ECE750: Usable Security and Privacy

Think Aloud

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

UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

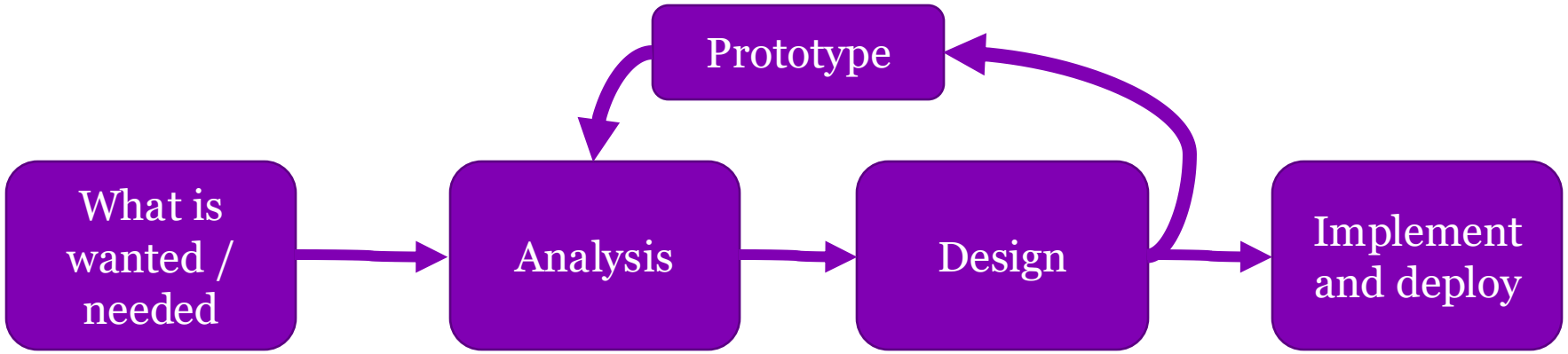
First, something random...

- 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

- Lab studies
- Think aloud studies
- Tasks and subtasks

Project lifecycle



Designing and Running a Study

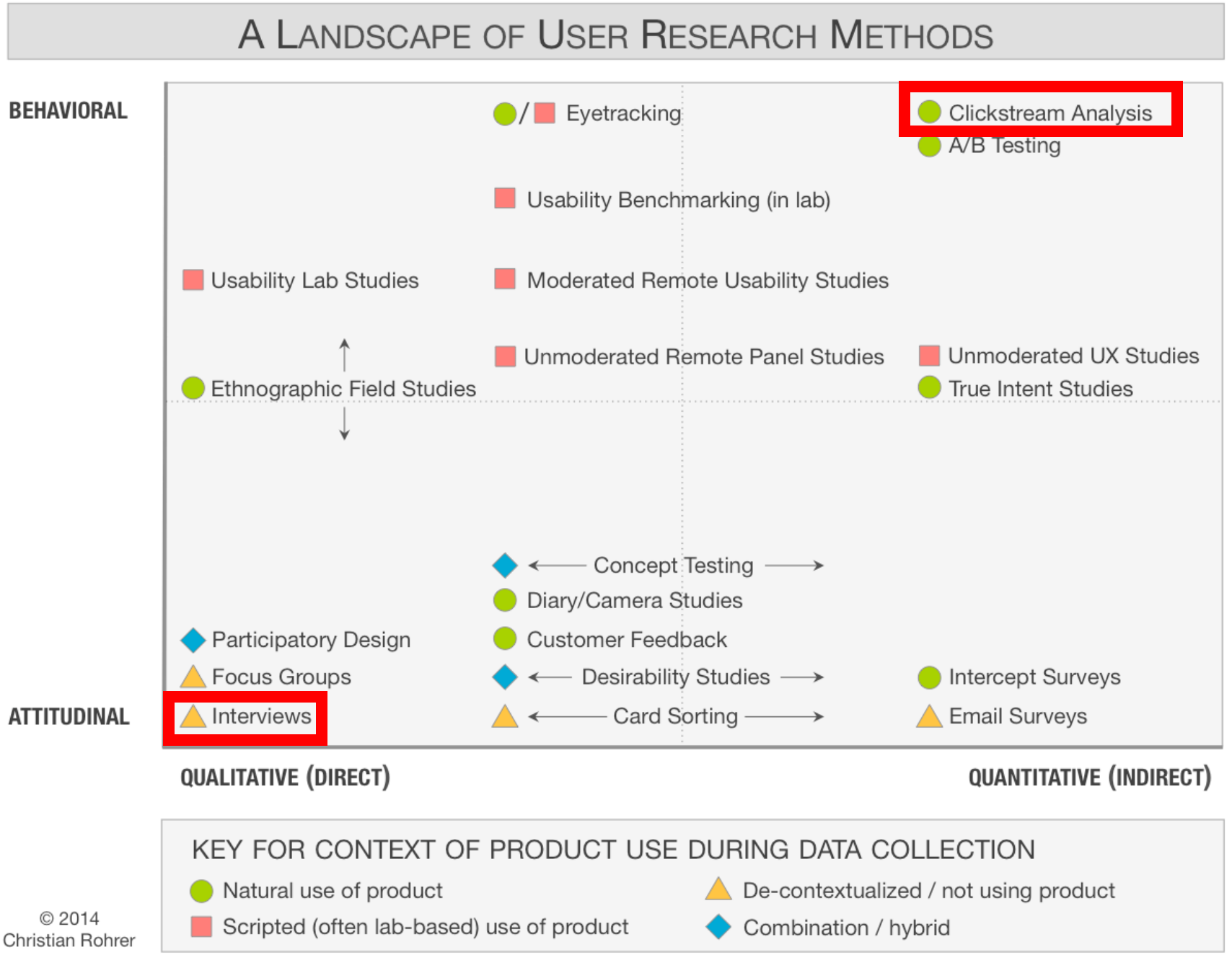
- Identify research questions
- Decide on the type of study and demographics
- Design study protocol
- Obtain ethics approval
- Design study
- Plan data analysis approach
- Pilot studies
- Revise study….
- Possibly pilot again
- Run main study with participants
- Analyze data
- (For Qualitative) iterate understanding of results
- Write paper

Methodologies: Many ways to test usability

- A/B Testing
- Affinity Diagraming
- Card Sorting
- Case Studies
- Cognitive Walkthrough
- Competitive Testing
- Critical Incident Technique
- Customer Experience Audit
- Desirability Testing
- Diary Studies
- Ergonomic Analysis
- Experience Sampling
- Experiments
- Eye tracking
- Fly-on-the-wall Observation
- Focus Groups
- Graffiti Walls
- Heuristic Evaluation
- Interviews
- KJ Technique
- Observation
- Participatory Action Research

Interviews – users express their attitudes by providing qualitative answers to questions.

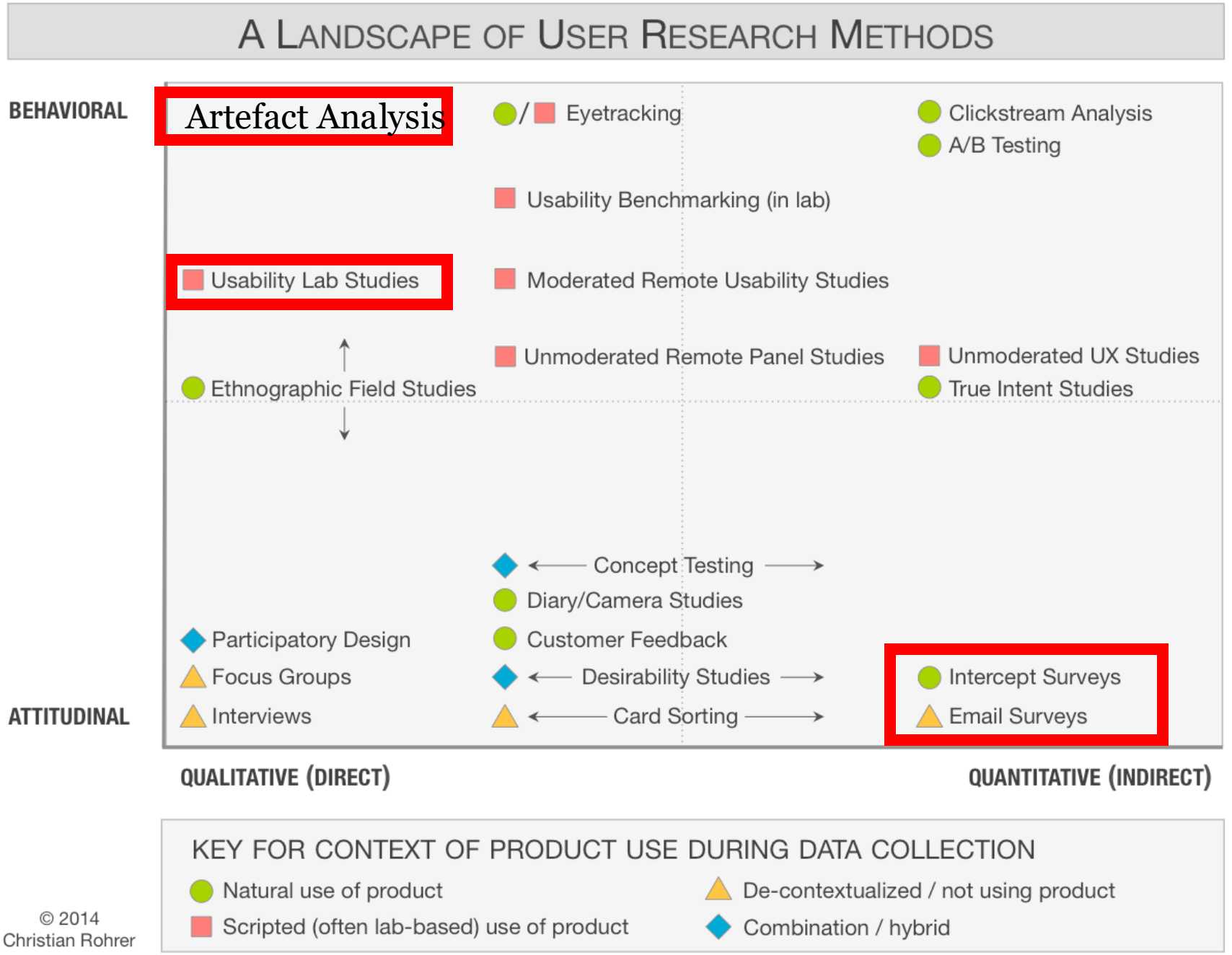
Clickstream Analysis – measure the links users click on to get quantitative data on what users do.



