YOU GET WHERE YOU'RE LOOKING FOR

The Impact of Information Sources on Code Security

PRESENTED BY SADRA SETAREHDAN AND KATHERINE LAMBERT

OVERVIEW OF STUDY

- mobile device market growing in popularity => number of applications developed grows too
- previous research found that most of these apps/devices are insecure
- this paper dives into the possible root cause for these programming errors
- while many development issues have been identified in the past, we still know very little of how these security issues make their way into apps

QUESTIONS EXPLORED

1. What do Android developers do when they encounter a security- or privacy-relevant issue?

2. Which information sources do they use to look up security- or privacy-relevant questions?

3. Does the use of Stack Overflow really lead to less secure code than the use of other resources?

4. Is the official Android documentation really less usable, resulting in less functional code compared to other resources?

GENERAL STEPS

Based on survey results conducted a lab study to see how developers handle challenges given different resources [4]

Drew conclusions from the study and lab findings, conclusing what needs to be addresses in order to mitigate the problem

Surveyed 295 app developers to understand challenges faced during development and how developers approach them

Surveyed Stack Overflow questions for security problems and connected lab challenges/examples with real-world scenarios

RELATED WORK

Security and Privacy Flaws in Mobile Apps

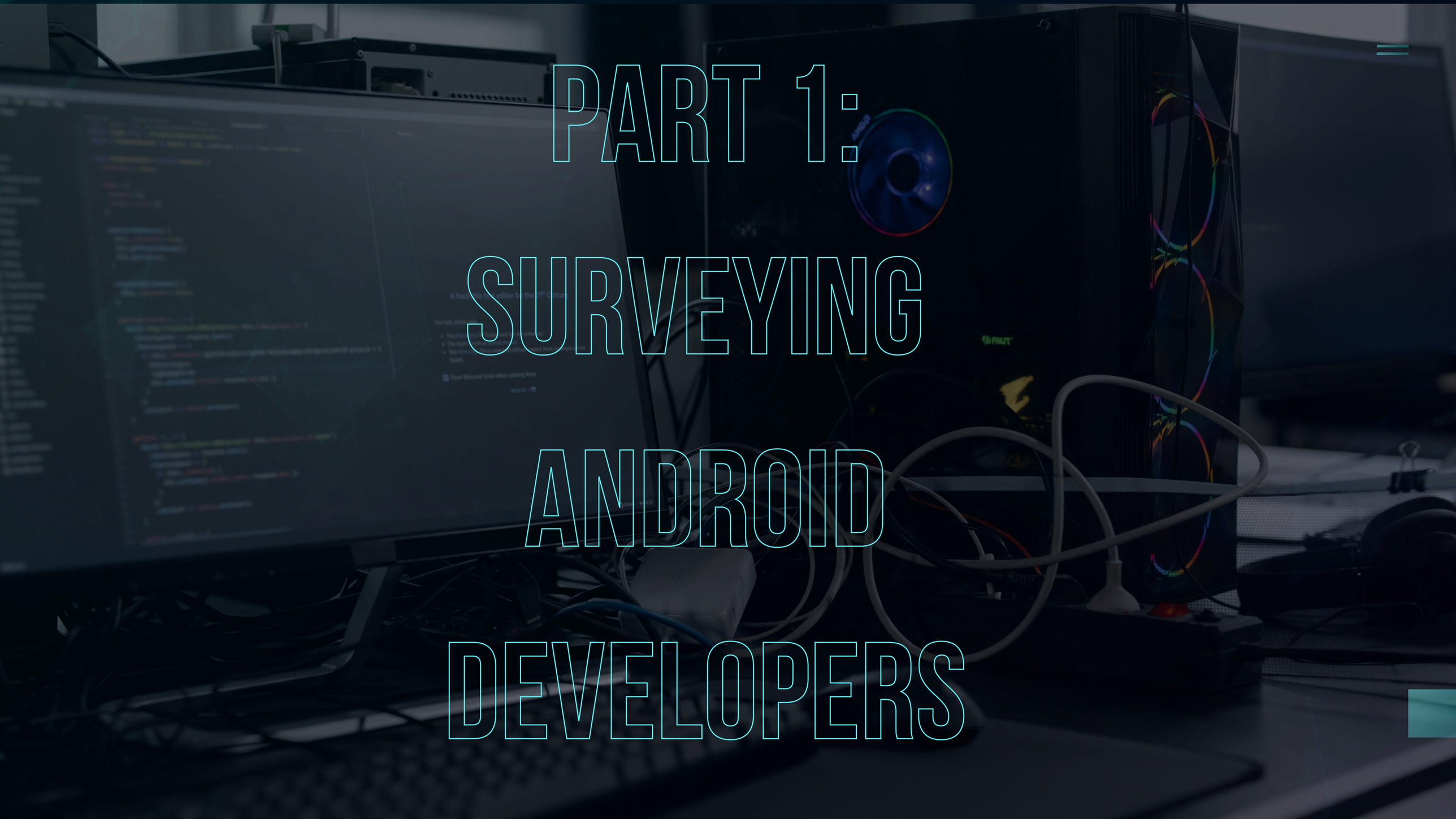
- Fahl et al: 8% of 13,500 popular Android apps contained misconfigured TLS code vulnerable to Man-In-The-Middle attacks
- Onwuzurike and De Cristofaro: the same problems remain prevalent several years later
- Egele et al: examined the use of cryptography – including block ciphers and message authentication codes
- Enck et al: reported widespread issues in Android apps
- Poeplau et al: reported that almost 10% of analyzed apps load code via insecure channels

