Think Aloud

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

01/02/2024

THE UNIVERSITY *of* EDINBURGH

Overview

- Coursework explained
- Recap: lab study
- Think aloud
- Take-home

Coursework overview

- Deadline: 24 March at 12:00pm
- PART A: Evaluate and re-design a security and privacy tool
  - Individual project, but some steps can be done in a group no more than 3 to help each other (student should pick and work on different tools than others in their group)
- Part B: Provide analysis and recommendation for cookie opt-out and behavioral advertising

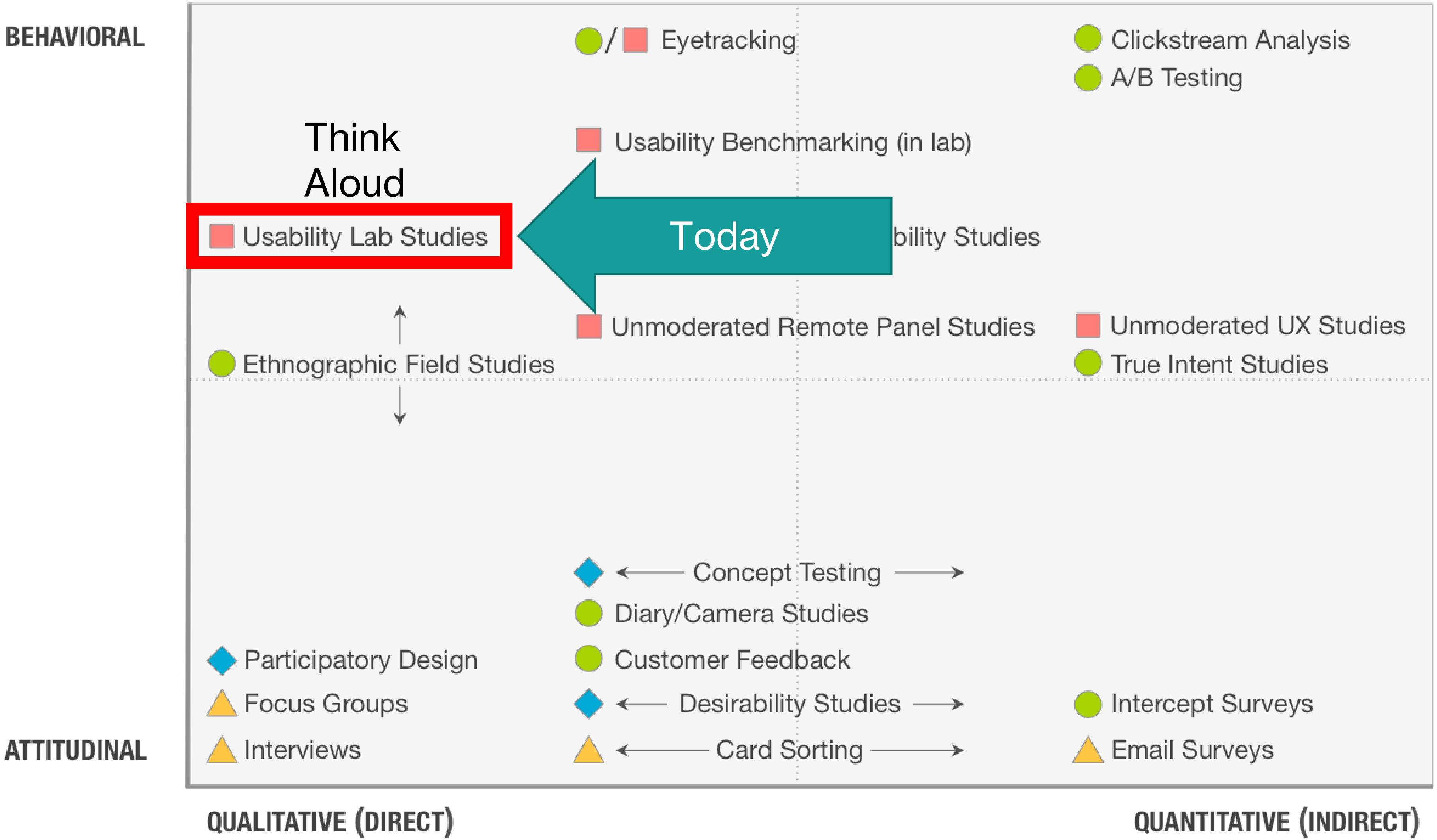
Lab studies are a simple idea. You ask a user to come into a physical space and ask them to interact with the interface there.

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

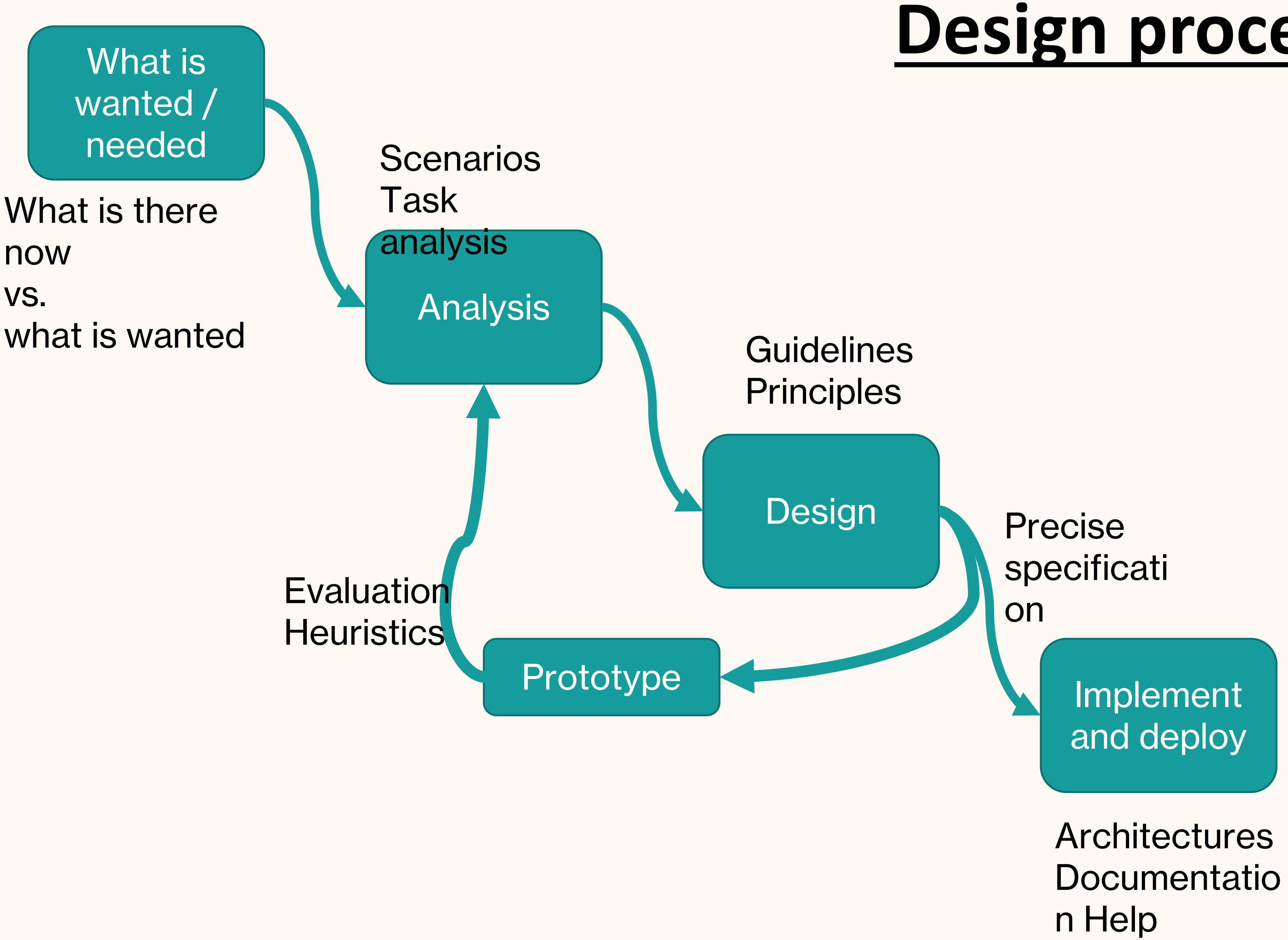


KEY FOR CONTEXT OF PRODUCT USE DURING DATA COLLECTION

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

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

Design process



What is wanted / needed

What is there now
vs.
what is wanted

Scenarios
Task analysis

Analysis

Guidelines
Principles

Design

Precise specification

Implement and deploy

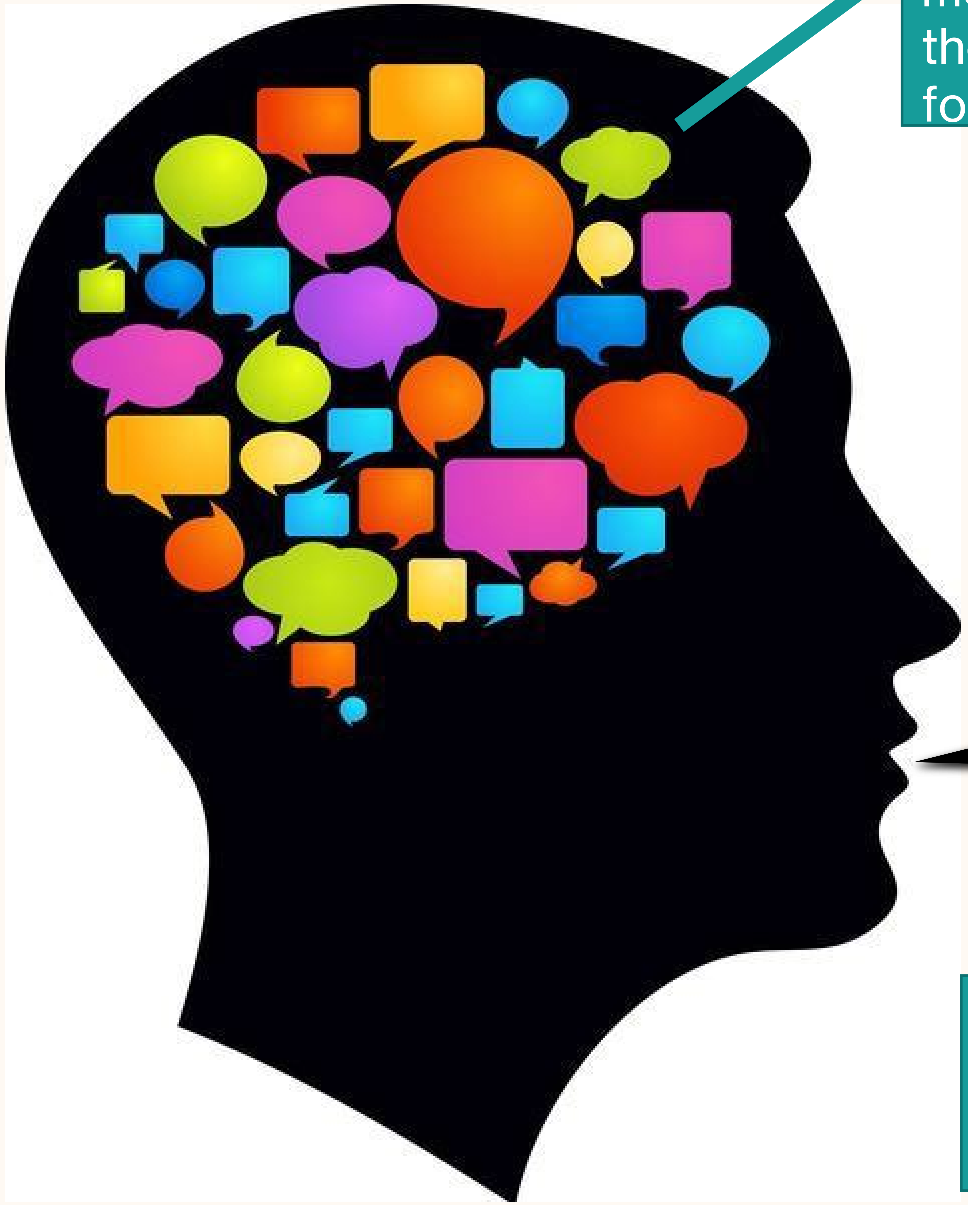
Architectures
Documentation Help

Prototype

Evaluation
Heuristics

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**.

