Think Aloud

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

04/02/2025

THE UNIVERSITY *of* EDINBURGH

Overview

- Recap
- Think aloud
- Take-home

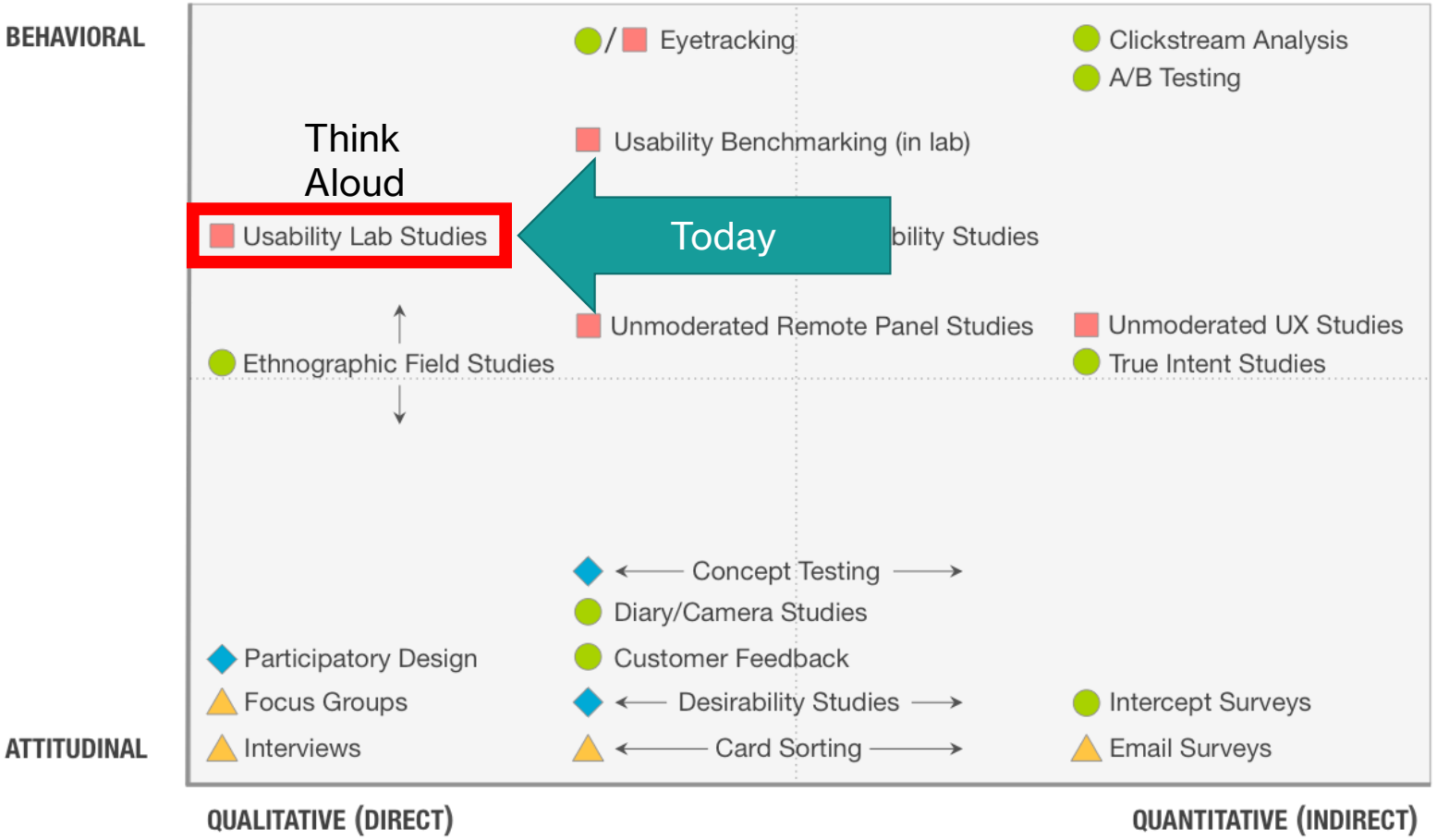
Lab studies are a simple idea. You ask a user to come into a physical space and ask them to interact with the interface there.

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. That can be bad for deception studies.

Think aloud

A Landscape of User Research Methods

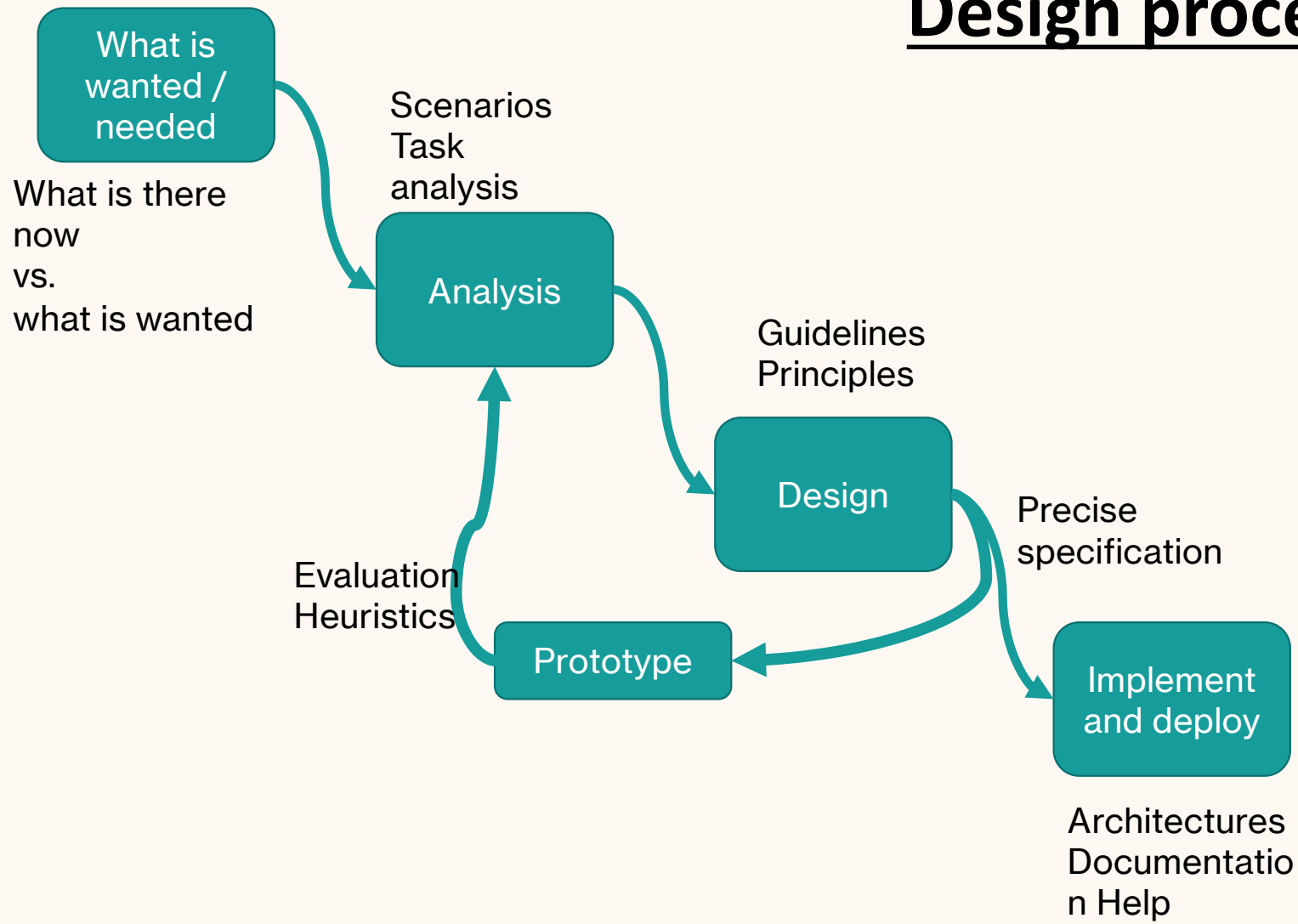


KEY FOR CONTEXT OF PRODUCT USE DURING DATA COLLECTION

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

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

Design process



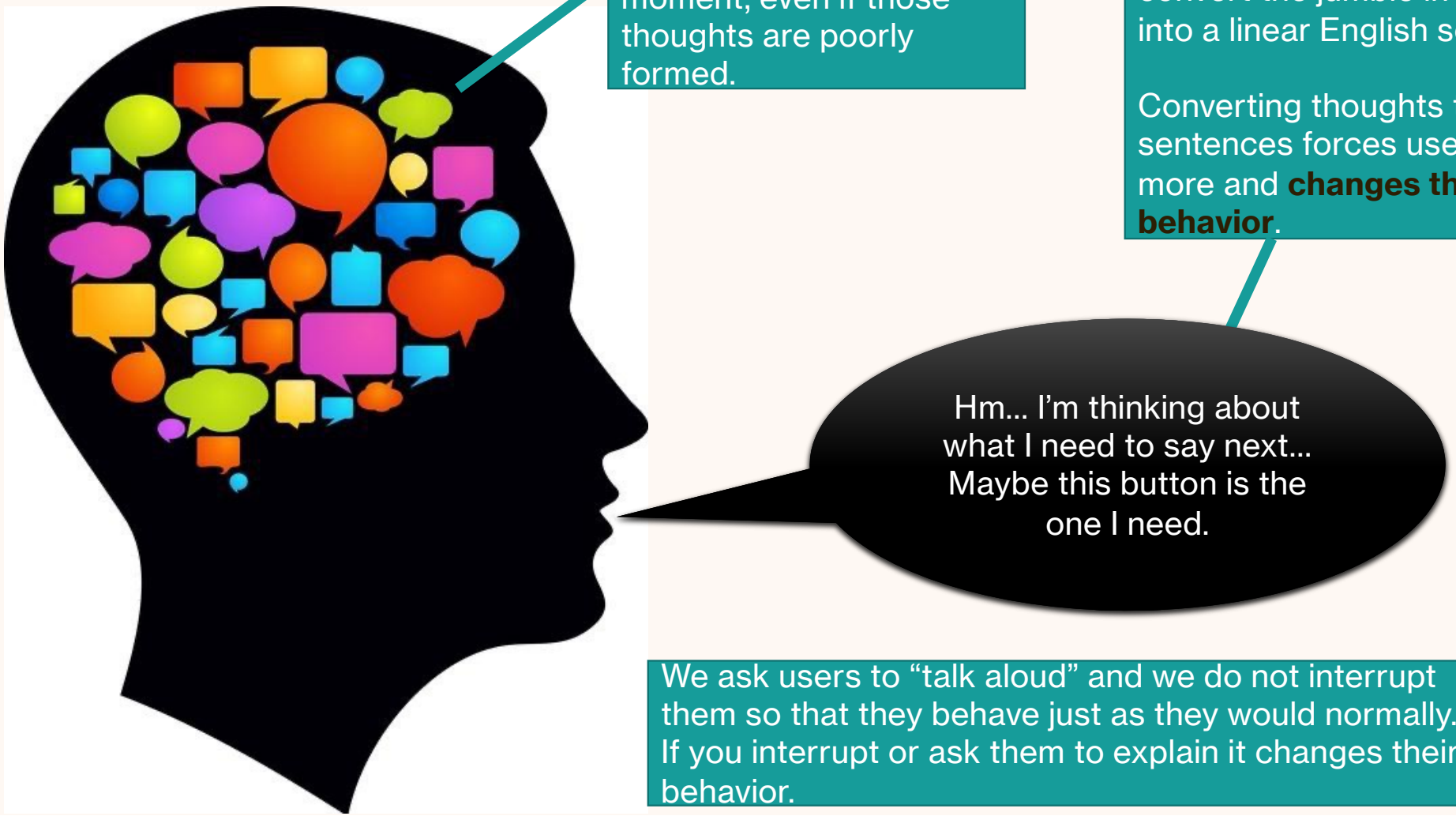
Think aloud

- Basic idea: Have a participant use the interface and speak aloud while they do so
- Think aloud is a very versatile, can be long or short, detailed or minimal, planned or ad-hoc
- Pros
  - Learn what the user is trying to do and why they click on some things
  - Very detailed information
  - Testing with about 5 users will find the majority of major (usability) issues
- Cons
  - Only possible
  - (Concurrent) Talking aloud changes how long a user spends on tasks so this method cannot be combined with timing

Think-Aloud aims to measure **what is in the person's head** at that moment, even if those thoughts are poorly formed.

