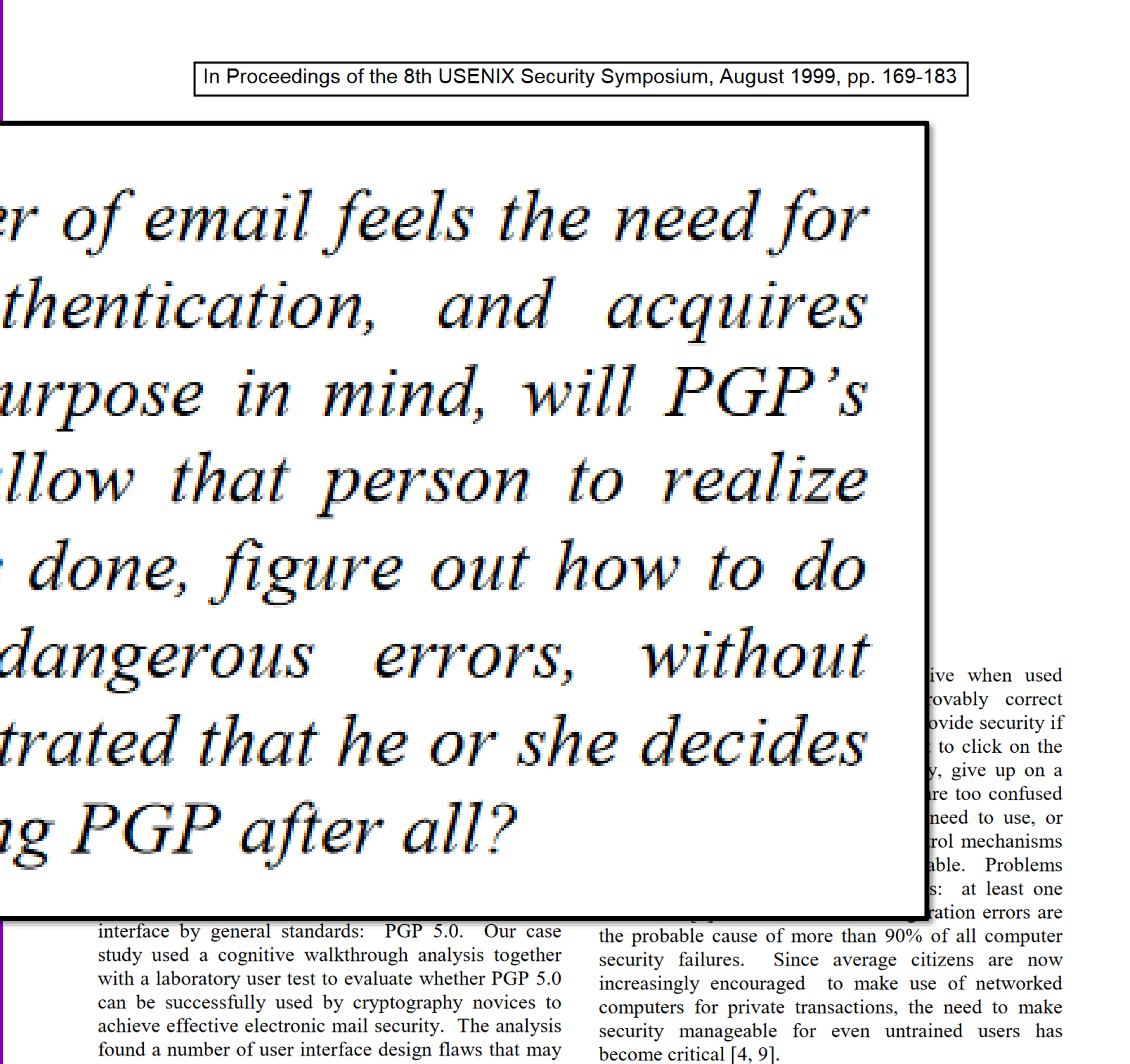
- Can people differentiate between a subdomain and a domain when reading a URL?
- Can users use [my new password manager] faster and with less errors than [the old password manager]?
- Does knowing how an app will use its permissions impact app installation decisions?
- What factors impact end-users' willingness to update software?
- Is the guidance given by some static analysis tools better at helping developers identify and fix security errors in their code?

Research Goals

- Automatically extract question and answer pairs from privacy policies.
- Collect social media posts people write while their account is protected.
- Accurately cluster phishing messages by scam.

Why
Enc

> *If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?*



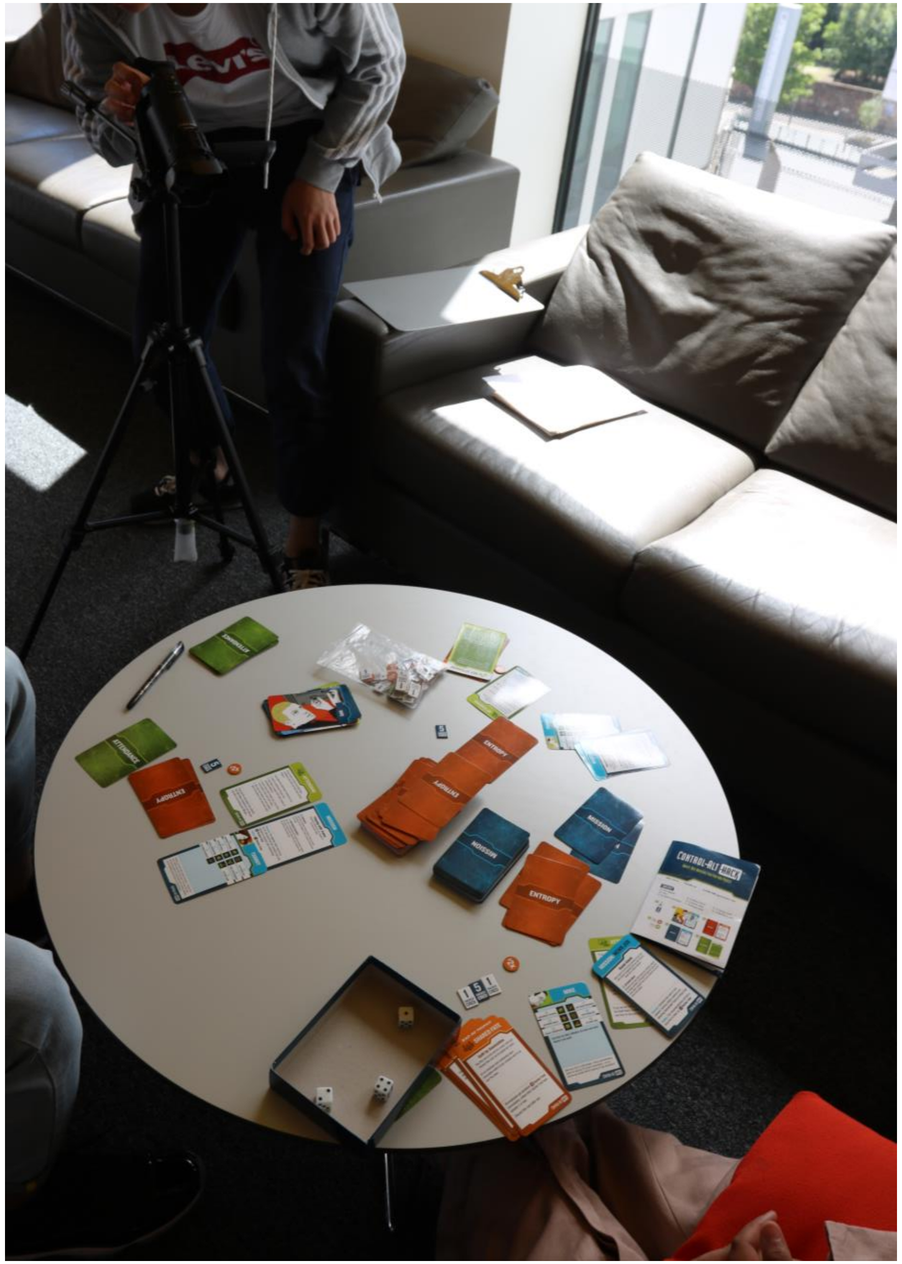
In Proceedings of the 8th USENIX Security Symposium, August 1999, pp. 169-183

interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may

ive when used
rovably correct
ovide security if
to click on the
y, give up on a
re too confused
need to use, or
rol mechanisms
able. Problems
s: at least one
ration errors are
the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical [4, 9].

Structuring Research

- Research question or goal
- **Literature review (what have others learned or done)**
- Methods planned to answer question or achieve goal
- Evaluate outcome
- Contextualize findings
- Writeup



Literature – state of the art

- Defining usability for security
- Problematic properties
  - Unmotivated user property
  - Abstraction property
  - Lack of feedback property
  - Barn door property
- PGP documentation and marketing
- Related work
  - There isn’t much….

Understanding the problem

Definition: Security software is usable if the people who are expected to use it:

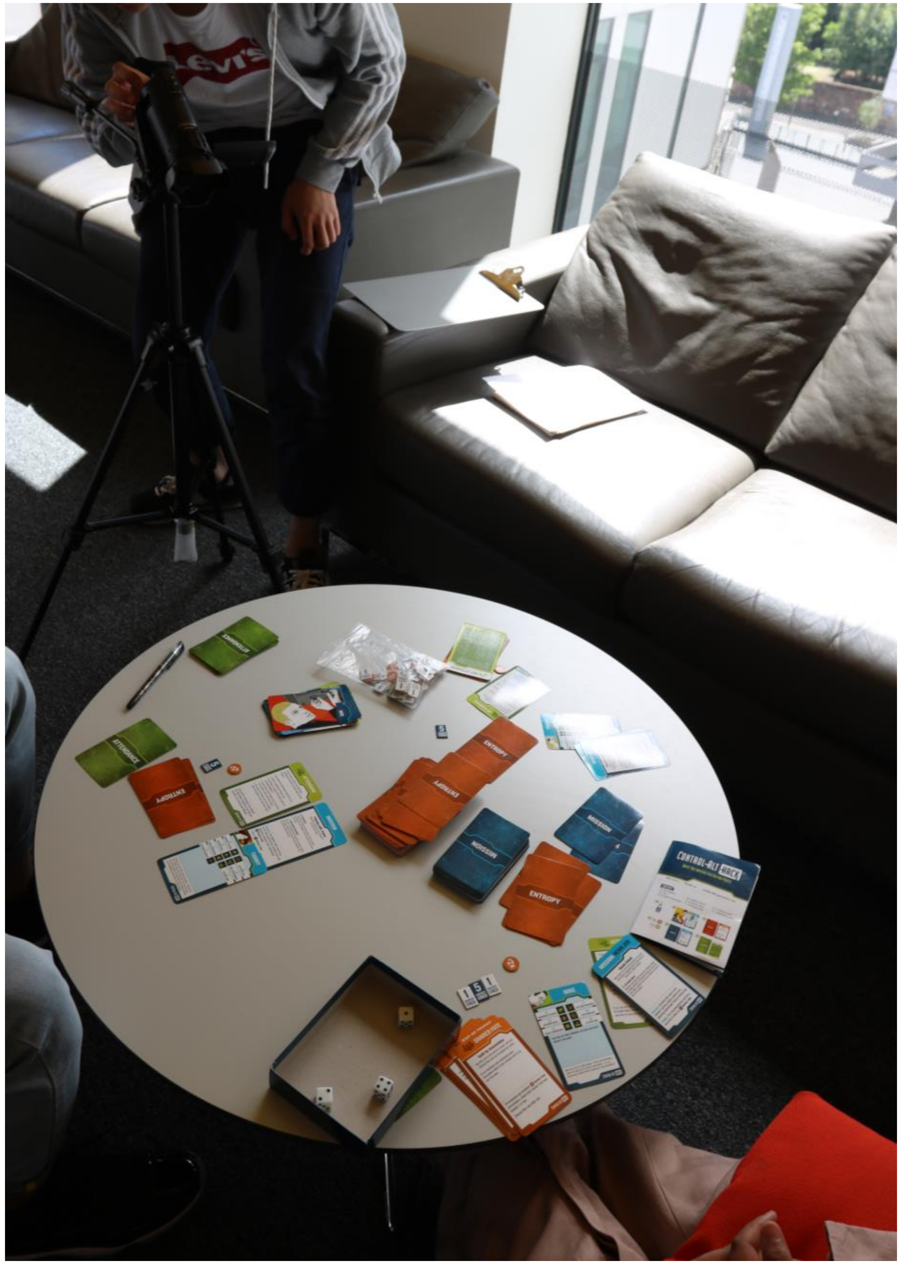
1. are reliably made aware of the security tasks they need to perform;
2. are able to figure out how to successfully perform those tasks;
3. don’t make dangerous errors; and
4. are sufficiently comfortable with the interface to continue using it.

PGP users need to:

- understand that privacy is achieved by encryption, and figure out how to encrypt email and how to decrypt email received from other people
- understand that authentication is achieved through digital signatures, and figure out how to sign email and how to verify signatures on email from other people
- understand that in order to sign email and allow other people to send them encrypted email a key pair must be generated, and figure out how to do so
- understand that in order to allow other people to verify their signature and to send them encrypted email, they must publish their public key, and figure out some way to do so
- understand that in order to verify signatures on email from other people and send encrypted email to other people, they must acquire those people's public keys
- manage to avoid such dangerous errors as accidentally failing to encrypt, trusting the wrong public keys, failing to back up their private keys, and forgetting their pass phrases
- be able to succeed at all of the above within a few hours of reasonably motivated effort

Structuring Research

- Research question or goal
- Literature review (what have others learned or done)
- **Methods planned to answer question or achieve goal**
- Evaluate outcome
- Contextualize findings
- Writeup

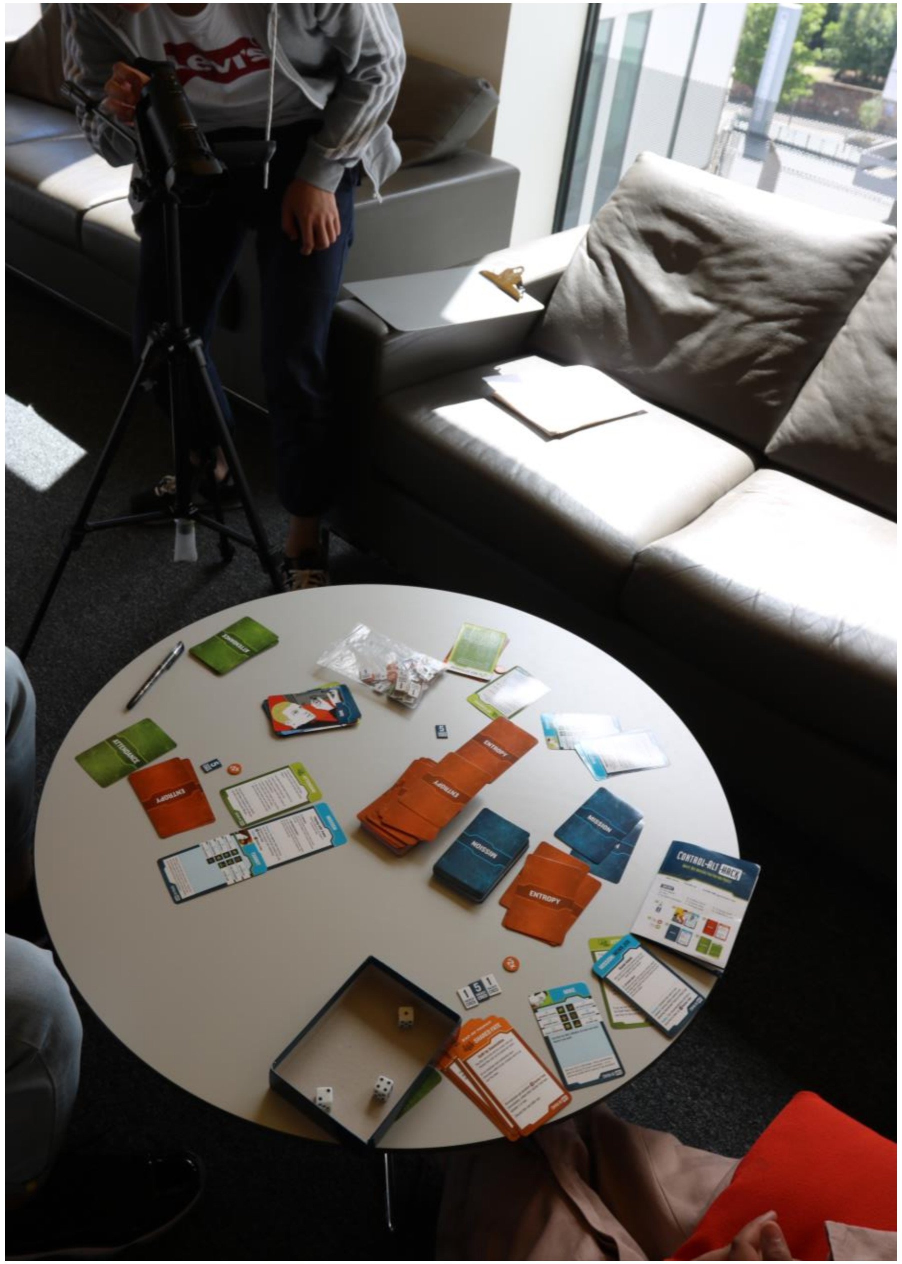


Tested usability using two methods

- Cognitive Walkthrough
    - A set of experts review the experts and make an informed guess about what will be problematic
    - Paired with heuristics – The experts state how the user interface supports or violates common HCI principles (Heuristics)
- Lab Study
    - Ask the participant to perform a set of tasks
    - Very similar to a think aloud, but without the talking aloud part

Structuring Research

- Research question or goal
- Literature review (what have others learned or done)
- Methods planned to answer question or achieve goal
- **Evaluate outcome**
- Contextualize findings
- Writeup



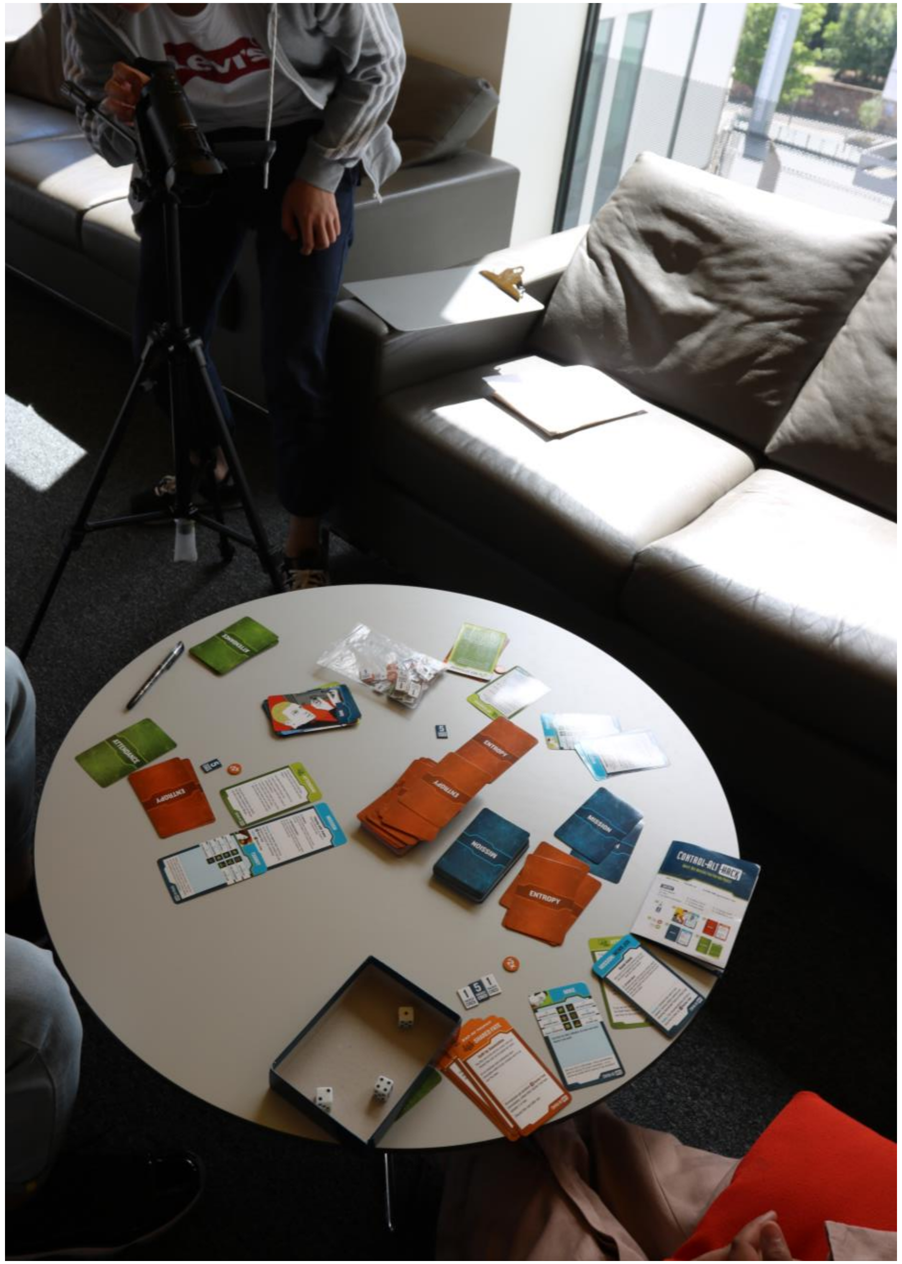
Cognitive walkthrough outcomes

- **Visual metaphors** – Do key and lock pictures make sense?
- **Different key types** – Public vs private keys, or maybe signing and encryption keys?
- **Key server** – Used for sharing keys
- **Key management policy** – Trust and validity ratings
- **Consistency** – Use of the same terms everywhere