Hm... I'm thinking about what I need to say next... Maybe this button is the one I need.

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

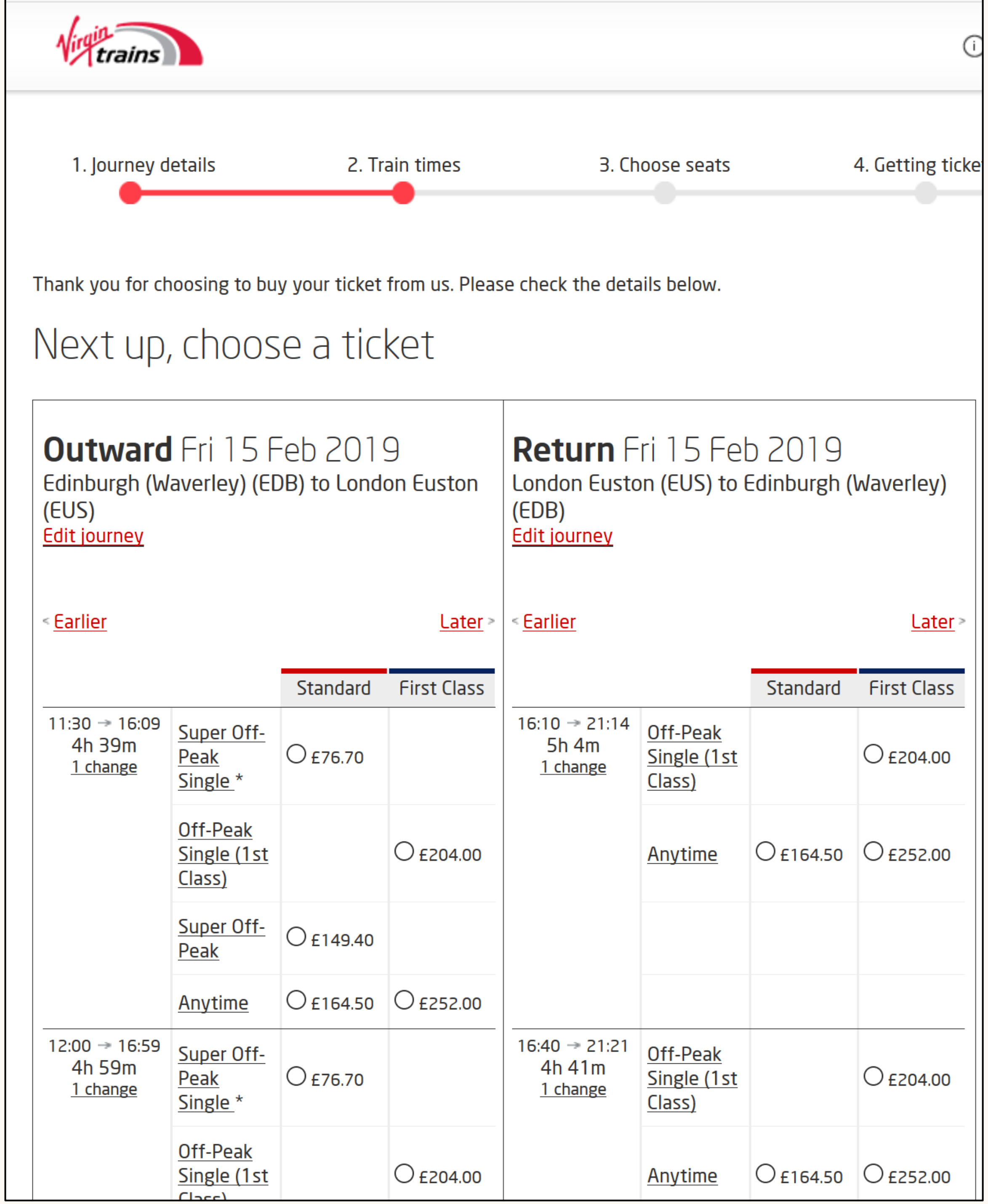
- Large information asymmetry between participant and researcher
  - The researcher likely understand security of their tool
  - Participant likely doesn’t even know that security problem exists
- Deception studies are common
  - You told the participant to accomplish task A, but you are really looking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



1. Journey details 2. Train times 3. Choose seats 4. Getting ticke

Thank you for choosing to buy your ticket from us. Please check the details below.

Next up, choose a ticket

Outward Fri 15 Feb 2019
Edinburgh (Waverley) (EDB) to London Euston (EUS)
Edit journey

< Earlier Later >

		Standard	First Class
11:30 → 16:09 4h 39m 1 change	Super Off-Peak Single *	○ £76.70	
	Off-Peak Single (1st Class)		○ £204.00
	Super Off-Peak	○ £149.40	
	Anytime	○ £164.50	○ £252.00
12:00 → 16:59 4h 59m 1 change	Super Off-Peak Single *	○ £76.70	
	Off-Peak Single (1st Class)		○ £204.00

Return Fri 15 Feb 2019
London Euston (EUS) to Edinburgh (Waverley) (EDB)
Edit journey

< Earlier Later >

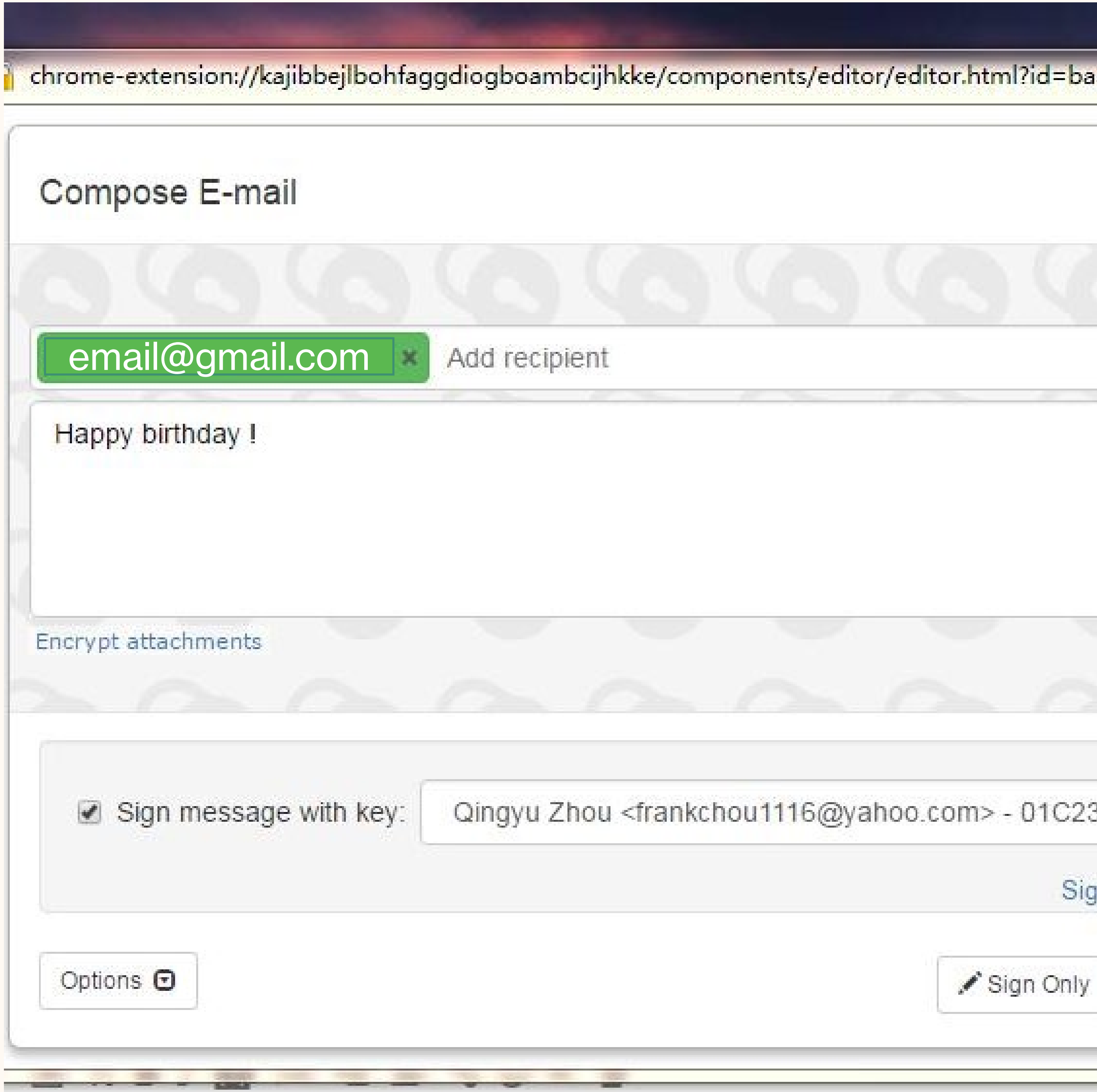
		Standard	First Class
16:10 → 21:14 5h 4m 1 change	Off-Peak Single (1st Class)		○ £204.00
	Anytime	○ £164.50	○ £252.00
16:40 → 21:21 4h 41m 1 change	Off-Peak Single (1st Class)		○ £204.00
	Anytime	○ £164.50	○ £252.00

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



chrome-extension://kajibbejlbohfaggdiogboambcijhkke/components/editor/editor.html?id=ba

Compose E-mail

email@gmail.com

Happy birthday !

☑ Sign message with key: Qingyu Zhou <frankchou1116@yahoo.com> - 01C23

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

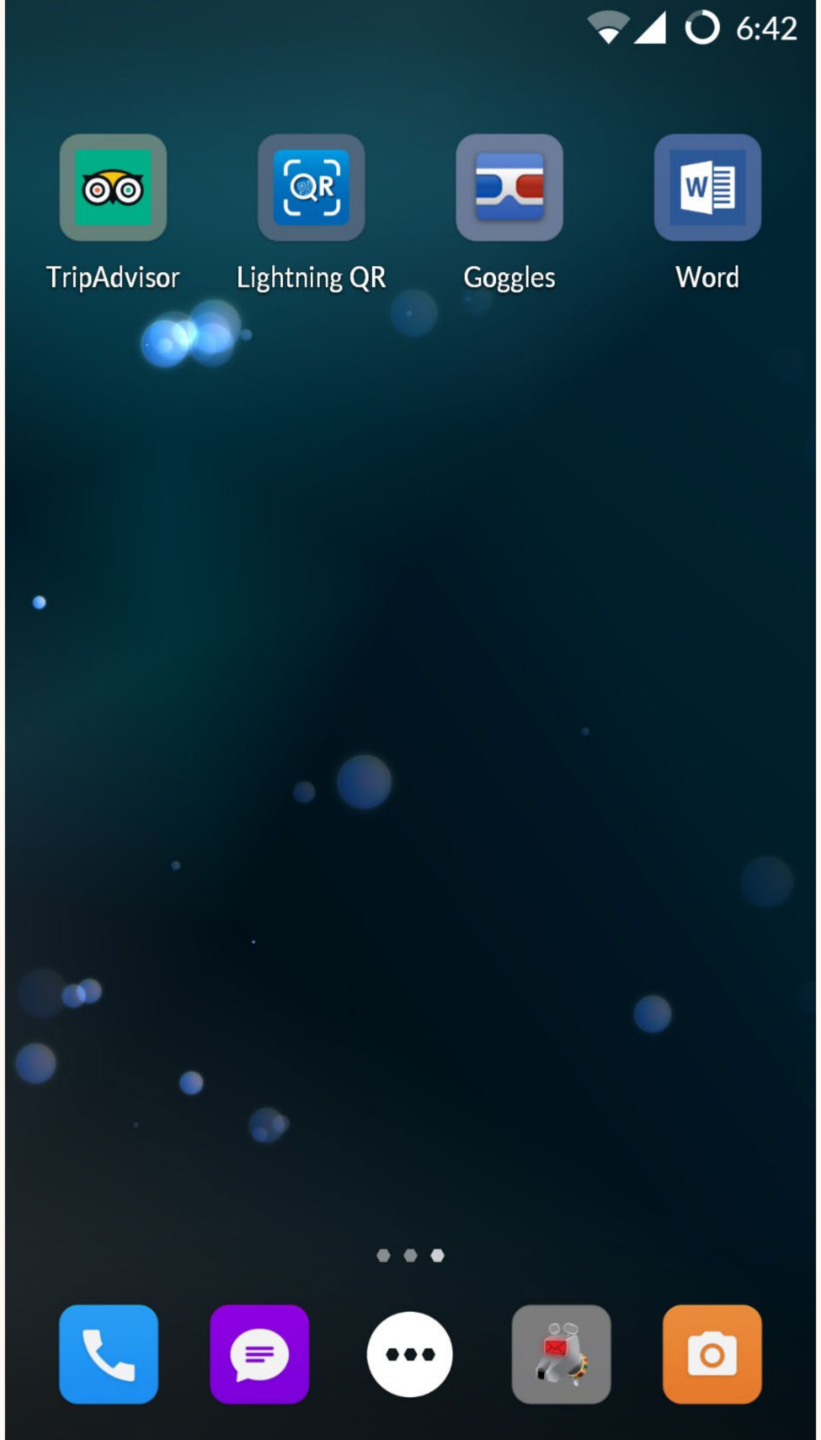
Primary and secondary tasks

- 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:

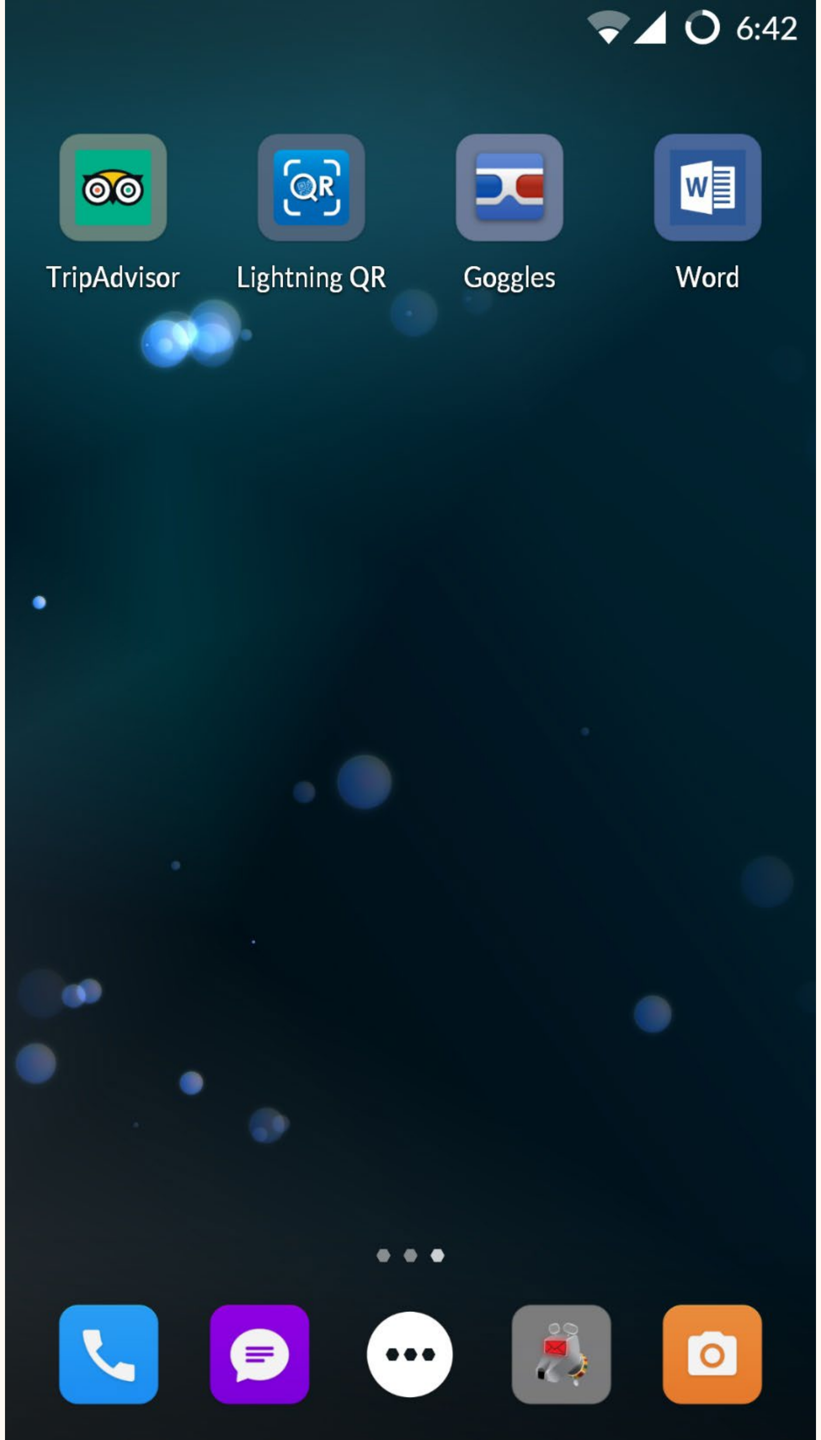
Task: Set an alarm for 7:00am

Task: Set an alarm for 7:00am



Task: Set an alarm for 7:00am

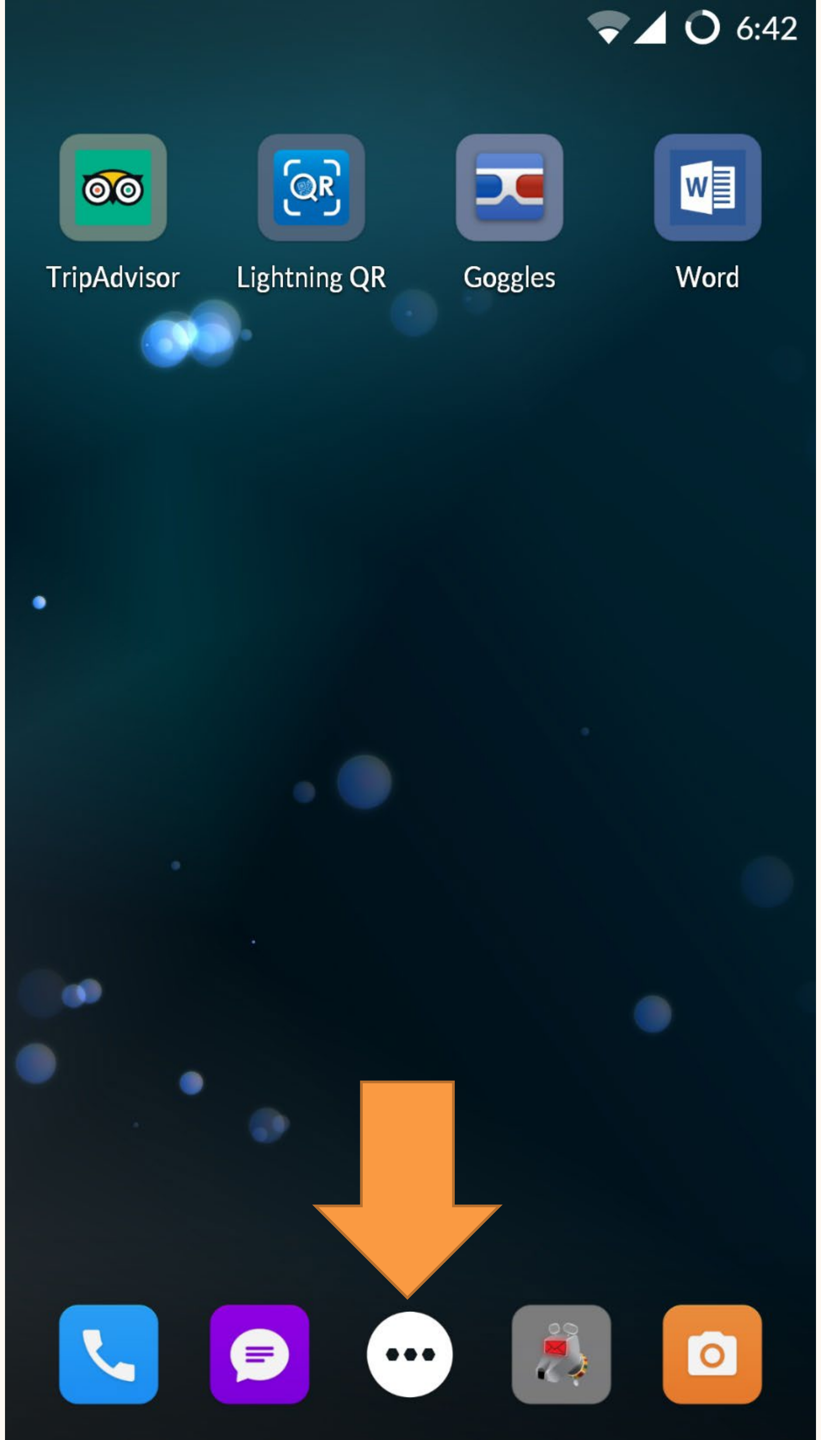
Subtask 1:
Find an app that supports “alarm clock” type functionality.



Task: Set an alarm for 7:00am

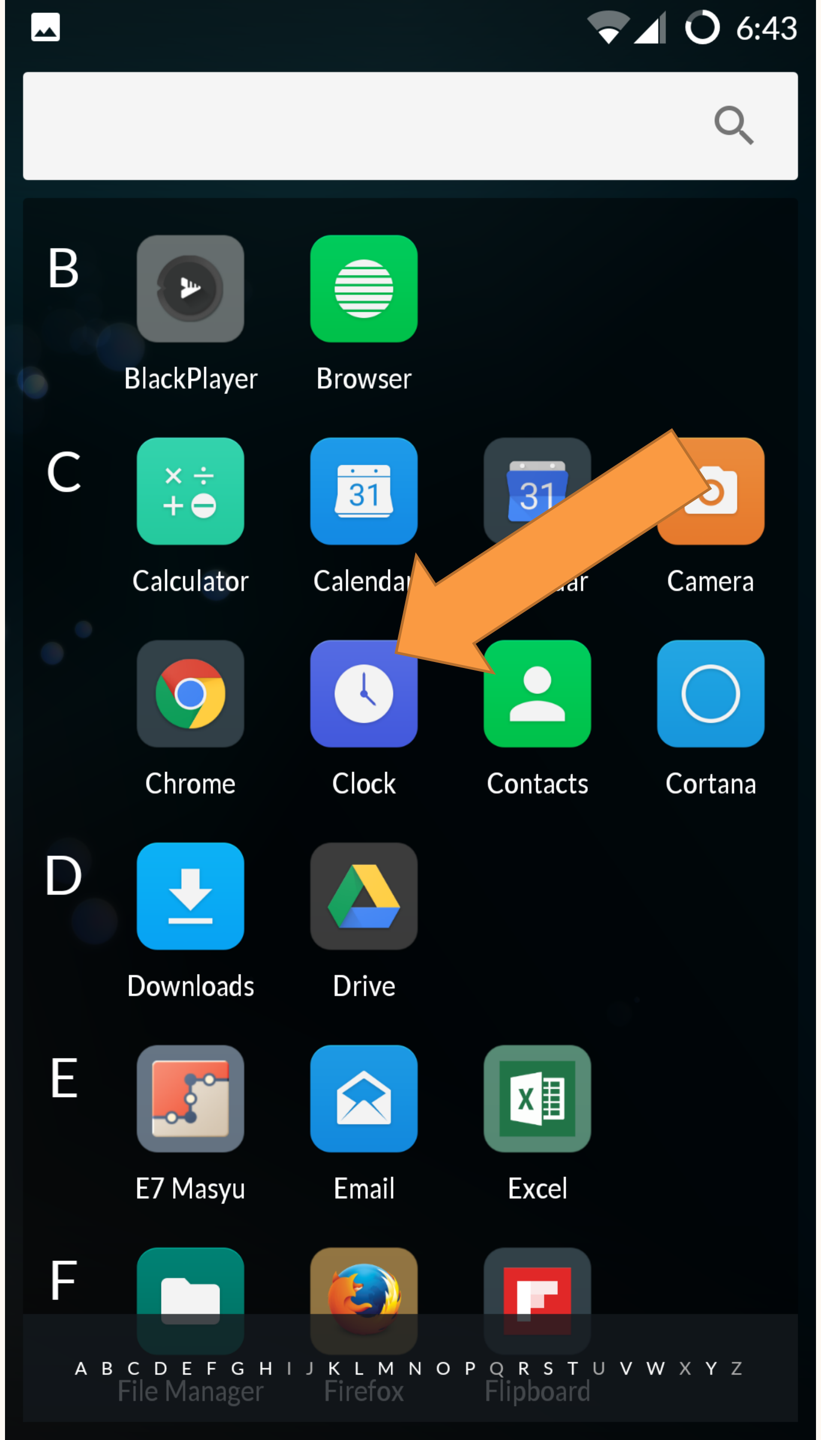
Subtask 1:
Find an app that supports “alarm clock” type functionality.