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

Lab Studies – users perform a set of tasks often talking about their experience as they do so.

Surveys – Ask about user opinion often with multiple choice answers.



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

Think-pair-share

For each of the following problems, name one behavioral question you could ask and one attitudinal question.

- Mobile phone login
- Cookie dialogs
- Fake news
- Encryption of all webpages by default

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

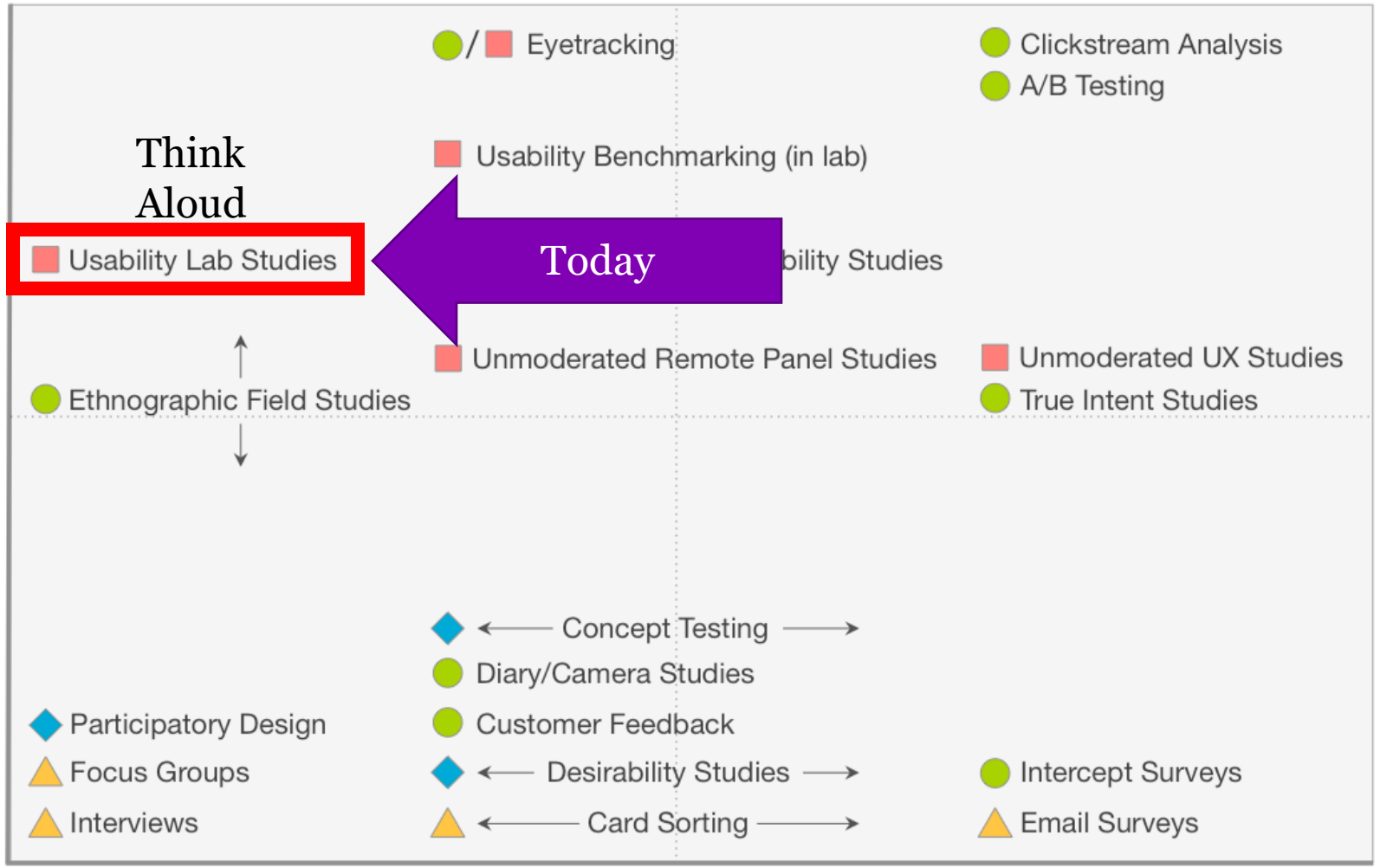
- Basic idea: Have a participant come to a physical place (lab) and interact with the interface there
- You setup the lab so it mimics the situation you want to test
- Pros
  - **Full control over the environment** so limited confounds
  - **Detailed data** from each subject
  - Ability to **ask them 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.

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

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-

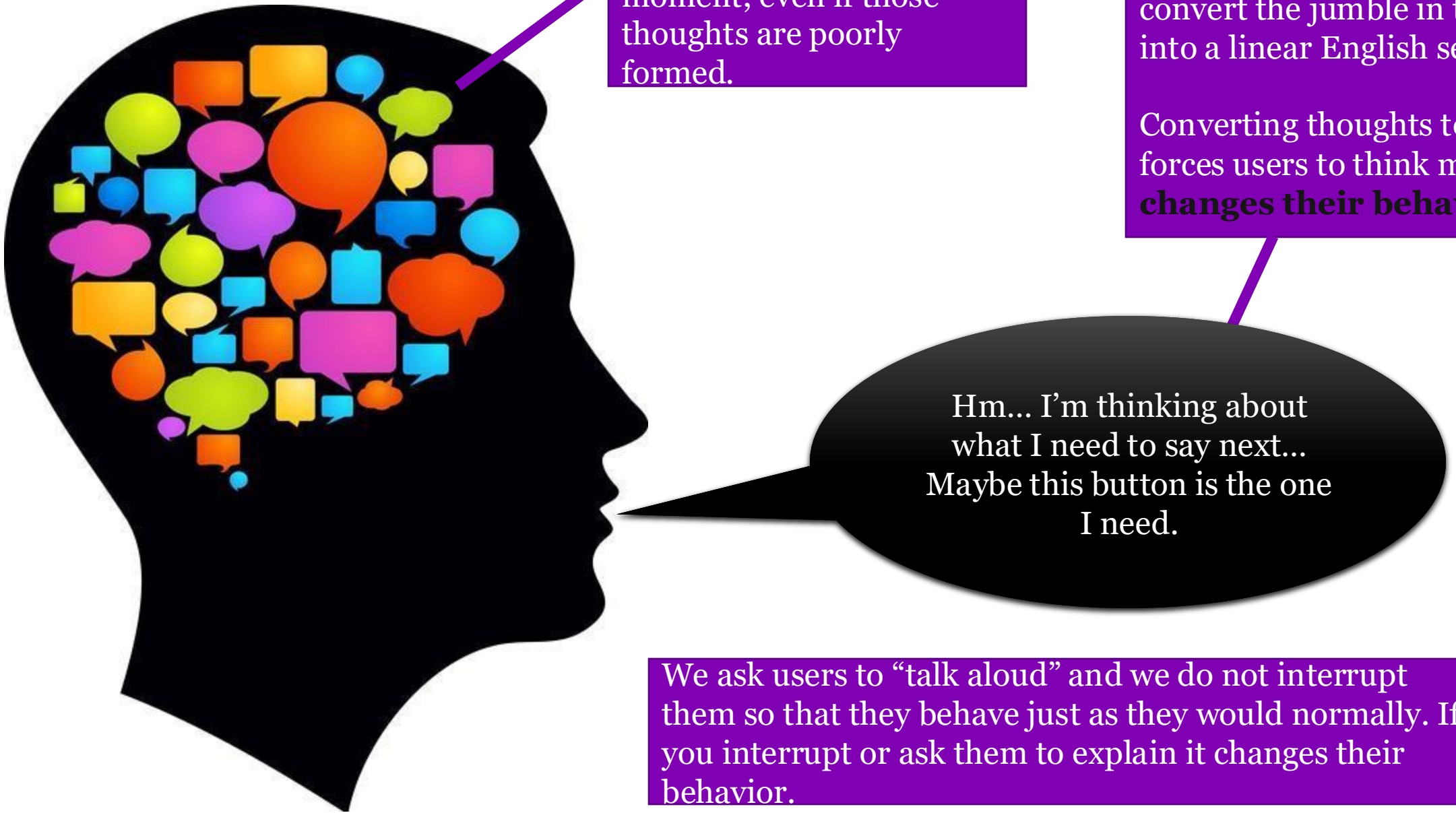
Think aloud

- 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 to conduct one participant at a time
  - Better if done in person
  - (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.