If we ask the user to **"explain"** their thoughts then they have to convert the jumble in their head into a linear English sentence.

Converting thoughts to sentences forces users to think more and **changes their behavior**.



We ask users to "talk aloud" and we do not interrupt them so that they behave just as they would normally. If you interrupt or ask them to explain it changes their behavior.

What is different about security

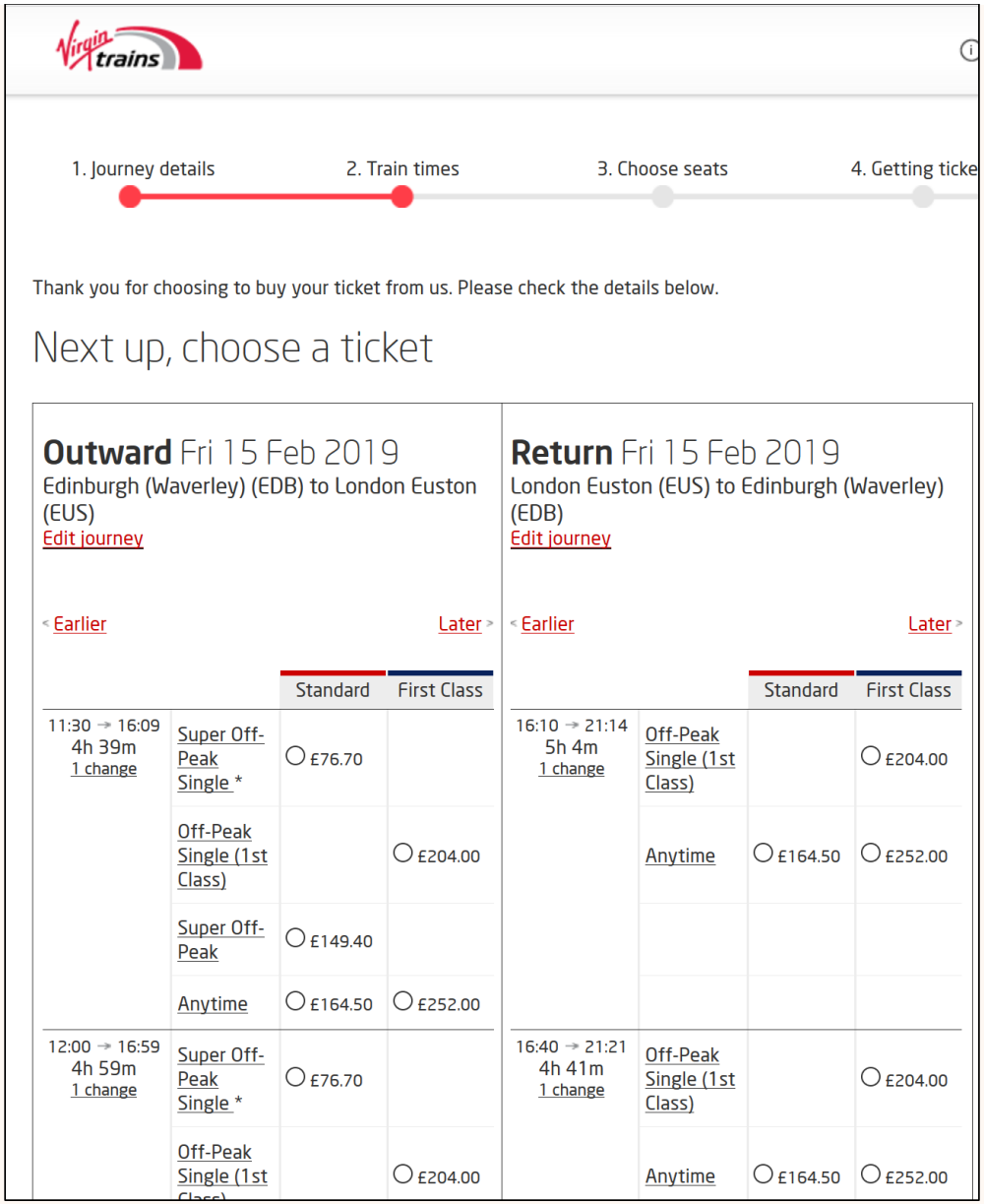
- Large information asymmetry between participant and researcher
  - The researcher likely understand security of their tool
  - Participant likely doesn’t even know that security problem exists
- Deception studies are common
  - You told the participant to accomplish task A, but you are really looking to see if they do B activity

HCI Think-Aloud:
Book a train

* Easy to see when you have succeeded or failed

* Easy to see when a mistake is made

* Participant and researcher need similar knowledge

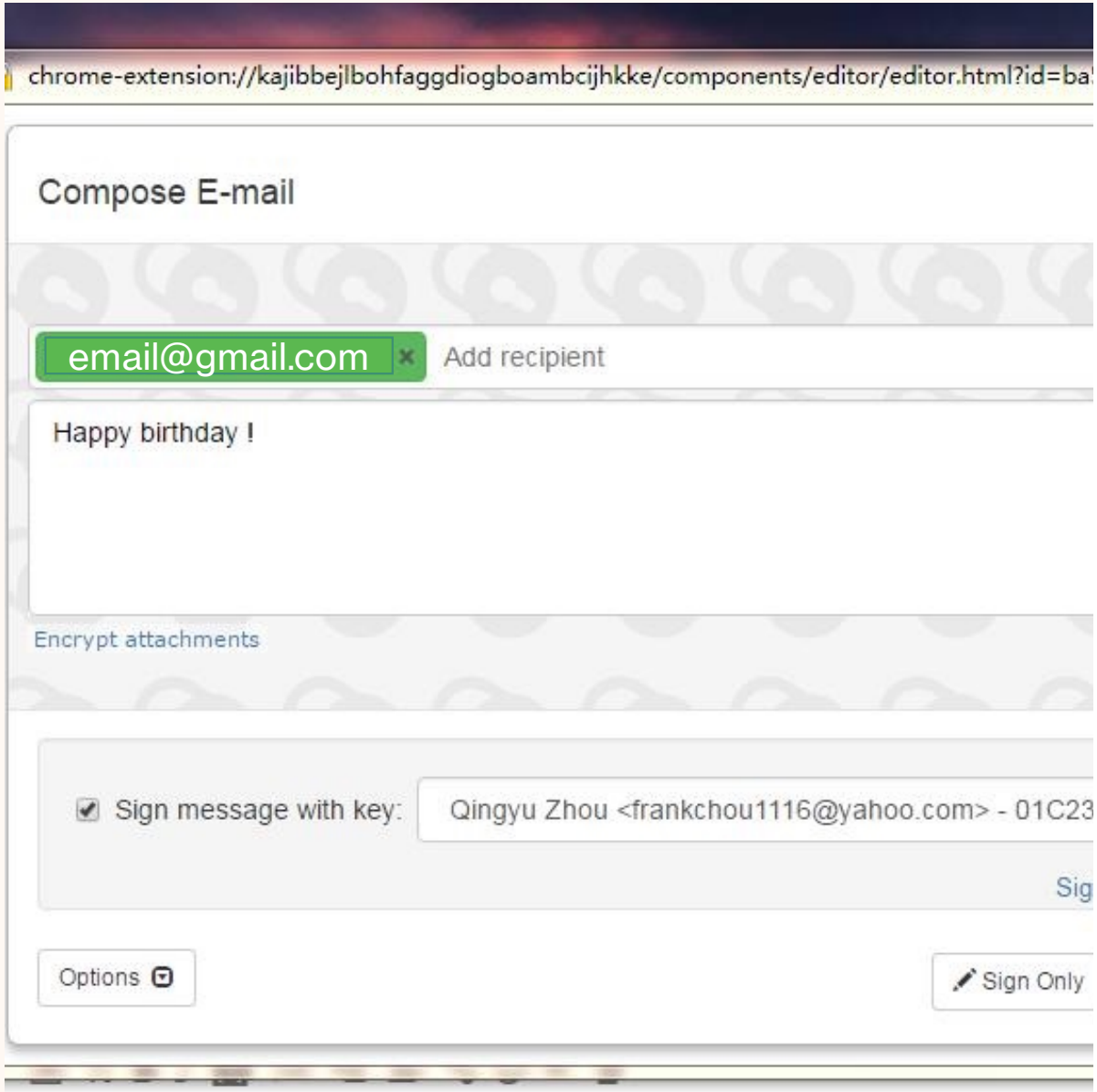


USEC Think-Aloud:
Email encryption

* Challenging to see if succeeded or failed

* Mistakes are subtle and easy to miss

* Researcher needs much more knowledge than the participant



A think-aloud requires

- Research the security technology
  - What must the participant do **to be secure**?
  - What kinds of **errors might be dangerous**?
- Pre-planning
  - Make sure tasks are interesting to the researcher
  - Knowing what you want to take notes on
- Precise running
  - **Not biasing the participant**
  - Knowing exactly what you are going to say
  - Giving them tasks they can preform
- Post-analysis
  - Number and type of errors
  - What the interface did to cause those errors
  - Recommendation on how to fix the interface