Subtask 2:
Find a list of all apps



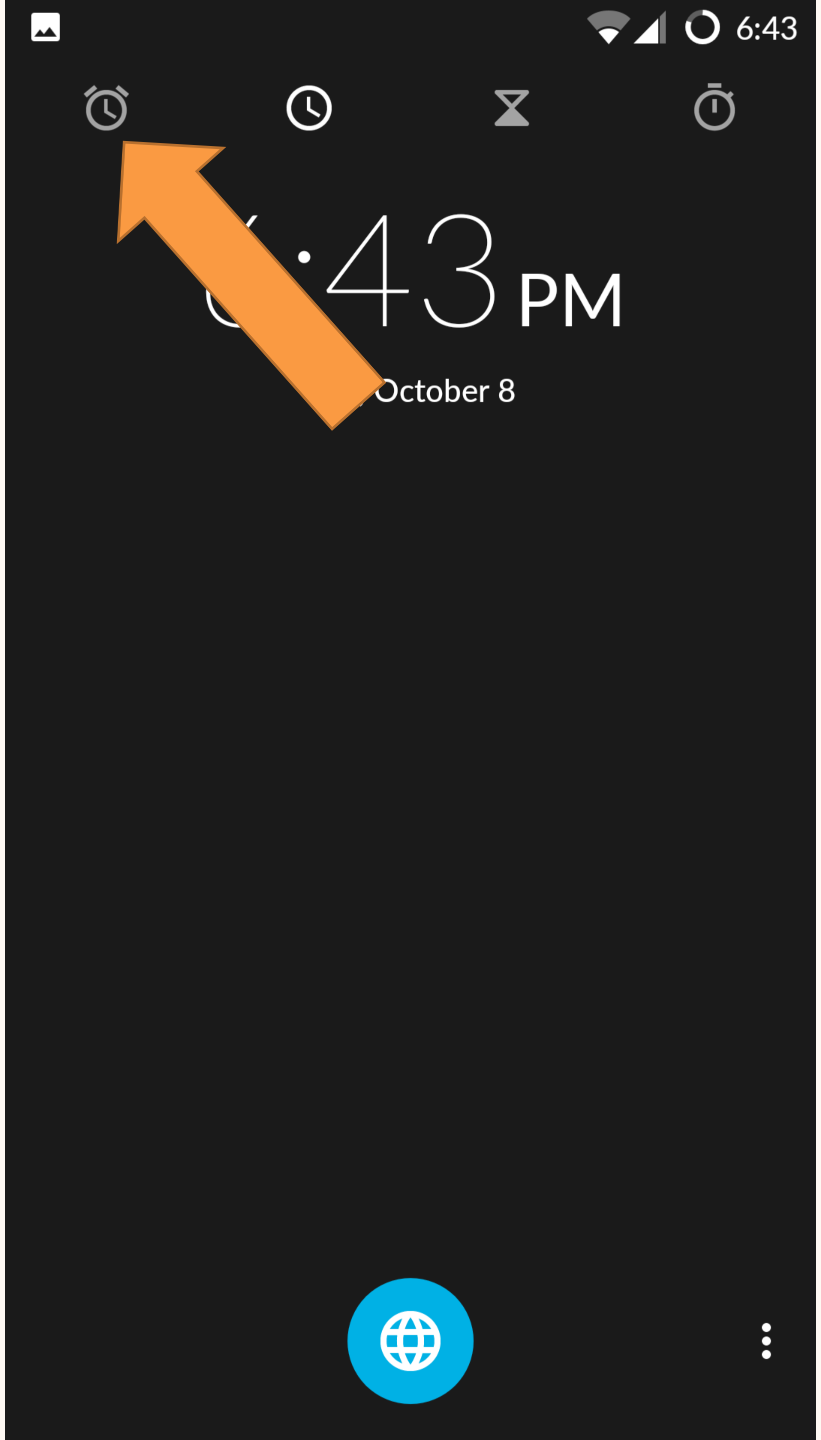
Task: Set an alarm for 7:00am

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



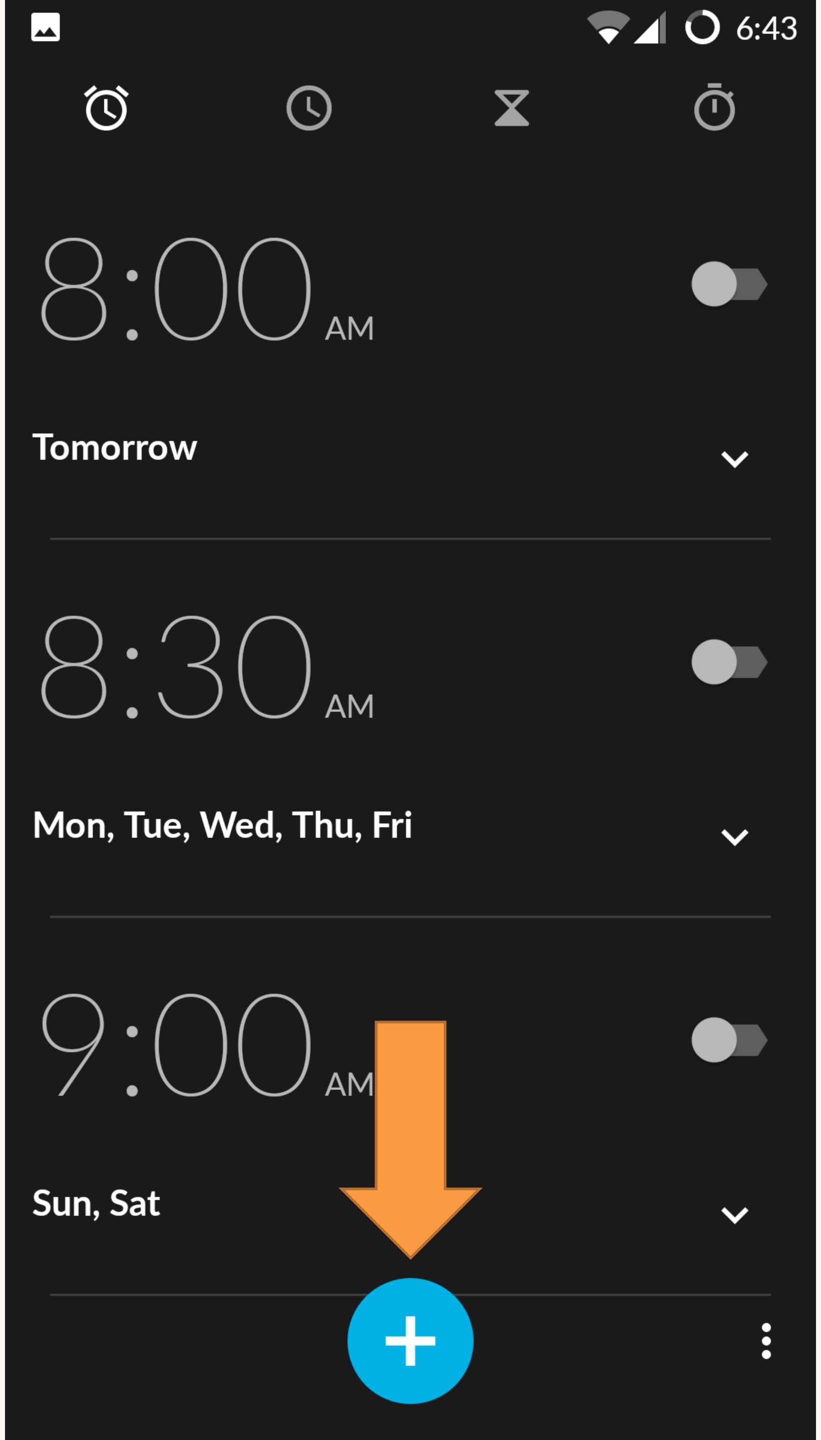
Task: Set an alarm for 7:00am

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



Task: Set an alarm for 7:00am

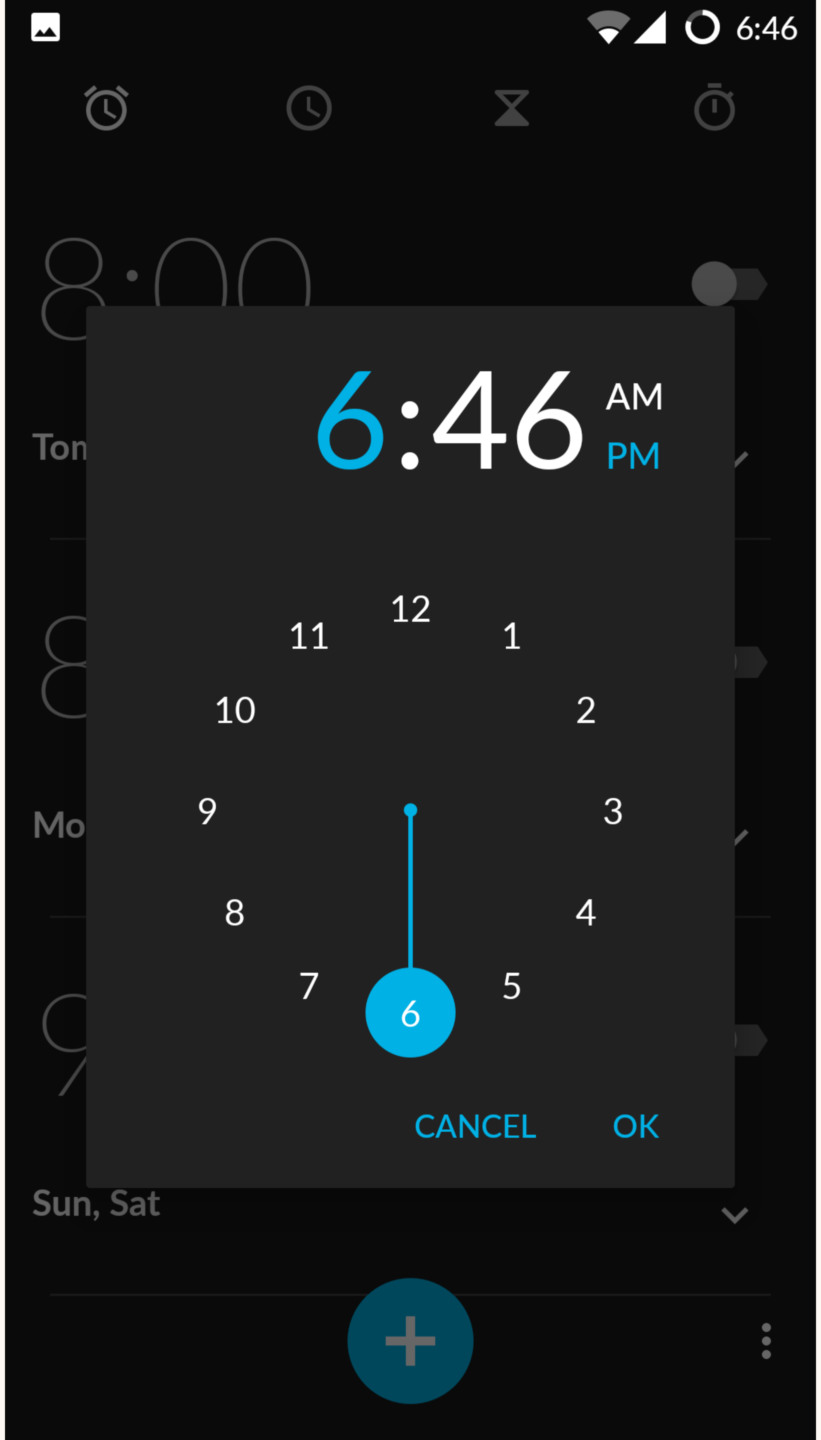
Subtask 3:
Create a new scheduled alarm.



Task: Set an alarm for 7:00am

Subtask 3:
Create a new scheduled alarm.