Non-security frameworks: Cognitive Process Theory of Writing

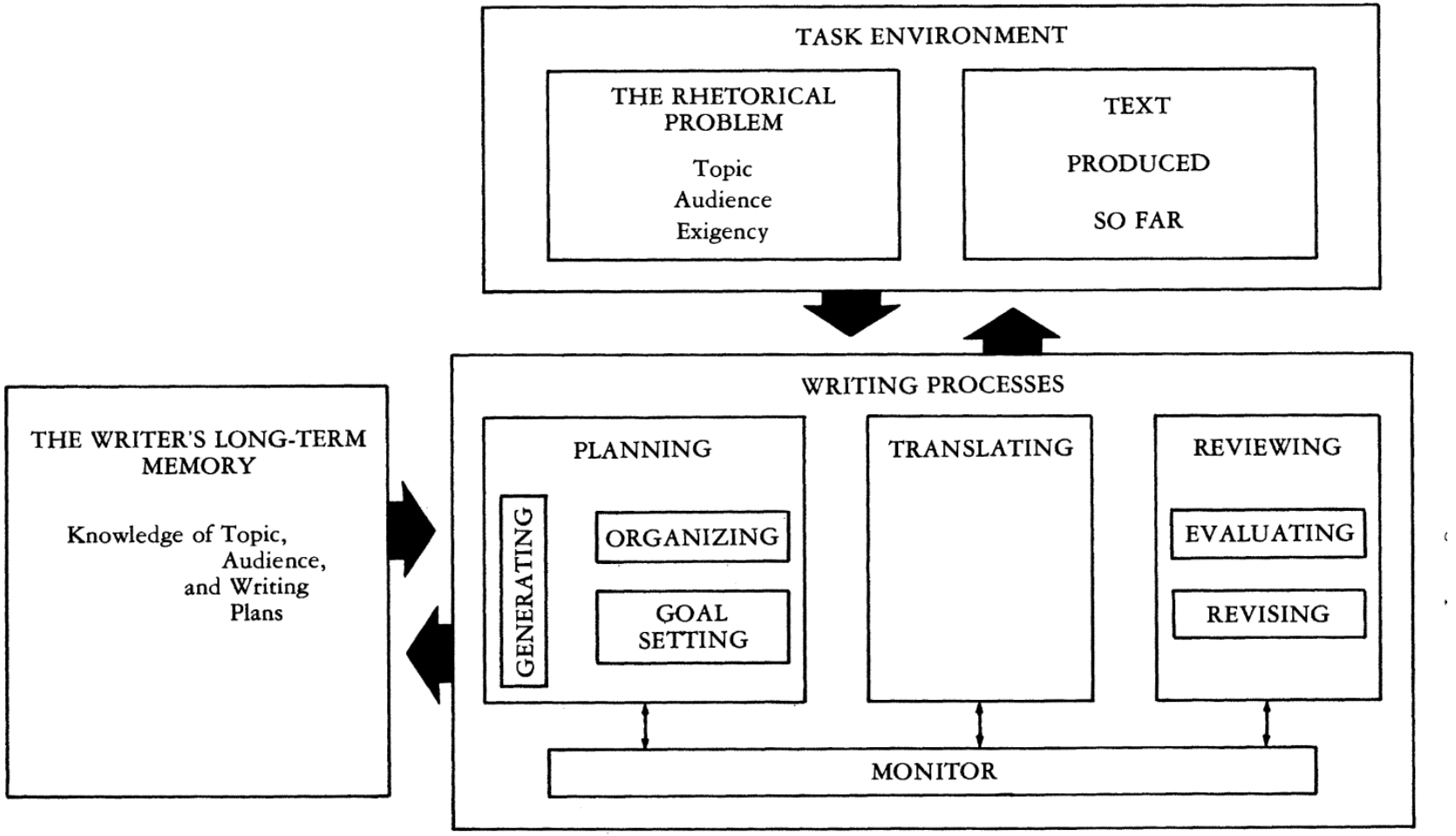


Figure 1. Structure of the writing model. (For an explanation of how to read a process model, please see Footnote 11, pages 386-387.)

"A cognitive process theory of Writing" by Linda Flower and John R. Hayes

What is different about security

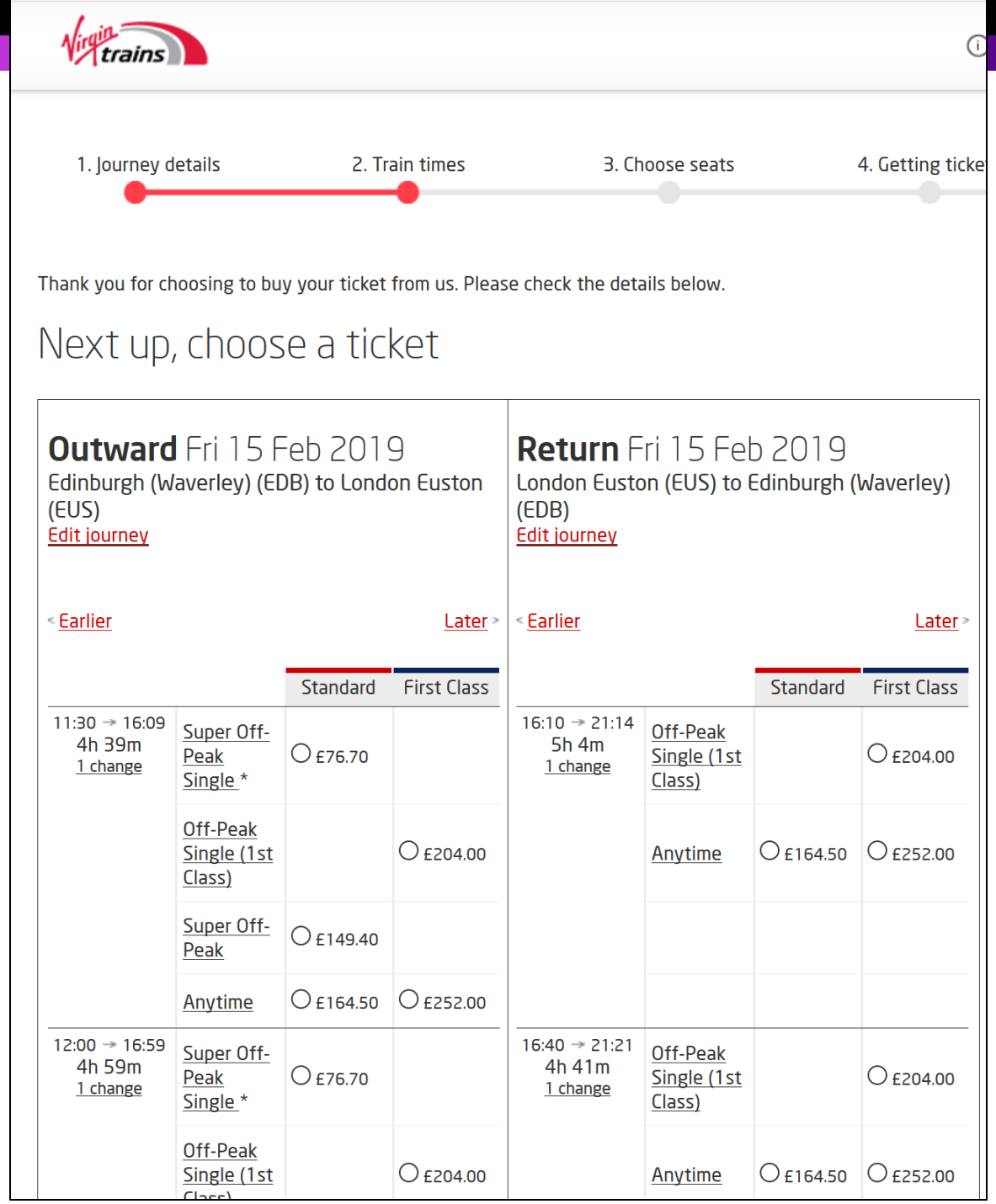
- Large information asymmetry between participant and researcher
  - The researcher likely understand security of their tool
  - Participant likely doesn't even know that security problem exists
- Deception studies are common
  - You told the participant to accomplish task A, but you are really looking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