- **Too much information** – Information like key size, hashes, and trust
- **Irreversible actions**
  - Accidentally deleting the private key
  - Accidentally publicizing a key
  - Accidentally revoking a key
  - Forgetting the pass phrase
  - Failing to back up the key rings

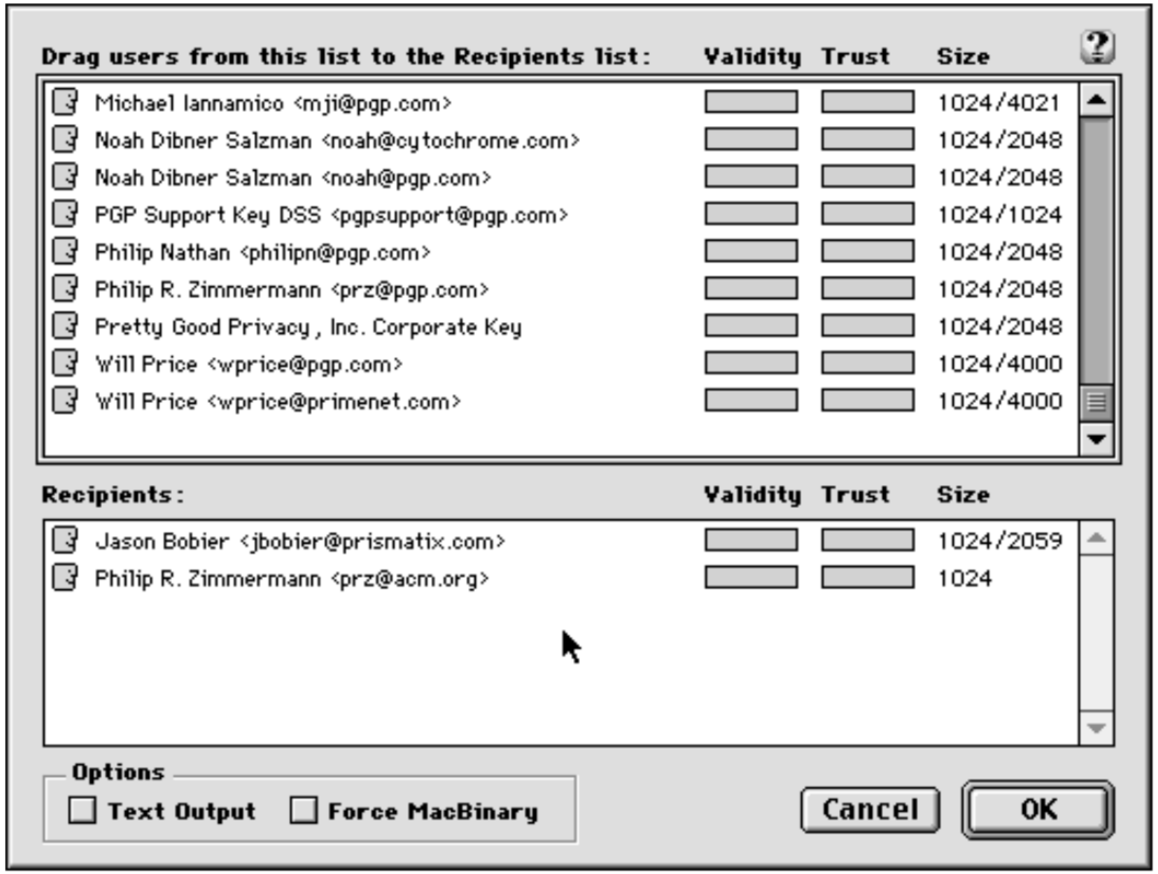
Structuring Research

- Research question or goal
- Literature review (what have others learned or done)
- **Methods planned to answer question or achieve goal**
- **Evaluate outcome**
- Contextualize findings
- Writeup



Lab Study

- Participants physically come to lab
- Scenario creates a realistic situation likely to produce expected issues
    - Task was to send a secret message to a given set of email addresses.
- Participant given a scenario, but was aware that encrypting email was part of the study



Drag users from this list to the Recipients list:	Validity	Trust	Size
Michael Iannamico <mji@pgp.com>			1024/4021
Noah Dibner Salzman <noah@cytochrome.com>			1024/2048
Noah Dibner Salzman <noah@pgp.com>			1024/2048
PGP Support Key DSS <pgpsupport@pgp.com>			1024/1024
Philip Nathan <philipn@pgp.com>			1024/2048
Philip R. Zimmermann <prz@pgp.com>			1024/2048
Pretty Good Privacy, Inc. Corporate Key			1024/2048
Will Price <wprice@pgp.com>			1024/4000
Will Price <wprice@primenet.com>			1024/4000

Recipients:	Validity	Trust	Size
Jason Bobier <jbobier@prismatix.com>			1024/2059
Philip R. Zimmermann <prz@acm.org>			1024

Options

□ Text Output □ Force MacBinary

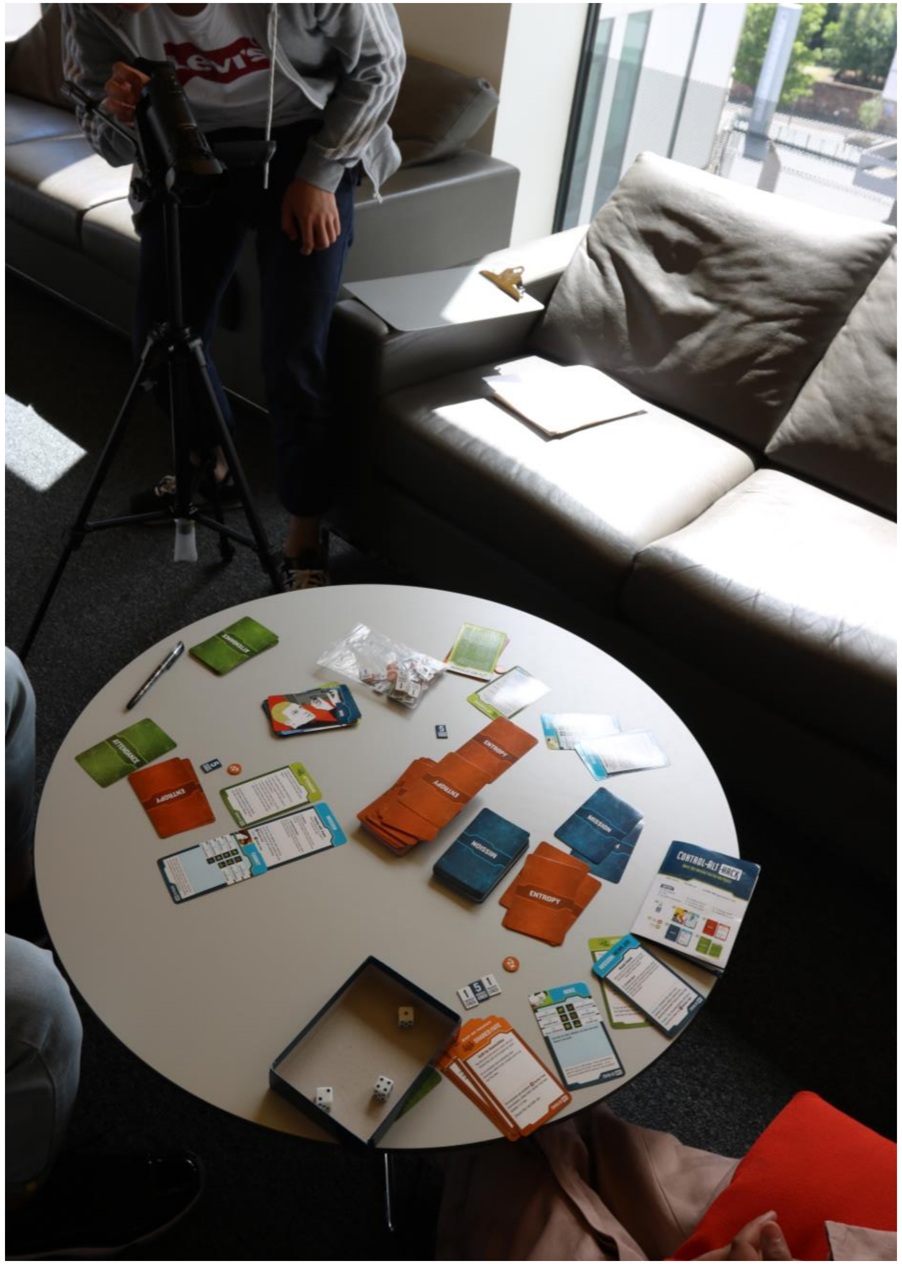
Lab study

- 12 participants with CS backgrounds
- Participant had to send several emails to team members (the researchers)
  - Creating a key pair
  - Sending their public key to team members
  - Getting team members' public keys
  - Sending the email
  - Decrypting response email

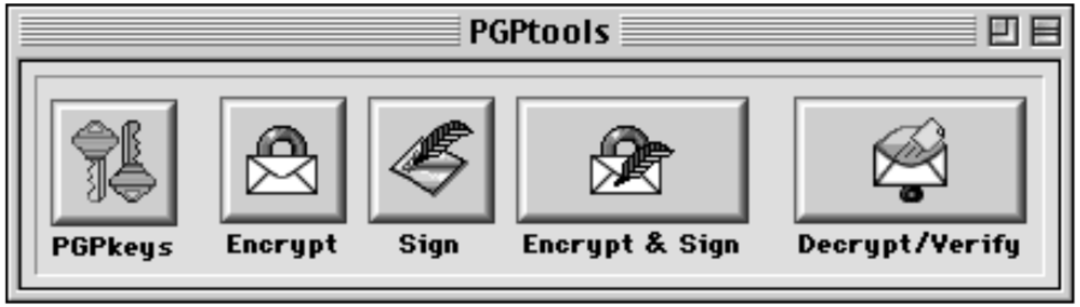
- 3 – emailed the private key to the team member
  - 1 never realized the error
- 1 – forgot their pass phase and had to re-generate keys
- 1 – never figured out how to encrypt
- 7 – used their public keys to encrypt
  - 1 created a separate key pair for each team member
- 3 – successfully sent an encrypted email to the whole team and were able to decrypt an response email

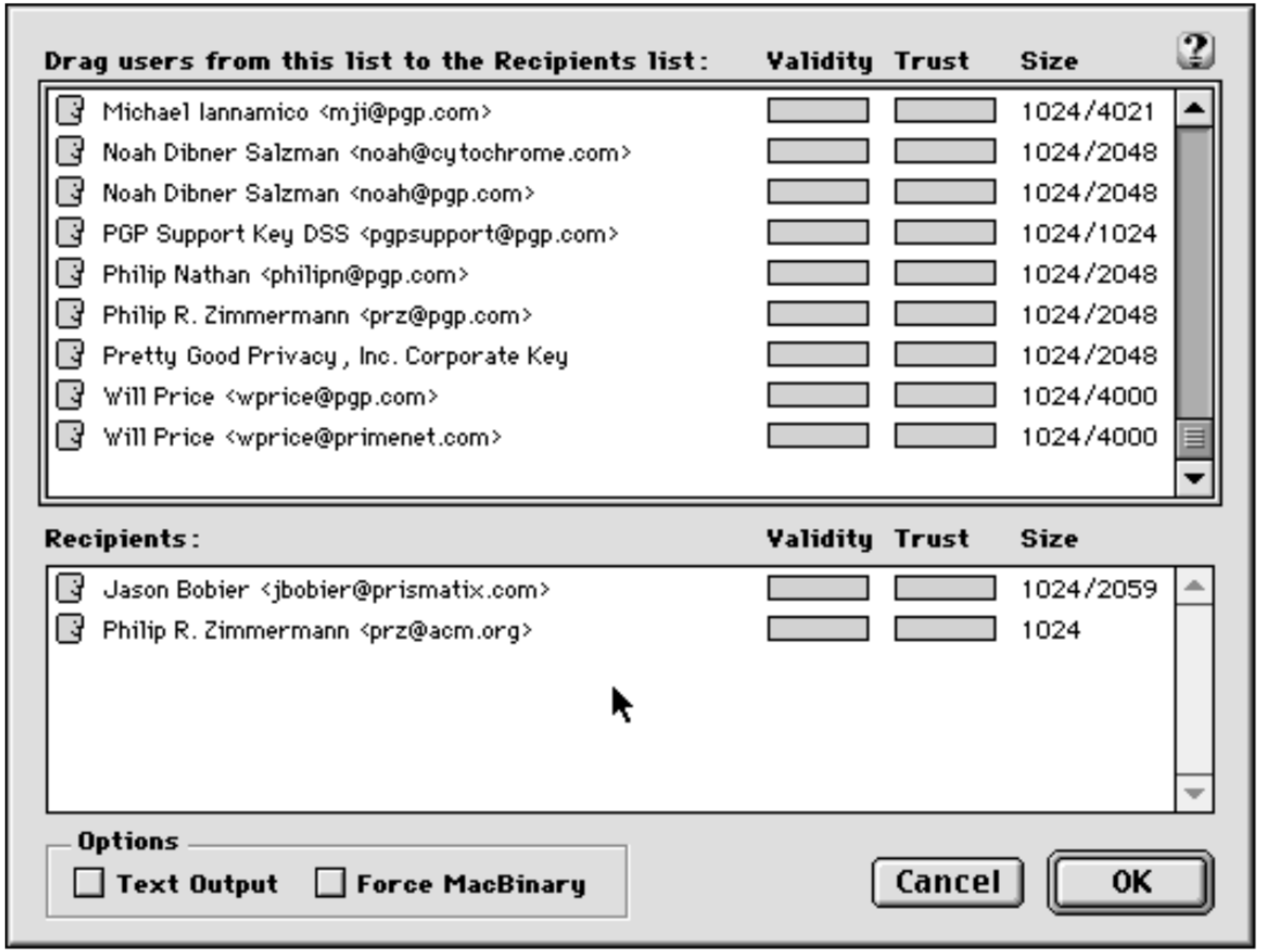
Structuring Research

- Research question or goal
- Literature review (what have others learned or done)
- Methods planned to answer question or achieve goal
- Evaluate outcome
- **Contextualize findings**
- Writeup



Whitten and Tygar evaluated PGP encryption in 1999, surely it must be more usable now.





Drag users from this list to the Recipients list:	Validity	Trust	Size
Michael Iannamico <mji@pgp.com>	▭	▭	1024/4021
Noah Dibner Salzman <noah@cytochrome.com>	▭	▭	1024/2048
Noah Dibner Salzman <noah@pgp.com>	▭	▭	1024/2048
PGP Support Key DSS <pgpsupport@pgp.com>	▭	▭	1024/1024
Philip Nathan <philipn@pgp.com>	▭	▭	1024/2048
Philip R. Zimmermann <prz@pgp.com>	▭	▭	1024/2048
Pretty Good Privacy, Inc. Corporate Key	▭	▭	1024/2048
Will Price <wprice@pgp.com>	▭	▭	1024/4000
Will Price <wprice@primenet.com>	▭	▭	1024/4000

Recipients:	Validity	Trust	Size
Jason Bobier <jbobier@prismatix.com>	▭	▭	1024/2059
Philip R. Zimmermann <prz@acm.org>	▭	▭	1024

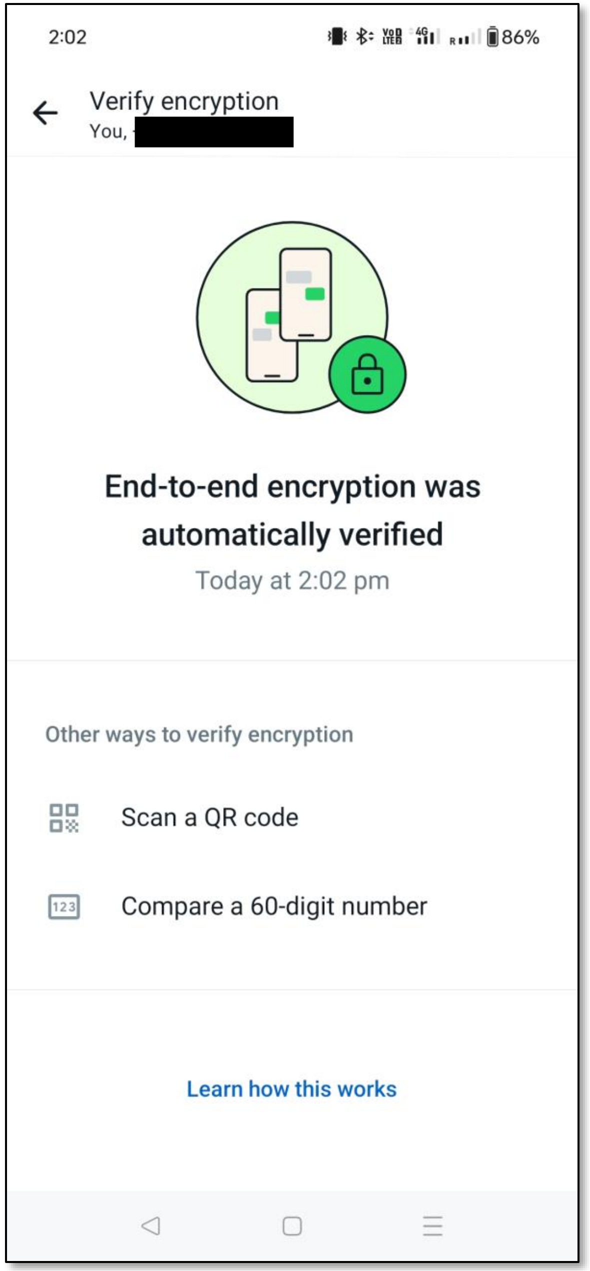
Options

□ Text Output □ Force MacBinary

"SECURE" MESSAGING

WhatsApp

- All messages, including group chats, are end-to-end encrypted
- The “ends” are the WhatsApp app on both devices
- Keys are managed by WhatsApp itself and shared with the devices as needed



Verify encryption

You, [redacted]