Help users think aloud

https://www.nngroup.com/videos/think-aloud/

Task and subtask

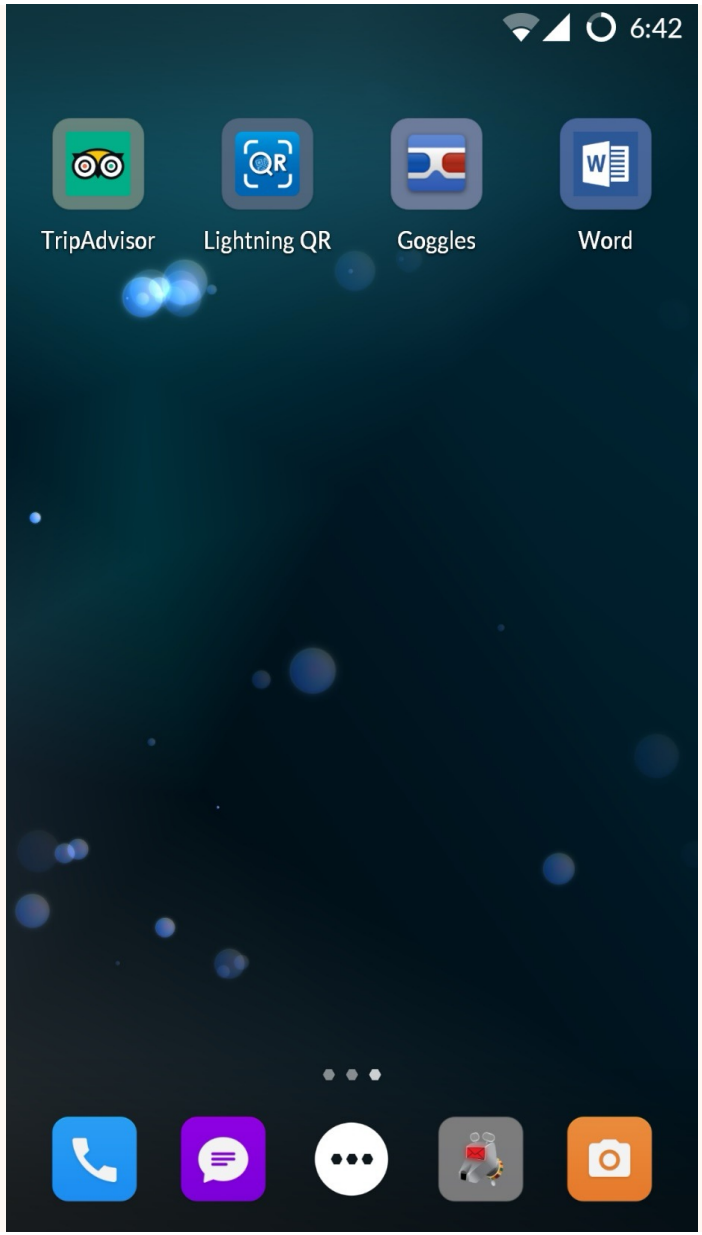
Primary and secondary tasks

- A “primary task” is basically something **someone wants to do**. It is typically high level and expresses some state or activity that user wants to achieve.
  - Determine if I need to buy anything fridge-related from the store.
  - Spend an hour playing not-too-challenging games
  - Play the song I just thought of.
- A “secondary task” or “subtask” is a **smaller task that the user must accomplish to complete** the primary task.
  - What was the name of the song I’m thinking of?
  - Which music service is likely to have it?
  - There are two versions, which one do I want to play?

Simple example:

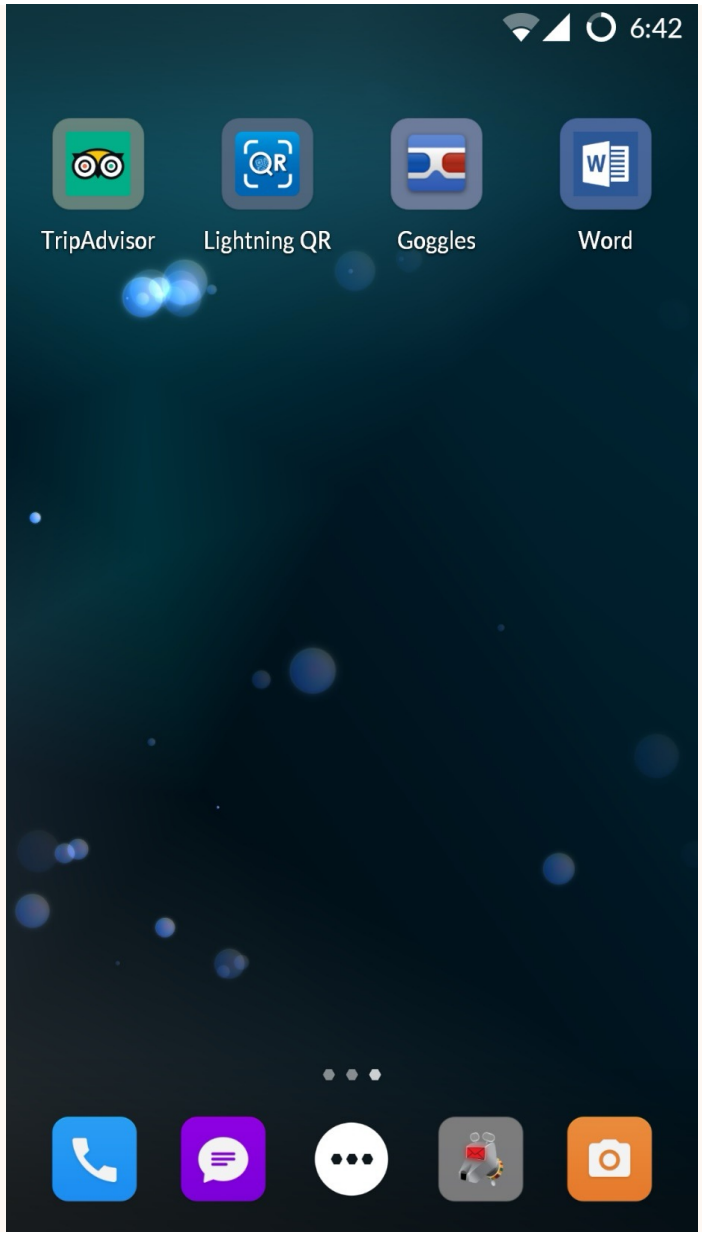
Task: Set an alarm for 7:00am

Task: Set an alarm for 7:00am



Task: Set an alarm for 7:00am

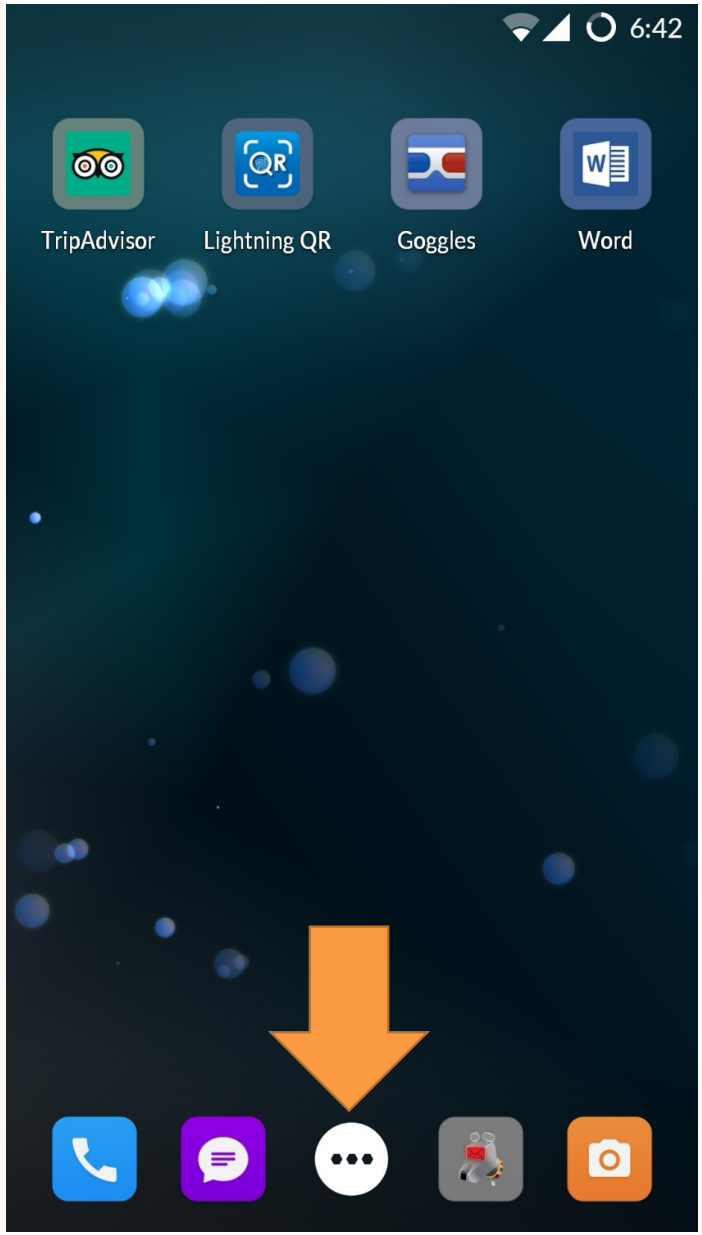
Subtask 1:
Find an app that supports “alarm clock” type functionality.



Task: Set an alarm for 7:00am

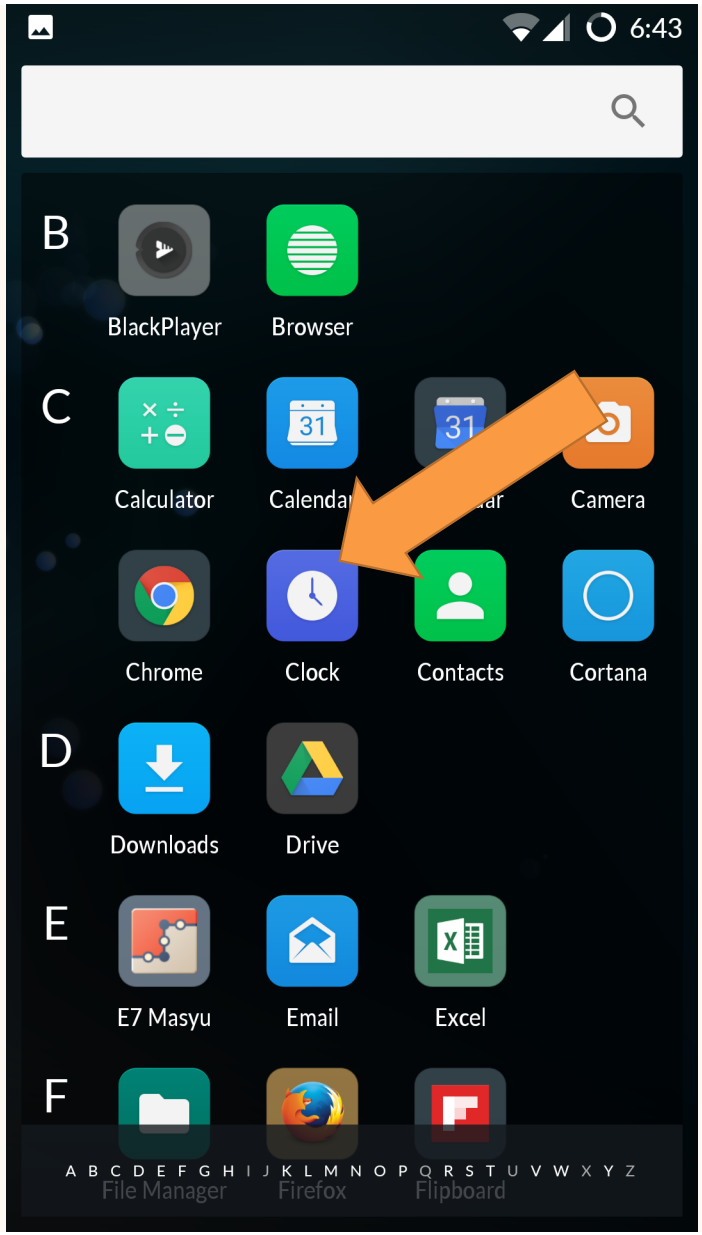
Subtask 1:
Find an app that supports “alarm clock” type functionality.