Understanding of Devlopers

- Georgiev et al: confusion about the many parameters, options, and defaults of TLS libraries contributed to developer errors
- Balebako et al: privacy policies are not considered important and that privacy concerns are frequently outweighed by other questions
- many developers are not aware of the privacy or security implications of third-party advertising and analytics libraries they use

Using online Q&A Resources

- Linares-Vásquez et al: investigated how changes to Android APIs trigger activities on Stack Overflow
- Nadi et al: analyze Stack Overflow posts to identify common difficulties with Java cryptography APIs



PART 1: SURVEYING ANDROID DEVELOPERS

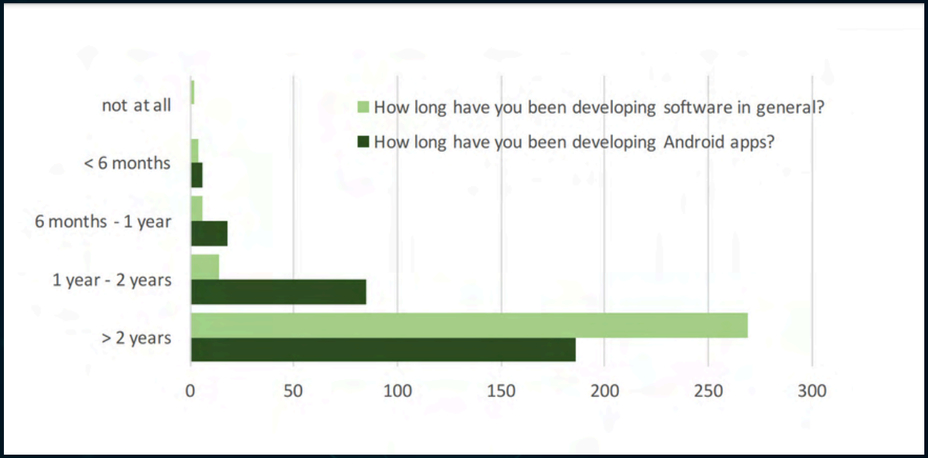
Why?

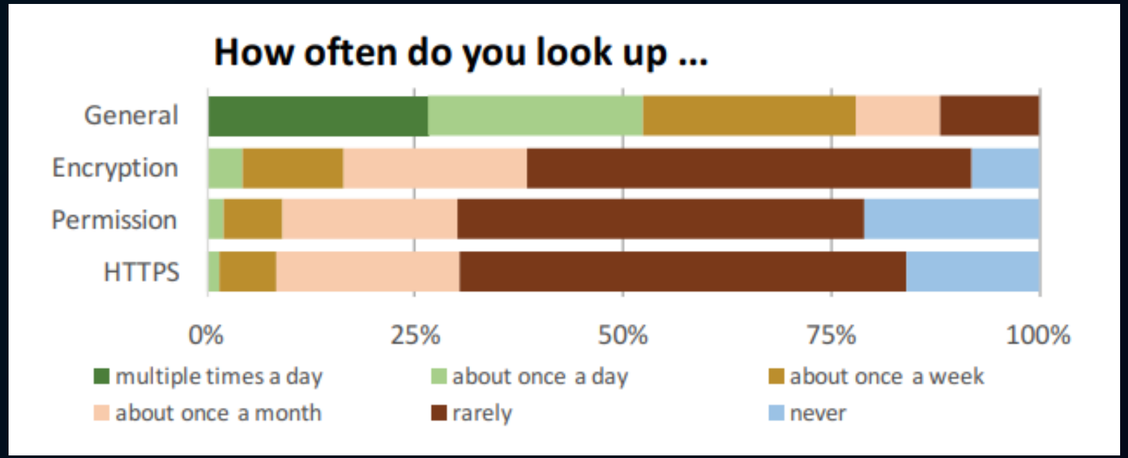
- To better understand the challenges developers face during the implementation of security-critical app components
- Results from this survey helped motivate the design of the lab experiment

What was done

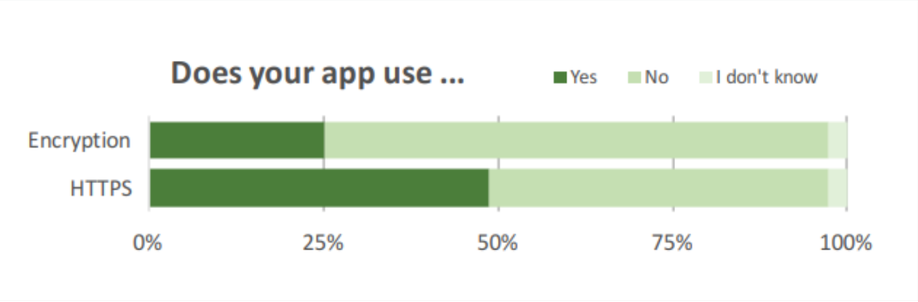
- collected a random sample of 50,000 email addresses of Android application developers listed in Google Play
- A total of 302 people completed the survey between April 2015 and October 2015