End-to-end encryption was automatically verified

Today at 2:02 pm

Other ways to verify encryption

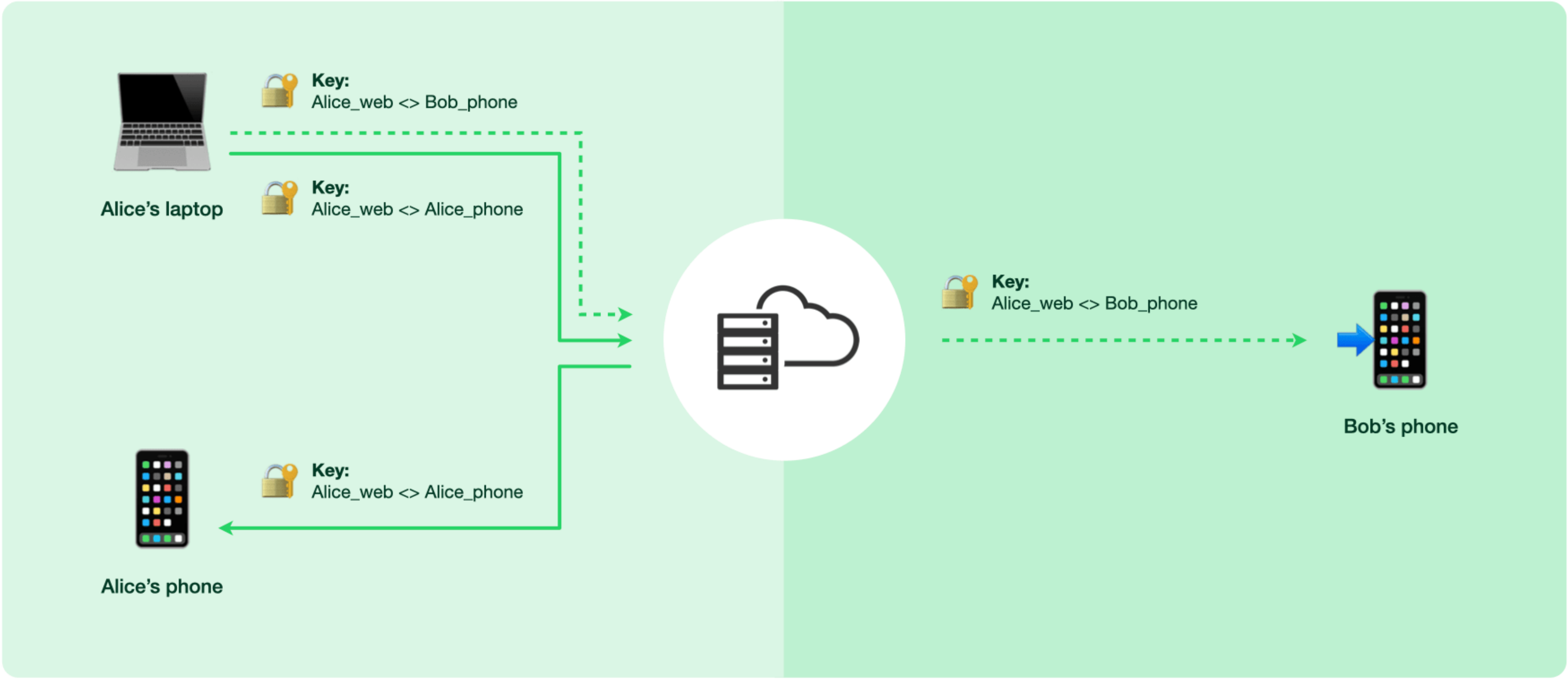
Scan a QR code

Compare a 60-digit number

Learn how this works

WhatsApp: syncing chats

Life of a message: Multi-Device (new)

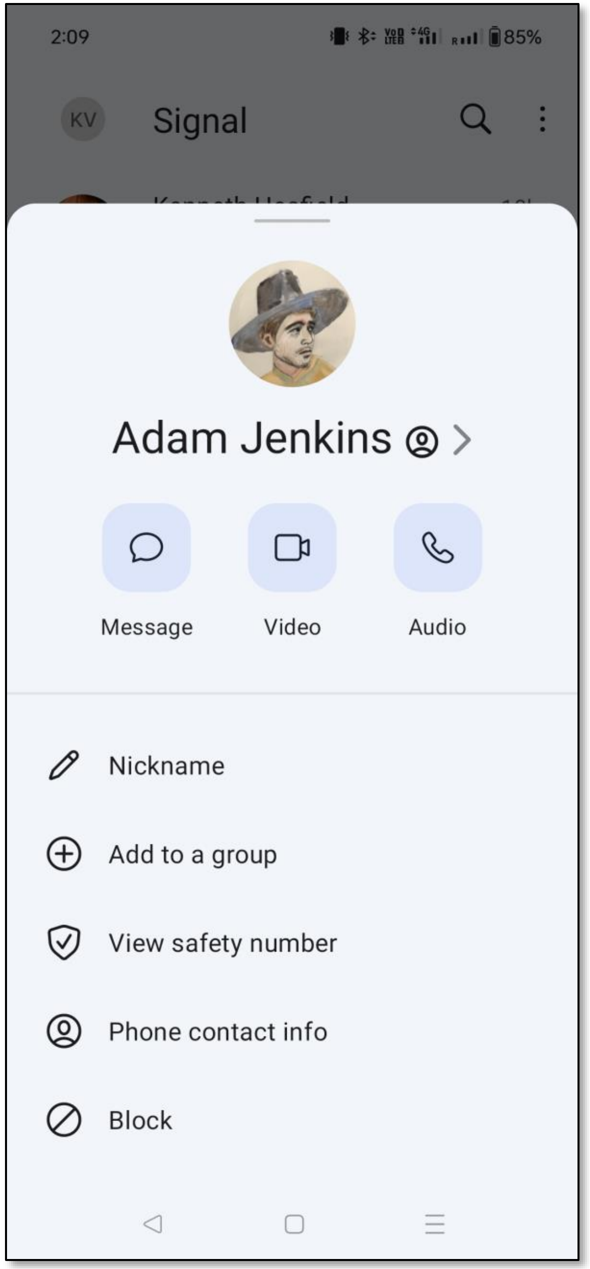


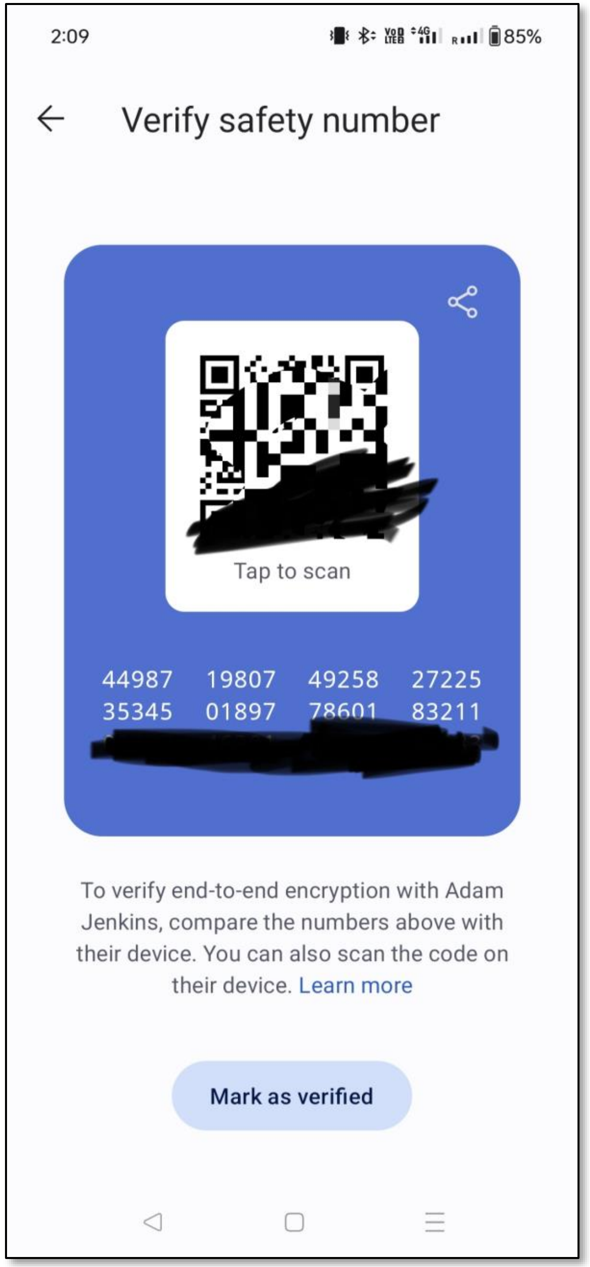
→ - - → End-to-end encrypted channels

https://engineering.fb.com/2021/07/14/security/whatsapp-multi-device/

Signal

- End to end encrypted
- The “ends” are the apps on both sides





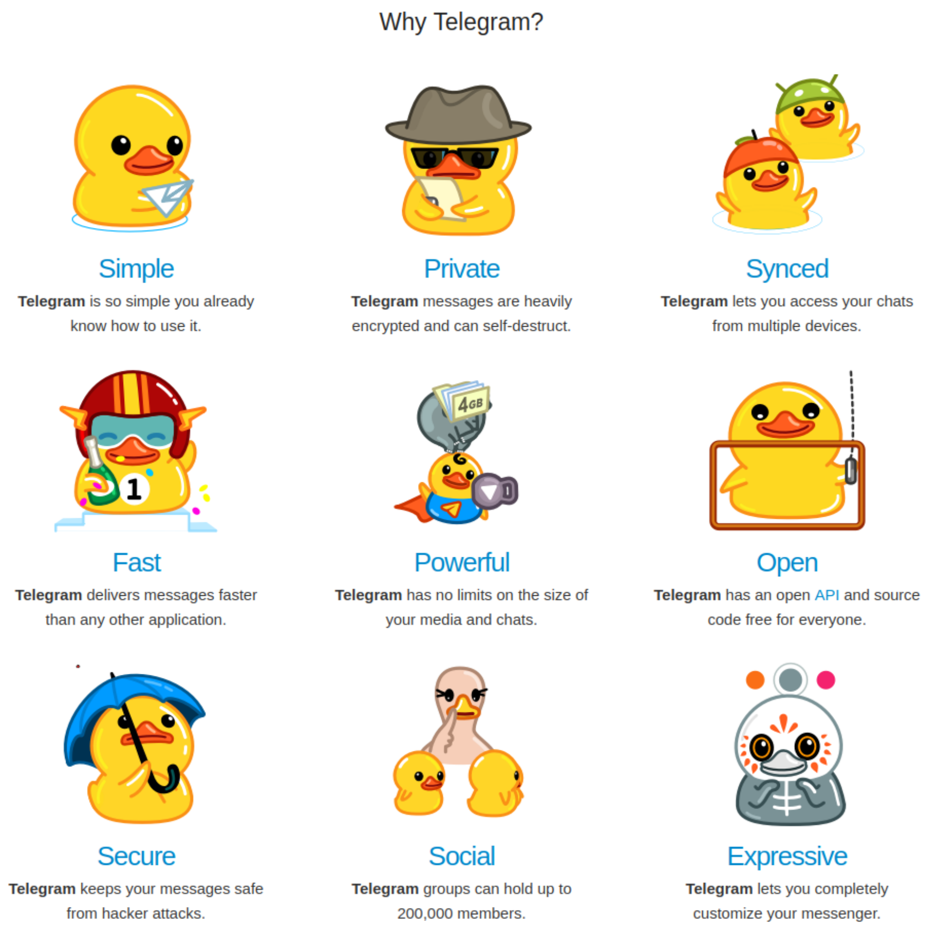
[redacted]

44987 19807 49258 27225
35345 01897 78601 83211
[redacted]

To verify end-to-end encryption with Adam Jenkins, compare the numbers above with their device. You can also scan the code on their device. Learn more

Telegram

- Only Secret chats are end-to-end encrypted
- Secret chats are more restricted than other messaging tools
- Video and audio calls are end-to-end encrypted



Why Telegram?

Simple

Telegram is so simple you already know how to use it.

Private

Telegram messages are heavily encrypted and can self-destruct.

Synced

Telegram lets you access your chats from multiple devices.

Fast

Telegram delivers messages faster than any other application.

Powerful

Telegram has no limits on the size of your media and chats.

Open

Telegram has an open API and source code free for everyone.

Secure

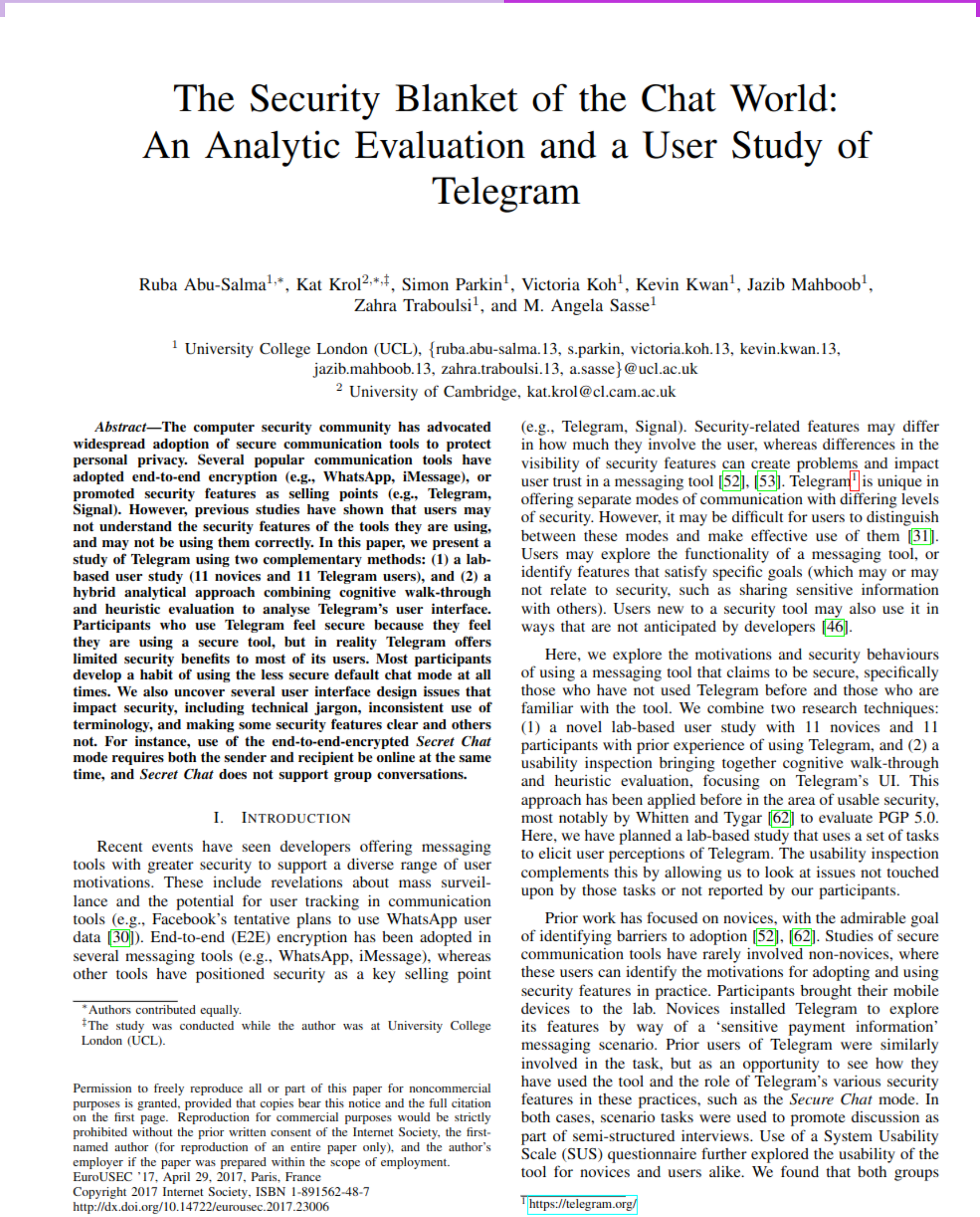
Telegram keeps your messages safe from hacker attacks.

Social

Telegram groups can hold up to 200,000 members.

Expressive

Telegram lets you completely customize your messenger.



The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram

Ruba Abu-Salma[1,*], Kat Krol[2,*,‡], Simon Parkin[1], Victoria Koh[1], Kevin Kwan[1], Jazib Mahboob[1], Zahra Traboulsi[1], and M. Angela Sasse[1]

[1] University College London (UCL), {ruba.abu-salma.13, s.parkin, victoria.koh.13, kevin.kwan.13, jazib.mahboob.13, zahra.traboulsi.13, a.sasse}@ucl.ac.uk

[2] University of Cambridge, kat.krol@cl.cam.ac.uk

***Abstract*—The computer security community has advocated widespread adoption of secure communication tools to protect personal privacy. Several popular communication tools have adopted end-to-end encryption (e.g., WhatsApp, iMessage), or promoted security features as selling points (e.g., Telegram, Signal). However, previous studies have shown that users may not understand the security features of the tools they are using, and may not be using them correctly. In this paper, we present a study of Telegram using two complementary methods: (1) a lab-based user study (11 novices and 11 Telegram users), and (2) a hybrid analytical approach combining cognitive walk-through and heuristic evaluation to analyse Telegram's user interface. Participants who use Telegram feel secure because they feel they are using a secure tool, but in reality Telegram offers limited security benefits to most of its users. Most participants develop a habit of using the less secure default chat mode at all times. We also uncover several user interface design issues that impact security, including technical jargon, inconsistent use of terminology, and making some security features clear and others not. For instance, use of the end-to-end-encrypted *Secret Chat* mode requires both the sender and recipient be online at the same time, and *Secret Chat* does not support group conversations.**

I. Introduction

Recent events have seen developers offering messaging tools with greater security to support a diverse range of user motivations. These include revelations about mass surveillance and the potential for user tracking in communication tools (e.g., Facebook's tentative plans to use WhatsApp user data [30]). End-to-end (E2E) encryption has been adopted in several messaging tools (e.g., WhatsApp, iMessage), whereas other tools have positioned security as a key selling point (e.g., Telegram, Signal). Security-related features may differ in how much they involve the user, whereas differences in the visibility of security features can create problems and impact user trust in a messaging tool [52], [53]. Telegram[1] is unique in offering separate modes of communication with differing levels of security. However, it may be difficult for users to distinguish between these modes and make effective use of them [31]. Users may explore the functionality of a messaging tool, or identify features that satisfy specific goals (which may or may not relate to security, such as sharing sensitive information with others). Users new to a security tool may also use it in ways that are not anticipated by developers [46].

Here, we explore the motivations and security behaviours of using a messaging tool that claims to be secure, specifically those who have not used Telegram before and those who are familiar with the tool. We combine two research techniques: (1) a novel lab-based user study with 11 novices and 11 participants with prior experience of using Telegram, and (2) a usability inspection bringing together cognitive walk-through and heuristic evaluation, focusing on Telegram's UI. This approach has been applied before in the area of usable security, most notably by Whitten and Tygar [62] to evaluate PGP 5.0. Here, we have planned a lab-based study that uses a set of tasks to elicit user perceptions of Telegram. The usability inspection complements this by allowing us to look at issues not touched upon by those tasks or not reported by our participants.

Prior work has focused on novices, with the admirable goal of identifying barriers to adoption [52], [62]. Studies of secure communication tools have rarely involved non-novices, where these users can identify the motivations for adopting and using security features in practice. Participants brought their mobile devices to the lab. Novices installed Telegram to explore its features by way of a 'sensitive payment information' messaging scenario. Prior users of Telegram were similarly involved in the task, but as an opportunity to see how they have used the tool and the role of Telegram's various security features in these practices, such as the *Secure Chat* mode. In both cases, scenario tasks were used to promote discussion as part of semi-structured interviews. Use of a System Usability Scale (SUS) questionnaire further explored the usability of the tool for novices and users alike. We found that both groups

[*] Authors contributed equally.

[‡] The study was conducted while the author was at University College London (UCL).

[1] https://telegram.org/

EuroUSEC '17, April 29, 2017, Paris, France
Copyright 2017 Internet Society, ISBN 1-891562-48-7
http://dx.doi.org/10.14722/eurousec.2017.23006

When asked about encryption, six participants (three novices and three users) provided explanations relating to security and safety. These included *"an extra barrier of security"*, *"more time is needed to know the content of the message"*, and *"making chats safe from hacking until they get deleted from the servers."*

COGNITIVE WALKTHROUGH

Inspection techniques

- Inspection techniques are a class of methodologies where the evaluation is done by one or more experts without involving participants or potential users.
- Pros:
  - Cheaper and faster to run than studies on users.
  - Leverage the knowledge of experts.
- Cons:
  - Experts are not users and may miss issues a real user would identify.
  - Bias towards more common errors which may be less problematic.
  - Different inspection techniques define "usability" differently.
- Examples:
  - GOMES, expert interviews, body storming, heuristic evaluation, cognitive walkthrough, ergonomic analysis.

Heuristic Evaluation

- Basic idea: Have an expert evaluate an interface based on a common set of criteria (heuristics).
- Experts have a broad knowledge of human behavior as well as subject specific knowledge, so their opinion is valuable.
- Pros
  - Can be done by even a single person.
  - No ethics, recording, or other human-related problems.
  - Minimal expense to find a large number of potentially expensive problems.
- Cons
  - Experts are not the same as end users, they will miss some things.
  - Heuristics are the most common types of problems, but they do not represent all problems.

Nielsen's 10 Heuristics

"Heuristics" are simple rules that can be easily applied and are true in most situations. Using the ten heuristics to the right we can detect a large percentage of usability issues.