Subtask 2:
Find a list of all apps



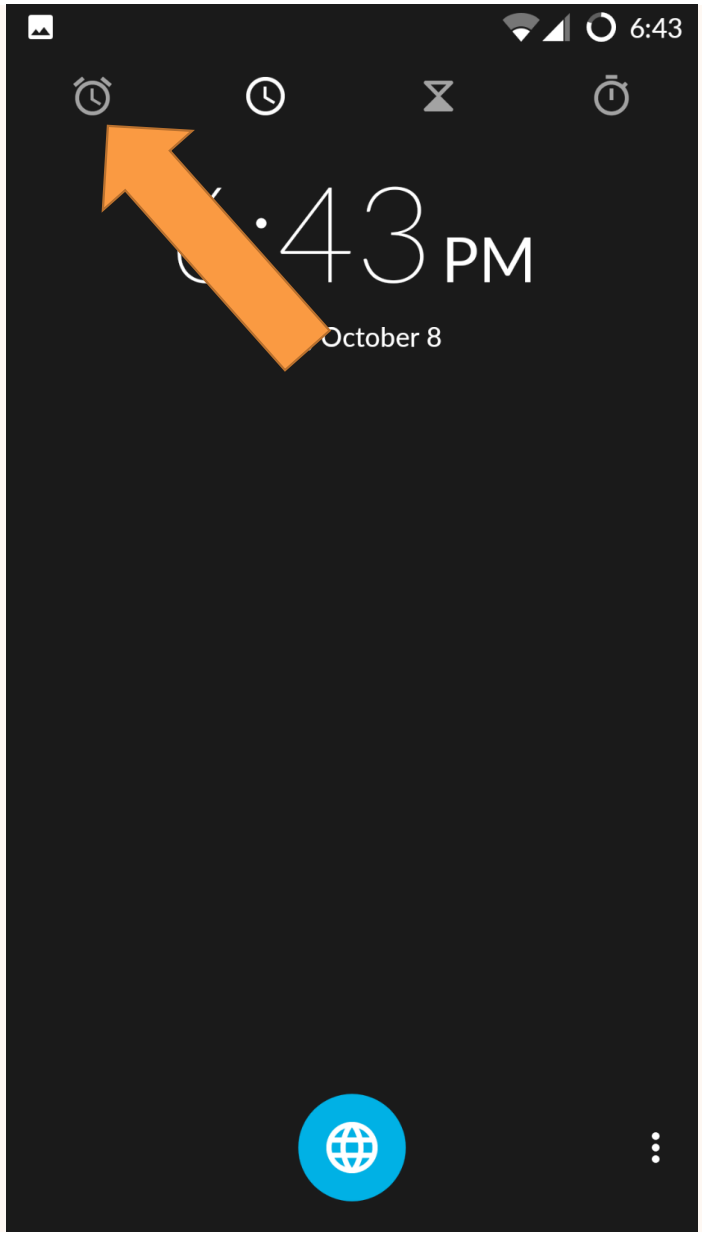
Task: Set an alarm for 7:00am

Subtask 1:
Find an app that supports “alarm clock” type functionality.



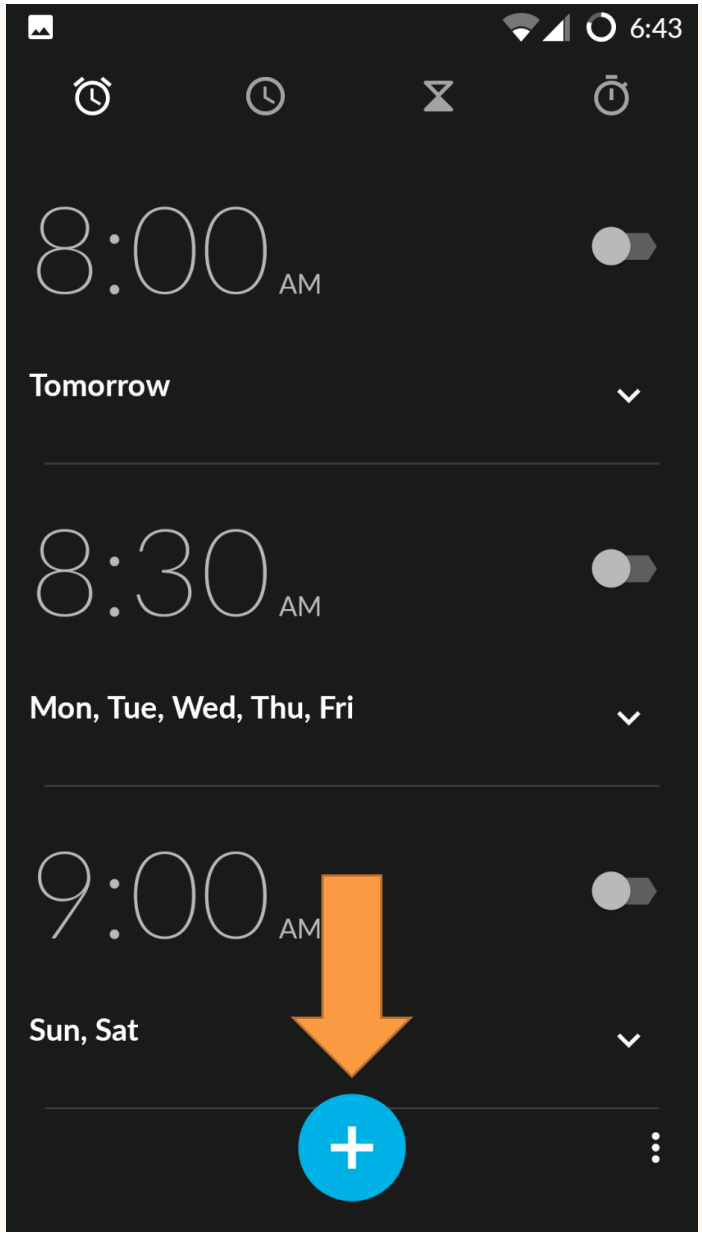
Task: Set an alarm for 7:00am

Subtask 1:
Find an app that supports “alarm clock” type functionality.



Task: Set an alarm for 7:00am

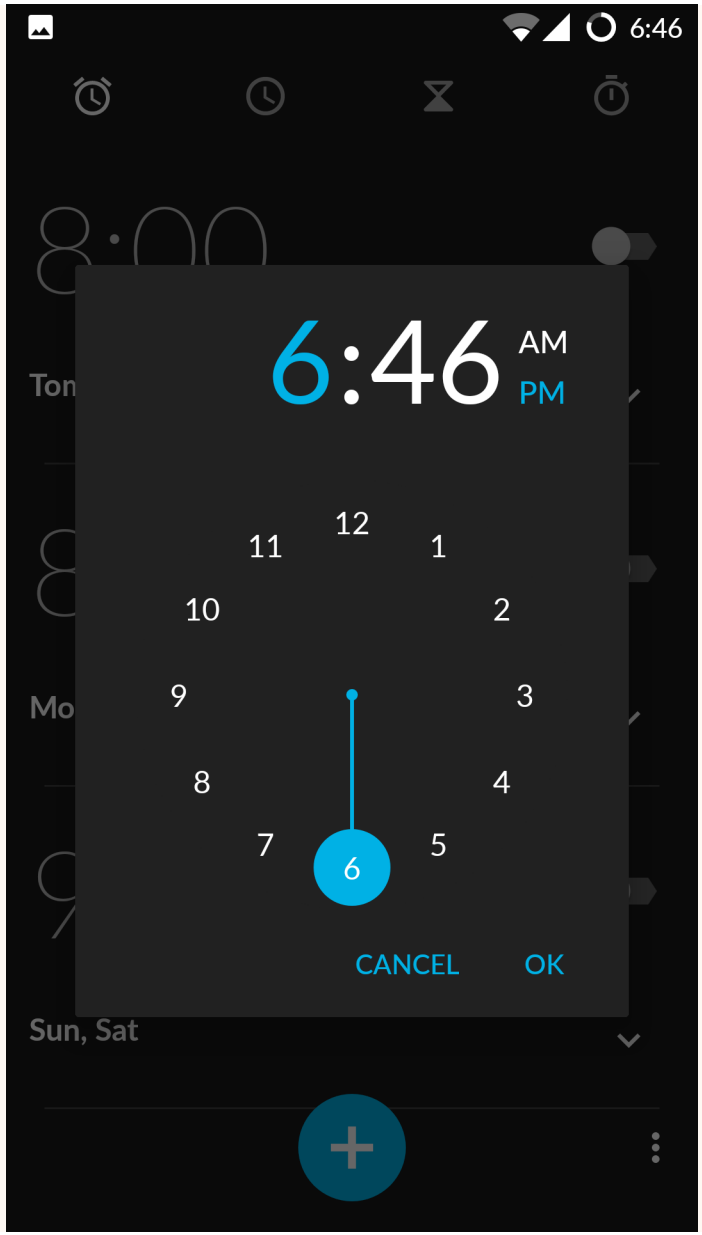
Subtask 3:
Create a new scheduled alarm.



Task: Set an alarm for 7:00am

Subtask 3:
Create a new scheduled alarm.

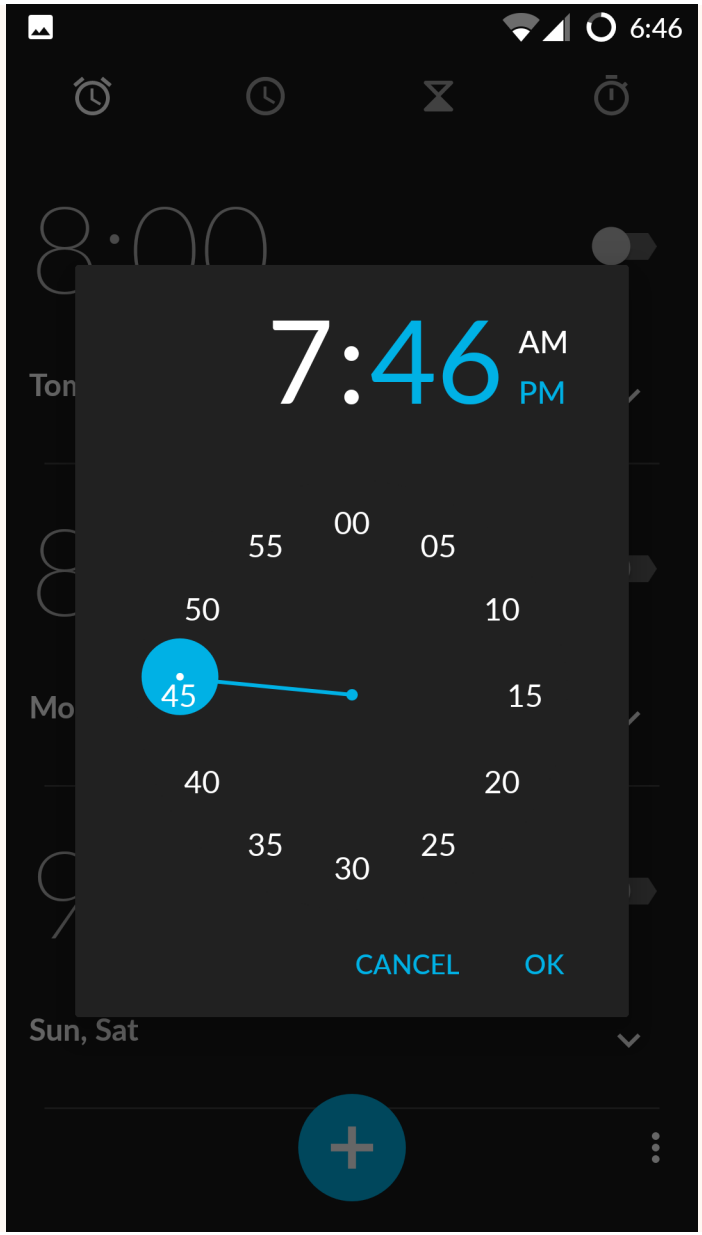
Subtask 4:
Set the hour to 7



Task: Set an alarm for 7:00am

Subtask 3:
Create a new scheduled alarm.