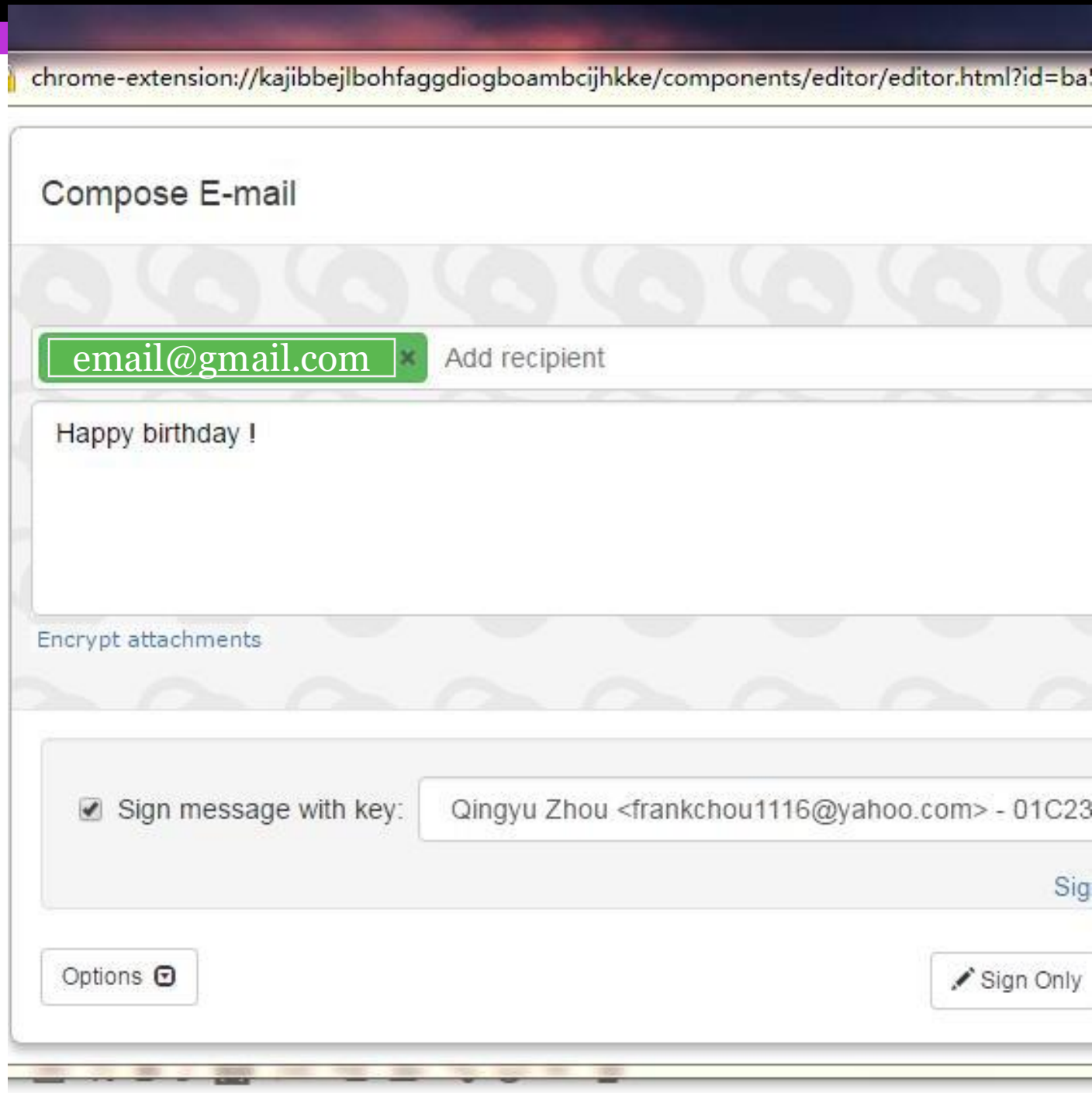


USEC Think-Aloud:
Email encryption

* 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

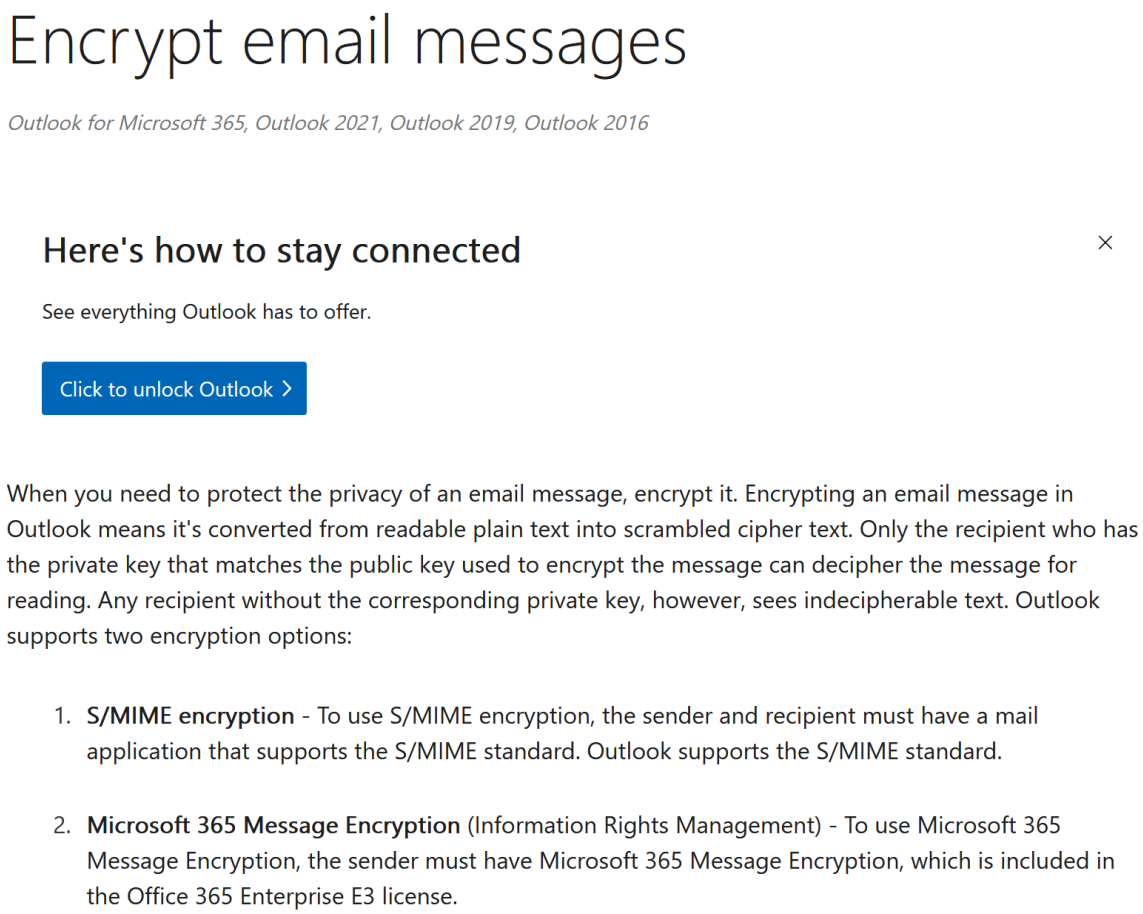
- Research the security technology
  - What must the participant do **to be secure**?
  - What kinds of **errors might be dangerous**?
- Pre-planning
  - Make sure tasks are interesting to the researcher
  - Knowing what you want to take notes on
- Precise running
  - **Not biasing the participant**
  - 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/

Pair-share: Encrypt email on Microsoft Outlook

- Open the link below to read about how to encrypt email on Microsoft Outlook
- Read through the instructions and make a list of what different tasks a person would need to do to encrypt an email (according to the instructions)
- Where would you expect a normal person to make mistakes or get frustrated?



Encrypt email messages

Outlook for Microsoft 365, Outlook 2021, Outlook 2019, Outlook 2016

Here's how to stay connected

See everything Outlook has to offer.

Click to unlock Outlook >

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.