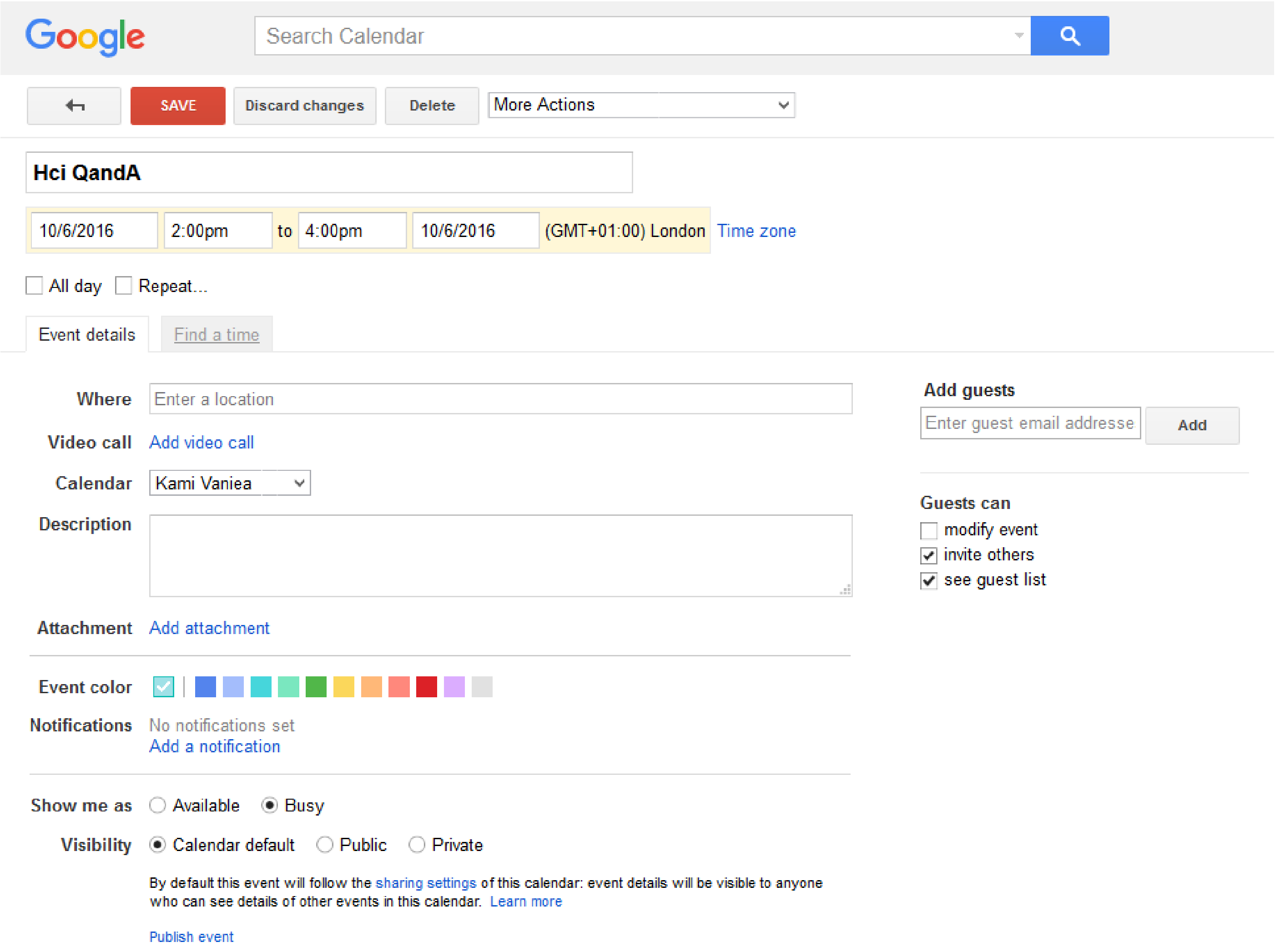
1. Visibility of system status
2. Match between system and the real world
3. User control and freedom
4. Consistency and standards
5. Error prevention
6. Recognition rather than recall
7. Flexibility and efficiency of use
8. Aesthetics and minimalist design
9. Help users recognize, diagnose, and recover from errors
10. Help and documentation

Visibility of system status

- The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
- Why
  - People learn from seeing the feedback of their actions
  - Knowledge of system state is necessary for some actions

Visibility of system status

Me adding a Q&A session to my Google calendar



Hci QandA

10/6/2016 2:00pm to 4:00pm 10/6/2016 (GMT+01:00) London

□ All day □ Repeat...

Calendar: Kami Vaniea

Notifications: No notifications set

Show me as: ○ Available ● Busy

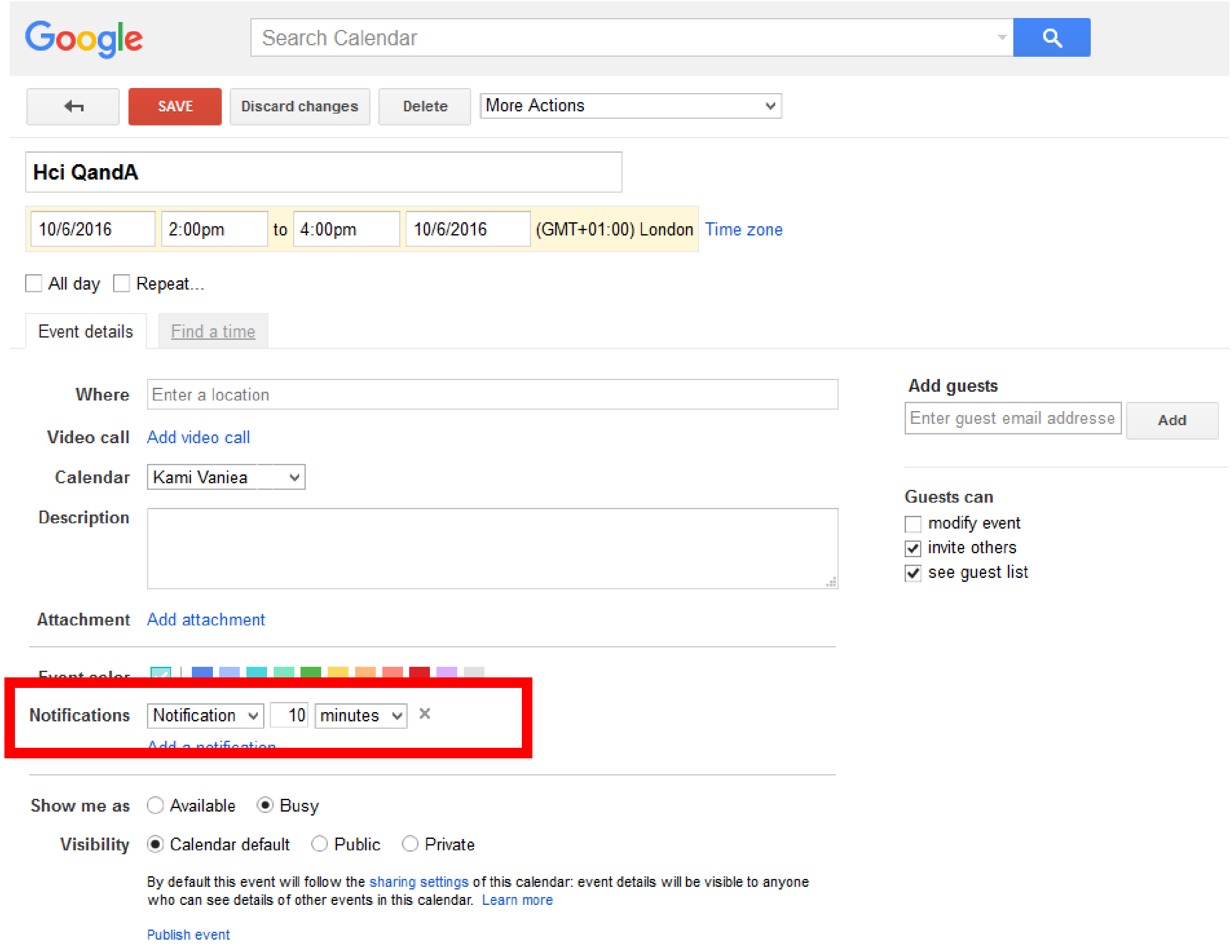
Visibility: ● Calendar default ○ Public ○ Private

By default this event will follow the sharing settings of this calendar: event details will be visible to anyone who can see details of other events in this calendar. Learn more

Guests can
□ modify event
☑ invite others
☑ see guest list

Visibility of system status

Better add a reminder or
I might forget to go



Hci QandA

10/6/2016 2:00pm to 4:00pm 10/6/2016 (GMT+01:00) London Time zone

□ All day □ Repeat...

Event details | Find a time

Where: Enter a location

Video call: Add video call

Calendar: Kami Vaniea

Description:

Attachment: Add attachment

Event color

Notifications: Notification 10 minutes ×

Add a notification

Show me as: ○ Available ● Busy

Visibility: ● Calendar default ○ Public ○ Private

By default this event will follow the sharing settings of this calendar: event details will be visible to anyone who can see details of other events in this calendar. Learn more

Publish event

Add guests

Enter guest email addresse | Add

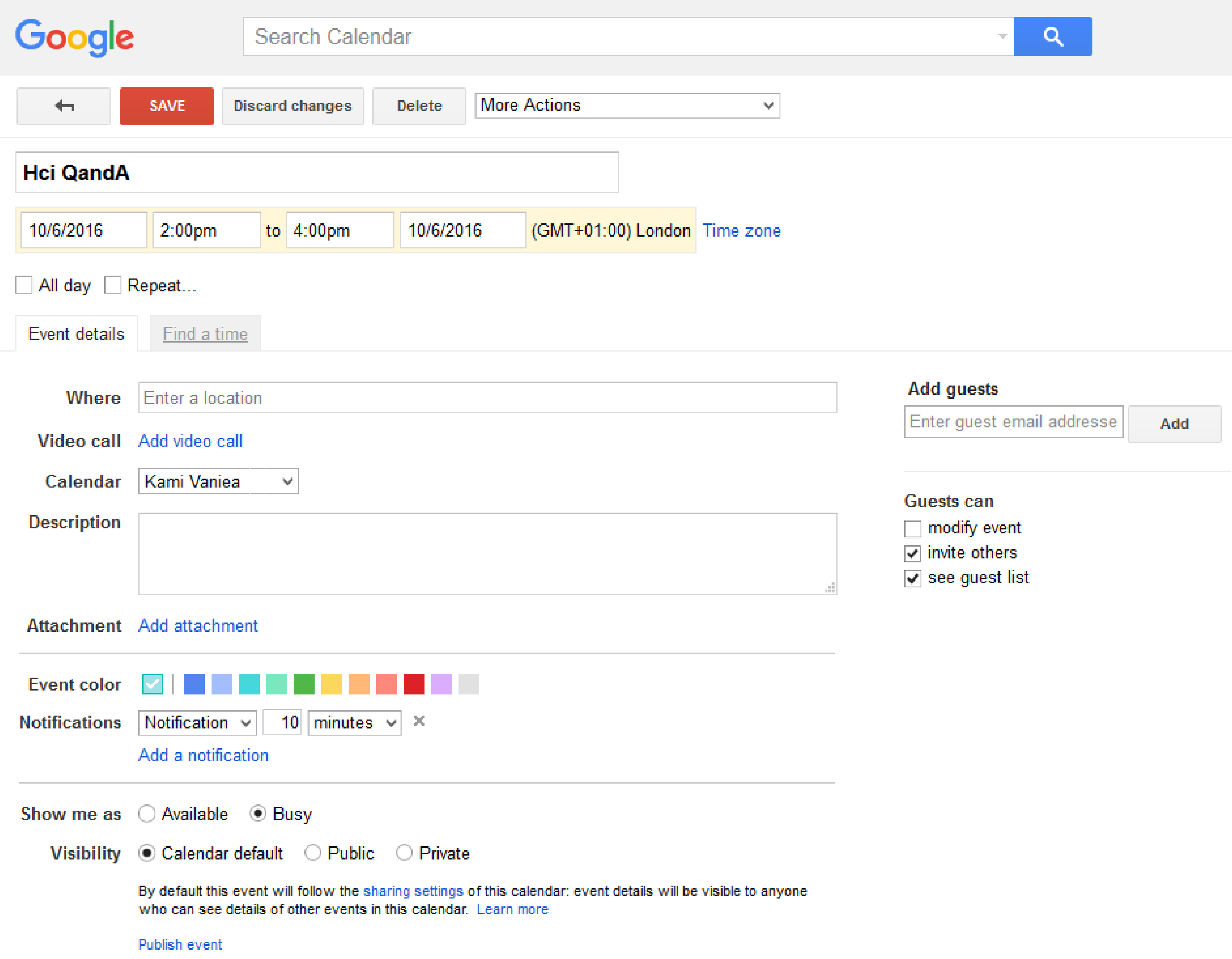
Guests can

□ modify event

☑ invite others

☑ see guest list

Is the reminder saved?



Hci QandA

10/6/2016 2:00pm to 4:00pm 10/6/2016 (GMT+01:00) London Time zone

□ All day □ Repeat...

Event details | Find a time

Where: Enter a location

Video call: Add video call

Calendar: Kami Vaniea

Description:

Attachment: Add attachment

Event color: ☑

Notifications: Notification 10 minutes ✕

Add a notification

Show me as: ○ Available ● Busy

Visibility: ● Calendar default ○ Public ○ Private

By default this event will follow the sharing settings of this calendar: event details will be visible to anyone who can see details of other events in this calendar. Learn more

Publish event

Add guests

Enter guest email addresse Add

Guests can

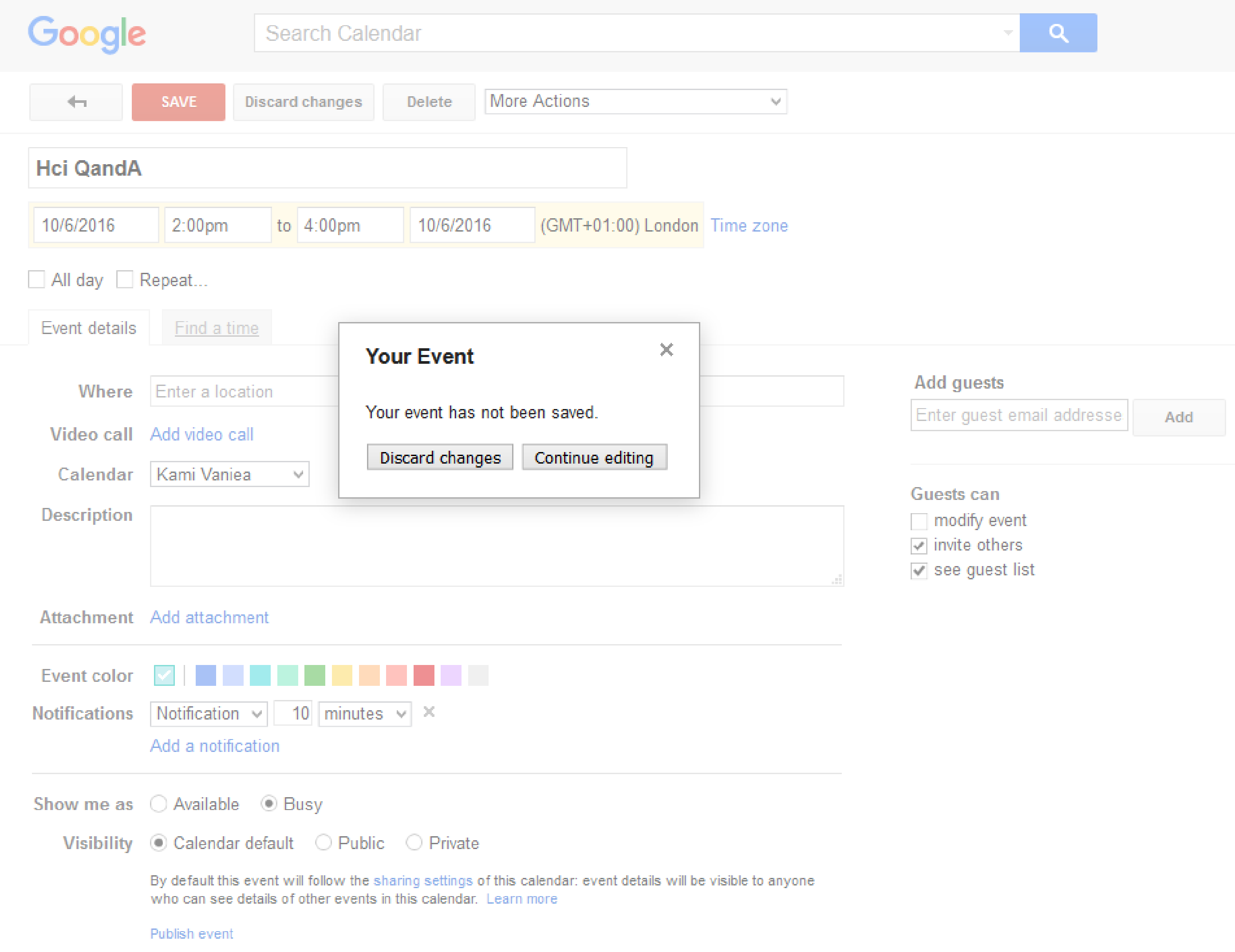
□ modify event

☑ invite others

☑ see guest list

Visibility of system status

I clicked the back button without clicking “save” and get a warning.



Hci QandA

10/6/2016 2:00pm to 4:00pm 10/6/2016 (GMT+01:00) London Time zone

□ All day □ Repeat...

Your Event

Your event has not been saved.

Where: Enter a location

Video call: Add video call

Calendar: Kami Vaniea

Description:

Attachment: Add attachment

Event color:

Notifications: Notification 10 minutes ✕

Add a notification

Show me as: ○ Available ● Busy

Visibility: ● Calendar default ○ Public ○ Private

By default this event will follow the sharing settings of this calendar: event details will be visible to anyone who can see details of other events in this calendar. Learn more