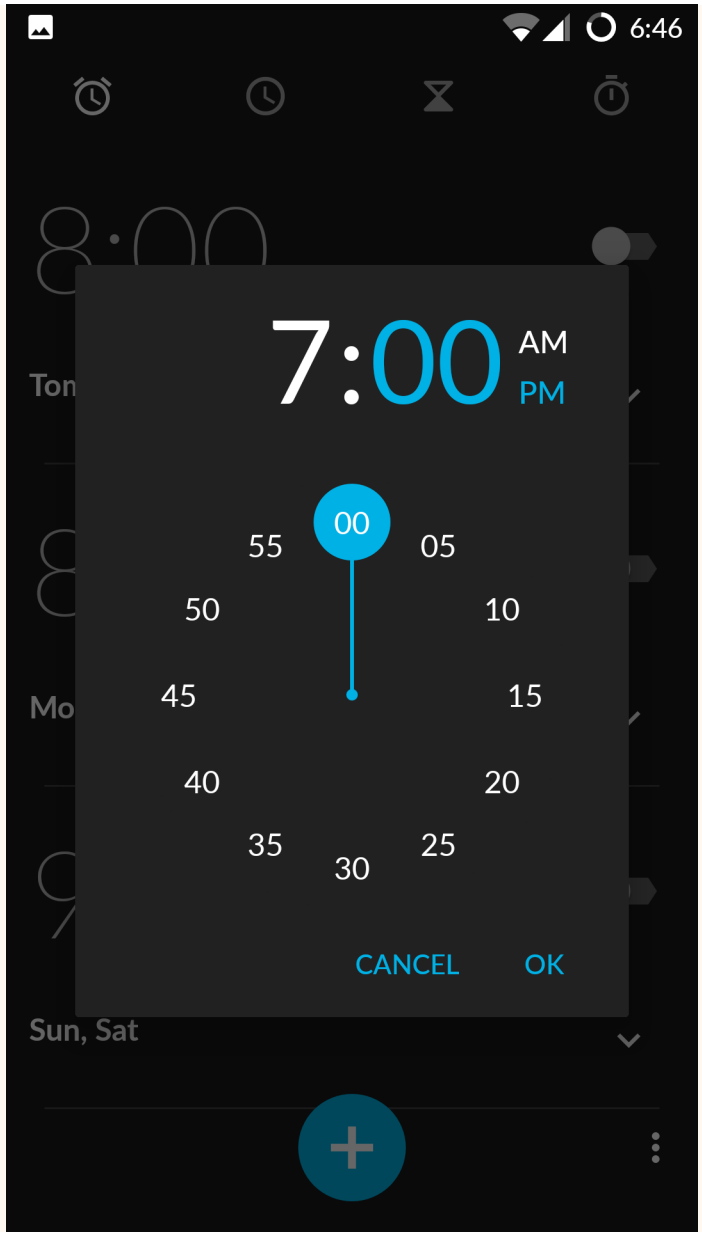
Subtask 5:
Set minutes to 00



Task: Set an alarm for 7:00am

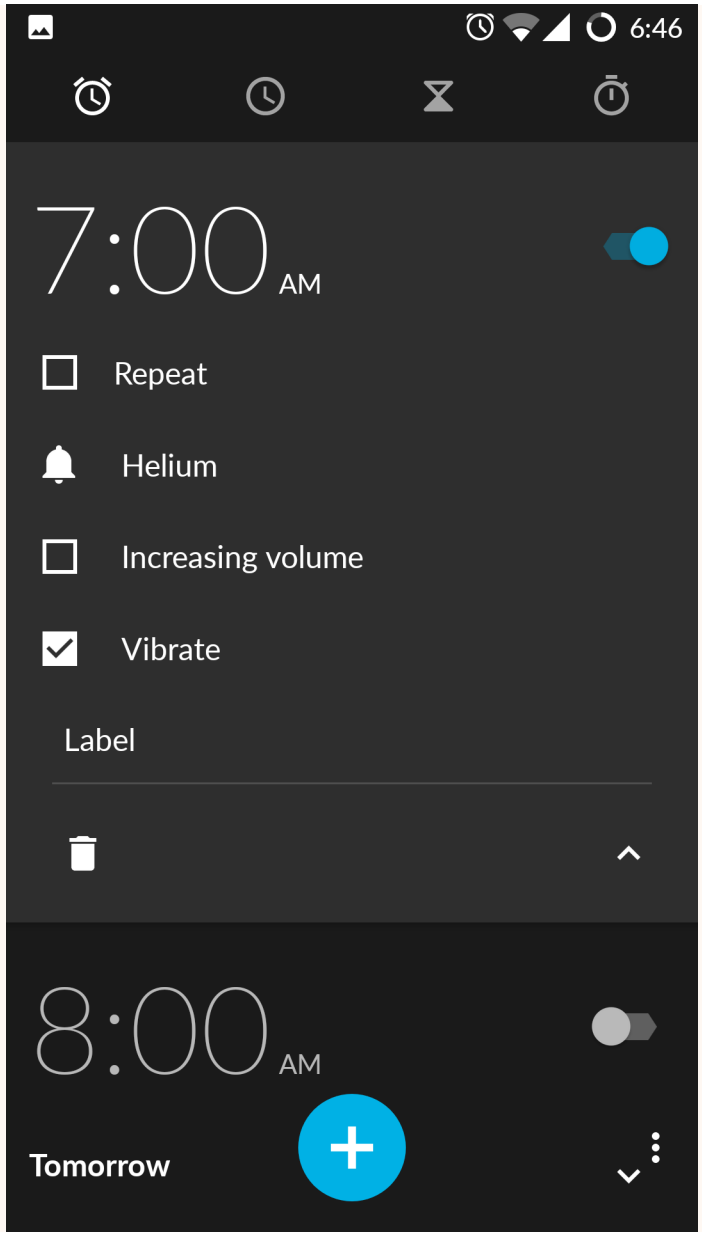
Subtask 3:
Create a new scheduled alarm.

Subtask 6:
Set to “AM”

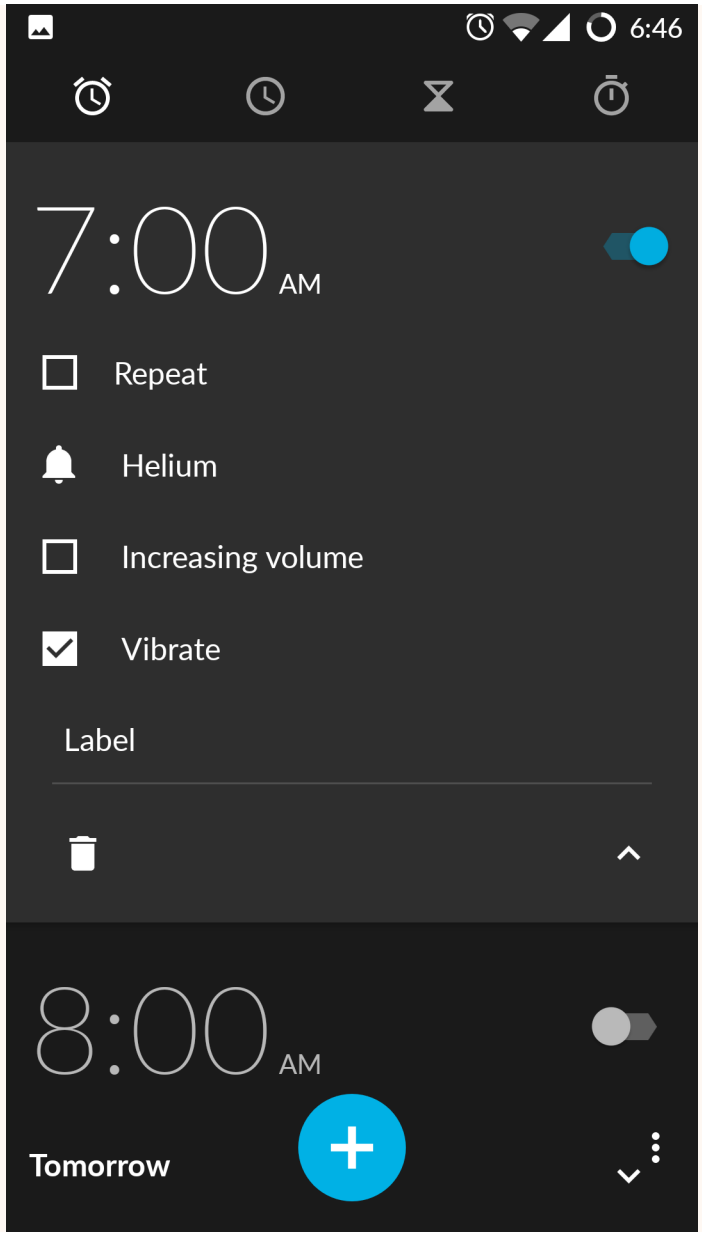


Task: Set an alarm for 7:00am

Subtask 7:
Check that the time has been correctly set and the alarm is now “on”



Task Completed!



How to design a (think aloud) study?

- Understanding the security and privacy implications of the technology
  - Ask (yourself) a set of questions
    - What is the purpose of this technology?
    - What threats is the technology designed to protect users against?
    - How should an end-user interact with this technology to ensure that they are “safe”?
  - Who are the targeted users?

- Think about what tasks you will ask users to do
  - E.g., Log in to UoE's VPN; store a new password via Apple's password manager
- Design how you can instruct the users in an experiment, avoid jargon and bias
  - Bad example: *Today we will be studying the fact that Android devices take a long time to log in. I will be asking you to log into a provided Android phone several times in front of a camera to see if you can log in quickly*
  - Good example: *This study is about the usability of Android phone login screens. Today I will be asking you to log into a provided Android phone several times in front of a camera. We are using the camera so that we can identify small issues that make the login screen harder to use*

- Who are involved?
  - Instructor / experimenter
  - User (participant)
  - (Observer / notetaker)

Take home and practice: Think Aloud Design Kit on Learn

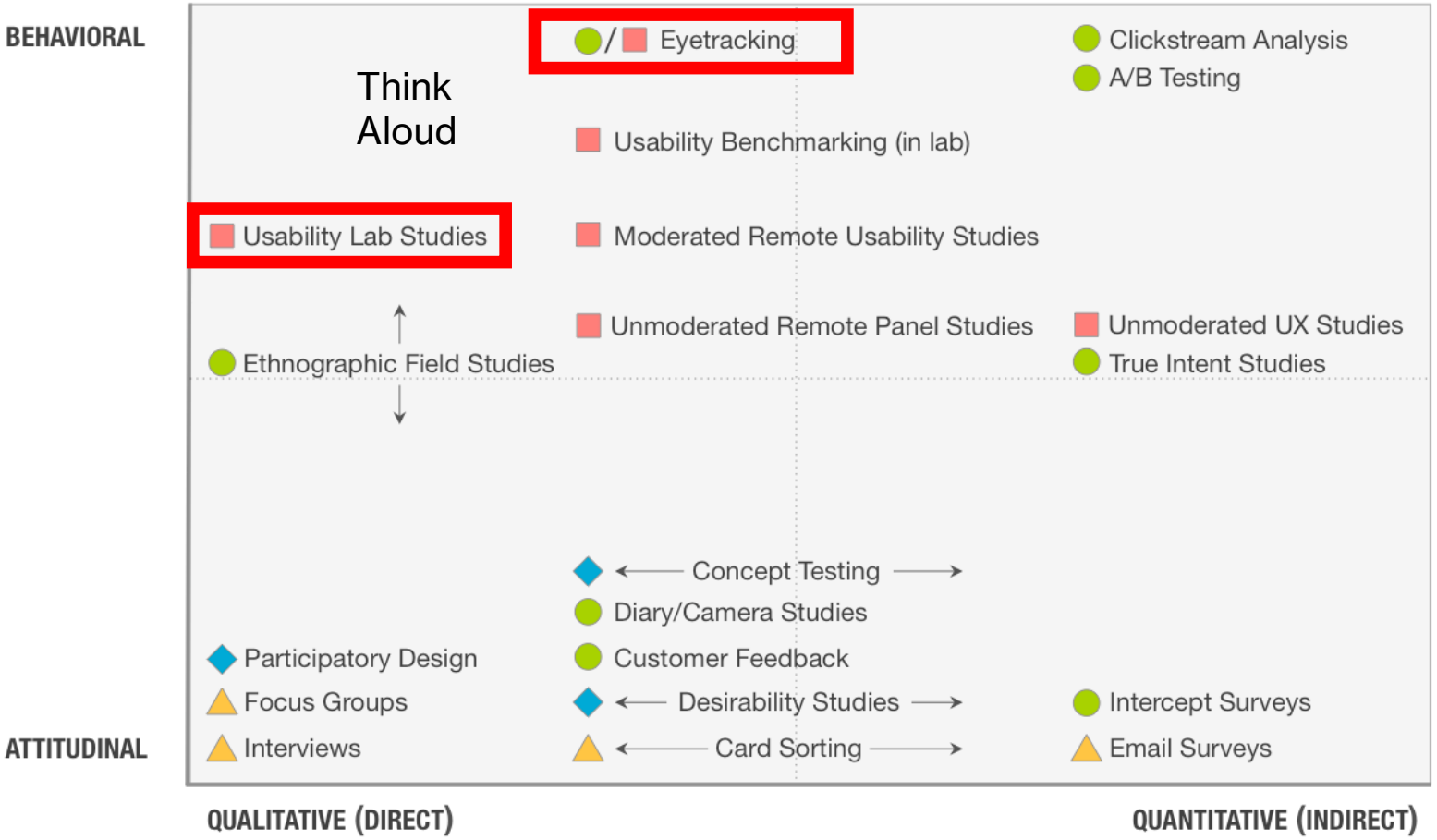
Concurrent and retrospective think-aloud