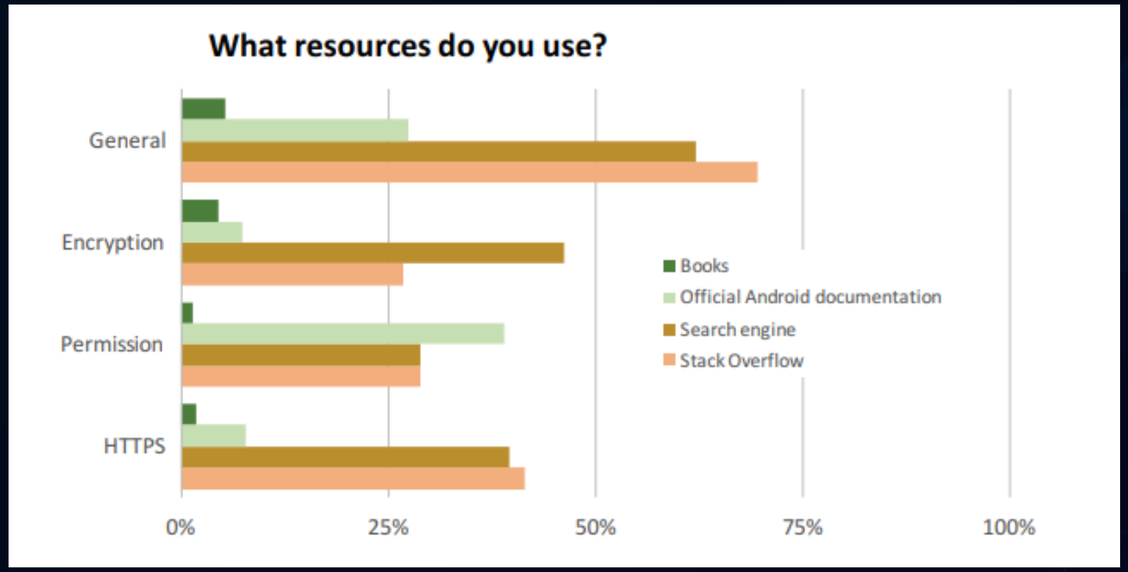
Education and Experience





Security and Permissions



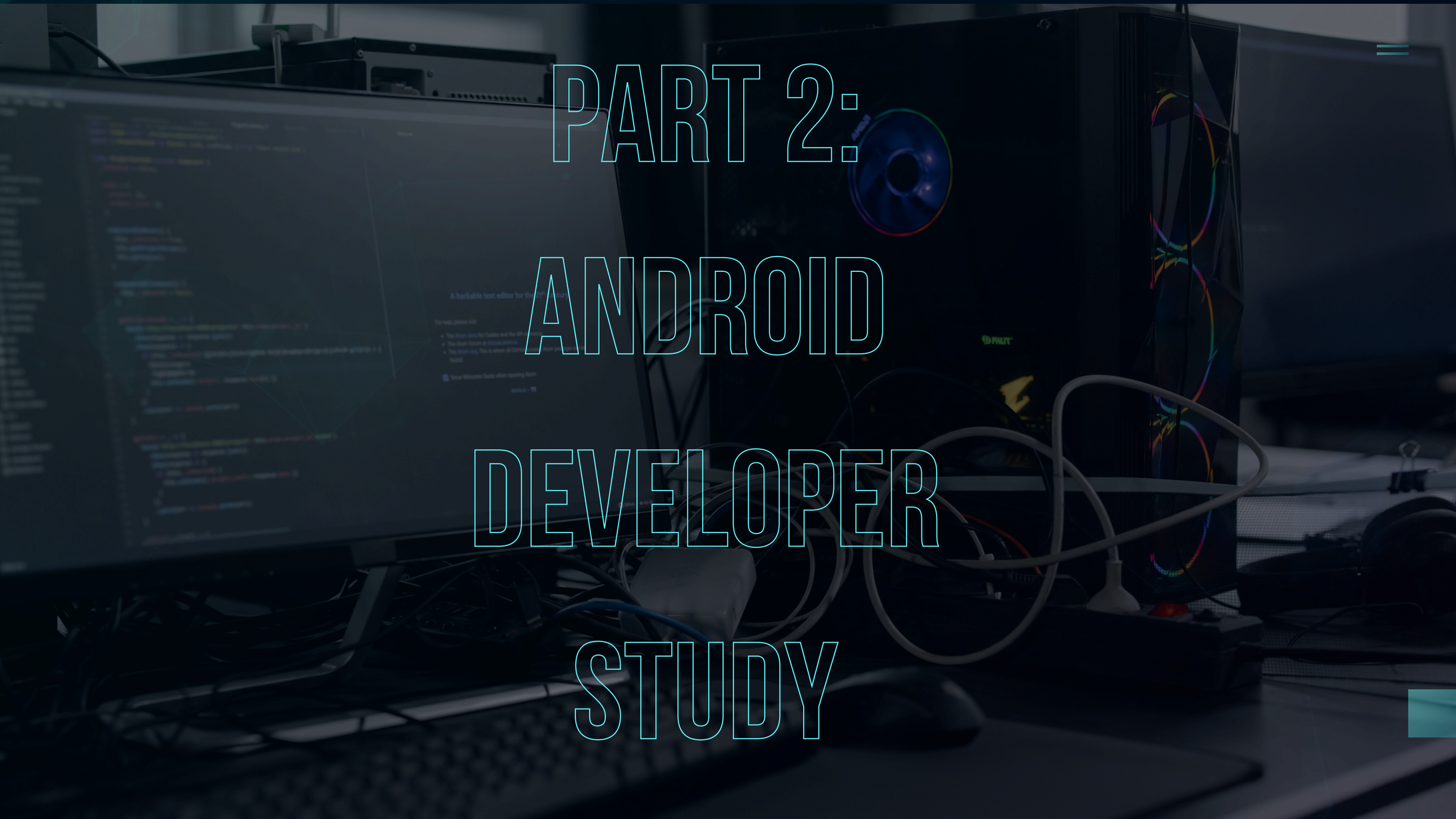


Encountering General Problems

> Stack Overflow 69.5%
< Search Engine 62.0%
> Official Android documentation 27.5%

Conclusions

- Many Android developers must deal with security or privacy issues periodically, but do not handle them consistently enough to become experts
- The quality of documentation is especially critical for these topics.