Publish event

Add guests

Enter guest email addresse

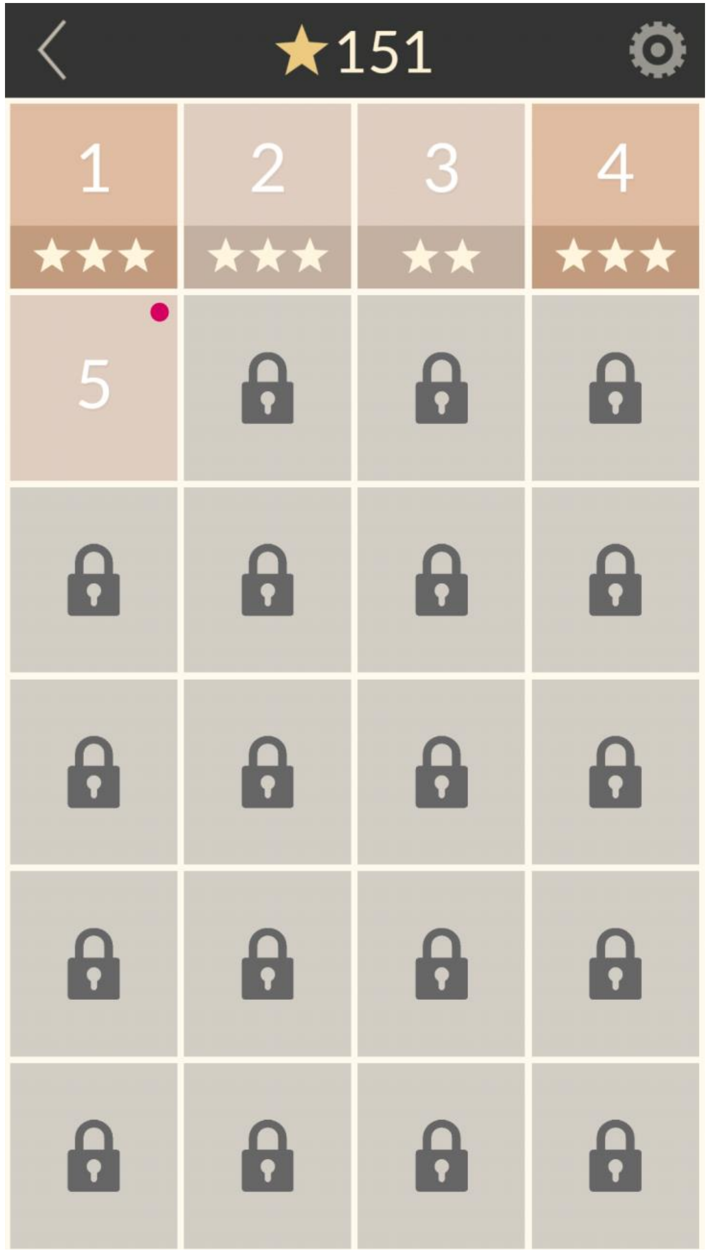
Guests can

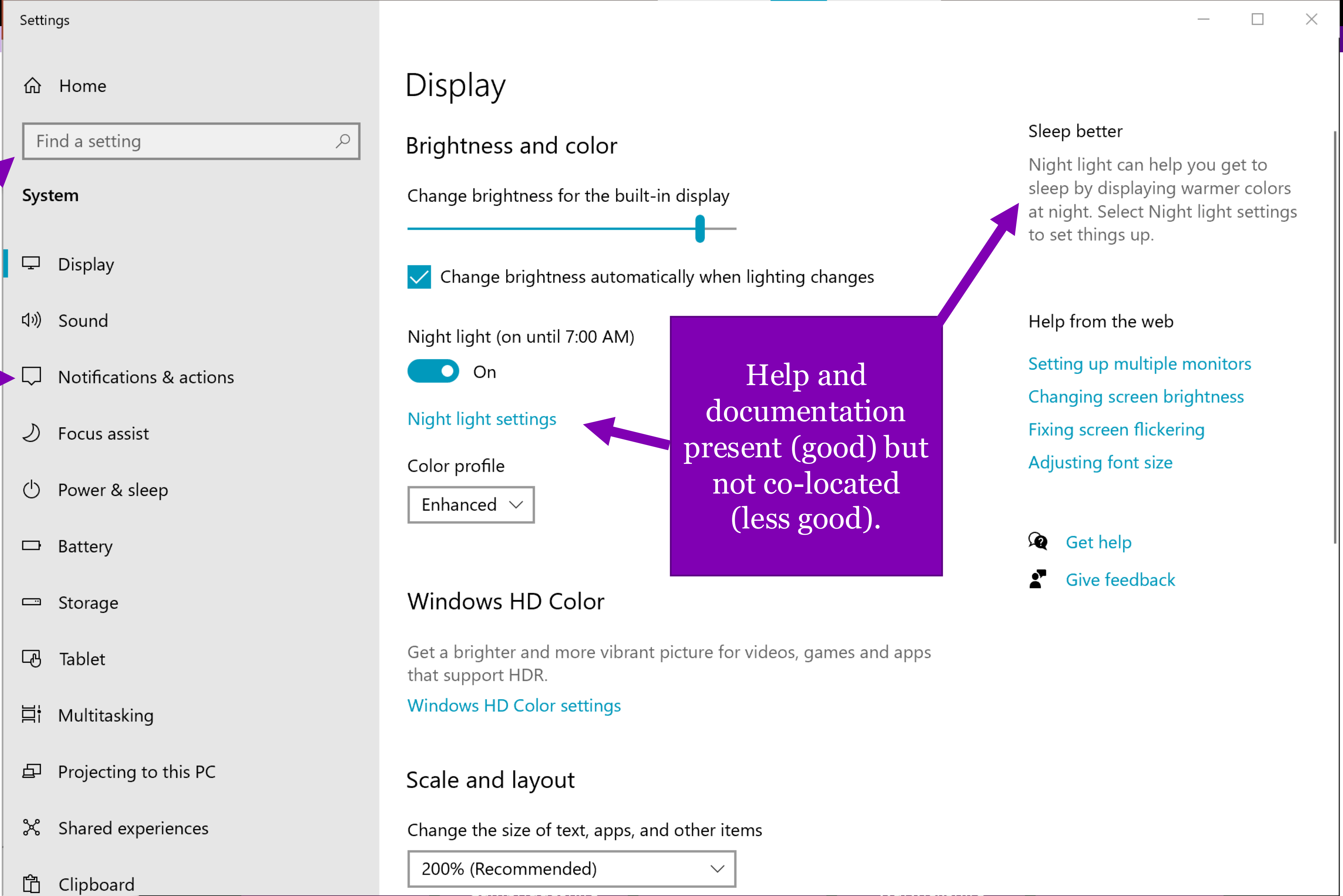
□ modify event

☑ invite others

☑ see guest list

Good example: clear which levels have been played, how they did, what level the player is currently on, and what levels are still locked.





Display

Brightness and color

Change brightness for the built-in display

☑ Change brightness automatically when lighting changes

Night light (on until 7:00 AM)

● On

Night light settings

Color profile

Enhanced

Windows HD Color

Get a brighter and more vibrant picture for videos, games and apps that support HDR.

Windows HD Color settings

Scale and layout

Change the size of text, apps, and other items

200% (Recommended)

Sleep better

Night light can help you get to sleep by displaying warmer colors at night. Select Night light settings to set things up.

Help from the web

Setting up multiple monitors

Changing screen brightness

Fixing screen flickering

Adjusting font size

Get help

Give feedback

Recall and Recognition both supported (good).

Help and documentation present (good) but not co-located (less good).

Cognitive Walkthrough

- A method that evaluates whether the order of cues and prompts in a system supports the way people process tasks and anticipate the “next steps” of a system.
- When to use it:
  - Initial evaluation of a system
  - Low budget
  - Walk-up-and-use systems or first-use situations
  - Have access to HCI experts
- When to not use it:
  - Formal evaluation of your own system with you as an evaluator.
  - Systems a user will use frequently.

Cognitive Walkthrough Process

- Briefing session to tell experts what to do.
- Evaluation period of 1-2 hours where:
  - Each expert works separately.
  - Take one pass to get a feel for the product.
  - Take a second pass to focus on specific features.
- Debrief session in which experts work together to prioritize problems.
  - Use most important problems to design a study to test if the identified problems are ones that hinder end users.
  - Write a report for the client explaining the problems found and the relative importance of each problem.

Number of evaluators & problems

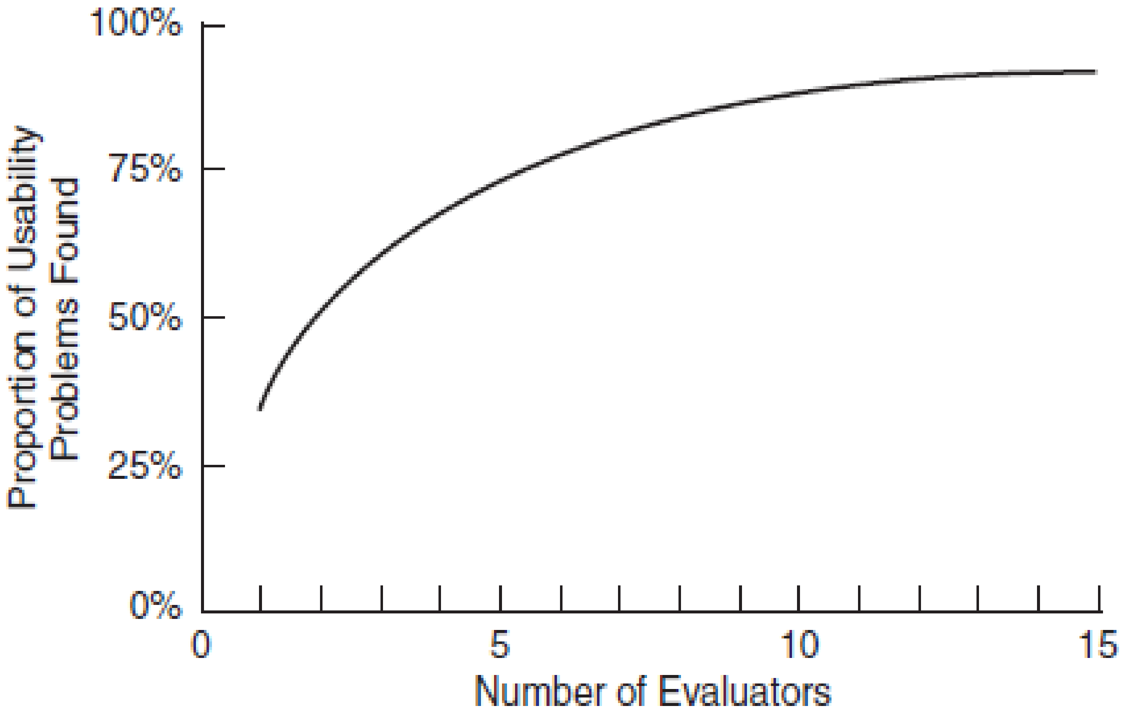


Figure 15.1 Curve showing the proportion of usability problems in an interface found by heuristic evaluation using various numbers of evaluators. The curve represents the average of six case studies of heuristic evaluation

Source: Usability Inspection Methods, J. Nielson & R.L. Mack ©1994. Reproduced with permission of John Wiley & Sons Inc.

Each evaluator:

Materials needed

- Persona
- Task persona is trying to accomplish
- List of “correct” steps
- Way to record answers to the 4 questions
- Way to record issues found
- Optionally: List of the heuristics

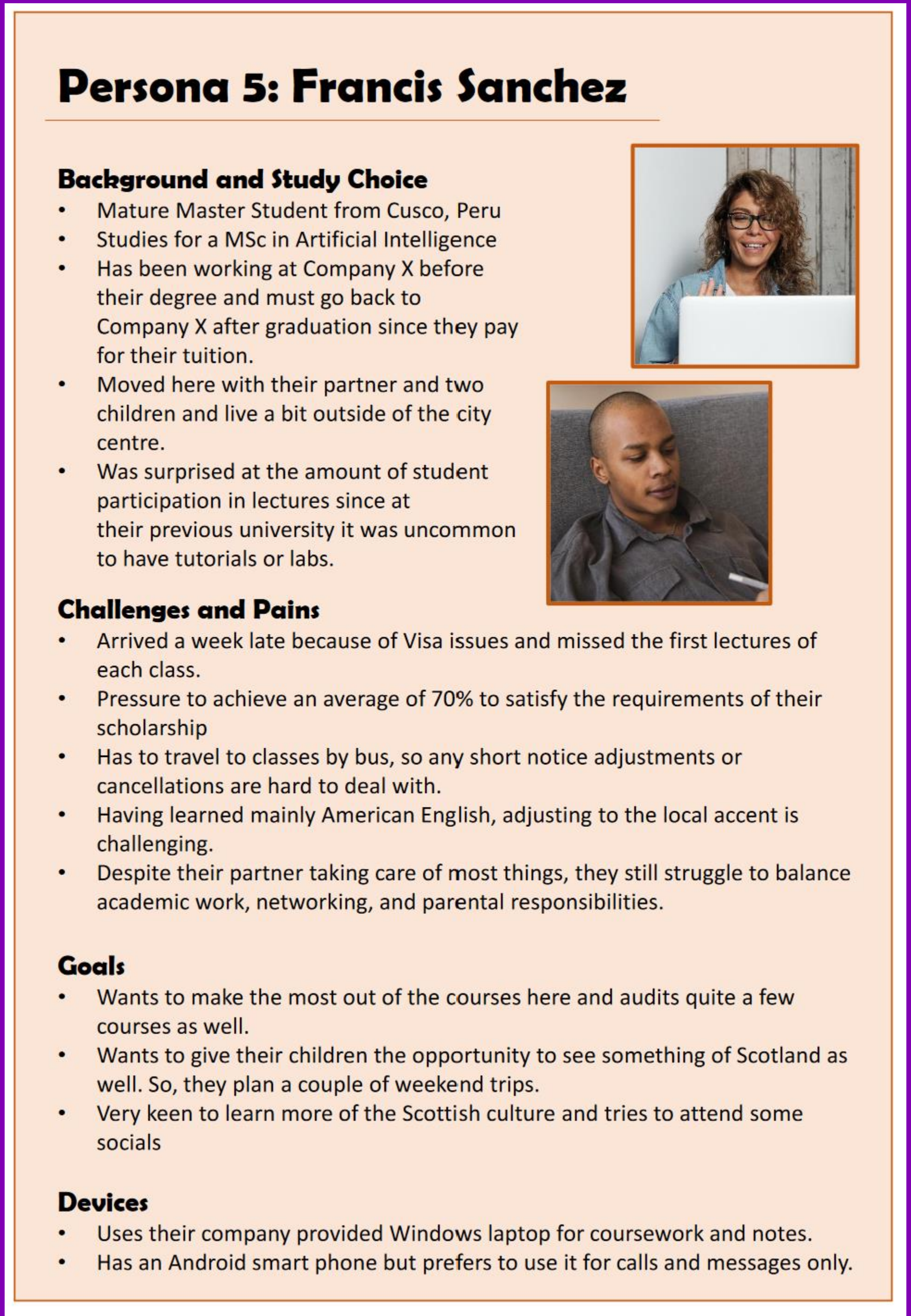
Process

- For each “correct” step:
  - Answer the four questions
  - Record any identified problems (poor aspects)
  - Record any notable good things (good aspects)
- After completing all steps, review the aspects recorded by other evaluators.
- Discuss most serious issues.

The four questions

1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

Task: Open the Tasks lecture slides in DrawboardPDF.



Persona 5: Francis Sanchez

Background and Study Choice

- Mature Master Student from Cusco, Peru
- Studies for a MSc in Artificial Intelligence
- Has been working at Company X before their degree and must go back to Company X after graduation since they pay for their tuition.
- Moved here with their partner and two children and live a bit outside of the city centre.
- Was surprised at the amount of student participation in lectures since at their previous university it was uncommon to have tutorials or labs.

Challenges and Pains

- Arrived a week late because of Visa issues and missed the first lectures of each class.
- Pressure to achieve an average of 70% to satisfy the requirements of their scholarship
- Has to travel to classes by bus, so any short notice adjustments or cancellations are hard to deal with.
- Having learned mainly American English, adjusting to the local accent is challenging.
- Despite their partner taking care of most things, they still struggle to balance academic work, networking, and parental responsibilities.

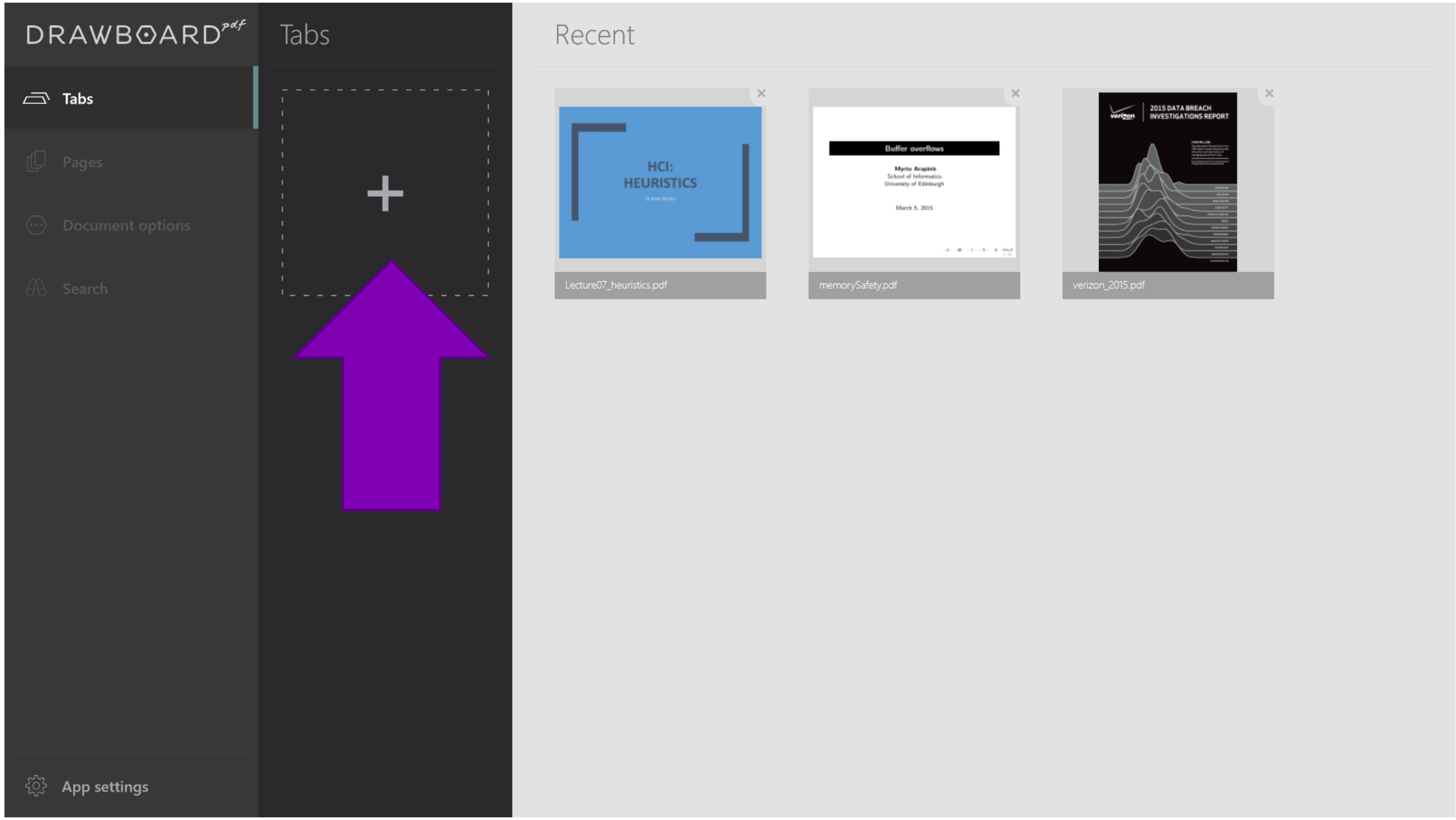
Goals

- Wants to make the most out of the courses here and audits quite a few courses as well.
- Wants to give their children the opportunity to see something of Scotland as well. So, they plan a couple of weekend trips.
- Very keen to learn more of the Scottish culture and tries to attend some socials

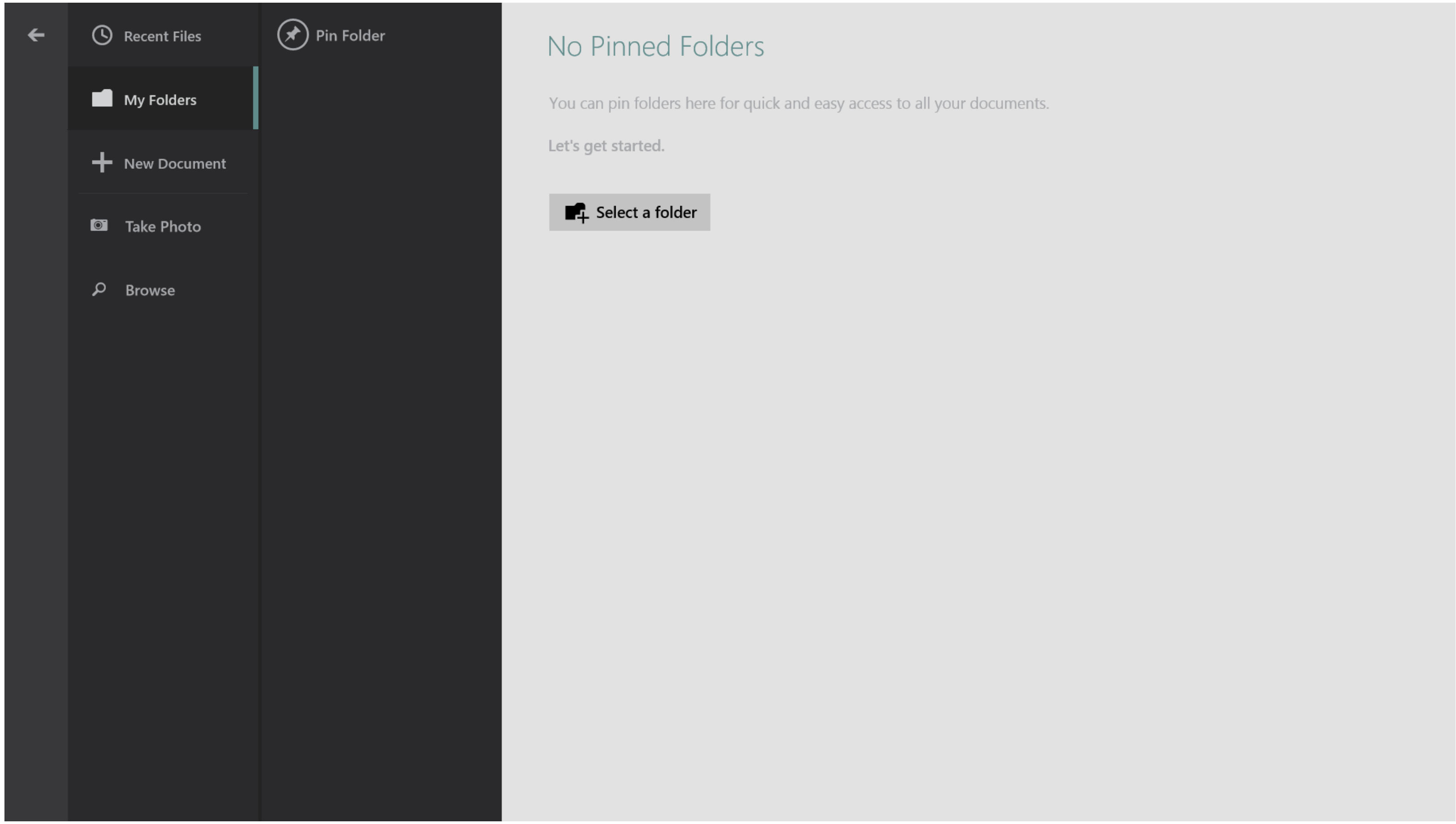
Devices

- Uses their company provided Windows laptop for coursework and notes.
- Has an Android smart phone but prefers to use it for calls and messages only.