Concurrent and retrospective think-aloud

- Concurrent: participants verbalizing thoughts while performing the task
- Retrospective: participants retrace their steps after completing the task
  - Pro: better timing; less disruption
  - Con: forgetting; recency effect

Think aloud + eye tracking

A Landscape of User Research Methods

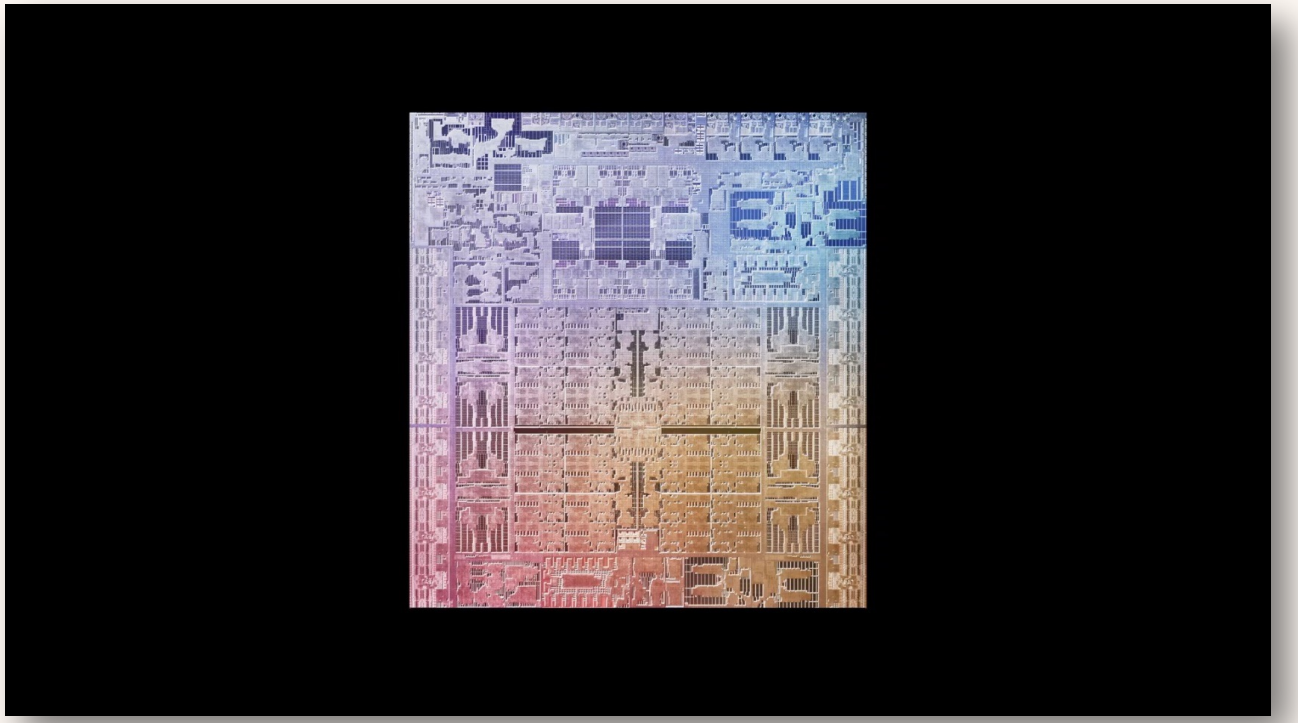


KEY FOR CONTEXT OF PRODUCT USE DURING DATA COLLECTION

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

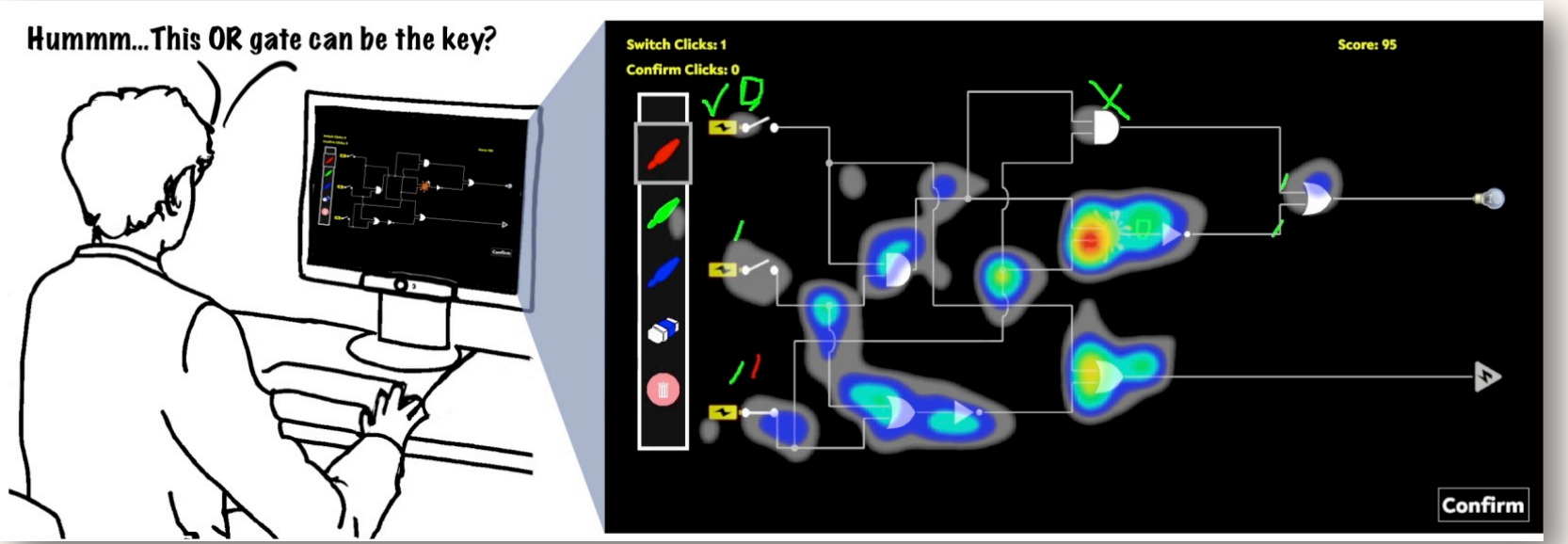
https://www.nngroup.com/articles/which-ux-research-methods/

How people perform (hardware) reverse engineering?