PART 2:
ANDROID
DEVELOPER
STUDY

Why ?

To examine how the resources developers access affect their security and privacy decision-making

How ?

- provided a skeleton Android app and asked participants to complete four programming tasks based on the skeleton
- each participant was assigned to one of four conditions:
  - Official Only
  - Stack Overflow Only
  - Book Only
  - Free Choice

How ?

- given four programming tasks in random order
- Security and privacy were not mentioned during the introduction to the study

The tasks: Each participant was assigned the same four tasks, but in a random order

- Secure Networking Task
- ICC Task
- Secure Storage Task
- Least Permissions Task:

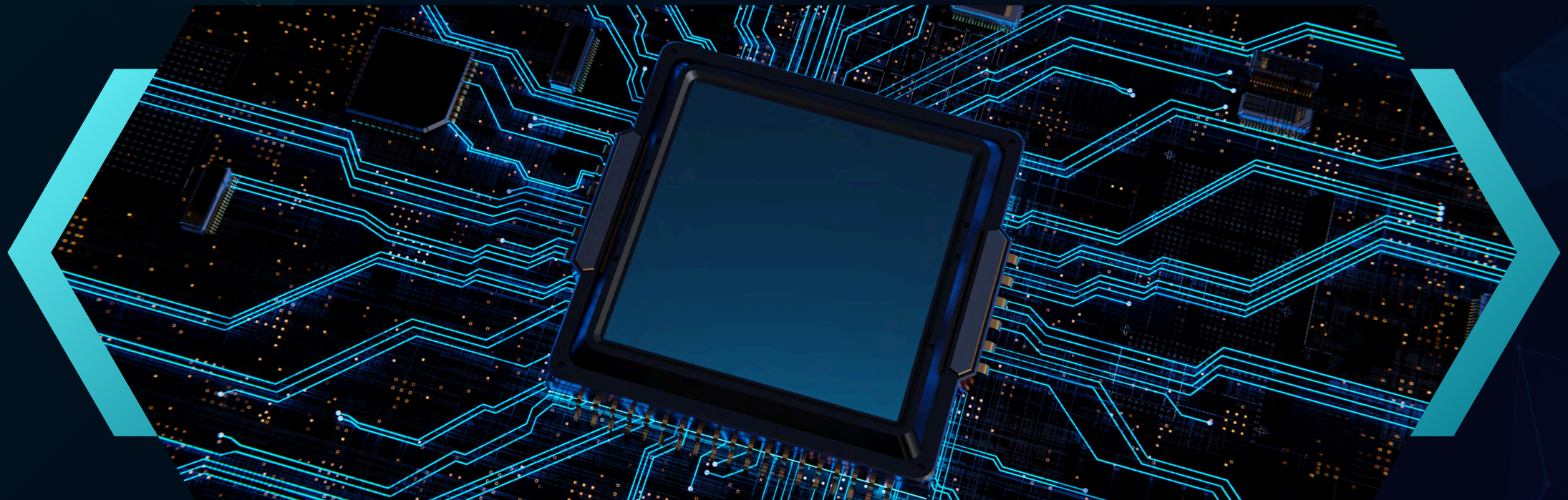
EXIT INTERVIEW

- participants were given a short exit interview about their experience
- ranking each task
- answering whether the documentation and resources participants had access to were easy to use
- whether the participant had used that documentation source before

DATA COLLECTION AND ANALYSIS

Scoring Programming Tasks:

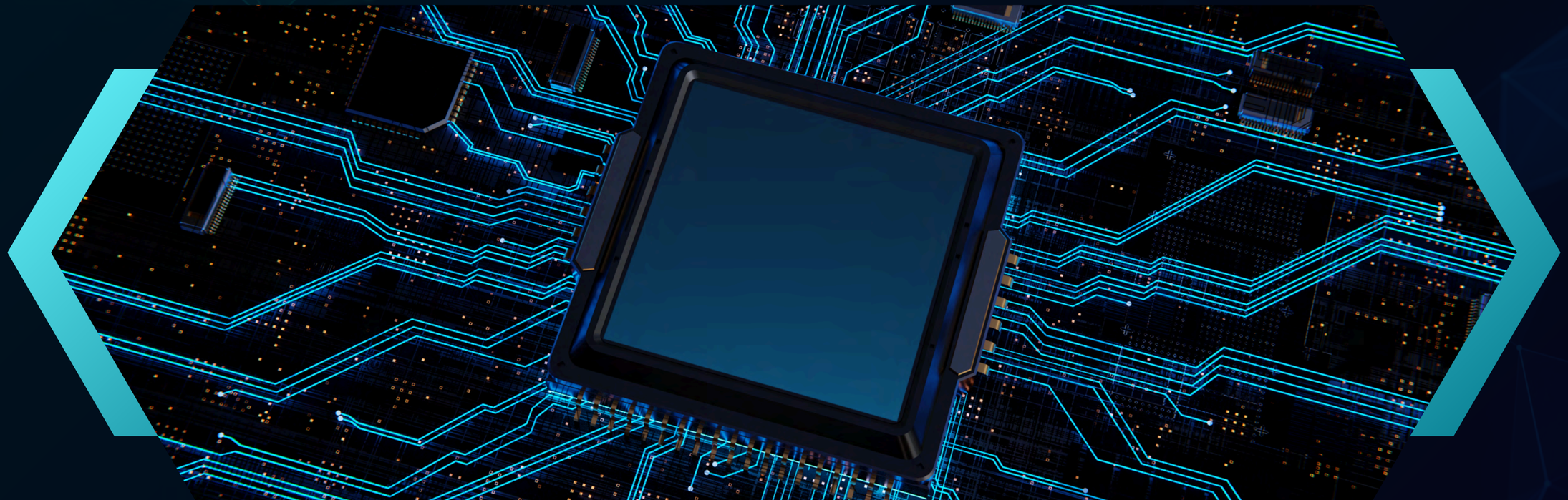
- For each programming task, assigned the participant a functionality score of 1 or 0
- manually coded each participant’s code to one of several possible strategies for solving the task, each of which was then labeled secure or insecure
- verified that functional and secure solutions exist for each task