1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?



1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

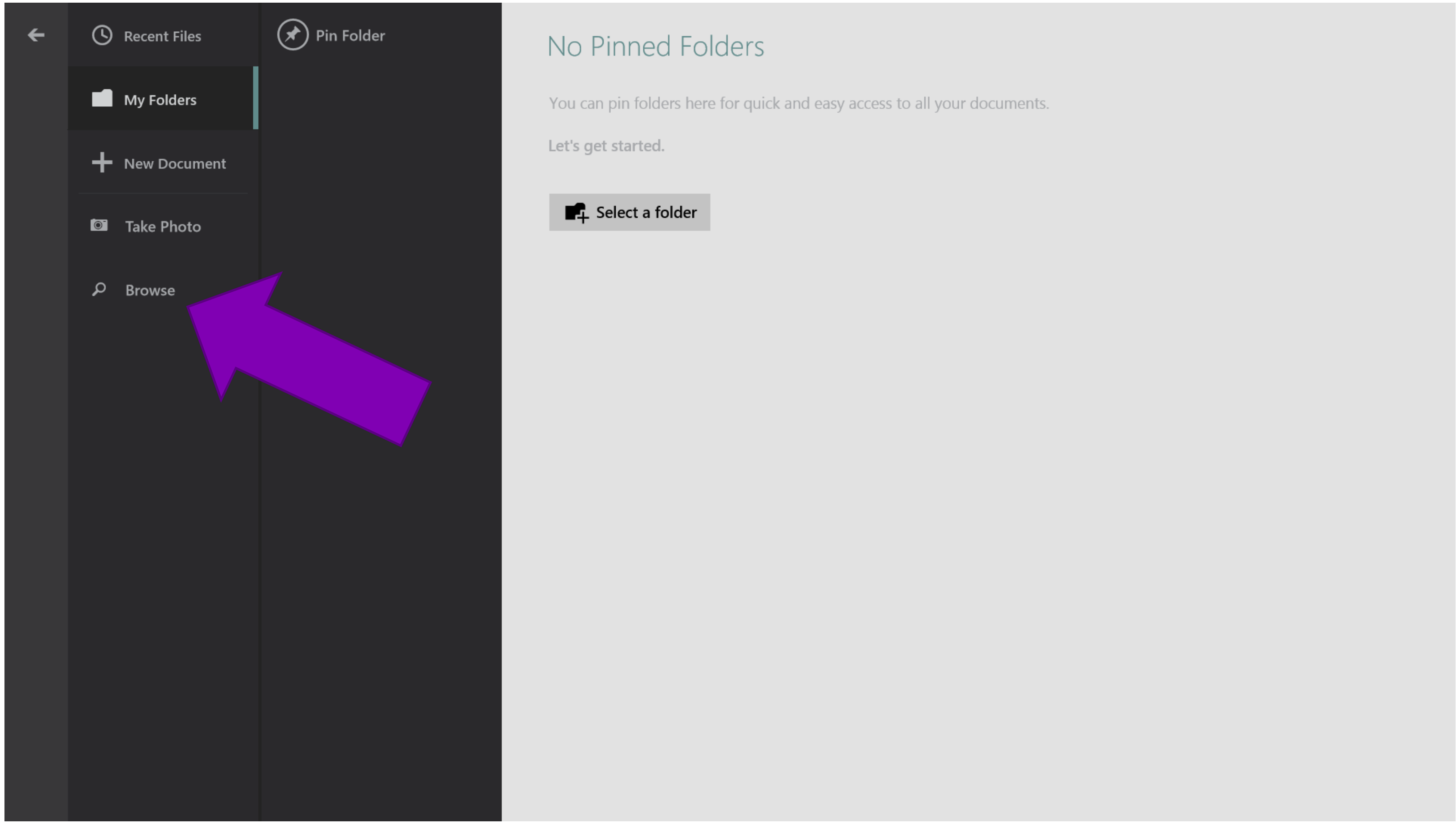


No Pinned Folders

You can pin folders here for quick and easy access to all your documents.

Let's get started.

1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

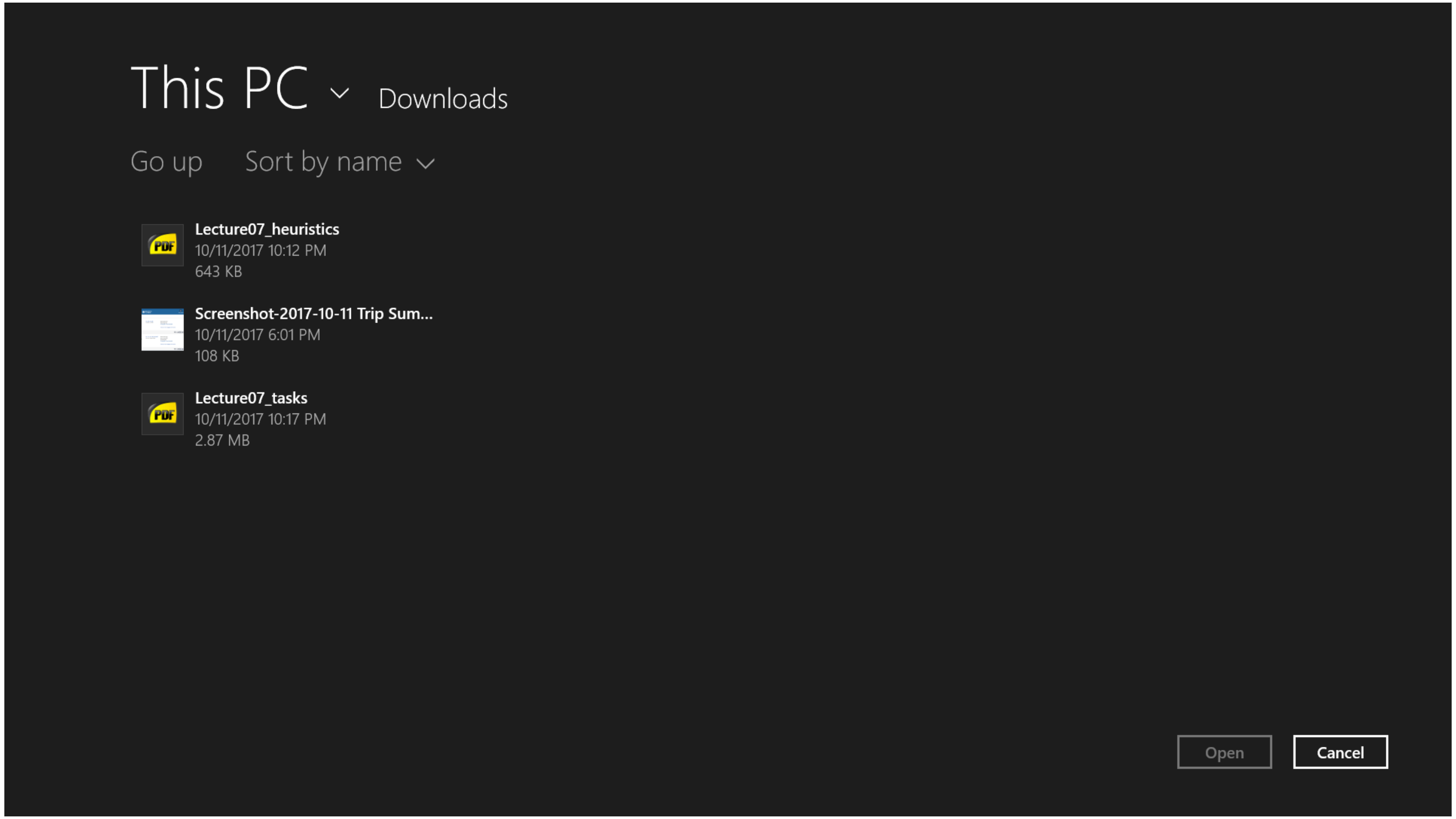


No Pinned Folders

You can pin folders here for quick and easy access to all your documents.

Let's get started.

1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?