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

Task and subtask

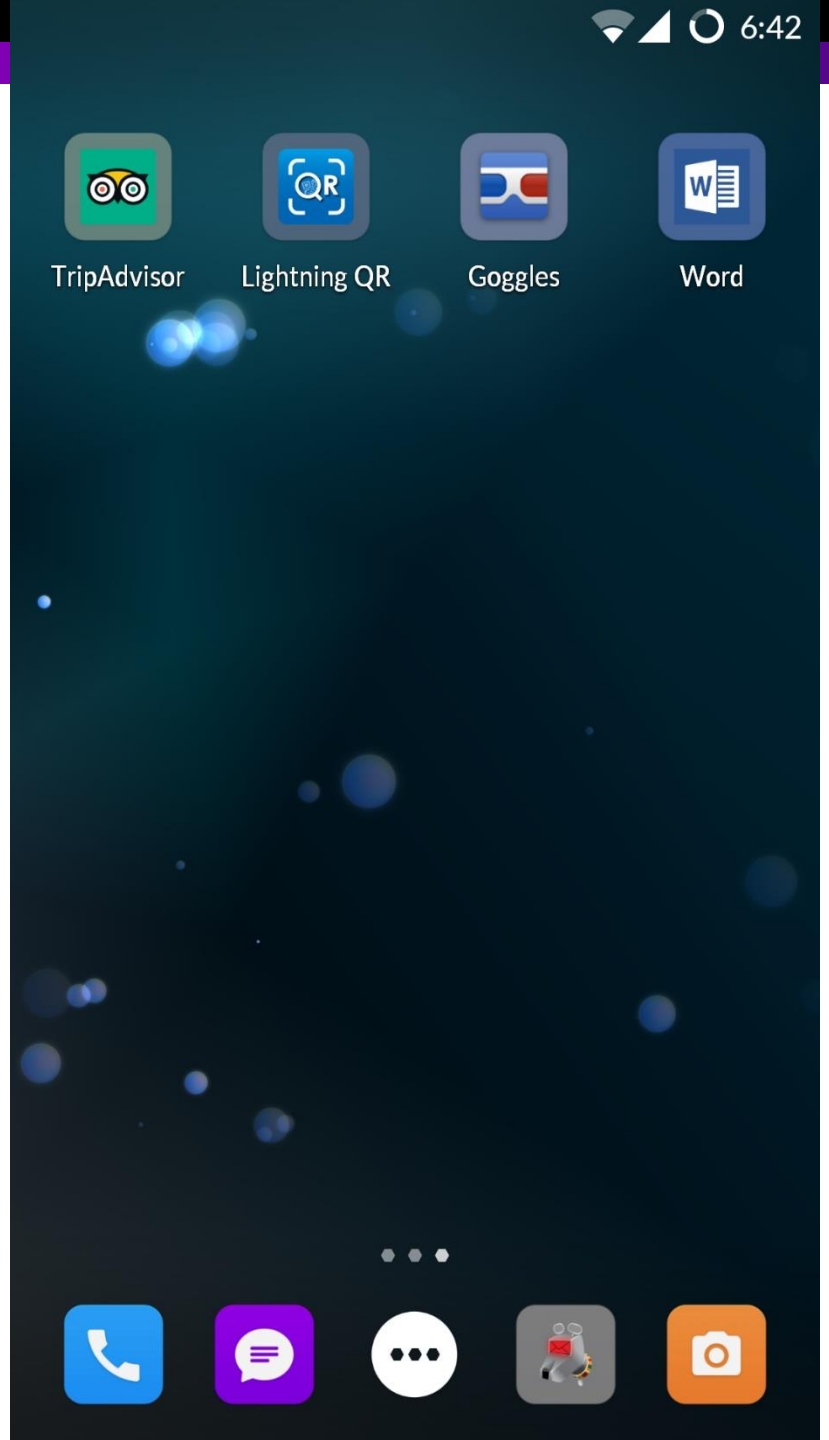
Primary and secondary tasks

- 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:

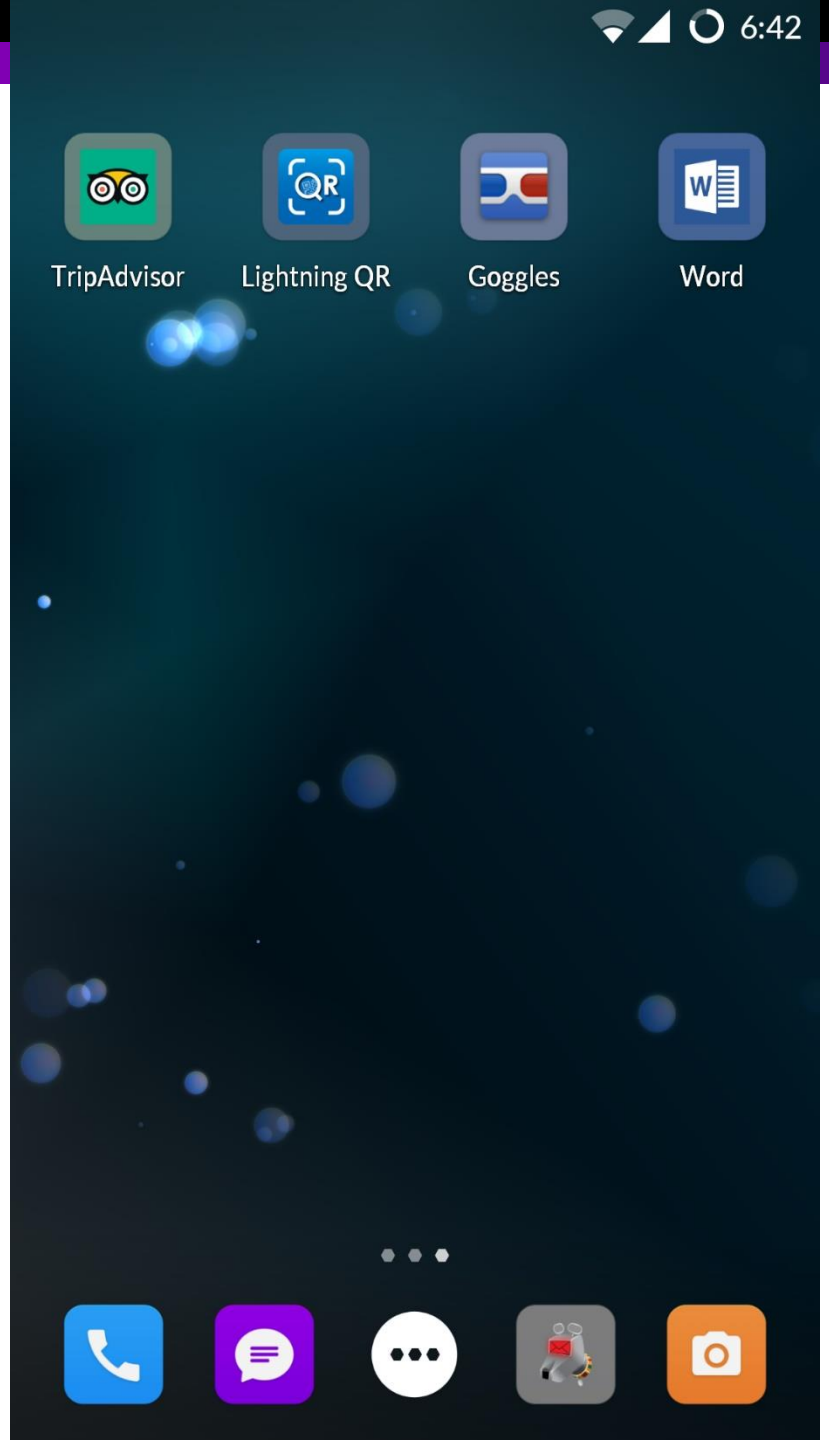
Task: Set an alarm for 7:00am

Task: Set an alarm for 7:00am



Task: Set an alarm for 7:00am

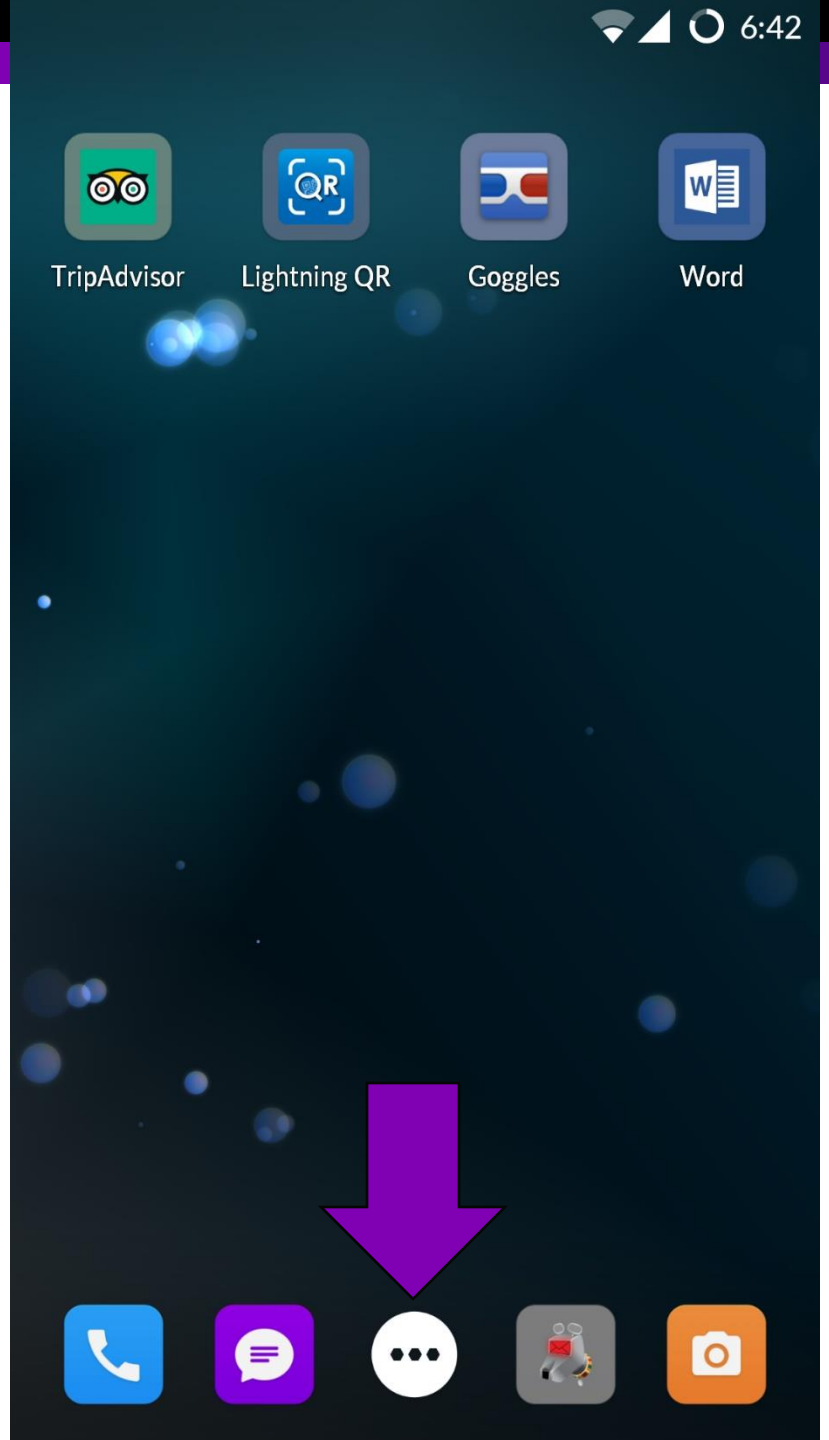
Subtask 1:
Find an app that supports “alarm clock” type functionality.