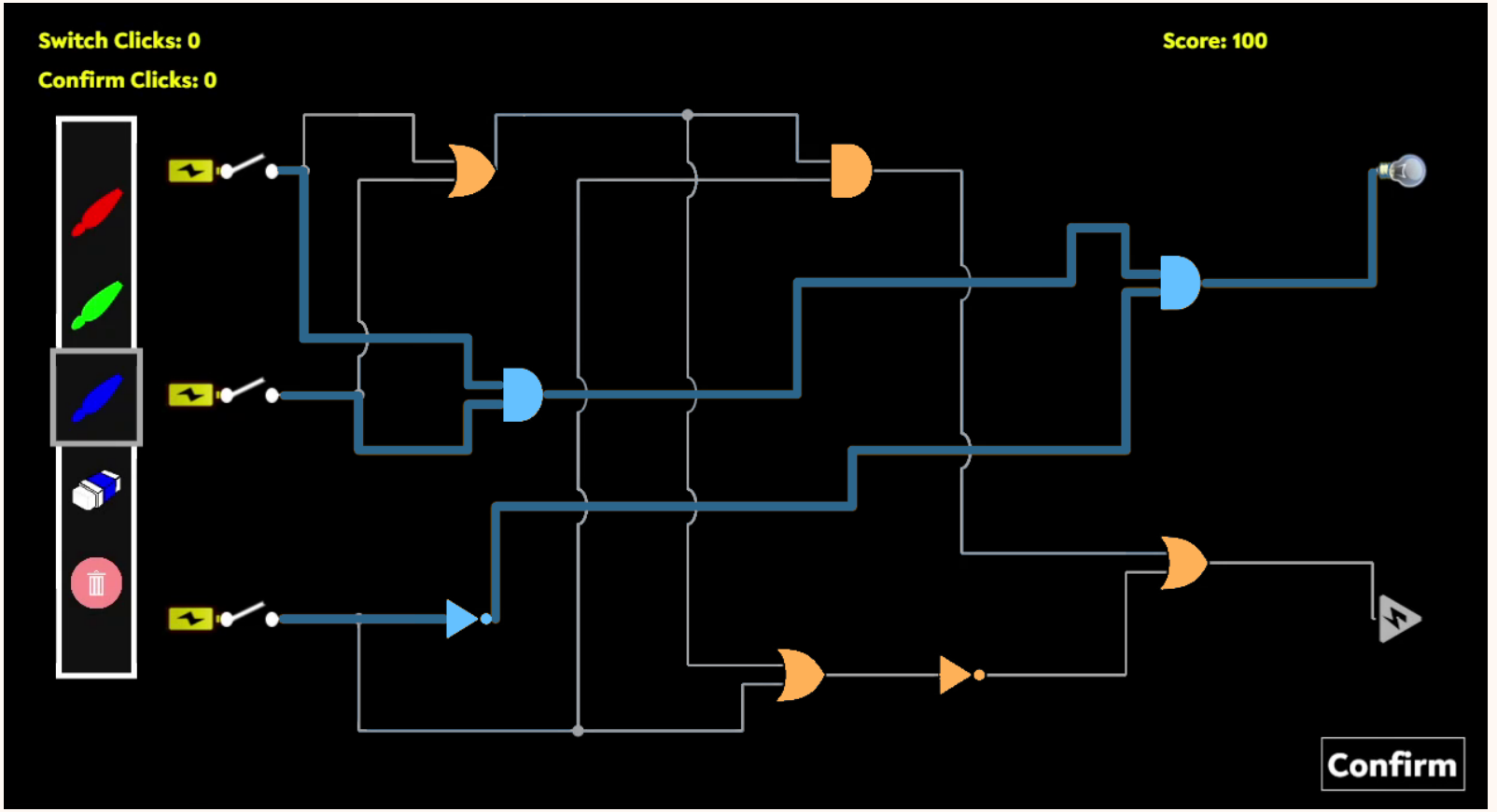


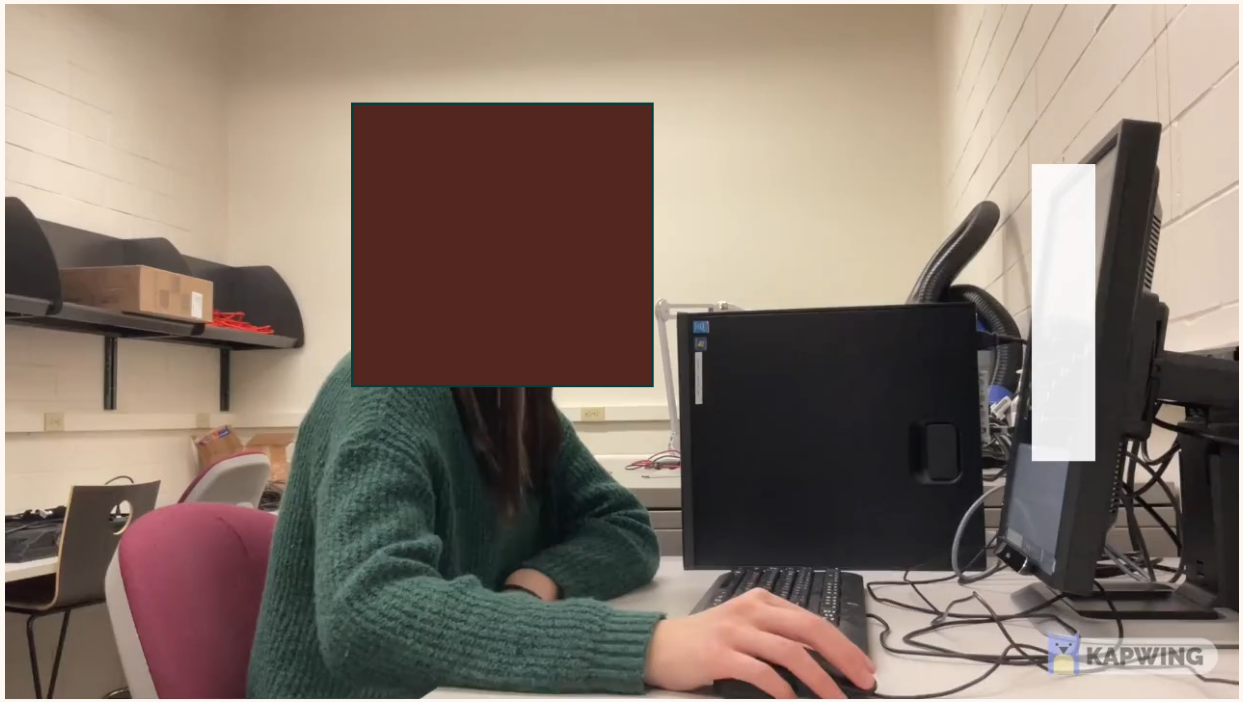
https://www.apple.com/in/newsroom/2022/03/apple-unveils-m1-ultra-the-worlds-most-powerful-chip-for-a-personal-computer/

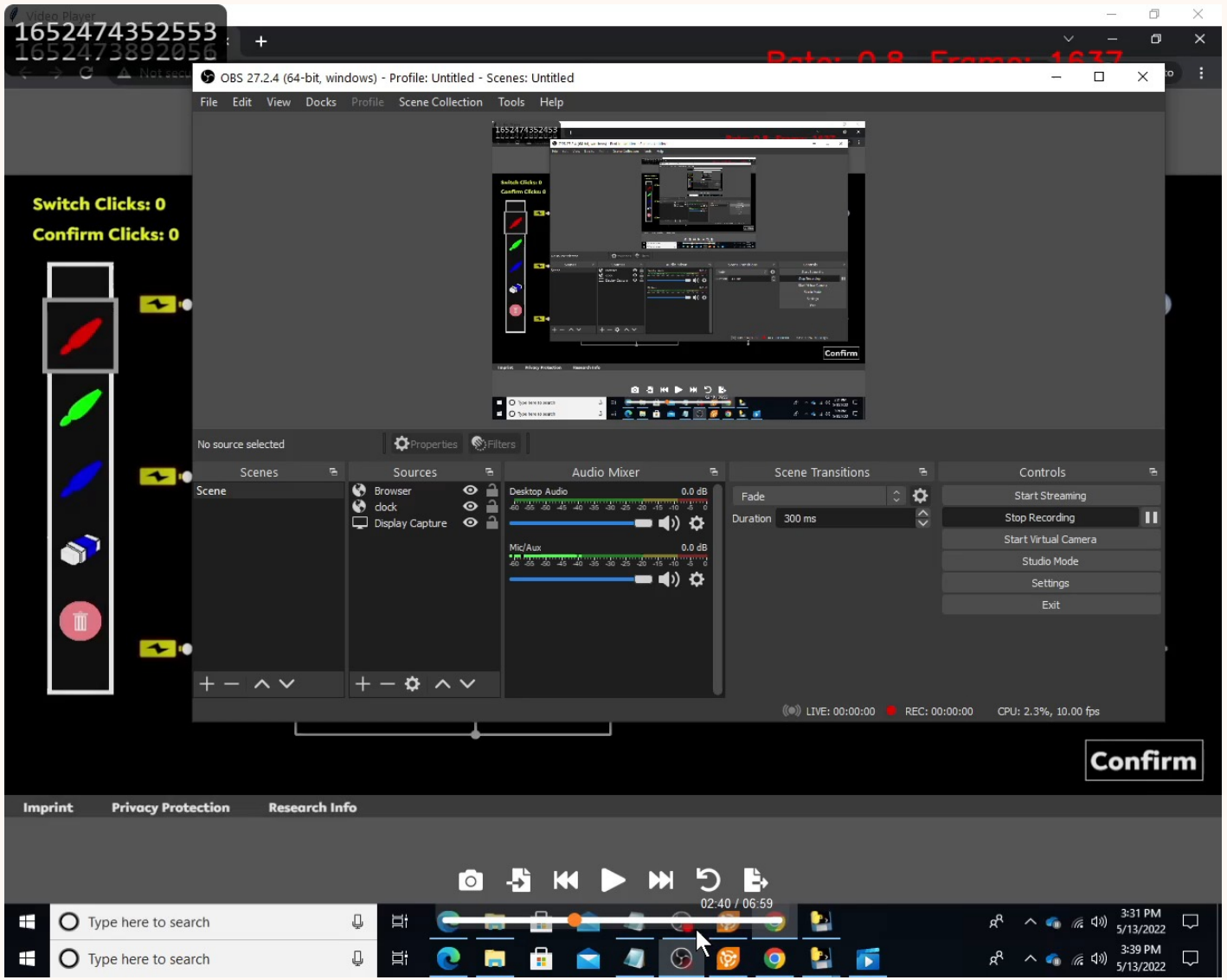
How people perform (hardware) reverse engineering?

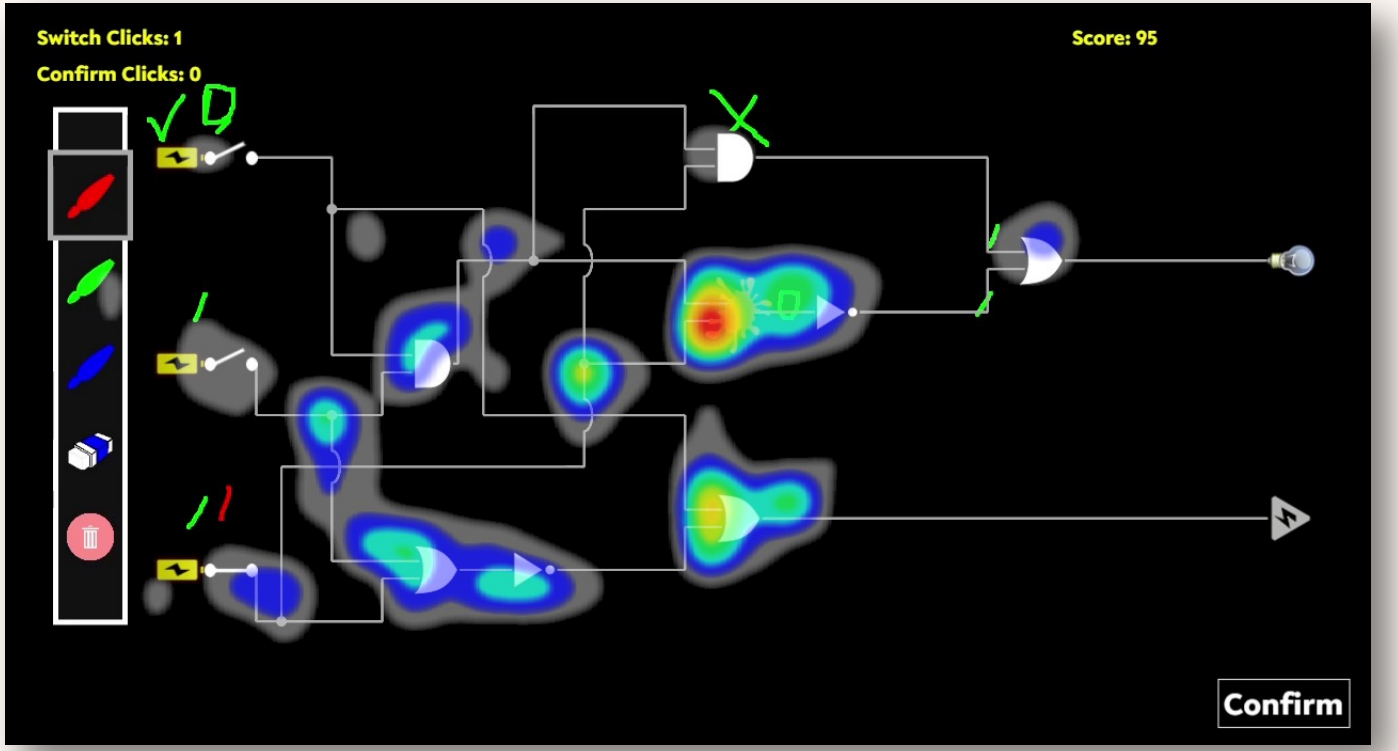


René Walendy, Markus Weber, Jingjie Li, Steffen Becker, Carina Wiesen, Malte Elson, Younghyun Kim, Kassem Fawaz, Nikol Rummel, and Christof Paar. I see an IC: A Mixed-Methods Approach to Study Human Problem-Solving Processes in Hardware Reverse Engineering. ACM CHI 2024 (to appear)