This PC Downloads

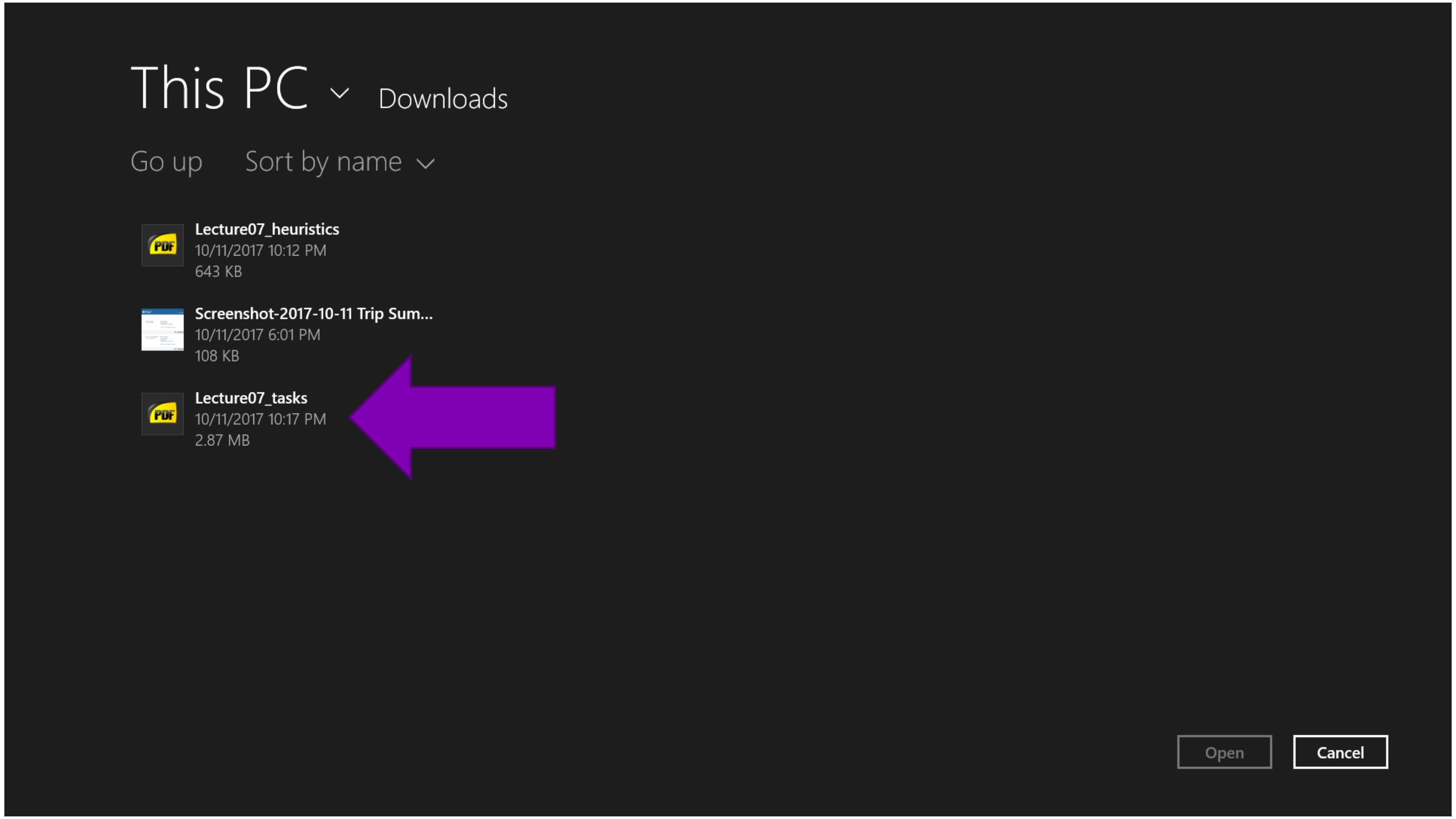
Go up Sort by name

Lecture07_heuristics
10/11/2017 10:12 PM
643 KB

Screenshot-2017-10-11 Trip Sum...
10/11/2017 6:01 PM
108 KB

Lecture07_tasks
10/11/2017 10:17 PM
2.87 MB

1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

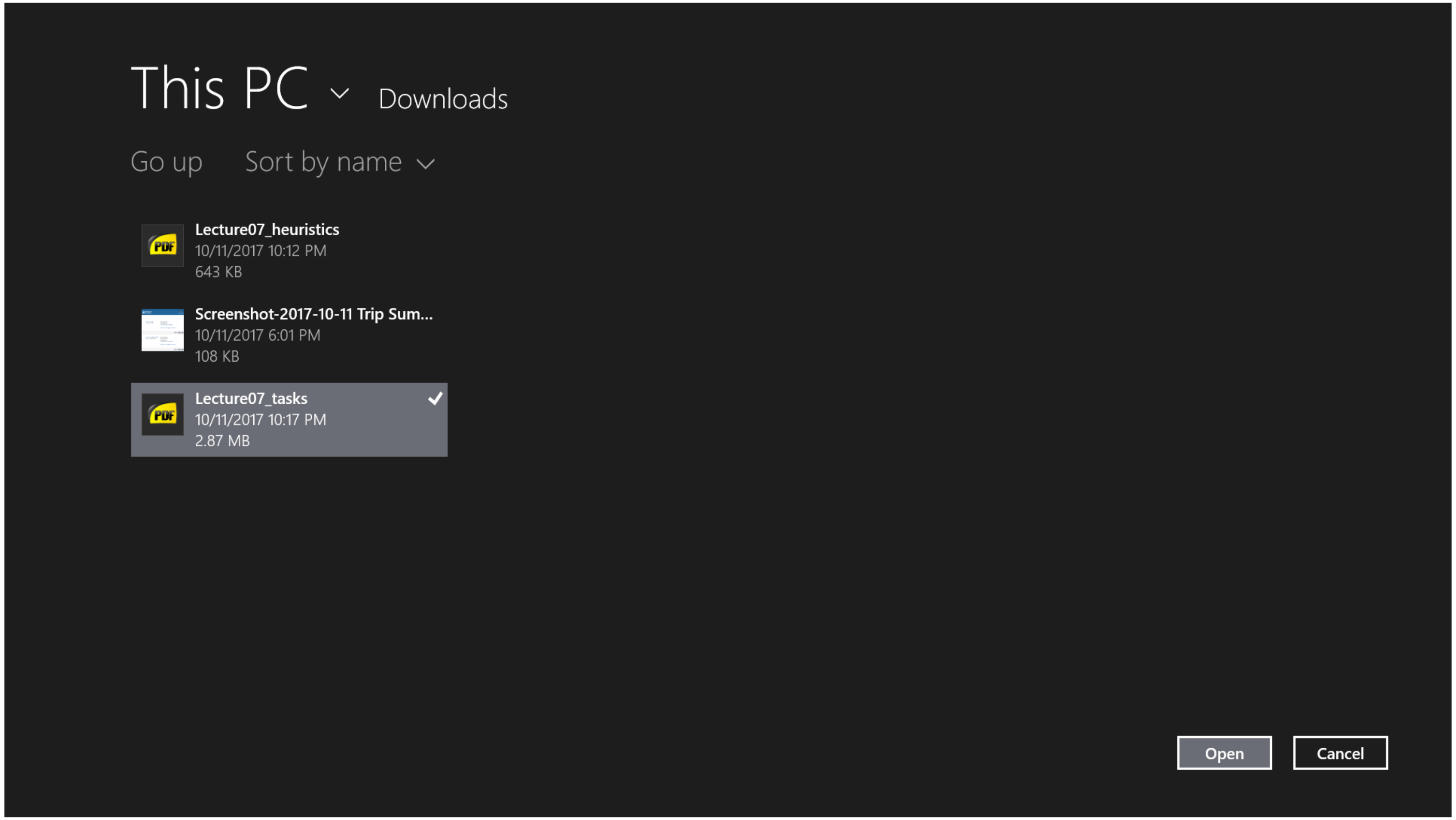


Lecture07_heuristics
10/11/2017 10:12 PM
643 KB

Screenshot-2017-10-11 Trip Sum...
10/11/2017 6:01 PM
108 KB

Lecture07_tasks
10/11/2017 10:17 PM
2.87 MB

1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

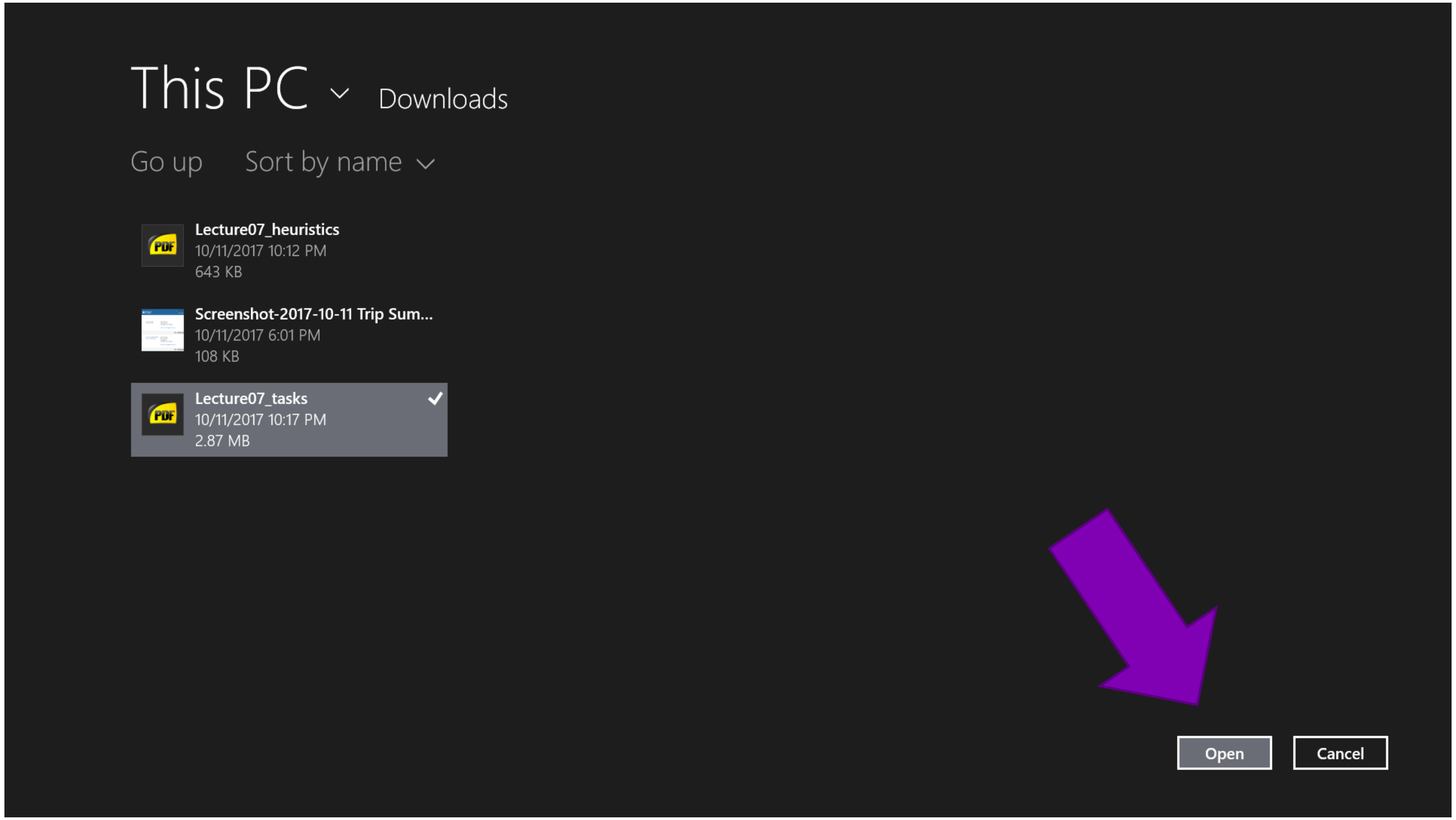


Lecture07_heuristics
10/11/2017 10:12 PM
643 KB

Screenshot-2017-10-11 Trip Sum...
10/11/2017 6:01 PM
108 KB

Lecture07_tasks ✓
10/11/2017 10:17 PM
2.87 MB

1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

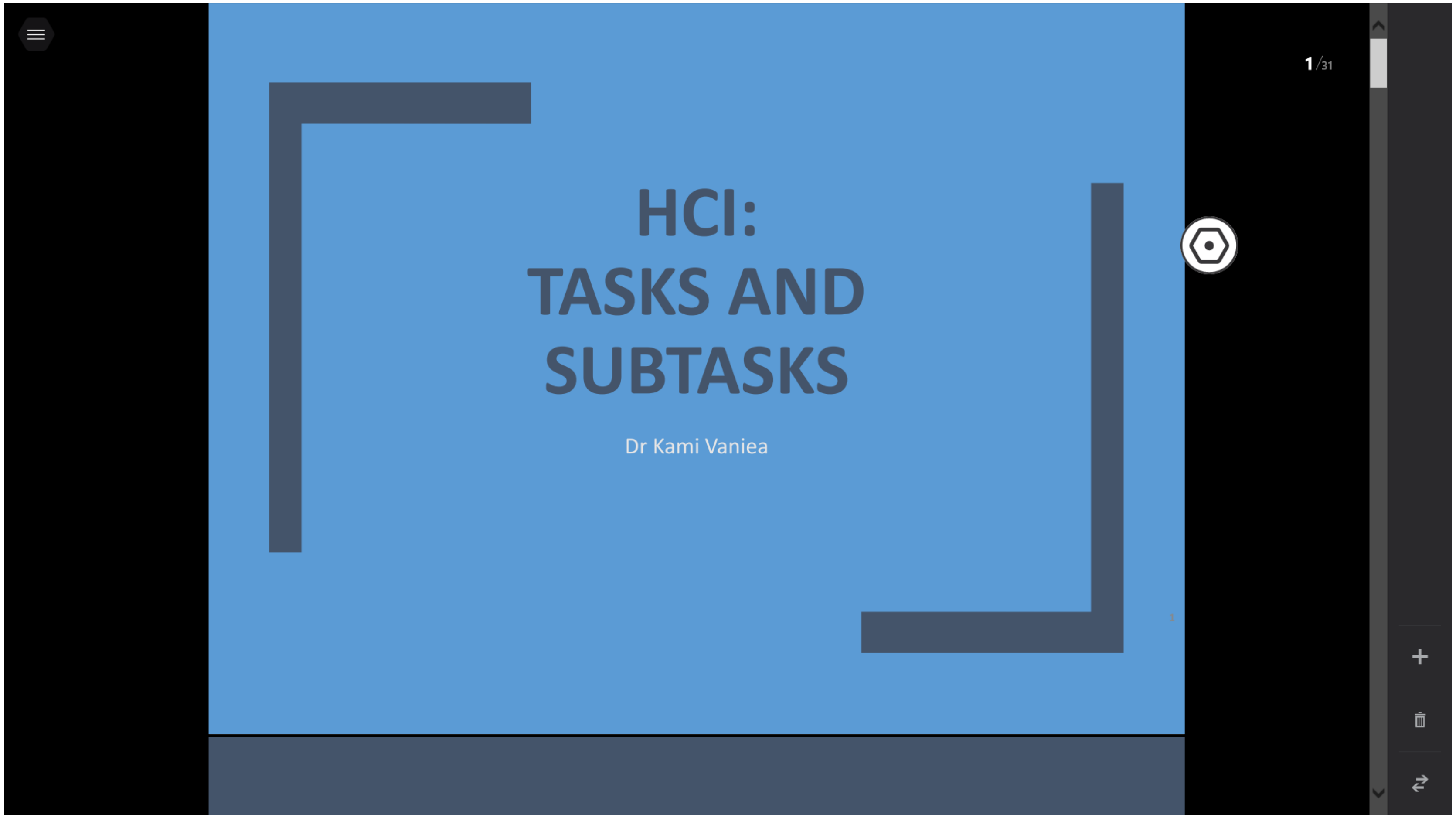


Lecture07_heuristics
10/11/2017 10:12 PM
643 KB

Screenshot-2017-10-11 Trip Sum...
10/11/2017 6:01 PM
108 KB

Lecture07_tasks ✓
10/11/2017 10:17 PM
2.87 MB

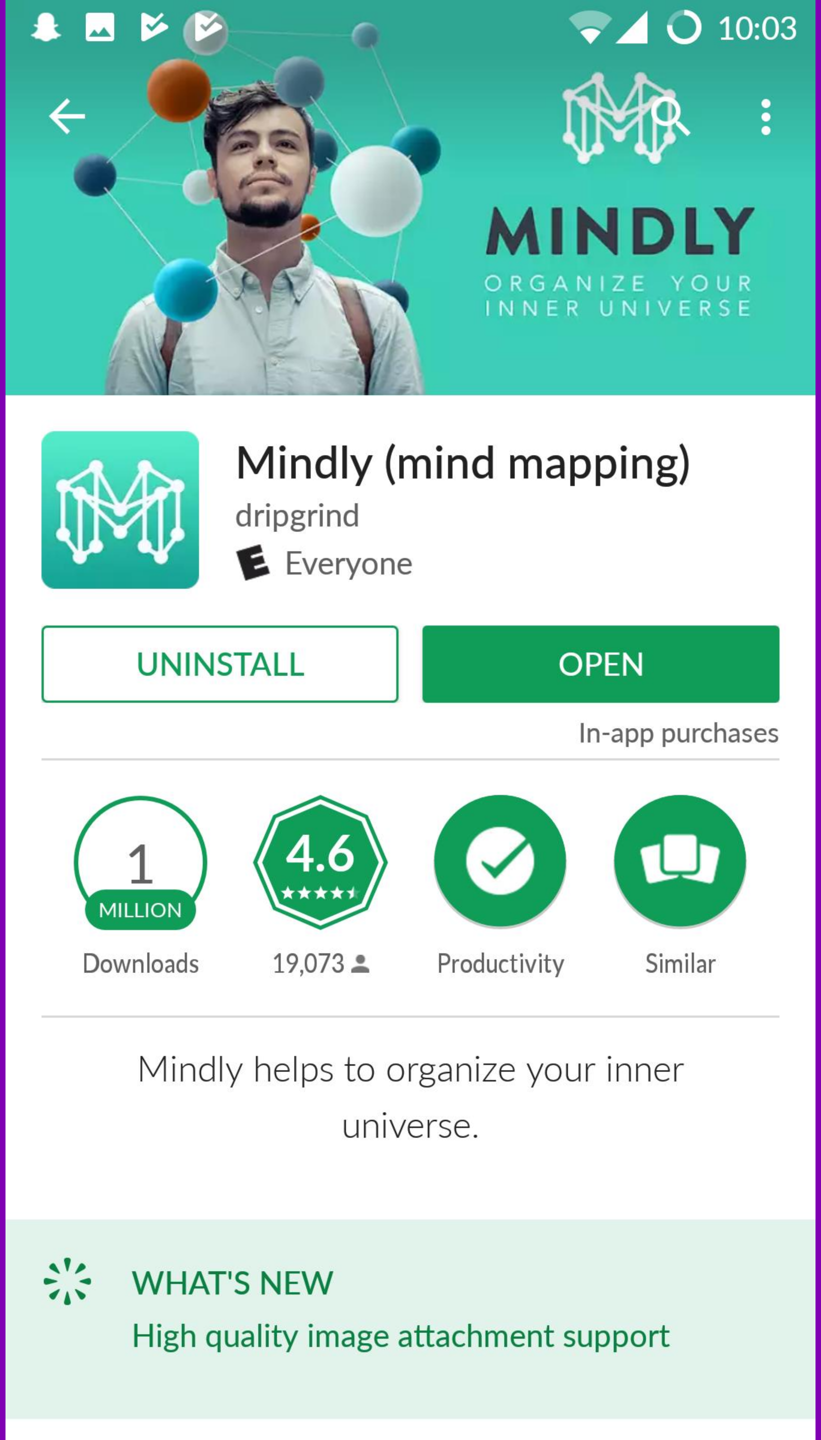
1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?



HCI:
TASKS AND SUBTASKS

Dr Kami Vaniea

Task: Delete a node from a mindmap



10:03

MINDLY

ORGANIZE YOUR INNER UNIVERSE

Mindly (mind mapping)

dripgrind

Everyone

In-app purchases

1 MILLION	4.6 ★★★★★		
Downloads	19,073	Productivity	Similar

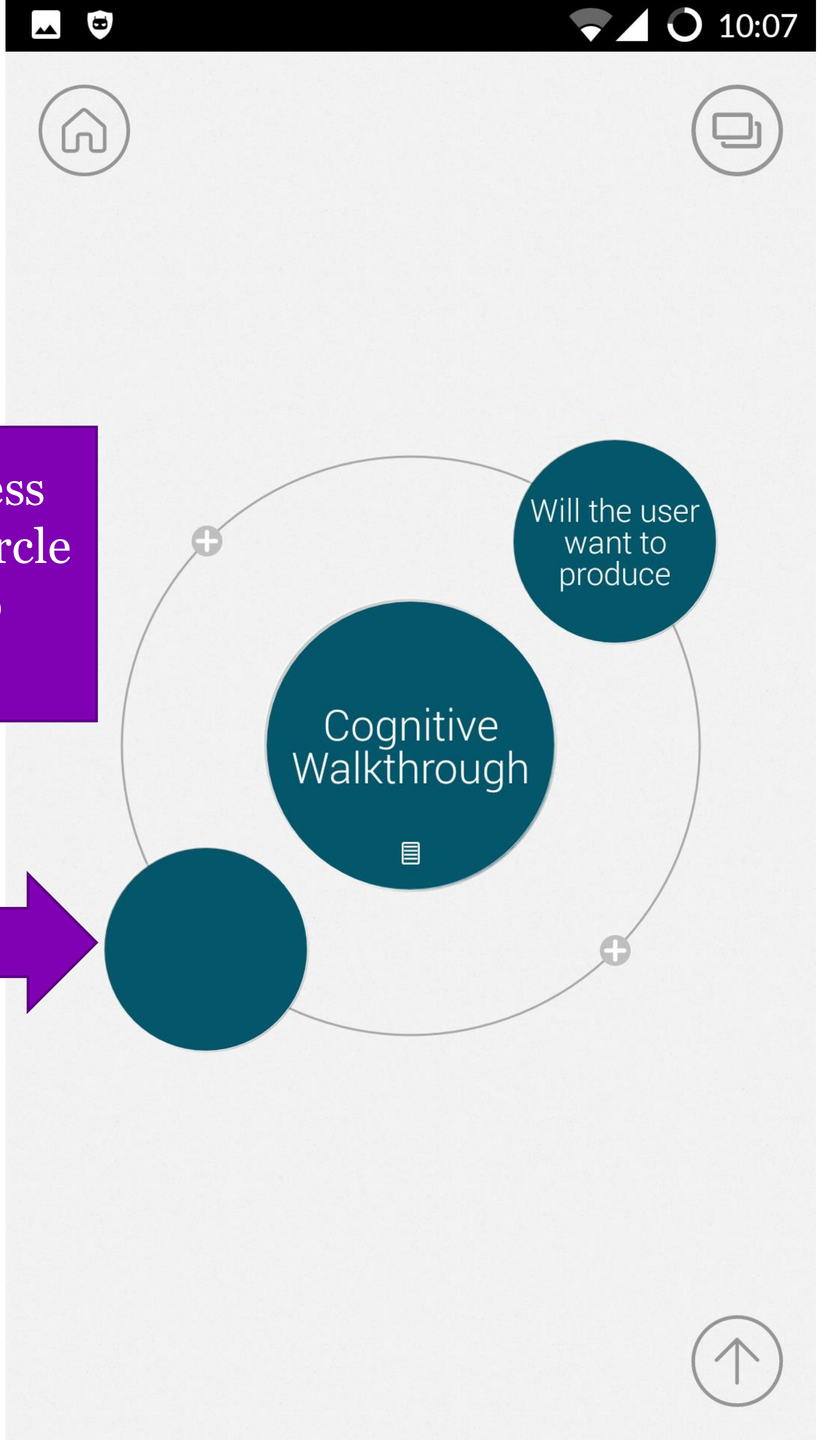
Mindly helps to organize your inner universe.

WHAT'S NEW

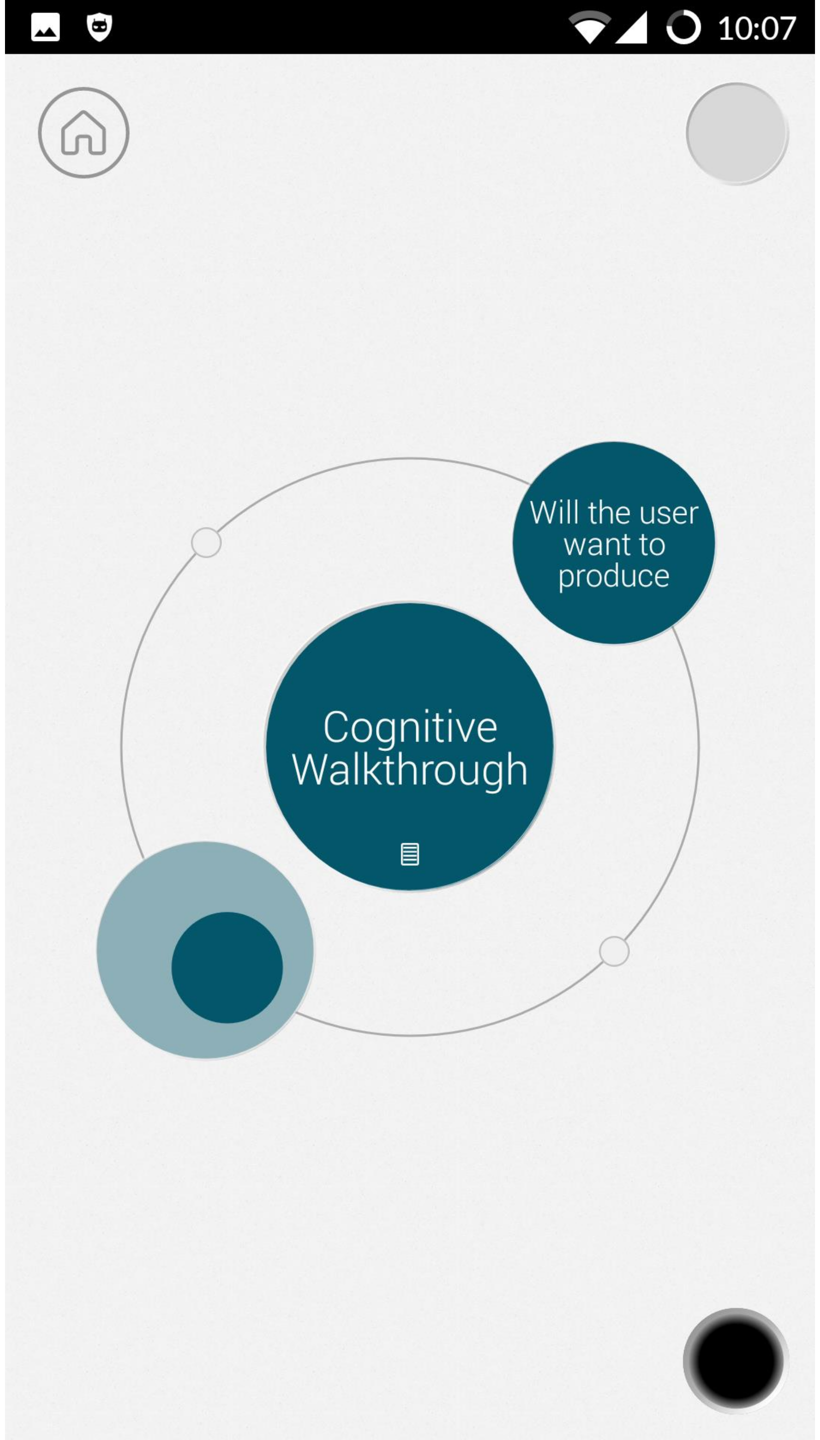
High quality image attachment support

1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

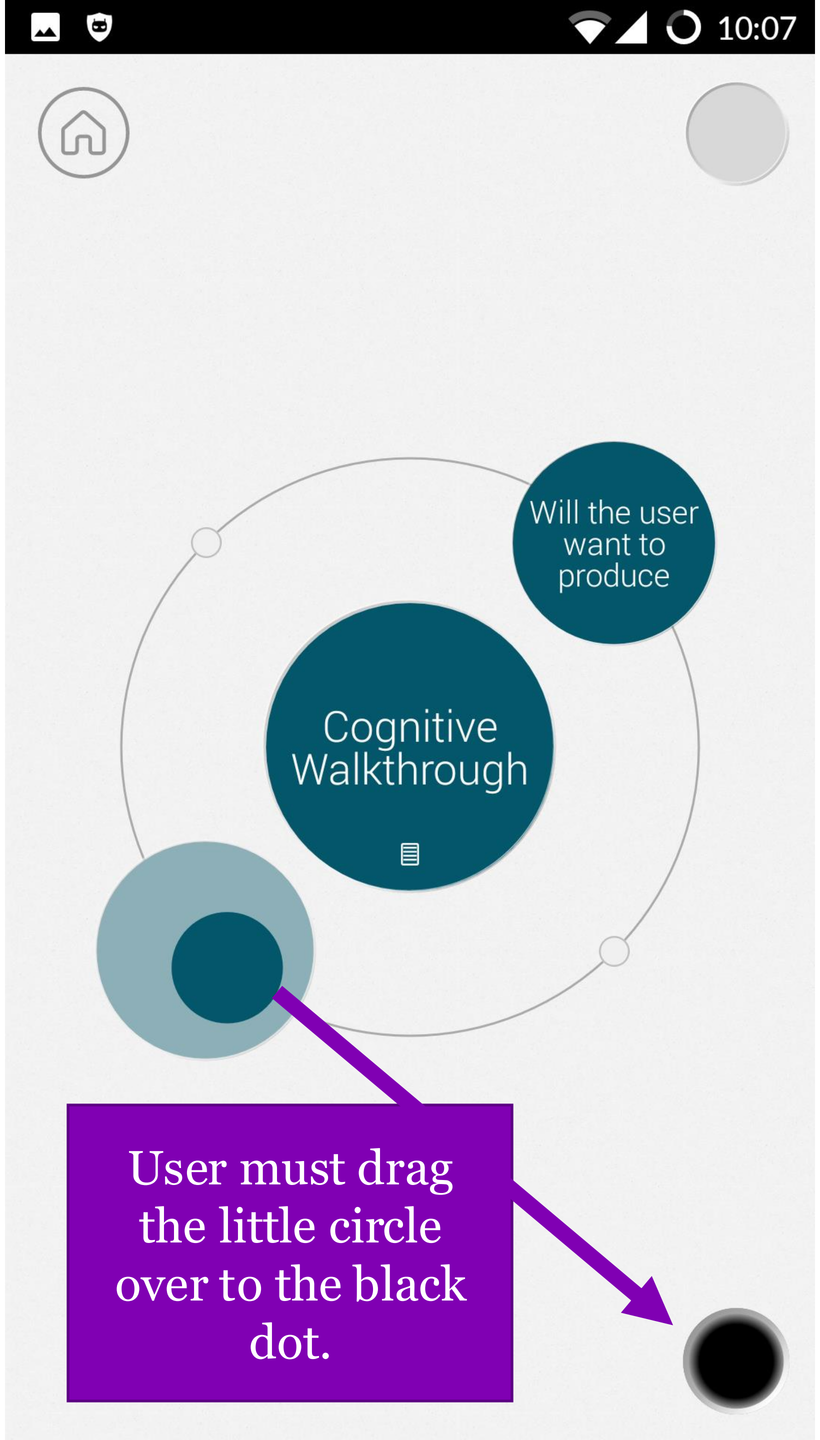
User must press and hold the circle they wish to delete.