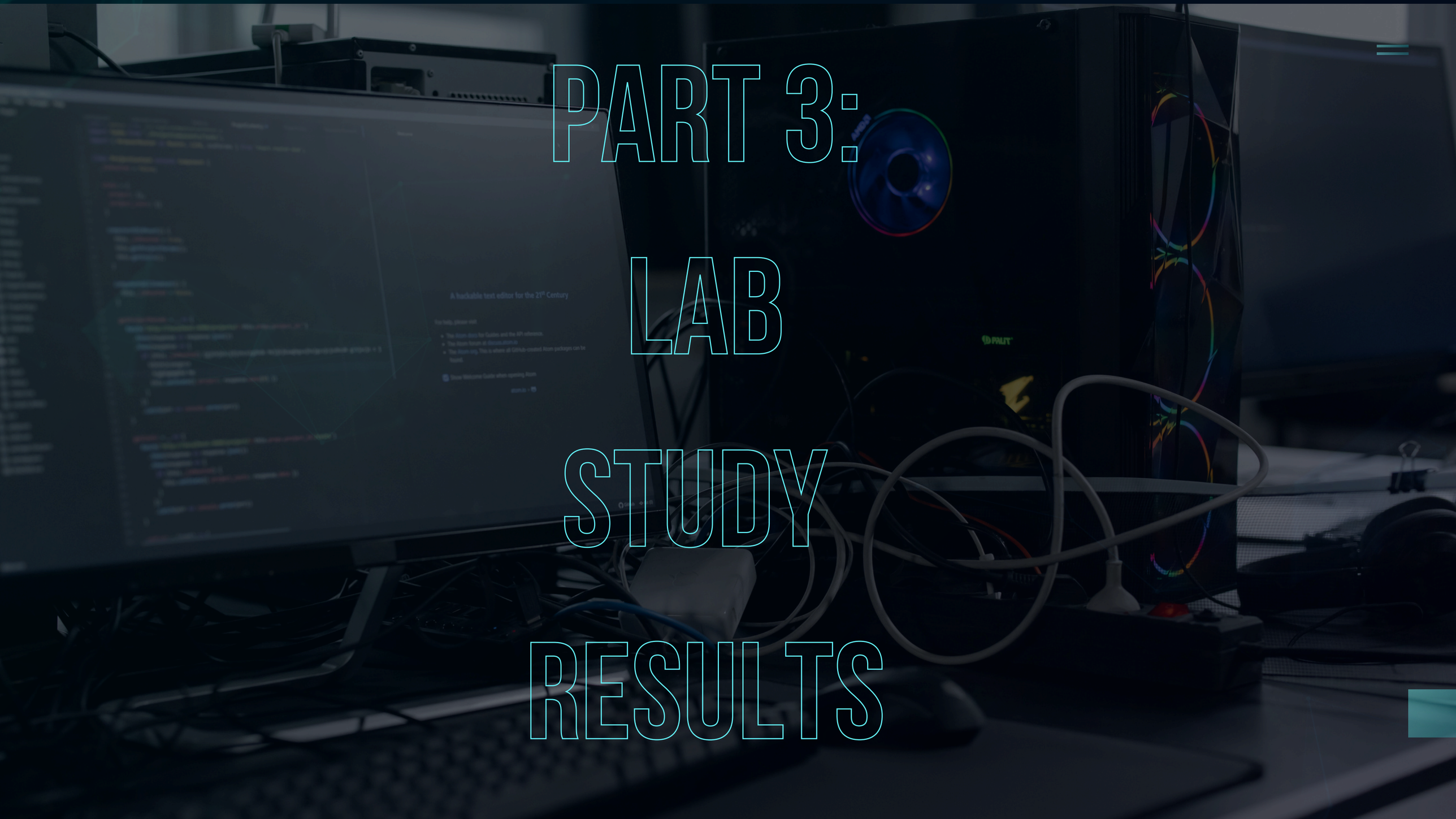


DATA COLLECTION AND ANALYSIS

Statistical Analysis

- used the non-parametric Kruskal-Wallis test to compare multiple samples and Wilcoxon Signed-Rank test to compare two samples
- To examine functional correctness and security across tasks and conditions, while accounting for multiple tasks per participant, used a cumulative-link (logit) mixed model (CLMM)





PART 3:

LAB

STUDY

RESULTS

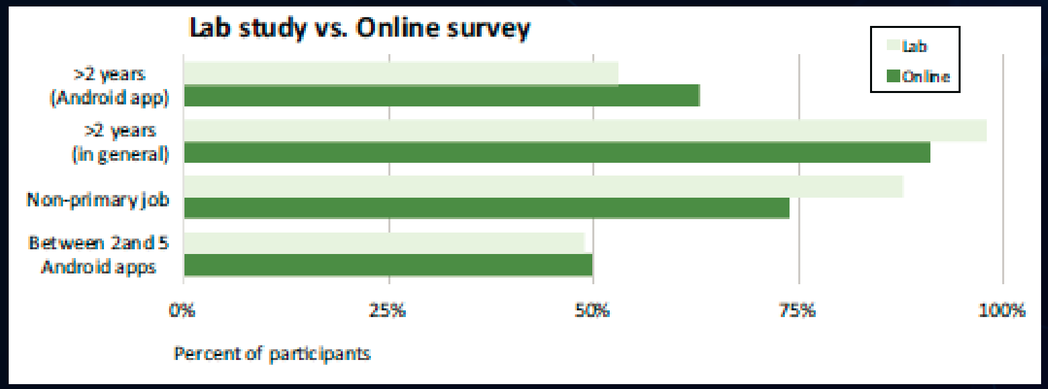
Participants

Total Participants: 56

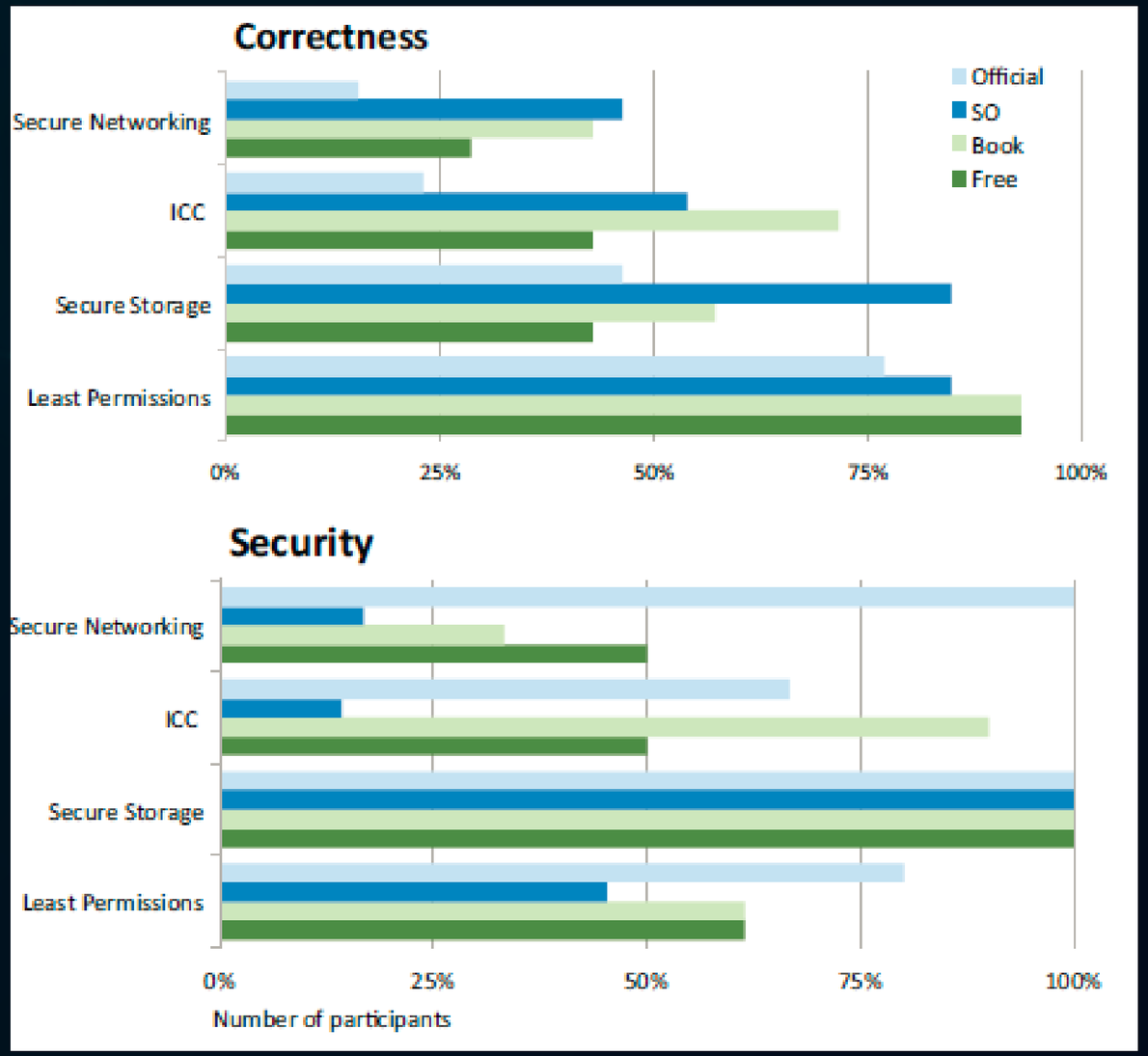
Total Eligible Participants: 54

Assigned condition			
Official: 13	SO: 13	Book: 14	Free: 14
Location of Study			
United States: 12 (22.2%)			Germany: 42 (77.8%)
Gender			
Male: 46 (85.2%)			Female: 8 (14.8%)
Country of Origin			
United States: 6 (11.1%)			Germany: 28 (51.9%)
India: 5 (9.3%)			Others: 15 (27.8%)
Professional Android Experience			
Yes: 14			No: 40
Ages			
mean = 26.0	median = 25		sd = 4.7