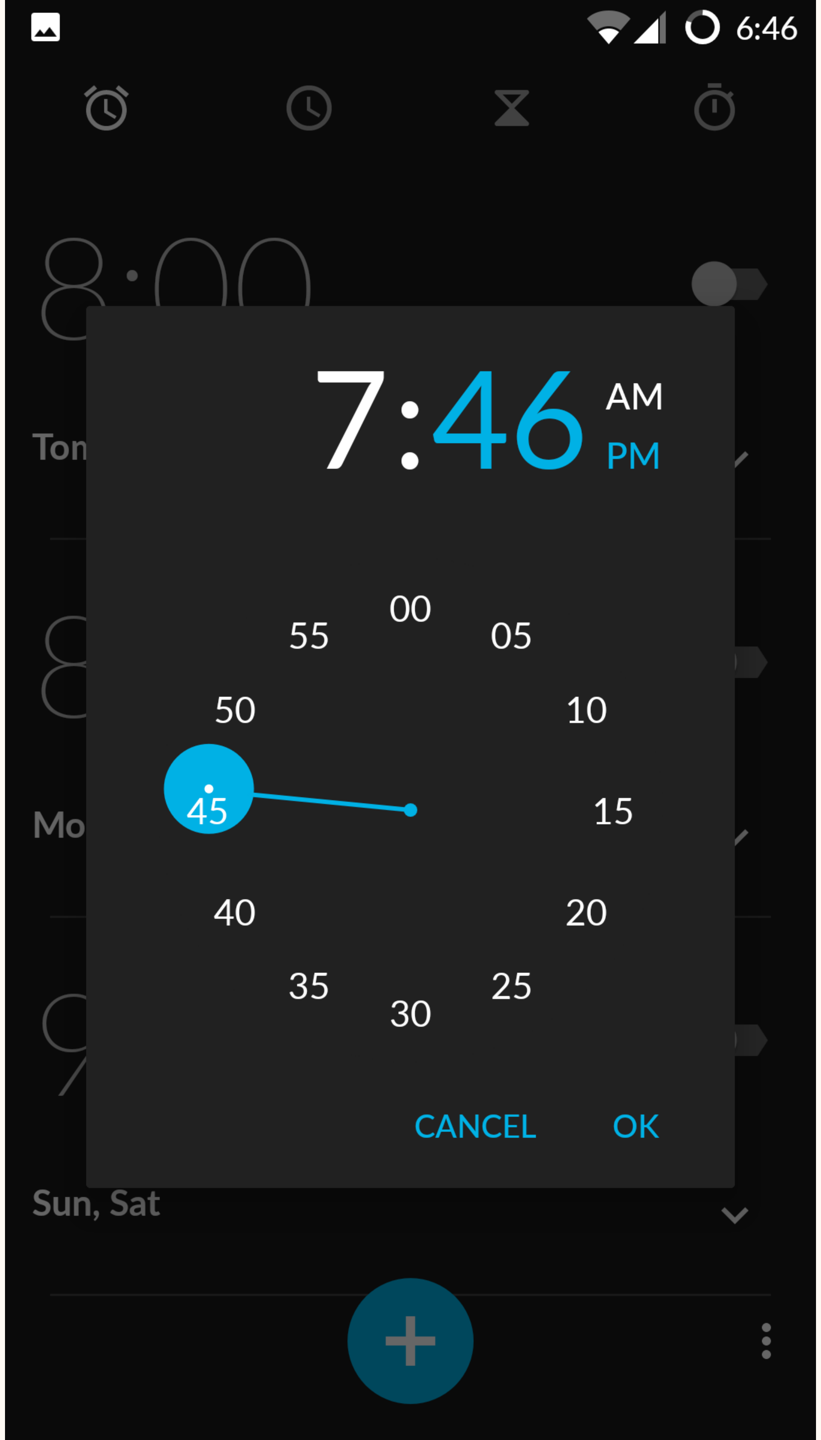
Subtask 4:
Set the hour to 7



Task: Set an alarm for 7:00am

Subtask 3:
Create a new scheduled alarm.

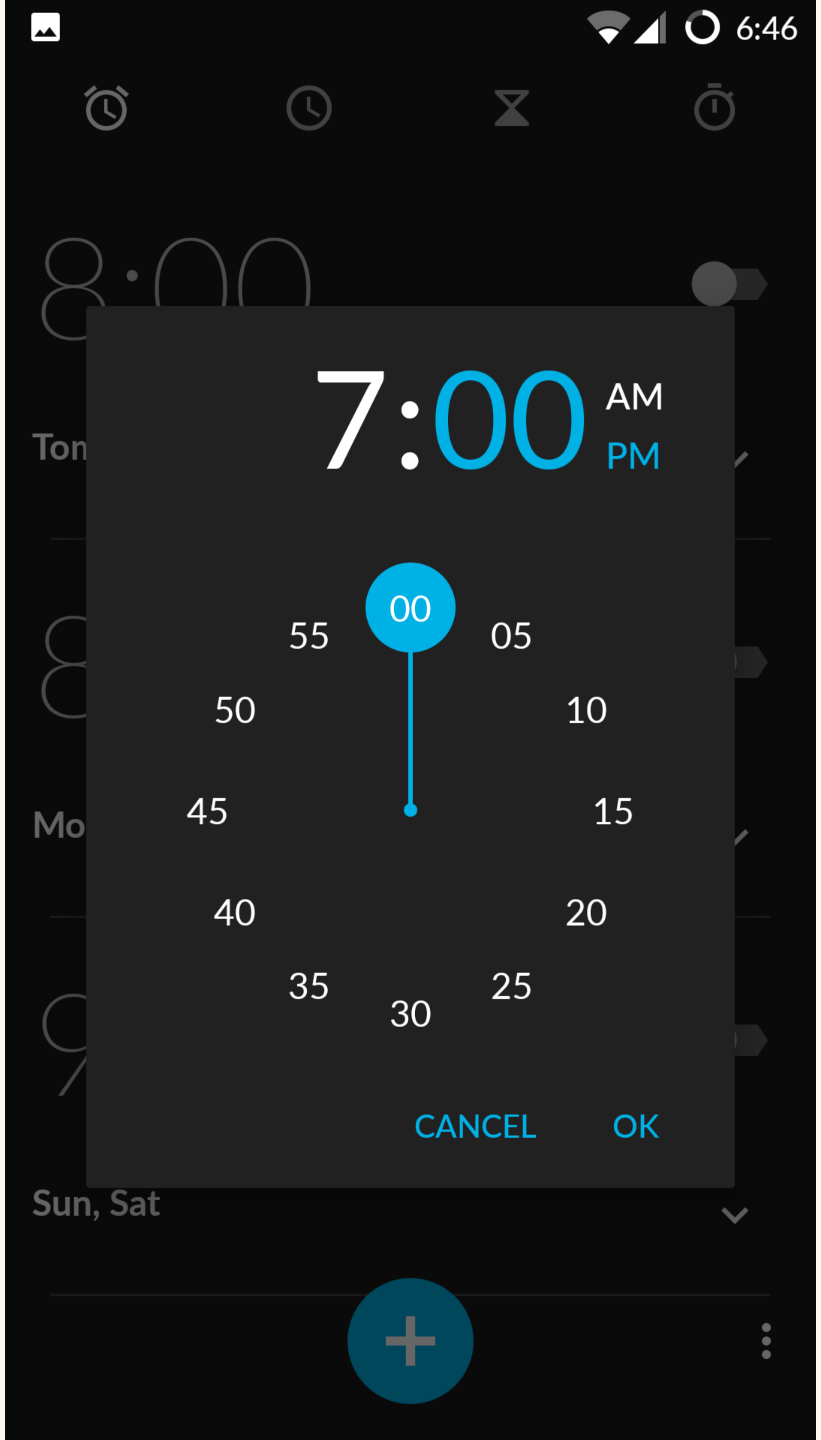
Subtask 5:
Set minutes to 00



Task: Set an alarm for 7:00am

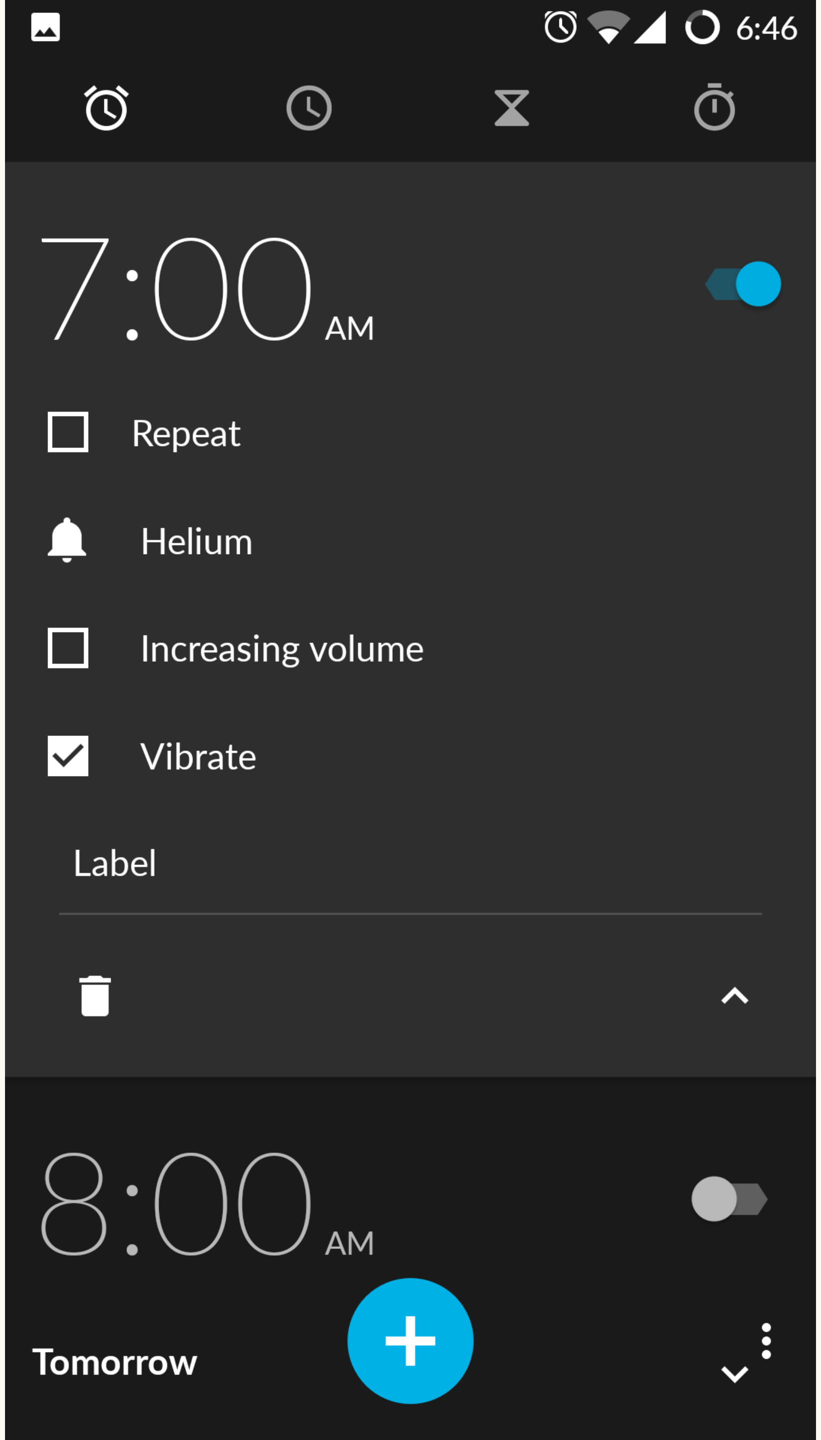
Subtask 3:
Create a new scheduled alarm.