Task: Set an alarm for 7:00am

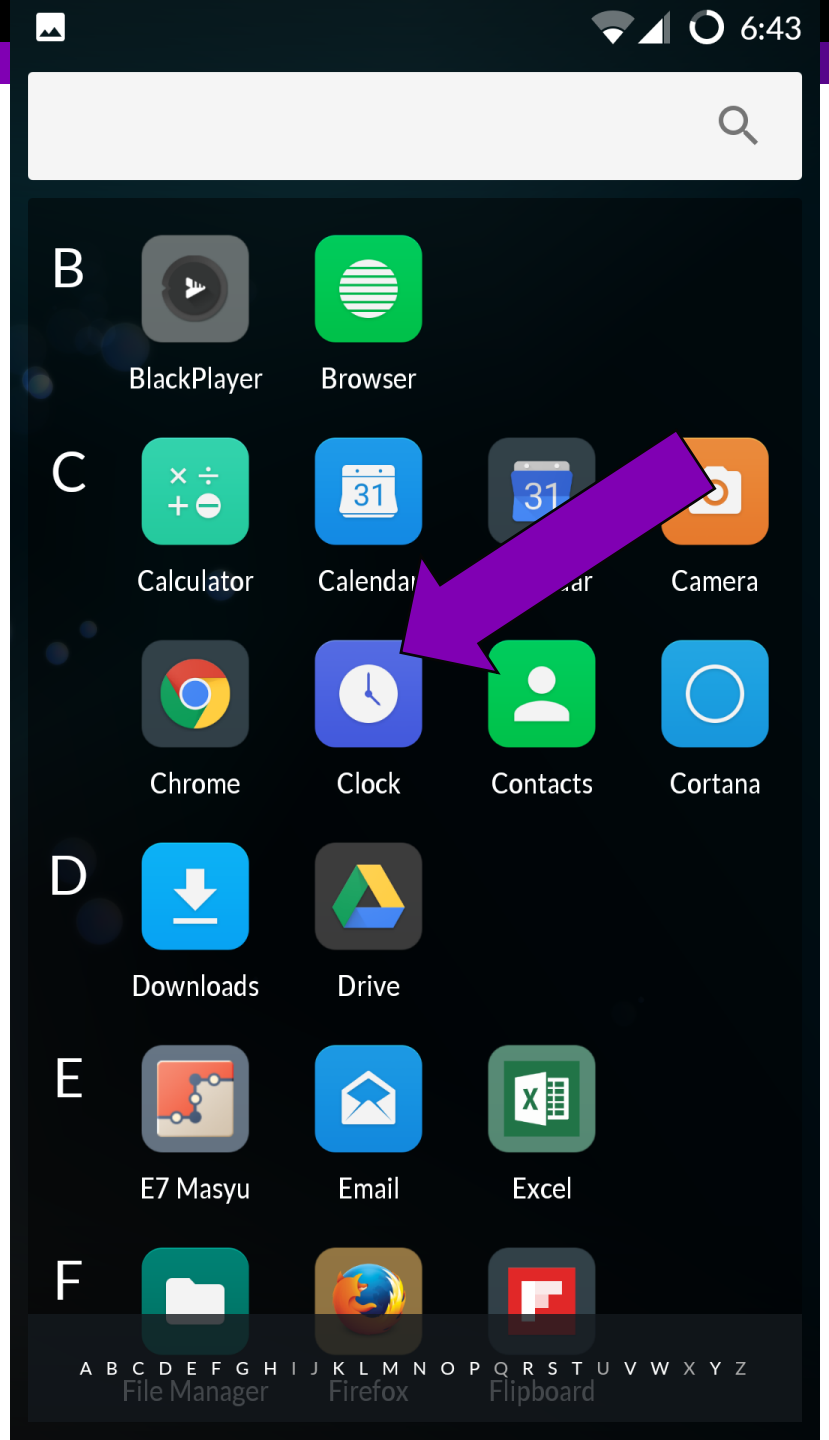
Subtask 1:
Find an app that supports “alarm clock” type functionality.

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.