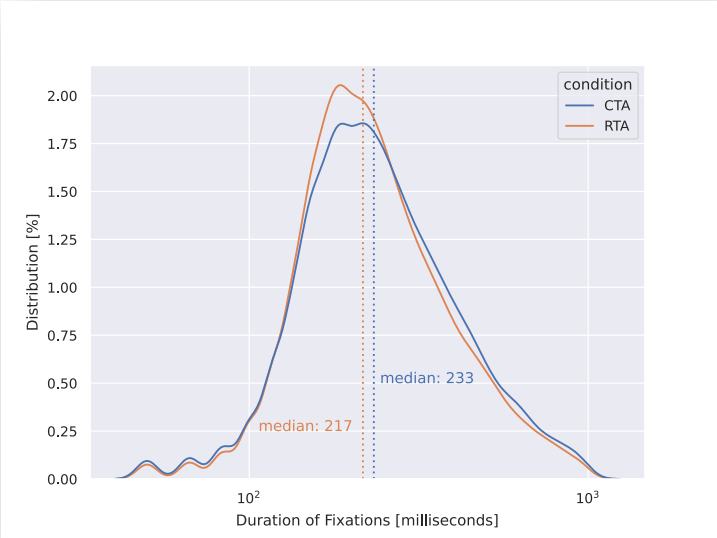

Switch Clicks: 0
Confirm Clicks: 0
Score: 100
Confirm


KAPWING

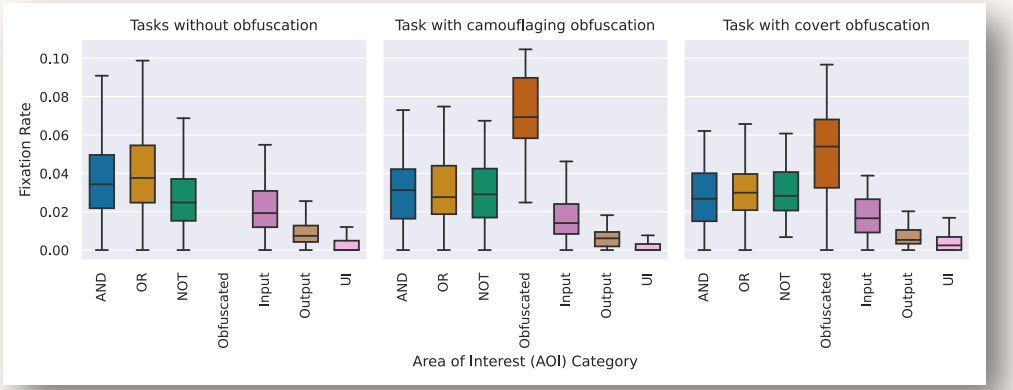

1652474352553
1652473892056
OBS 27.2.4 (64-bit, windows) - Profile: Untitled - Scenes: Untitled
File Edit View Docks Profile Scene Collection Tools Help
Switch Clicks: 0
Confirm Clicks: 0
No source selected
Properties
Filters
Scenes
Scene
Sources
Browser
clock
Display Capture
Audio Mixer
Desktop Audio 0.0 dB
Mic/Aux 0.0 dB
Scene Transitions
Fade
Duration 300 ms
Controls
Start Streaming
Stop Recording
Start Virtual Camera
Studio Mode
Settings
Exit
LIVE: 00:00:00
REC: 00:00:00
CPU: 2.3%, 10.00 fps
Confirm
Imprint
Privacy Protection
Research Info
02:40 / 06:59
Type here to search
Type here to search
3:31 PM
5/13/2022
3:39 PM
5/13/2022


Switch Clicks: 1
Confirm Clicks: 0
Score: 95
Confirm

Some findings



The impact of think aloud on people's eye fixations



Think aloud helps interpret and validate eye tracking statistics

Questions

Take-home: email encryption think-aloud

Encryption:
I want to send Bob a message that no one else can read

- I encrypt (lock) the message with Bob's **public key**.
- **Only Bob has his private key**, so only Bob can decrypt (unlock) the message.

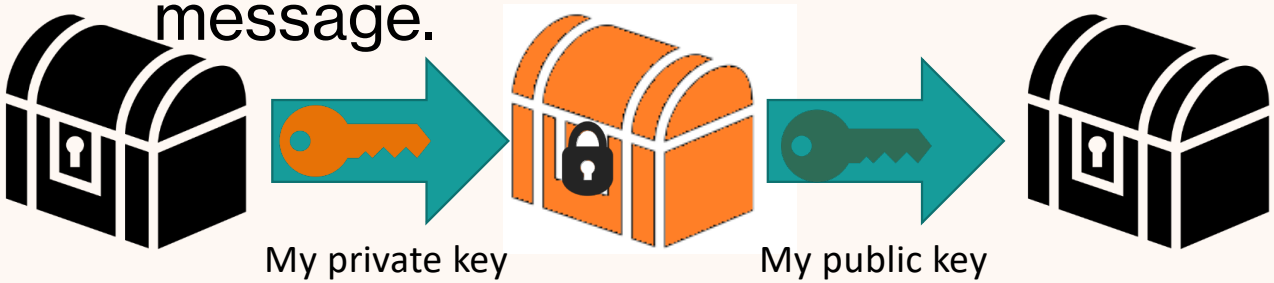
My public key

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

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzIo
XAUXH
KozHejfV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnq0CplgXcN2GJxfEHHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41
Ot
1zgxdMQkgb2H2xw28RYfYkdDouetelkOrFLrCy9ZF9KdMhA1eBH94KnwIQshdiZ
R
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u233
9hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuaWVh
IDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIACkFAIYKYvECGyMFCQImAYAHC
wkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QA
qew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrIjl2b+Q75/5t+EgXOHpR0PIxf
G
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTglvEYG3so2VueQoeXcq3dbY
p
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5albNQhQDPcTo0DgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQkJ7uQ5eFh4ZhsMgOmzLQ
D4
YiGr5welMFwAvxZOaRxEa9Vf48jiWvrxuJ8YfHWS0hEScNOcYC2P8q20IJwwE2
6T
lpdtrwCqtB1LYW1plFZhbmllYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAI
b
IwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkB
AAoJEJN2
zGX38dl9JJAIAIW0rxrIYsrmKS6CbW8MgTxxTDOXaCt1b7F0W0QZHskIUQhEcE
+a
XBYib1A5uHaatLfyjeXaD3qMEoZnQHoYMGE0GKu00wWsbhfoQzHPgwzRLkD1i7
5M
BIbaww0KWoVB9e4AkMakXJCnF5BXeo6AHRL2v15V205DikVnlCRXocKtu8b7Ln
kM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+KOdwPM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAITnSpEACgkQjy
xM

Signing:
I send Bob a message only I could have sent

- I encrypt (sign) the **message with my private key**. (Anyone can read it.)
- Only I have my private key, so **only I could have encrypted (signed)** the message.



My public key

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

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzIo
XAUXH
KozHejfV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnq0CplgXcN2GJxfEHHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41
Ot
1zgxdMQkgb2H2xw28RYfYkdDouetelkOrFLrCy9ZF9KdMhA1eBH94KnwIQshdiZ
R
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u233
9hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuaWVh
IDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIACkFAIYKYvECGyMFCQImAYAHC
wkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QA
qew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrIjl2b+Q75/5t+EgXOHpR0PIxf
G
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYG3so2VueQoeXcq3dbY
p
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5aIbNQhQDPcTo0DgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQkJ7uQ5eFh4ZhsMgOmzLQ
D4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrxuJ8YfHWS0hEScNOcYC2P8q20IJwwE2
6T
lpdtrwCqtB1LYW1plFZhbmlIYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAI
b
IwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkB
AAoJEJN2
zGX38dl9JJAIAIW0rxrIYsrmKS6CbW8MgTxxTDOXaCt1b7F0W0QZHskIUQhEcE
+a
XBYib1A5uHaatLfyjeXaD3qMEoZnQHoYMGE0GKu00wWsbhfoQzHPgwzRLkD1i7
5M
BIbaww0KWoVB9e4AkMakXJCnF5BXeo6AHRL2v15V205DikVnlCRXocKtu8b7Ln
kM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+KOdwPM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAITnSpEACgkQjy
xM

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)

More simply:

- Encryption ensures **confidentiality and integrity**
- Signatures ensure in **attribution and integrity**
- Both encryption and signatures are needed to ensure that the message is confidential, integral, and really from who you think it is from.

Authentication assumptions

- Public/private encryption also makes two fundamental assumptions which are surprisingly similar to the ones for passwords:

1. Only one person has the private key.

2. Everyone else in the world has a copy of the public key and a way of verifying that that key really belongs to who they think it belongs to.

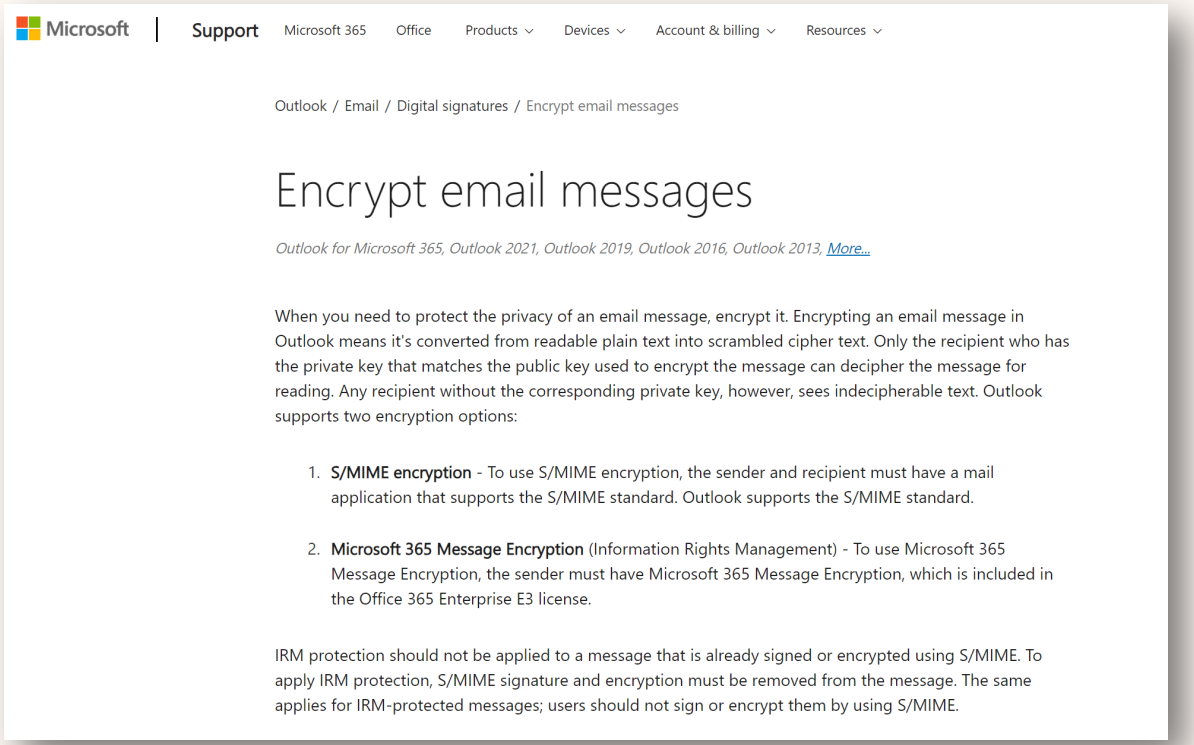
Authentication assumptions

- Public/private encryption also makes to fundamental assumptions which are surprisingly similar to the ones for passwords:

1. Only one person has the private key. (Possible)

2. Everyone else in the world has a copy of the public key and a way of verifying that that key really belongs to who they think it belongs to. (VERY hard problem called “key sharing”)

Lets try it (offline ☺)



https://support.microsoft.com/en-us/office/encrypt-email-messages-373339cb-bf1a-4509-b296-802a39d801dc

Take-home

- **(Blog)** Lau, E. and Peterson, Z., 2023. A research framework and initial study of browser security for the visually impaired. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 4679-4696).
- **(Blog)** Your own think aloud practice: design and observer notes
- Nielson Norman Group - Thinking Aloud: The #1 Usability Tool
- Video of Enigmail setup
- Video of Sending/Receiving keys