1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

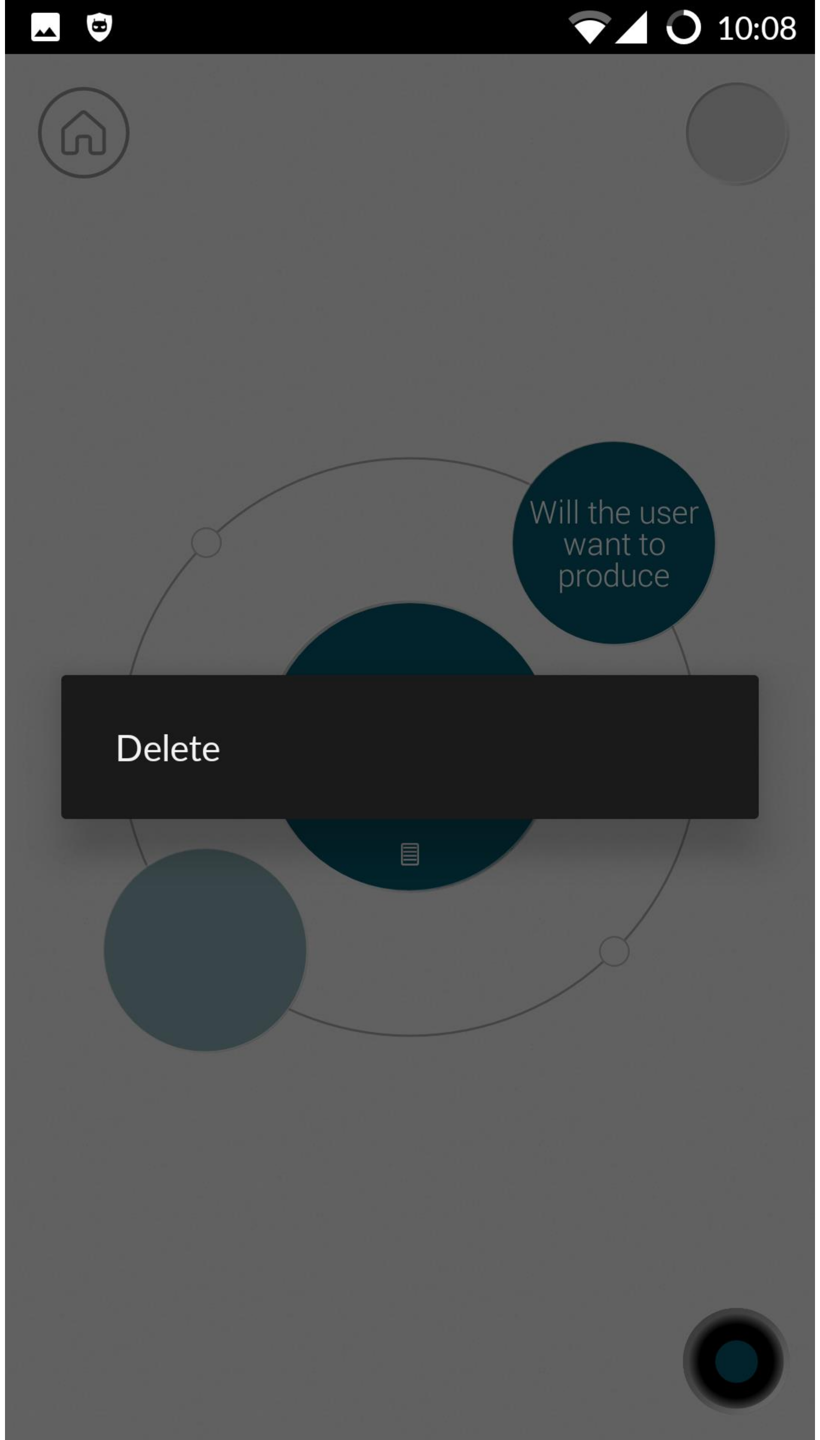


1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

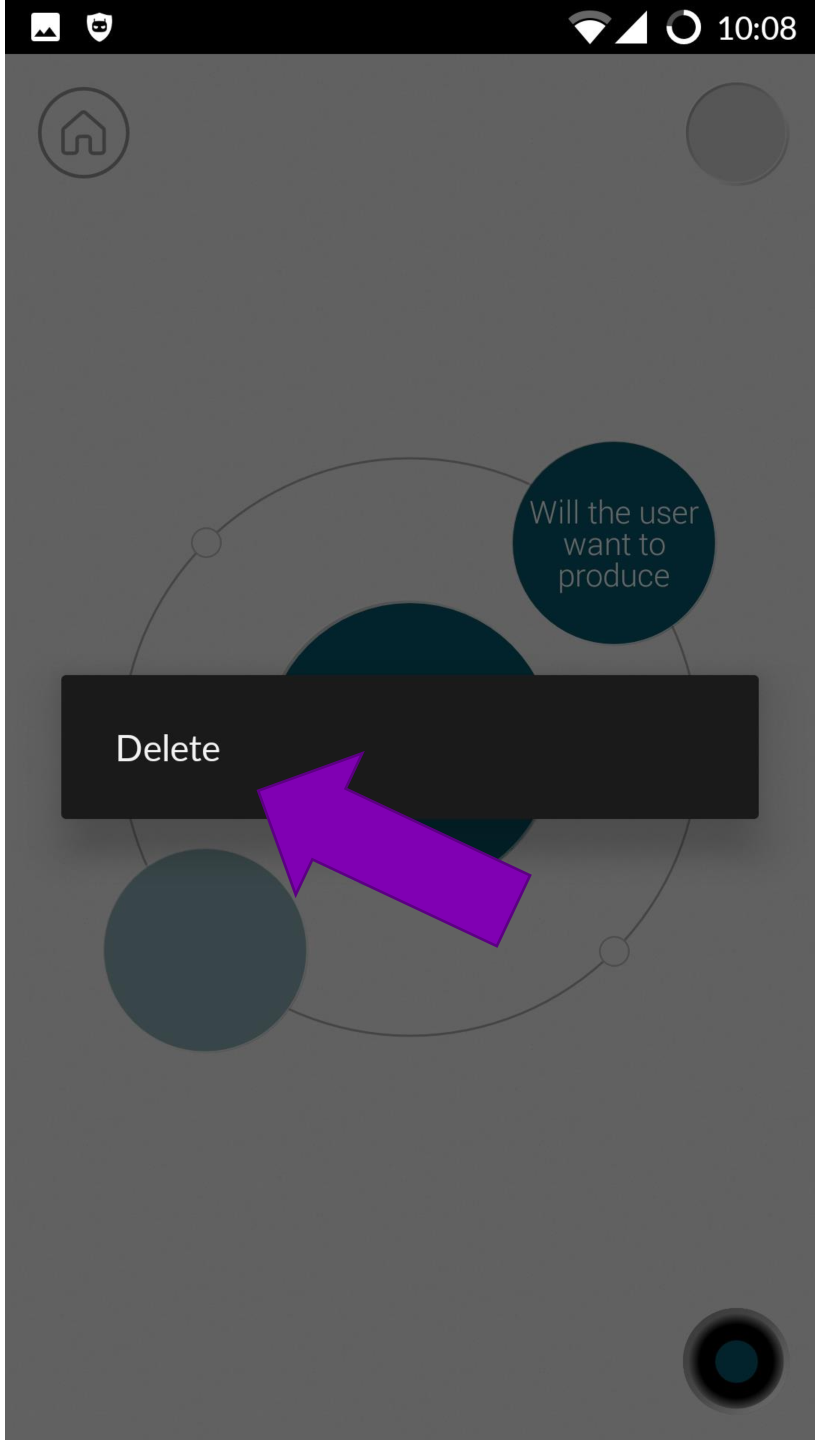


User must drag the little circle over to the black dot.

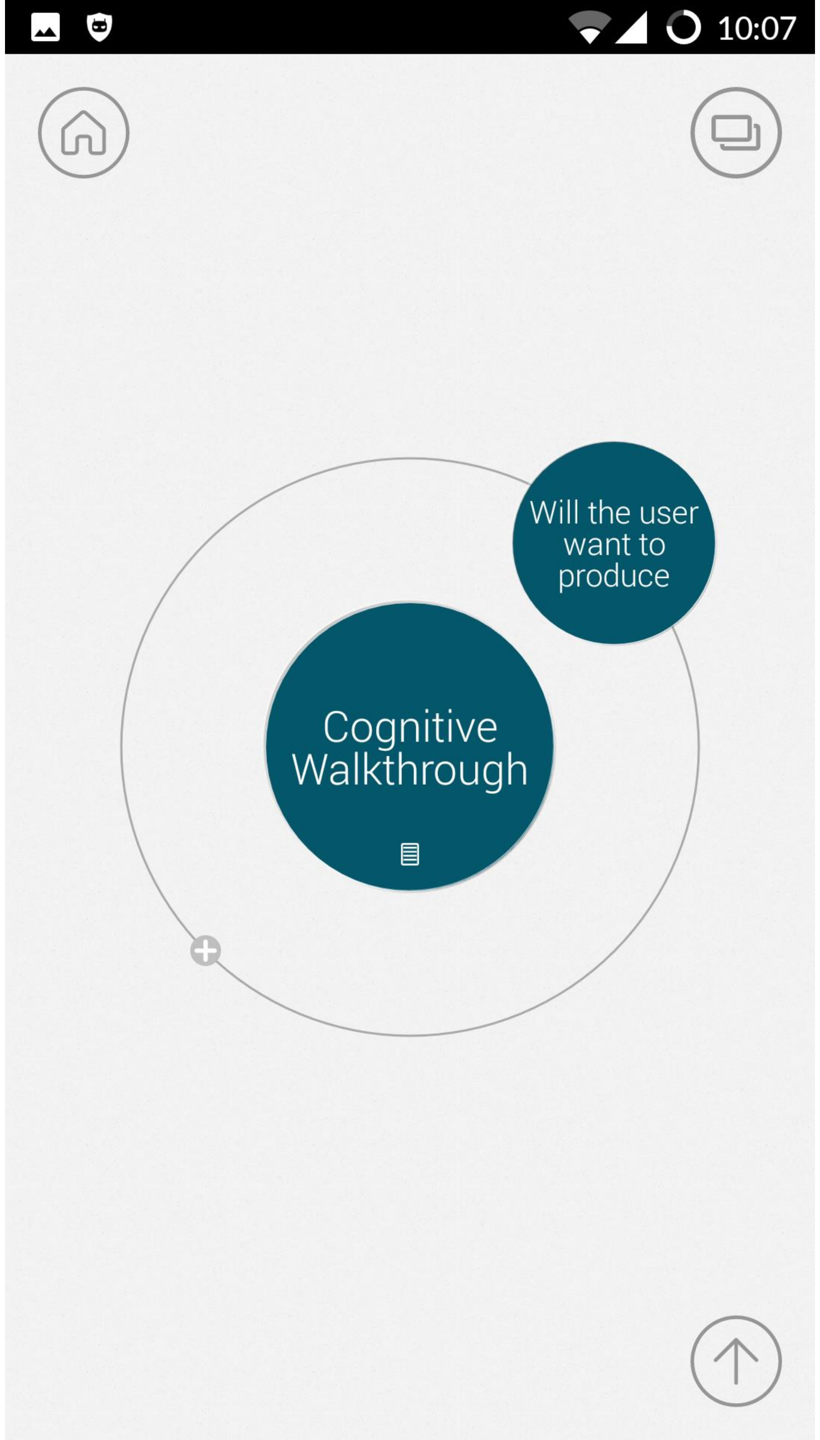
1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?



1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?



1. Will users want to produce whatever effect the action has?
2. Will users see the control (button, menu, label, etc.) for the action?
3. Once users find the control, will they recognize that it will produce the effect they want?
4. After the action is taken, will users understand the feedback they get, so they can confidently continue on to the next action?

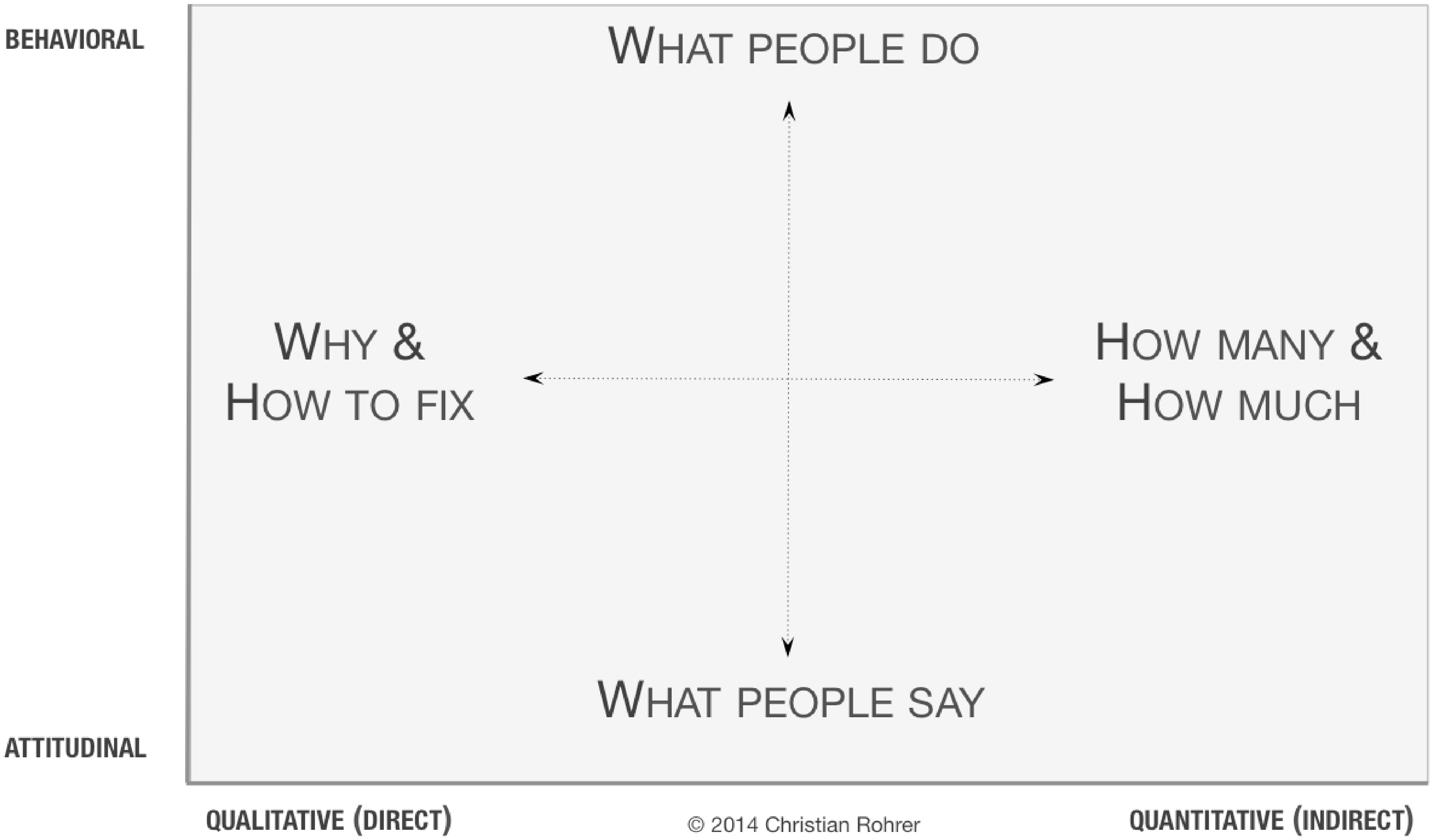


Cognitive Walkthrough outcome

	Q1: produce effect	Q2: see control	Q3: recognize effect	Q4: understand feedback
Push and hold	No. User wants to delete, not select. There are + symbols elsewhere to add a node, user may attempt to find a - symbol to directly delete rather than trying to select the node.	No. The control is invisible so there is no way to see it. User may also try tapping rather than a long hold, which will also prevent them from seeing it.	Yes.	Yes.
Drag circle	Yes.	Yes.	No. The black hole in the corner is not obviously a way to delete nodes. Users may see it, but they are likely to not recognize it as a way to delete.	Yes.
Tap “delete” button	Yes.	Yes.	Yes.	Yes.

LAB STUDY

QUESTIONS ANSWERED BY RESEARCH METHODS ACROSS THE LANDSCAPE



BEHAVIORAL

WHAT PEOPLE DO

WHY & HOW TO FIX

HOW MANY & HOW MUCH

WHAT PEOPLE SAY

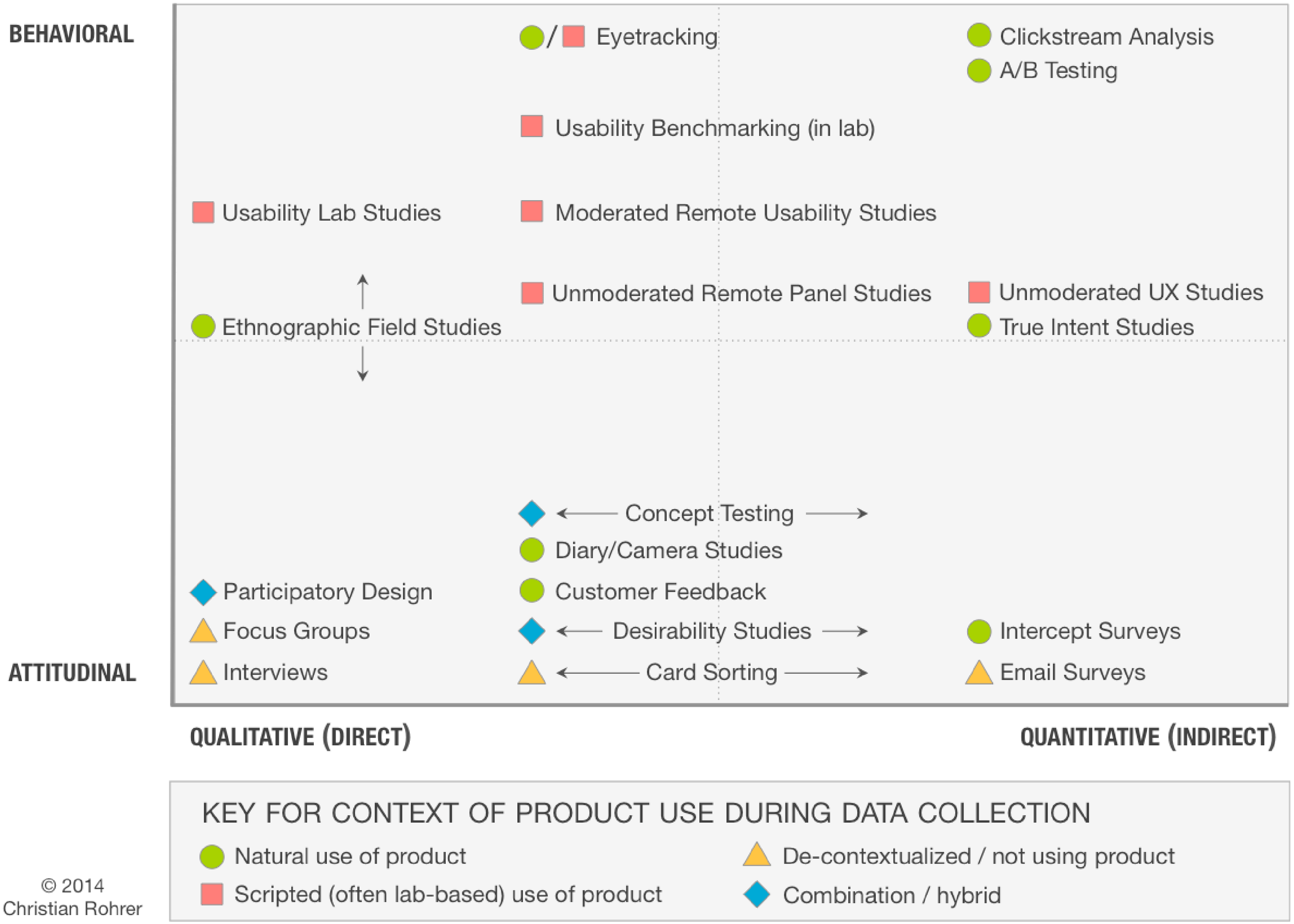
ATTITUDINAL

QUALITATIVE (DIRECT)

QUANTITATIVE (INDIRECT)

https://www.nngroup.com/articles/which-ux-research-methods/

A Landscape of User Research Methods



BEHAVIORAL

ATTITUDINAL

QUALITATIVE (DIRECT)

QUANTITATIVE (INDIRECT)

- ●/🟥 Eyetracking
- ● Clickstream Analysis
- ● A/B Testing
- 🟥 Usability Benchmarking (in lab)
- 🟥 Usability Lab Studies
- 🟥 Moderated Remote Usability Studies
- ● Ethnographic Field Studies
- 🟥 Unmoderated Remote Panel Studies
- 🟥 Unmoderated UX Studies
- ● True Intent Studies
- ◆ ← Concept Testing →
- ● Diary/Camera Studies
- ● Customer Feedback
- ◆ Participatory Design
- ▲ Focus Groups
- ◆ ← Desirability Studies →
- ● Intercept Surveys
- ▲ Interviews
- ▲ ← Card Sorting →
- ▲ Email Surveys

KEY FOR CONTEXT OF PRODUCT USE DURING DATA COLLECTION

● Natural use of product	▲ De-contextualized / not using product
🟥 Scripted (often lab-based) use of product	◆ Combination / hybrid

© 2014
Christian Rohrer

https://www.nngroup.com/articles/which-ux-research-methods/

Lab studies are a simple idea. You ask a user to come into a physical space and ask them to interact with the interface there.

Lab Study

- Basic idea: Have a participant come to a physical place (lab) and interact with the interface there
- You setup the lab so it mimics the situation you want to test
- Pros
  - Full control over the environment so limited confounds
  - Detailed data from each subject
  - Ability to ask them why they did something
- Cons
  - Small sample sizes
  - Being in the lab changes user behavior. They feel safer and their normal distractions are gone. They may also be more stressed.

Questions