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"



7:00 AM

☐ Repeat

Helium

☐ Increasing volume

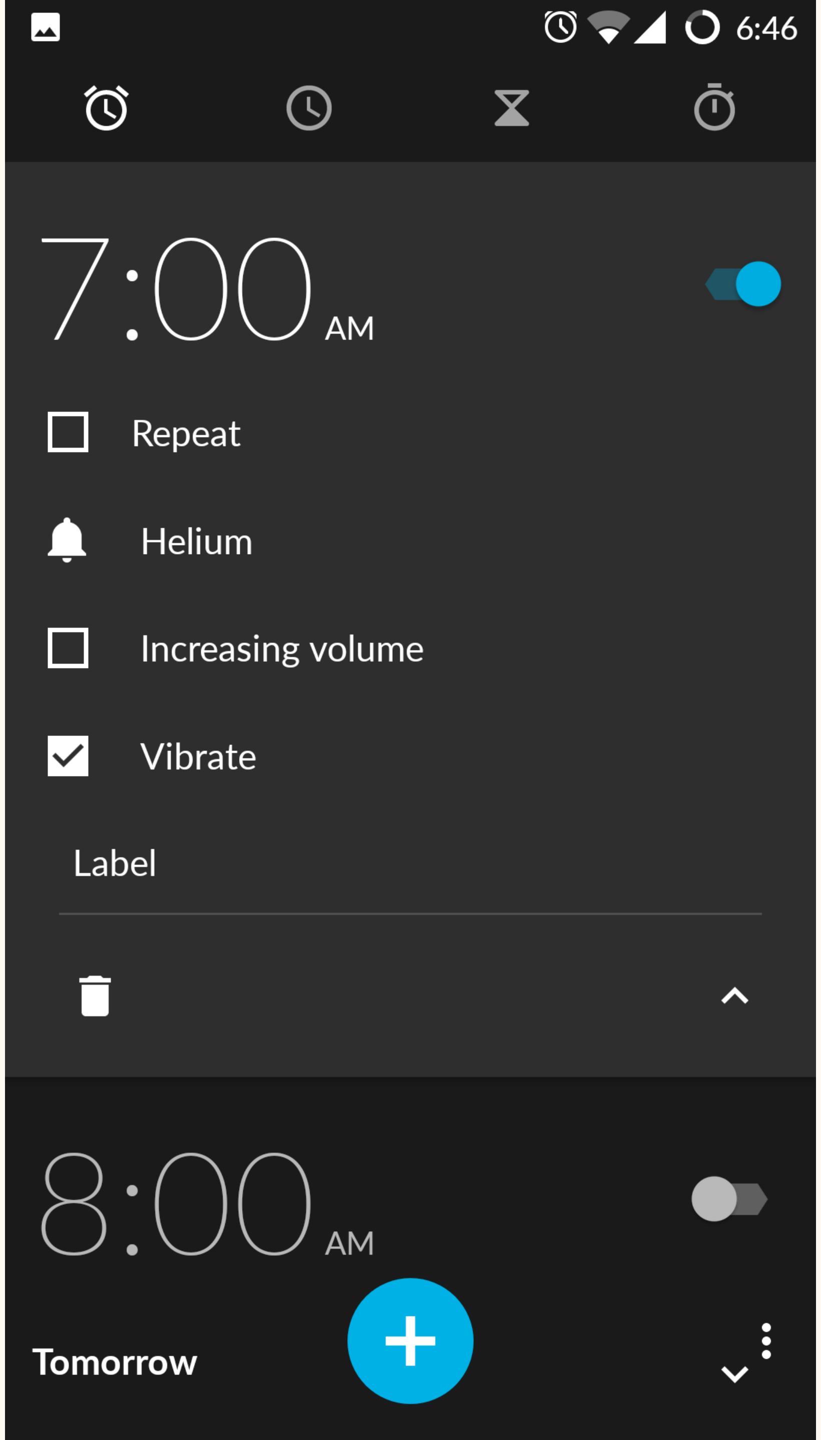
☑ Vibrate

Label

8:00 AM

Tomorrow

Task Completed!



7:00 AM

☐ Repeat

Helium

☐ Increasing volume

☑ Vibrate

Label

8:00 AM

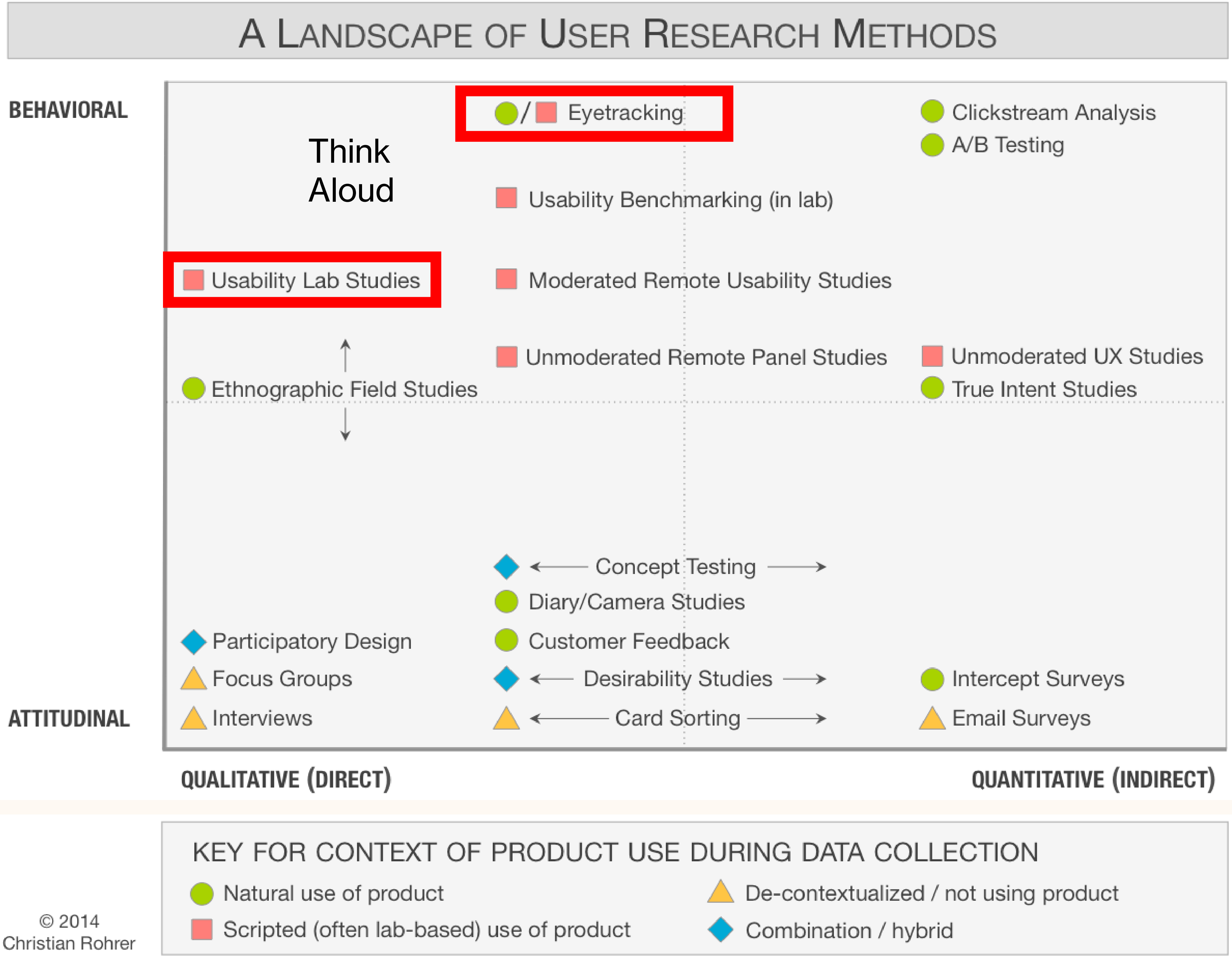
Tomorrow

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

BEHAVIORAL

ATTITUDINAL

QUALITATIVE (DIRECT)

QUANTITATIVE (INDIRECT)

Think Aloud

●/🟥 Eyetracking

● Clickstream Analysis

● A/B Testing

🟥 Usability Benchmarking (in lab)