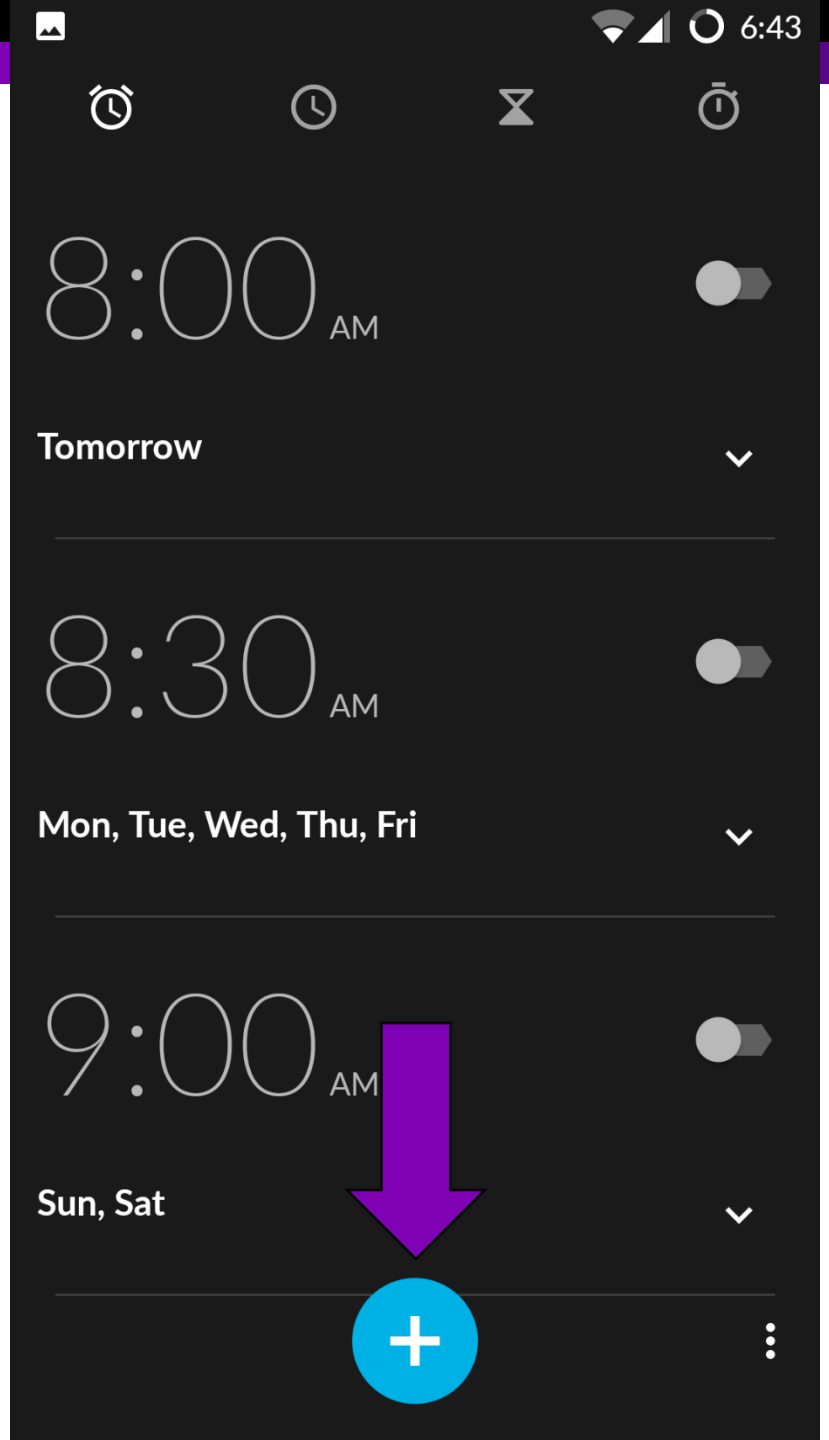


Task: Set an alarm for 7:00am

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

Task: Set an alarm for 7:00am

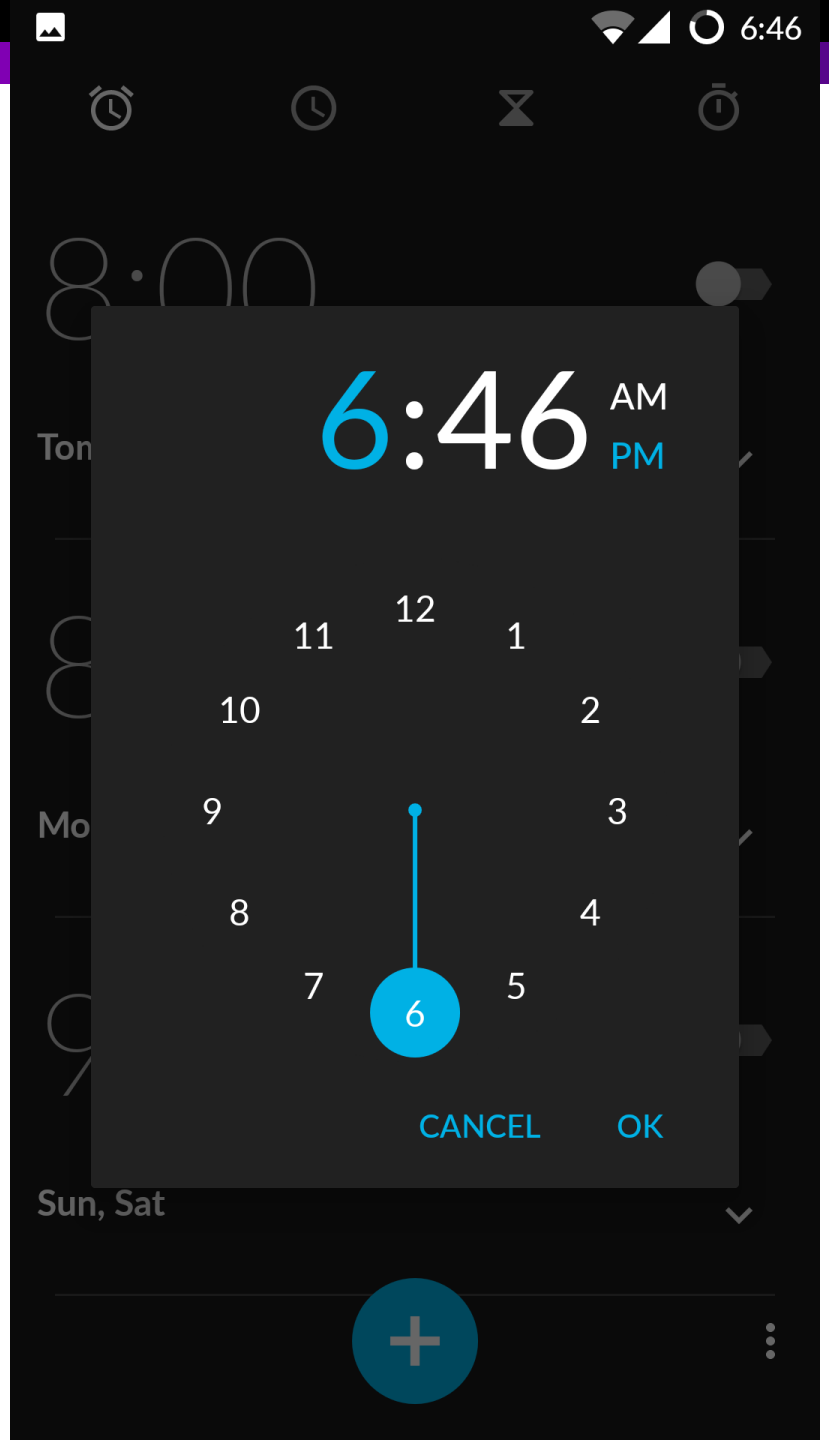
Subtask 3:
Create a new scheduled alarm.



Task: Set an alarm for 7:00am

Subtask 3:
Create a new scheduled alarm.

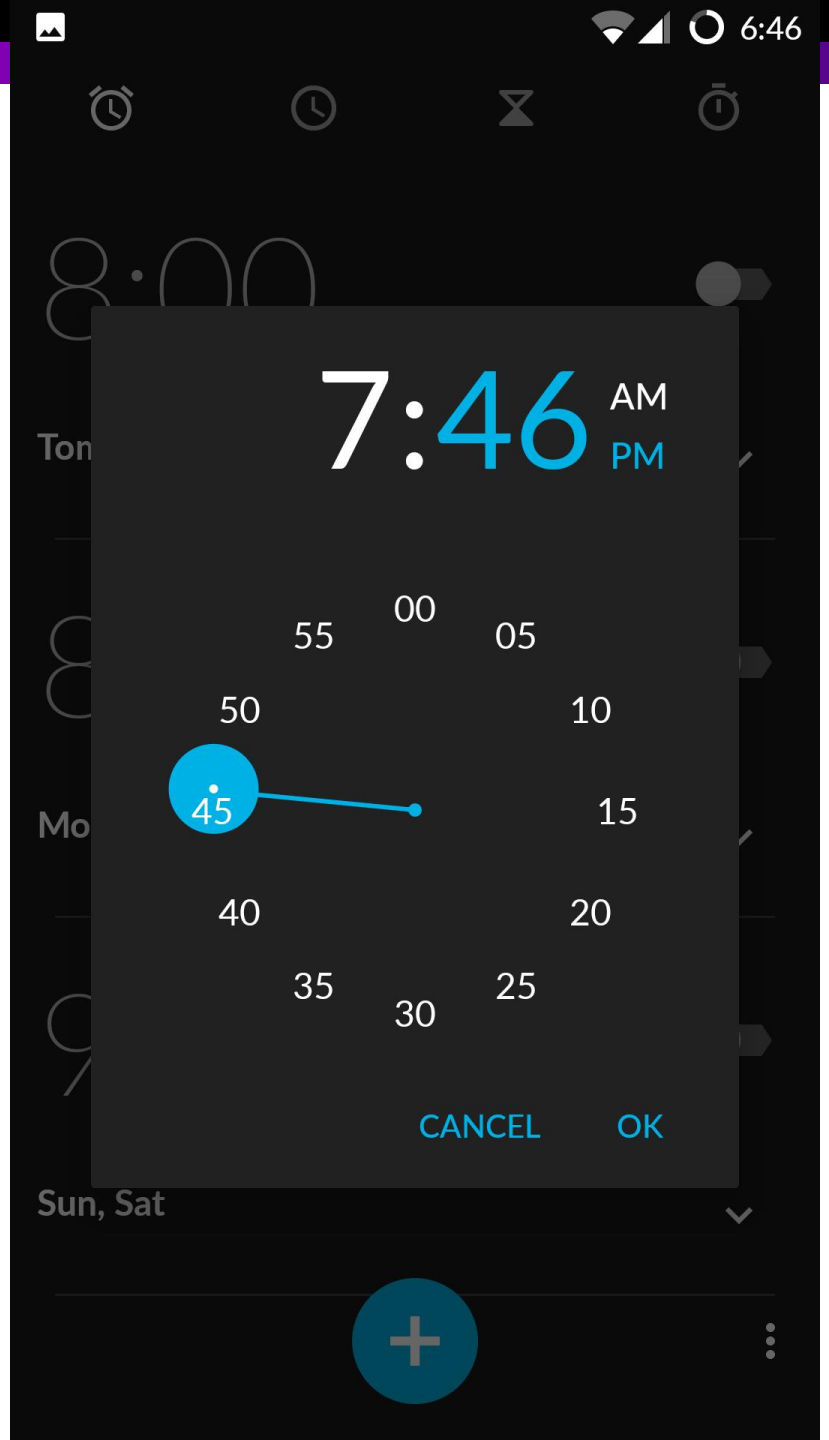
Subtask 4:
Set the hour to 7



Task: Set an alarm for 7:00am

Subtask 3:
Create a new scheduled alarm.

