Think Aloud

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

01/02/2024
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
Design process

What is wanted/needed → Analysis → Design → Implement and deploy

What is there now vs. what is wanted

Scenarios, Task analysis → Analysis

Guidelines, Principles → Design

Precise specification

Evaluation, Heuristics → Prototype

Architectures, Documentation, Help
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.

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

Think Aloud

- Usability Lab Studies
- Ethnographic Field Studies

ATTITUDINAL

QUALITATIVE (DIRECT)

- Participatory Design
- Focus Groups
- Interviews
- Concept Testing
- Diary/Camera Studies
- Customer Feedback
- Desirability Studies
- Card Sorting

QUANTITATIVE (INDIRECT)

- Clickstream Analysis
- A/B Testing
- Usability Benchmarking (in lab)
- Moderated Remote Usability Studies
- Unmoderated Remote Panel Studies
- Unmoderated UX Studies
- True Intent Studies
- 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
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?

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
mQENBFHMcgABCAC9WyD06K2LYh4y4eHN6suHLqMj+iSO+iUTuLEVnUzlo XAUxH
Ko2HejIv19xQaG8j93ZttxXKCo3aMESeOEoz6NglervoCse5Br4wqj8nHw65L
B2d6qnpCplgXcZGjxtEHfHjaf27CCosobCxPmeshUH4zHkke+g6DAtmIETBpYp41
Ot t9qmdMQkgb2Hxw28RYYxkddouetekcOrFlry9ZFHkMaTeHIHK4nlwqshiz R
QvEx2S+M8cKCb+s+Rch9Haan7EG9jWHQFRW4UUs5z0fevQp2kkRto7u233
9h3D
B/7+7XLMFQbOUZQ9B35w7IqHgYyjaJVsUj0dAEBBAAG0liktbWkgVmfwaVh
Idxr dmFuaVWqQGlzIsizCSHyY51az6JATB33EwvEIACkFAYlKyYvEcGyMFCQlmIAYHC
wkl
BwMCAQYVCAUQgsEFgIDAQaEAIQgAACKCRCRTdxxJ9/HZffG+CACShuxkje3QA
qew
GWh9K4cgDcyY0xQdqJwq3PHxmyZmQeN/latKcOrjl2b+Q7S5/St+EgjXOHgPRplxt
G
Z6o2Oep6A18fFXx3JgQZdvP0TjBlWnpOyMeBGTglvEY33so2VueOoexozq3dbYP
5vstvxtk+TKHPSioIT75P2zByqXLT5sabNBQDPCtoDqOgHFR+hFGsaKrK0y7eaeF
JqPmxX0+iL33J2QY9ZctIlyebwvHrIIPBU2JYVCQzdKj7u5se4Fr42HsMgOzmLQQ
D4
YlgRweMFAvxZ0aRHxEAst9V43iWxUJ8YHvSO0E5cnOCyZCPYq20lUjweZ
6T
lpdrwCqBrlYwIPfZhmmlvY8As2FtaUB2YW5pZWUeuJ9tPdkBqgQTQItALAl
b
wLJUWCyBspALCQghArwBHtUIAqKcQWAgMBhaABaAEQ5gHCMnAmhBABeABJWCmMeAhihB
AAJwJN2
zG383d8l9sUJAIAl0wrixYarmKs6C6B8M7TxXtD0QXAcnt7bF0W0QZhskiUQnEoC
+a
XBYivT5uHaatLtyjexD3qMEoZnH0yYMGeOEgKu02wWshbhoQ2HpgwzRLD57
SM
BibawowK0wOB39e4AkMWJXCNsF5Bcexe06AHRl27V325V05dKflvnC9xKu9B8L7
kM
clN7sLobt1deuYKoNQzZMo/0pVDkJp/EY5yJelV90yypZy/6wFBEhgtksXyeEznO
9w89u9Usa+9/P8p24JLMDSeyf177SRS/Y3P0IOZ6lnbC+KodwM7yu0yueu9zh
pizbV3geYHx2LWzVbYz/7xT345W6RRM0JWAIWwECAYMFaInSyEnCPQIgjty
-----END PGP PUBLIC KEY BLOCK-----
Signing:
I send Bob a message only I could have sent

• I encrypt (sign) the message with my private key. (Only I 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

mQENBFBHMcgABBCAC9WryDO6K2L3VHvy4eHN6suHLqMjSfUUtUeLvIlU7z0
XAUXH
KoHeJfIV/9XoG6j93ZSzasXXCQg3mAsESeEOz6fNGfQvece5jB4jHJ8j8Hw5bSL
B2dnqCDplgxN2GJxtEHbJu27CCSocbCJxPmeshUHh4Rh+gEdAtm1ETbYp41
Ot
1zqzdMQkgb2Hxzw28fRfYykeDuouetelkOrFRly9sF9KdMh1eTH94KnwlQshd1Z
R
QEYEX25+M8cKCb++lRc9H6an7E7G9WHOFRW40UsY5ZfoeYoqFZp2kko7o7u233
9hhD0
B/hb+7zLM6FCQbOUZQ9BD5w7iQHgY1YfJvslUj0dA6BEAAAG0lktbWkgVrmFusVwh
lDxr
dmFuaWVhQGluZ1i5ZCShyY51z6sJAT8EewEIACOkFA1YYKvECgyMFCQmlAYAHCl
wkl
BwMACAQYVCALCgESgIAAQaAIQaAXCnAAKCRCTdxxl9/HZtfG+CACShuXjx6QQA
gew
GWH9K4cGdiY0vDqJwq3PHxmyhZmQeVE/latKcOriizb+Q75/S1+EgX0HPQPhfG
iZ6zcOEpEa8f8iFx3J3gZDwrPD0jBWNopYoMBgTgLvEY3gs2oVuOeexb3db3bDy
P
sv5xvT+D+TKHQ6SioU775P2bZyq/XLT7abNBQnDPCtoxOdbhR+FWsgkRkr7eeaf
JaPnxX0+A3L33t2QY9cdI0gbywbrHMfr1B2YVCQDOkJu7u5eFh4ZhsMoLmzLQ
D4
Y1Gr5weMFAvxZ0aRxkEe9tVq48jVwxzVSJp080E5cNQCY2PCpQ20UJwTw6E
6T
lptdwrCqtb1LYWpplFzhrmlY5A8a2F0aUB2YW5pZWEuY29fP0ckBOg QTQAIALj
b
lwLJClCWYBspACoLChgHAWILBHui1AgkCkCwQWAaMBahvBAheABQWCMMeAhkbB
AAAQEUNB
zGX38d9J3UAIW9WxrlYammKS6C6bW8m7xxTxD0XCTtb7F0W0QZHSKMUQ4ECe
+a
XYBlytA5uHaatLyjyxeA3xMqEMoZnQ0H0YMEG06Gku0wWsbhfoQzHPgwzRLkD7T
5M
BibawkoWk0VoWB9e4AkMakjJCnF5BEXo6AhHRL2v15V205kVnCRXX0Ku8b7L
knM
clN7oLobMdrOueyKoNzBsnONF/oLvKdJp/0/ETYjUejV9klypZy/W6FQBeqSsXye6zN
9w9b9uUs9+7P8p34J3LDMSevT77zSRS/YP1OIEZ6NAb+C0RdWMPm7ulyeu9zhc
pzbv3gvEnH1zLVwZbYV/Z2X345F1WRRMAWJhEAECAAYFAlSiEyCgKQjy

My public key

My private key

-----END PGP PUBLIC KEY BLOCK-----
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 😊)

Take-home


• (Blog) Washington Post - Apple’s new Vision Pro is a privacy mess waiting to happen