🟥 Usability Lab Studies

🟥 Moderated Remote Usability Studies

🟥 Unmoderated Remote Panel Studies

🟥 Unmoderated UX Studies

● True Intent Studies

● Ethnographic Field Studies

◆ ← Concept Testing →

● Diary/Camera Studies

● Customer Feedback

◆ Participatory Design

▲ Focus Groups

▲ Interviews

◆ ← Desirability Studies →

▲ ← Card Sorting →

● Intercept Surveys

▲ Email Surveys

KEY FOR CONTEXT OF PRODUCT USE DURING DATA COLLECTION

● Natural use of product

🟥 Scripted (often lab-based) use of product

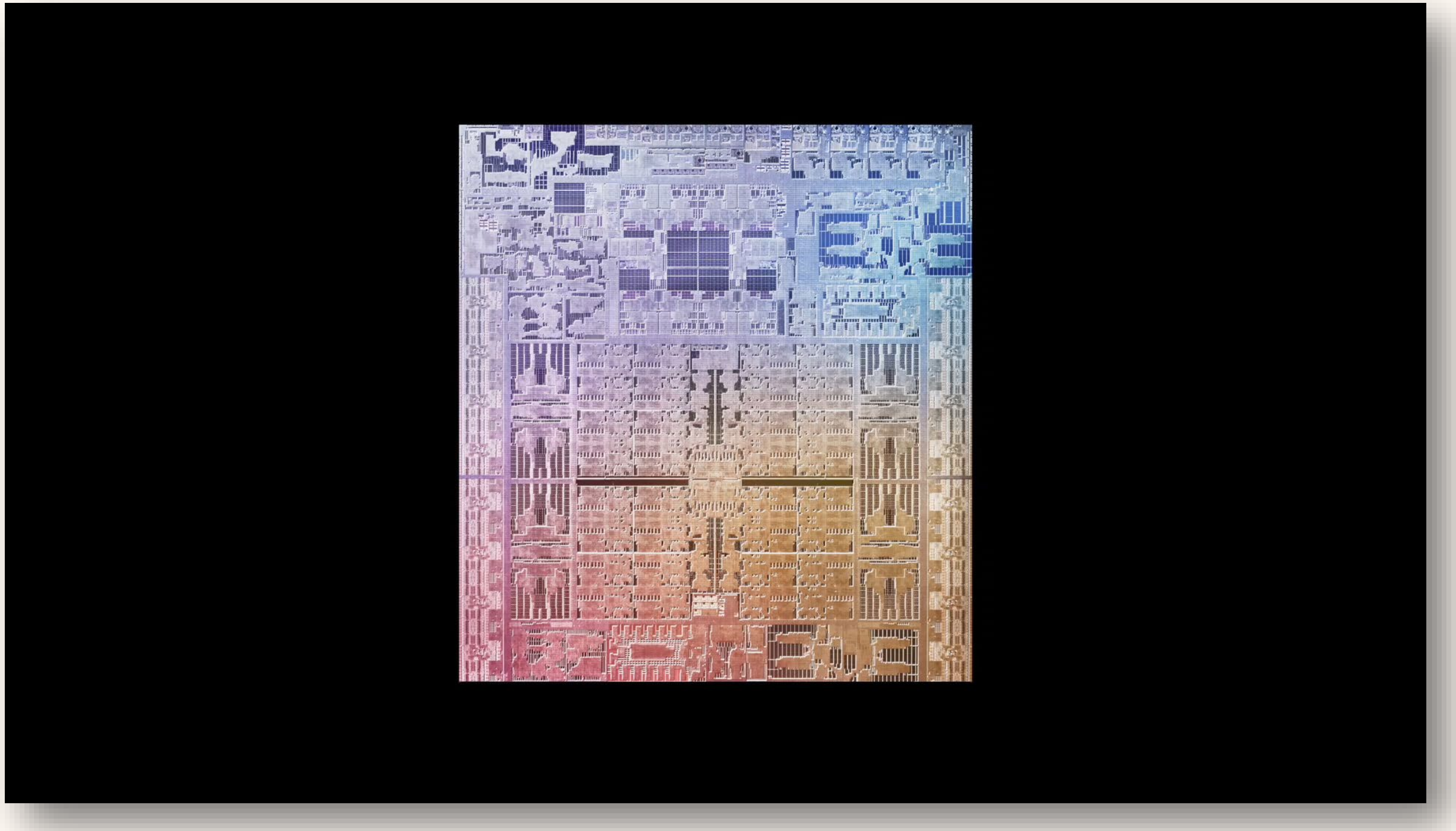
▲ De-contextualized / not using product

◆ Combination / hybrid

© 2014 Christian Rohrer

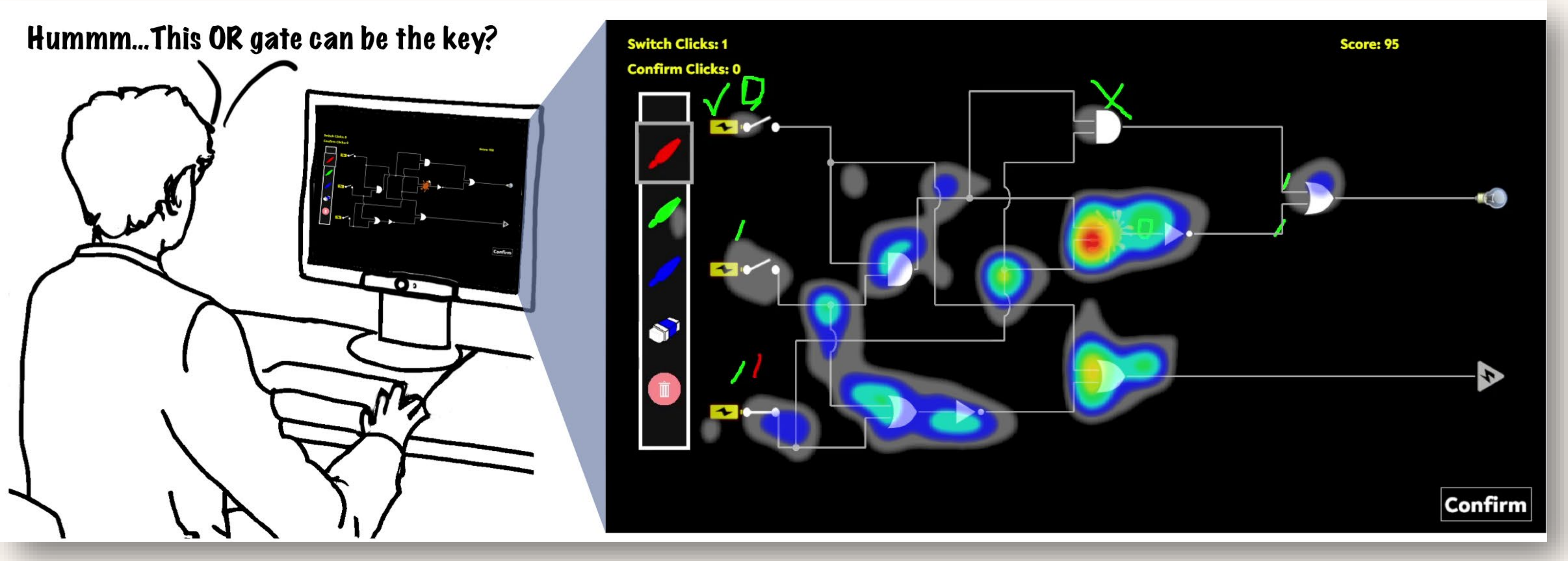
https://www.nngroup.com/articles/which-ux-research-

How people perform (hardware) reverse engineering?

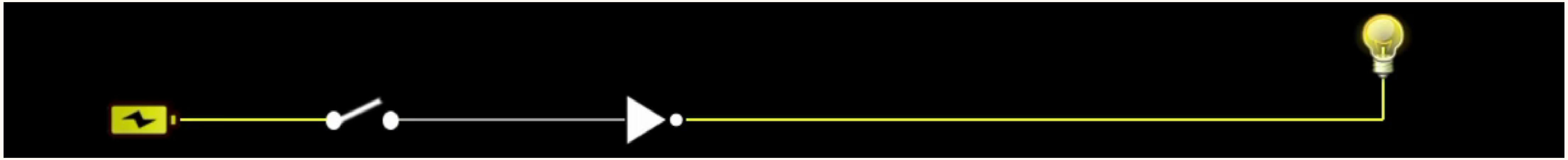


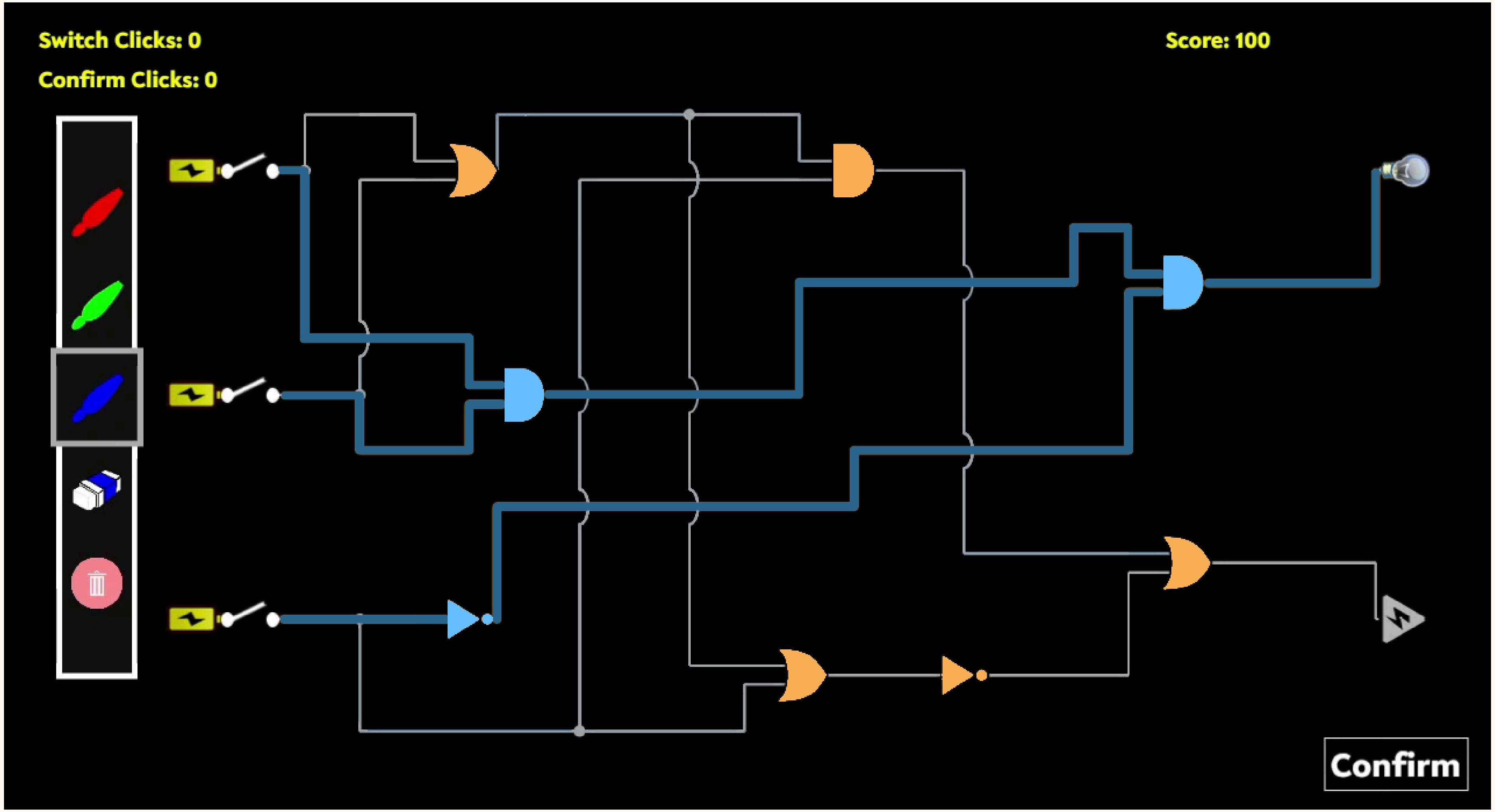
https://www.apple.com/in/newsroom/2022/03/apple-unveils-m1-ultra-the-worlds-most-powerful-chip-for-a-personal-computer/

How people perform (hardware) reverse engineering?

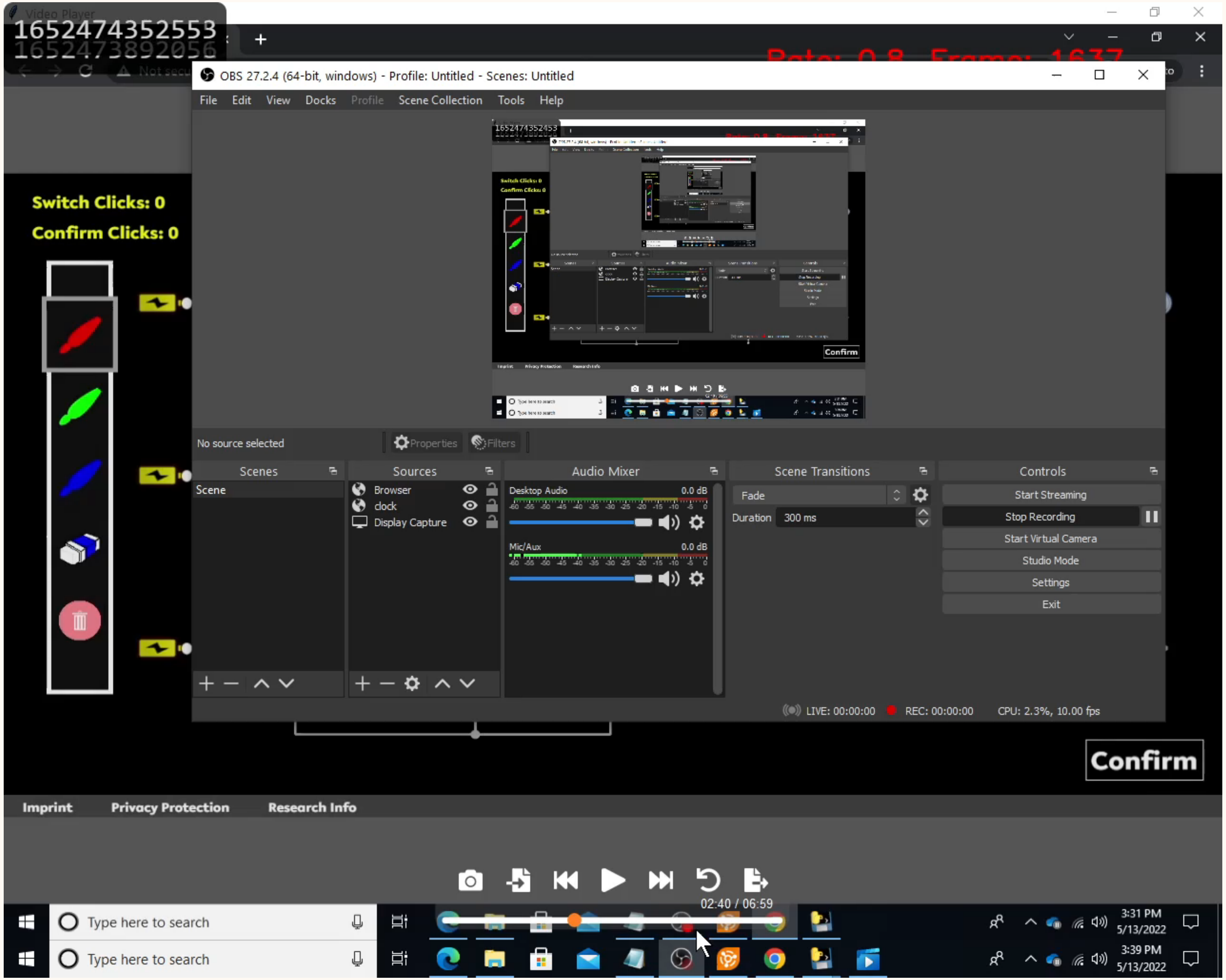


René Walendy, Markus Weber, Jingjie Li, Steffen Becker, Carina Wiesen, Malte Elson, Younghyun Kim, Kassem Fawaz, Nikol Rummel, and Christof Paar. I see an IC: A Mixed-Methods Approach to Study Human Problem-Solving Processes in Hardware Reverse Engineering. ACM CHI 2024 (to appear)




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

KAPWING



1652474352553
1652473892056

OBS 27.2.4 (64-bit, windows) - Profile: Untitled - Scenes: Untitled

Switch Clicks: 0
Confirm Clicks: 0

No source selected

Scene

Browser
clock
Display Capture

Desktop Audio 0.0 dB
Mic/Aux 0.0 dB

Fade
Duration 300 ms

LIVE: 00:00:00 REC: 00:00:00 CPU: 2.3%, 10.00 fps

02:40 / 06:59

3:31 PM
5/13/2022

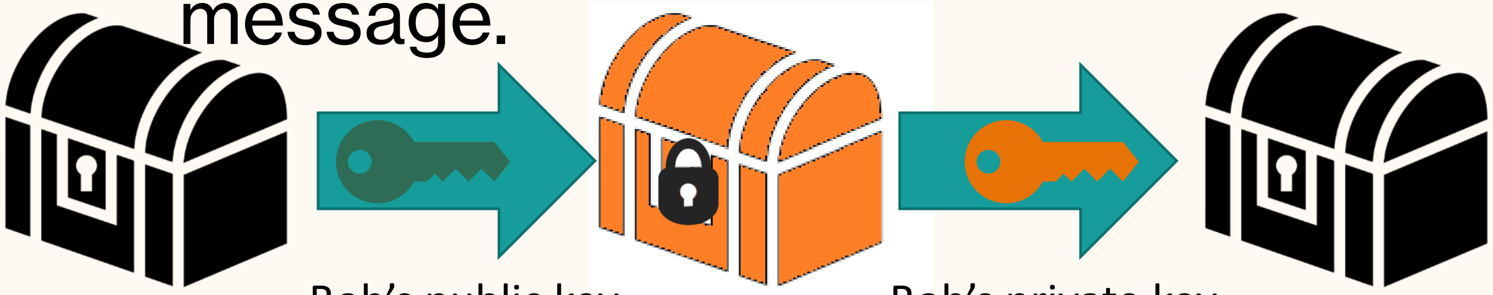
3:39 PM
5/13/2022

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.