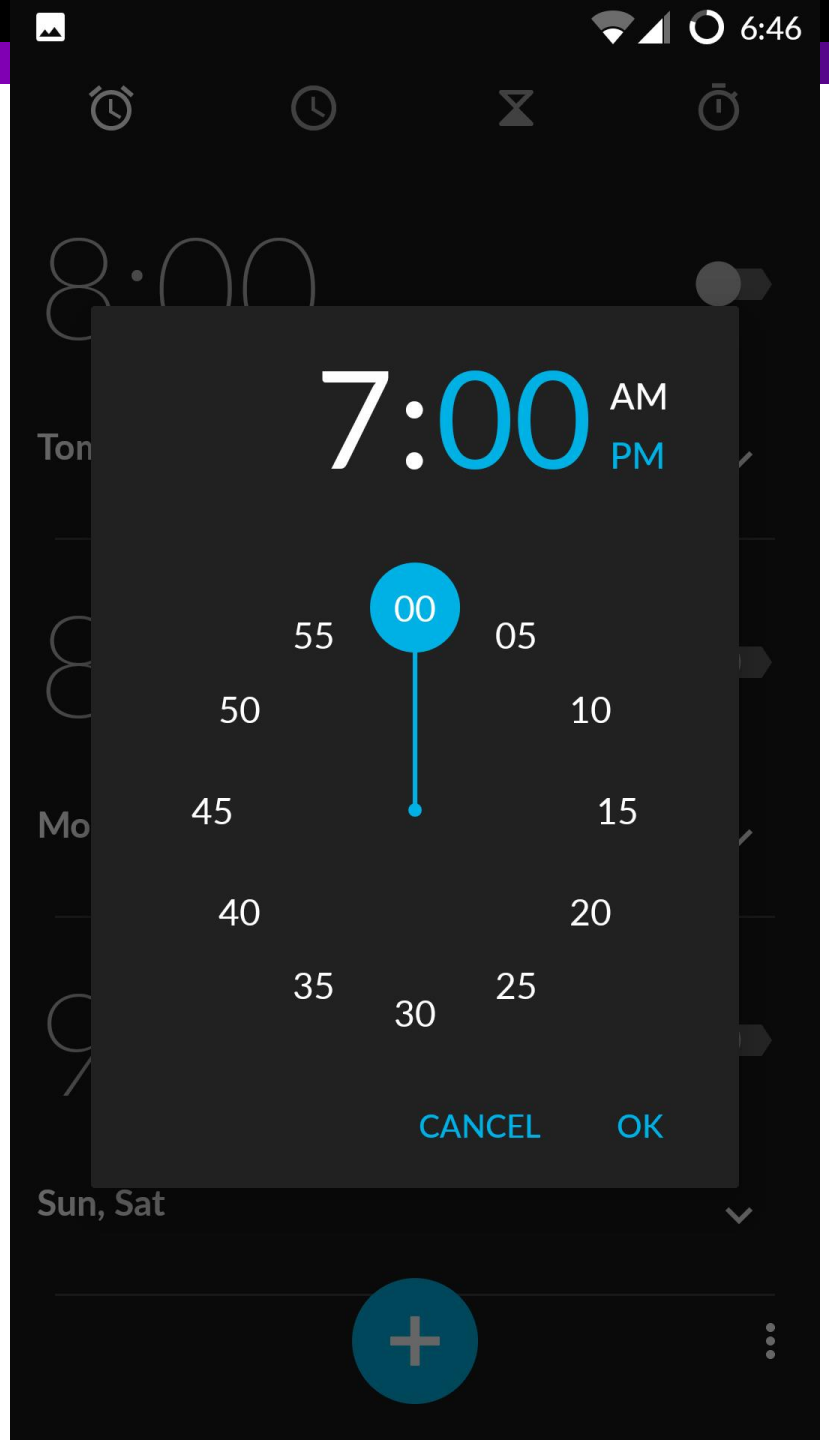
Subtask 5:
Set minutes to 00



Task: Set an alarm for 7:00am

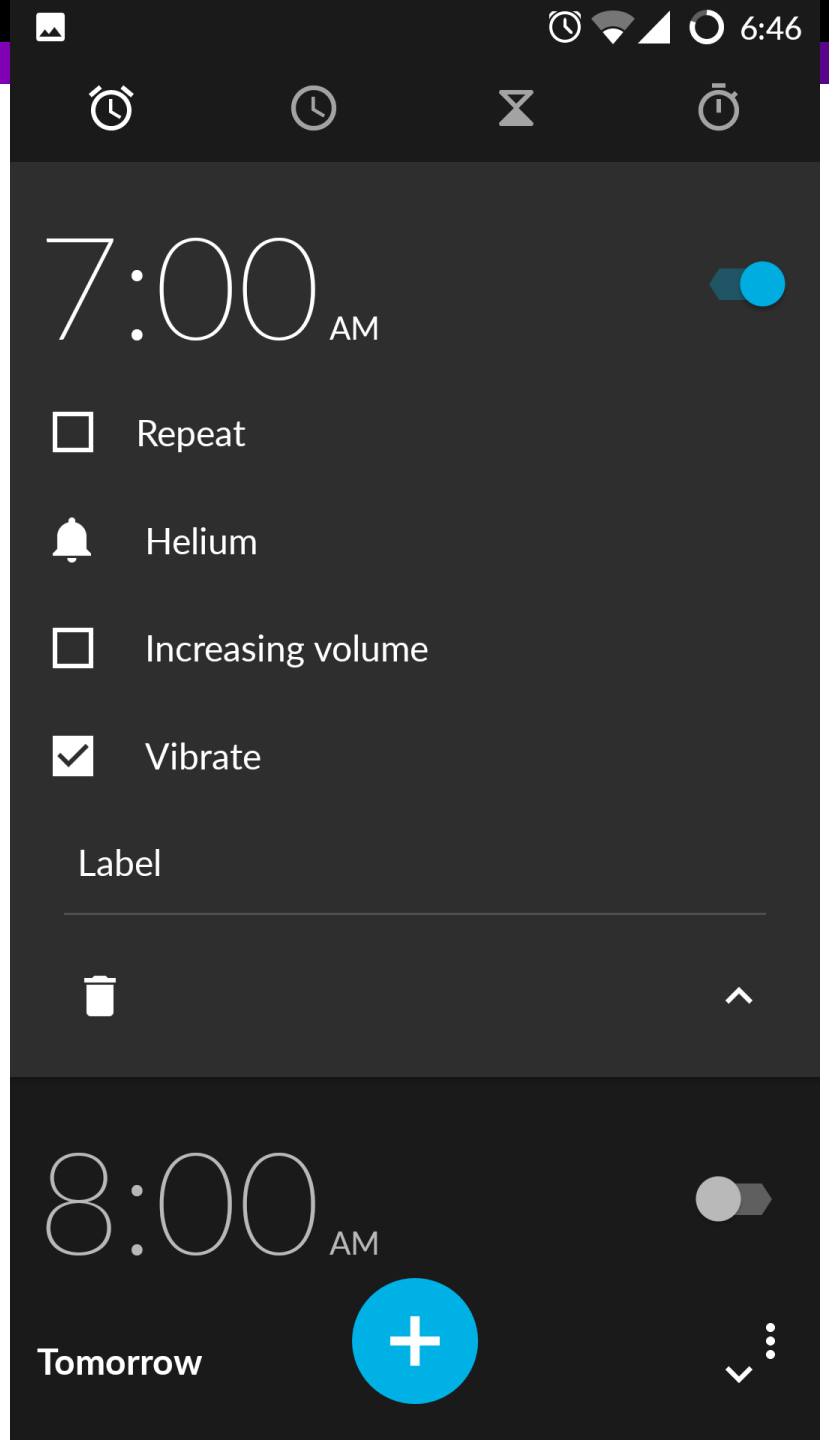
Subtask 3:
Create a new scheduled alarm.

Subtask 6:
Set to “AM”

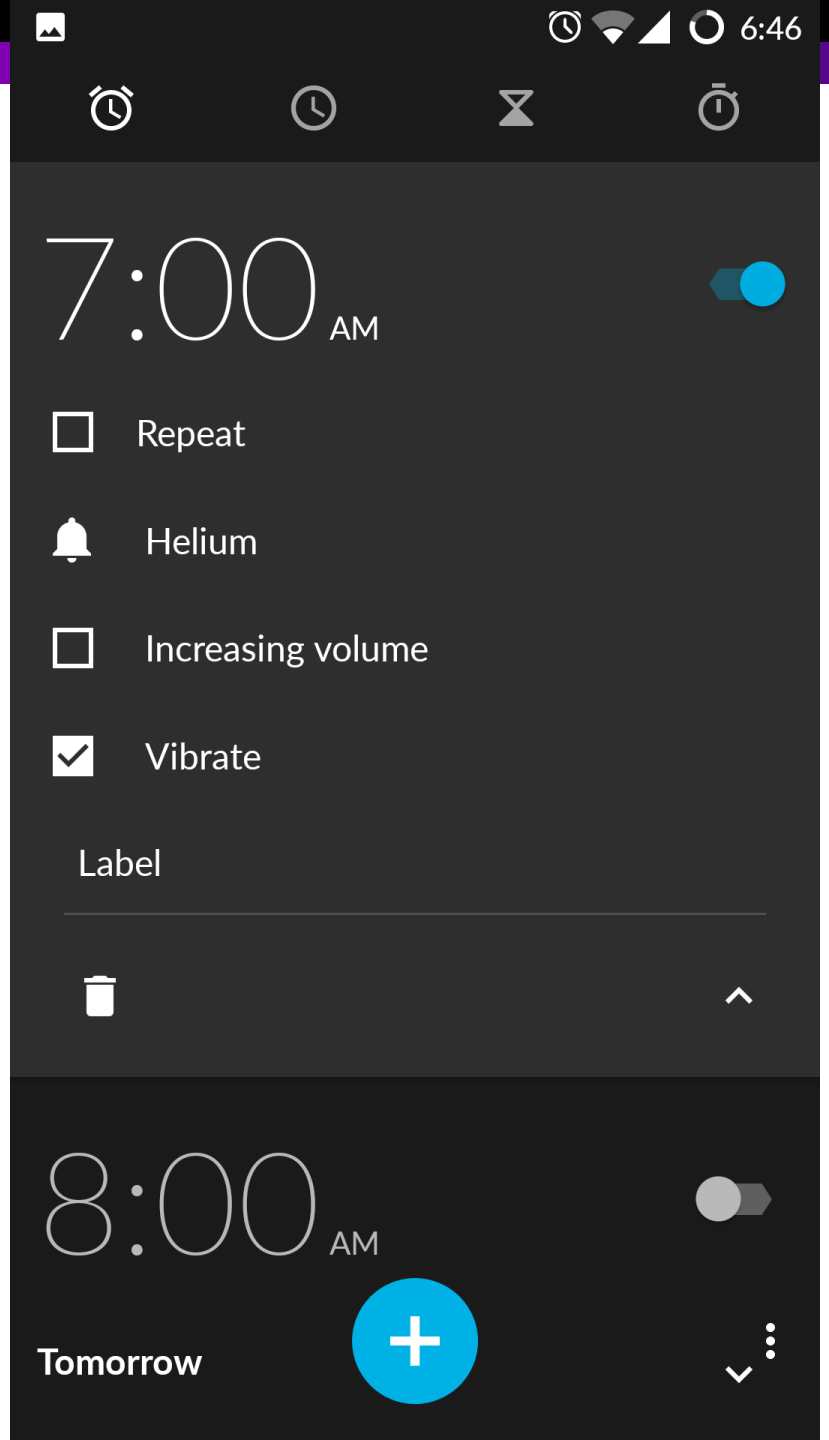


Task: Set an alarm for 7:00am

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



Task Completed!



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

Questions