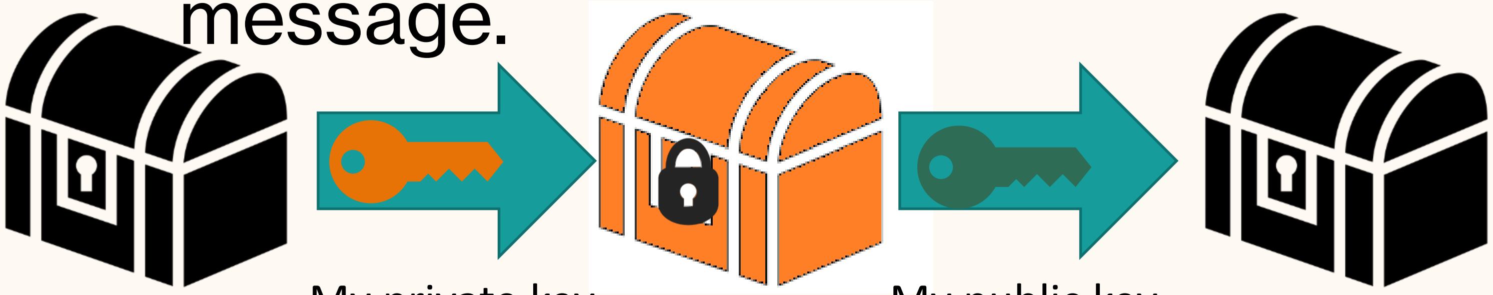
My public key

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

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+lUTuLEVnUzlo
XAUXH
KozHejfV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnq0CplgXcN2GJxfEHHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41
Ot
1zgxdMQkgb2H2xw28RYfYkdDouetelkOrFLrCy9ZF9KdMhA1eBH94KnwlQshdiZ
R
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u233
9hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuaWVh
IDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIACkFAlYKYvECGyMFCQlmAYAHC
wkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QA
qew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljI2b+Q75/5t+EgXOHpR0PIxf
G
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTglvEYG3so2VueQoeXcq3dbY
p
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5albNQhQDPcTo0DgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQkJ7uQ5eFh4ZhsMgOmzLQ
D4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrxuJ8YfHWS0hEScNOcYC2P8q20IJwwE2
6T
lpdtrwCqtB1LYW1pIFZhbmllYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAI
b
IwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkB
AAoJEJN2
zGX38dl9JJAIAIW0rxrlYsrmKS6CbW8MgTxxTDOXaCt1b7F0W0QZHsklUQhEcE
+a
XBYib1A5uHaatLfyjeXaD3qMEoZnQHoYMGE0GKu00wWsbhfoQzHPgwzRLkD1i7
5M
Blbaww0KWoVB9e4AkMakXJCnF5BXeo6AHRL2v15V205DikVnlCRXocKtu8b7Ln
kM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JlLMDSevjfT7zSRSl/YP3fOfZ6N4bc+KOdwPM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAlTnSpEACgkQjy
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

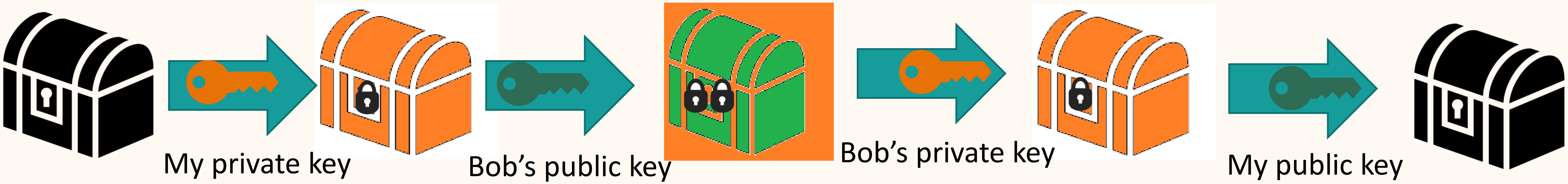
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+lUTuLEVnUzlo
XAUXH
KozHejfV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnq0CplgXcN2GJxfEHHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41
Ot
1zgxdMQkgb2H2xw28RYfYkdDouetelkOrFLrCy9ZF9KdMhA1eBH94KnwlQshdiZ
R
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u233
9hvH0
B/h+7xLM6FQbOUZQ9BD5w7lQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuaWVh
IDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIACkFAlYKYvECGyMFCQlmAYAHC
wkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QA
qew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljI2b+Q75/5t+EgXOHpR0Plxf
G
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTglvEYG3so2VueQoeXcq3dbY
p
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5albNQhQDPcTo0DgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrlPBJ2VYCDzQkJ7uQ5eFh4ZhsMgOmzLQ
D4
YiGr5welMFwAvxZOaRxEa9Vf48jiWvrxuJ8YfHWS0hEScNOcYC2P8q20lJwwE2
6T
lpdtrwCqtB1LYW1plFZhbmllYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAI
b
IwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkB
AAoJEJN2
zGX38dl9JJAIAIW0rxrlYsrmKS6CbW8MgTxxTDOXaCt1b7F0W0QZHsklUQhEcE
+a
XBYib1A5uHaatLfyjeXaD3qMEoZnQHoYMGE0GKu00wWsbhfoQzHPgwzRLkD1i7
5M
Blbaww0KWoVB9e4AkMakXJCnF5BXeo6AHRL2v15V205DikVnlCRXocKtu8b7Ln
kM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JlLMDSevjfT7zSRSl/YP3fOfZ6N4bc+KOdwPM7u5lyoeu9zh
pzibv3ge7VhH2xlWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAlTnSpEACgkQjy
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.

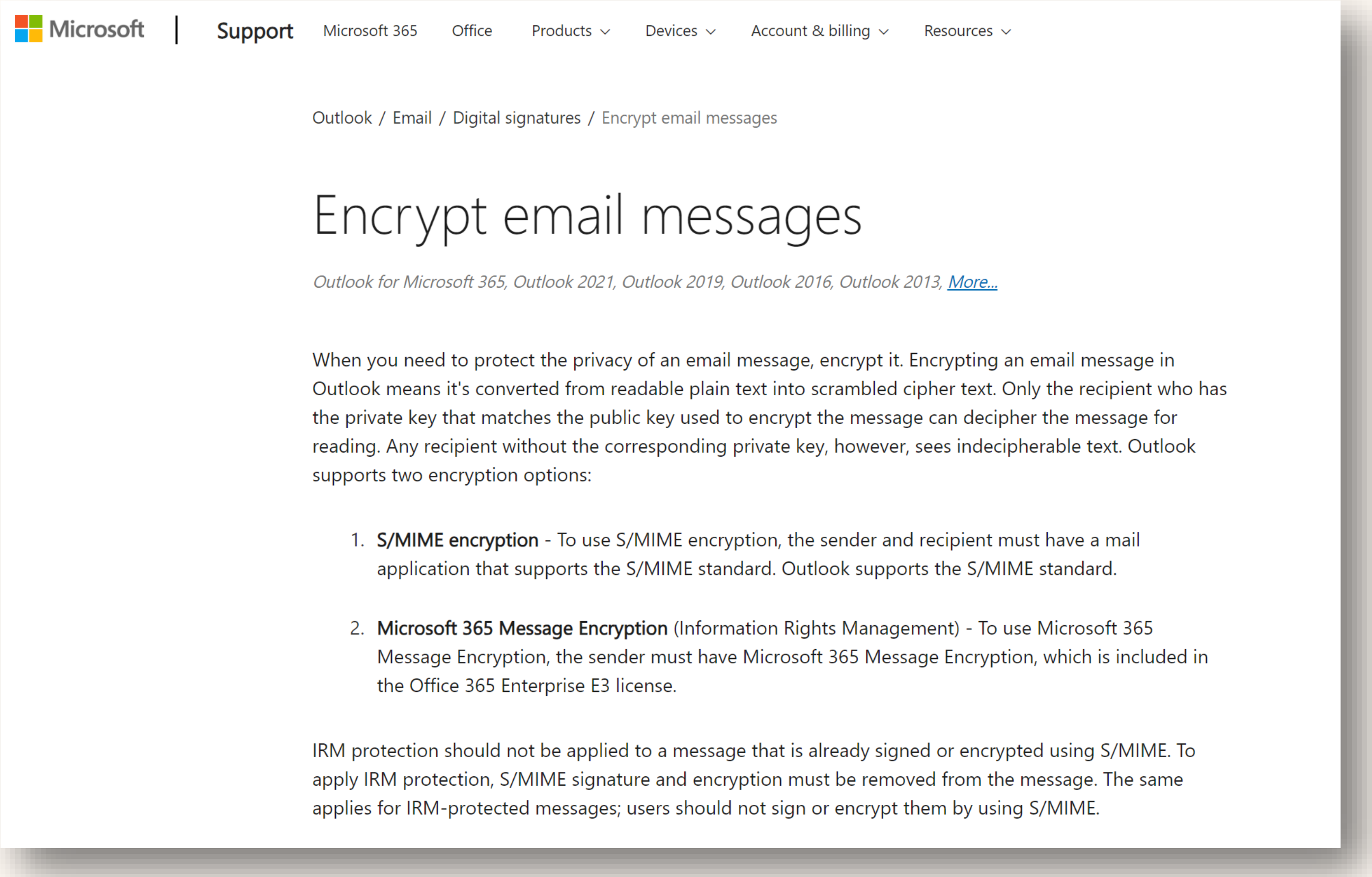
Authentication assumptions

- 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 ☺)



Microsoft | Support Microsoft 365 Office Products Devices Account & billing Resources

Outlook / Email / Digital signatures / Encrypt email messages

Encrypt email messages

Outlook for Microsoft 365, Outlook 2021, Outlook 2019, Outlook 2016, Outlook 2013, More...

When you need to protect the privacy of an email message, encrypt it. Encrypting an email message in Outlook means it's converted from readable plain text into scrambled cipher text. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading. Any recipient without the corresponding private key, however, sees indecipherable text. Outlook supports two encryption options:

1. **S/MIME encryption** - To use S/MIME encryption, the sender and recipient must have a mail application that supports the S/MIME standard. Outlook supports the S/MIME standard.
2. **Microsoft 365 Message Encryption** (Information Rights Management) - To use Microsoft 365 Message Encryption, the sender must have Microsoft 365 Message Encryption, which is included in the Office 365 Enterprise E3 license.

IRM protection should not be applied to a message that is already signed or encrypted using S/MIME. To apply IRM protection, S/MIME signature and encryption must be removed from the message. The same applies for IRM-protected messages; users should not sign or encrypt them by using S/MIME.

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

Take-home

- **(Blog)** Chiasson, S., van Oorschot, P.C. and Biddle, R., 2006, August. A Usability Study and Critique of Two Password Managers. In *USENIX Security Symposium* (Vol. 15, pp. 1-16).
- **(Blog)** Washington Post - Apple's new Vision Pro is a privacy mess waiting to happen