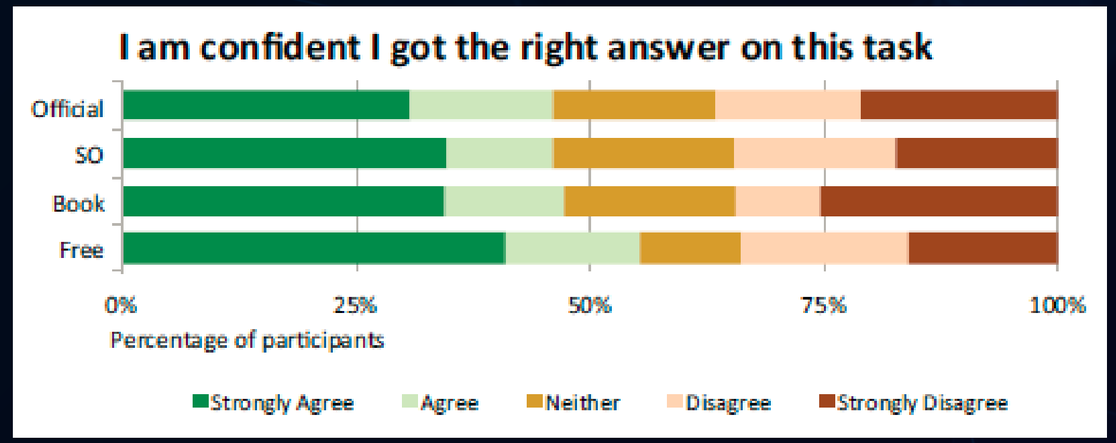
TABLE II



Functional Correctness Results



Factor	Coef.	Exp(coef)	SE	p-value
free	-1.054	0.349	0.613	0.085
official	-1.535	0.215	0.634	0.015*
book	-0.142	0.868	0.602	0.814
ICC	0.795	2.215	0.455	0.081
secure storage	1.280	3.597	0.468	0.006*
least permissions	3.299	27.092	0.632	< 0.001*
professional	1.004	2.728	0.501	0.045*



Security Results

SO: 51%

Free: 65%

Book: 73%

Official: 85%

Factor	Coef.	Exp(coef)	SE	*p*-value
free	1.112	3.040	0.623	0.074
official	2.218	9.184	0.796	0.005*
book	1.539	4.660	0.604	0.011*
ICC	0.763	2.144	0.666	0.252
least permissions	0.856	2.353	0.609	0.160

TABLE IV

Security Results

Considering Security while Programming

Observed Security Thinking

79% didn’t mention security

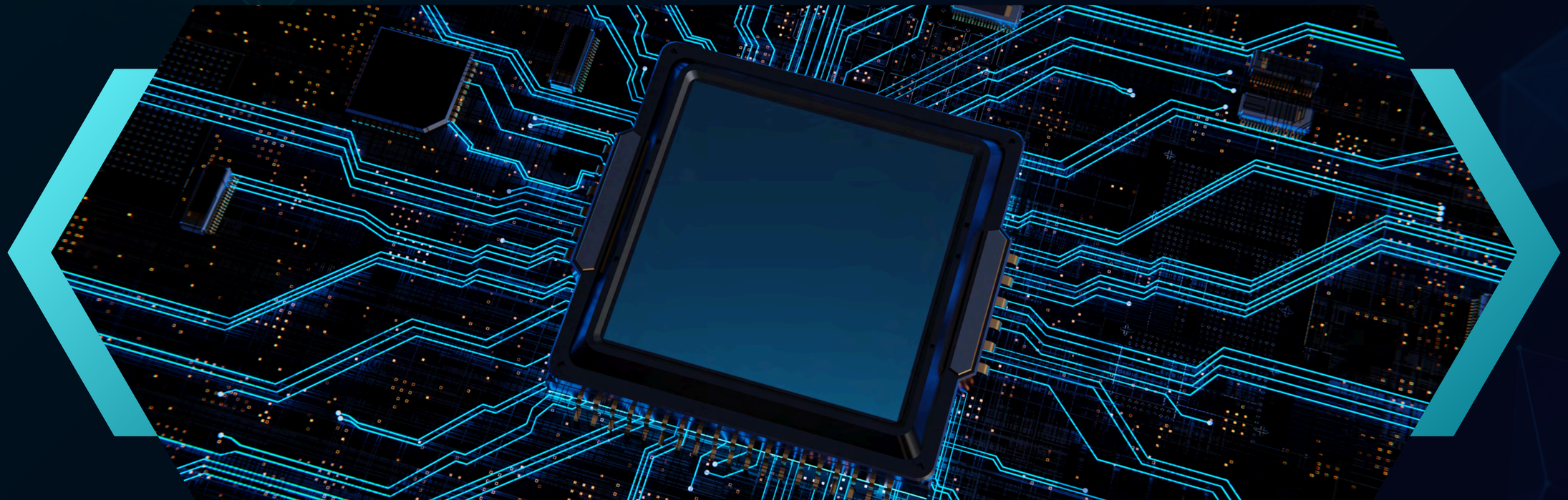
Self-reported Security Thinking

60% mentioned security

USE OF RESOURCES

Lookup Behavior Across Conditions:

- 22.8 queries for SO
- 14.5 for the Official
- 21.1 queries for Free



Use of Resources

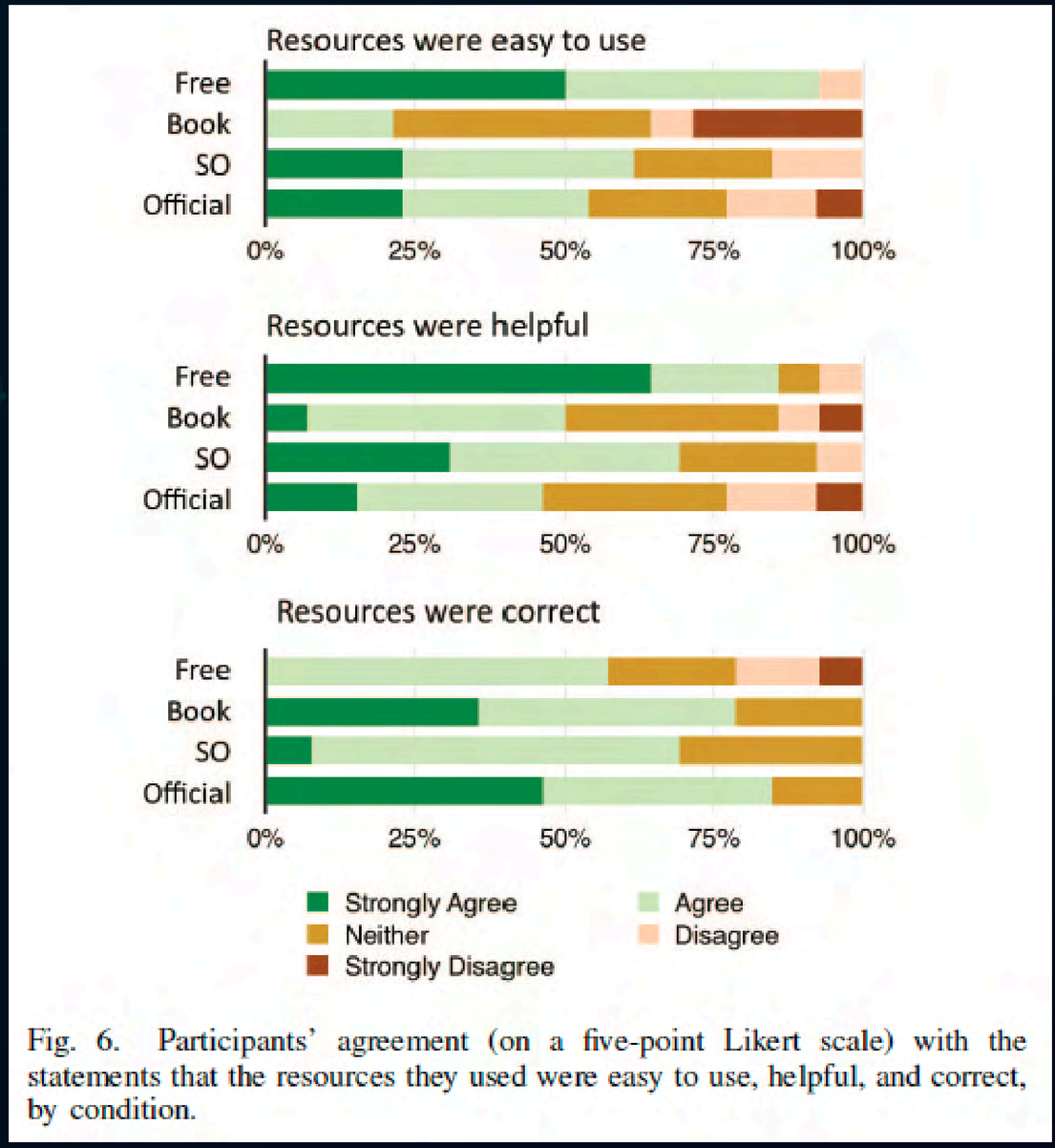


Fig. 6. Participants' agreement (on a five-point Likert scale) with the statements that the resources they used were easy to use, helpful, and correct, by condition.

Quality of Stack Overflow Responses

Answers in the thread include ...	Count	
Useful answers	35	(85.4%)
Useless answers	6	(14.6%)
Discussion of security implications	12	(29.3%)
Working code examples	20	(48.8%)
Only secure code examples	7	(17.0%)
Only insecure code examples	10	(24.4%)
...but also discussion of security implications	3	(30.0%)
Secure links	23	(56.1%)
Insecure links	6	(14.6%)
Links to GitHub	4	(9.8%)
Links to other code repositories	1	(2.4%)
Links to other Stack Overflow threads	4	(9.8%)
Only secure code examples and secure links	3	(7.3%)

TABLE V
PROPERTIES OF THE 41 ON-TOPIC STACK OVERFLOW THREADS ACCESSED DURING THE LAB STUDY.

Stack Overflow Threads			
with code snippets		**without code snippets**	
mean	97.7	mean	3.9
median	12	median	2.5
sd	163.9	sd	4.4
W = 319.5, p = 0.00217, α = 0.025 (B-H)			
with secure code snippets		**with insecure code snippets**	
mean	204.3	mean	70.2
median	145	median	14
sd	209.3	sd	122.4
W = 73, p = 0.188			
with security implications		**without security implications**	
mean	135.2	mean	17.4
median	16	median	3
sd	207	sd	37
W = 239.5, p = 0.0308, α = 0.05 (B-H)			

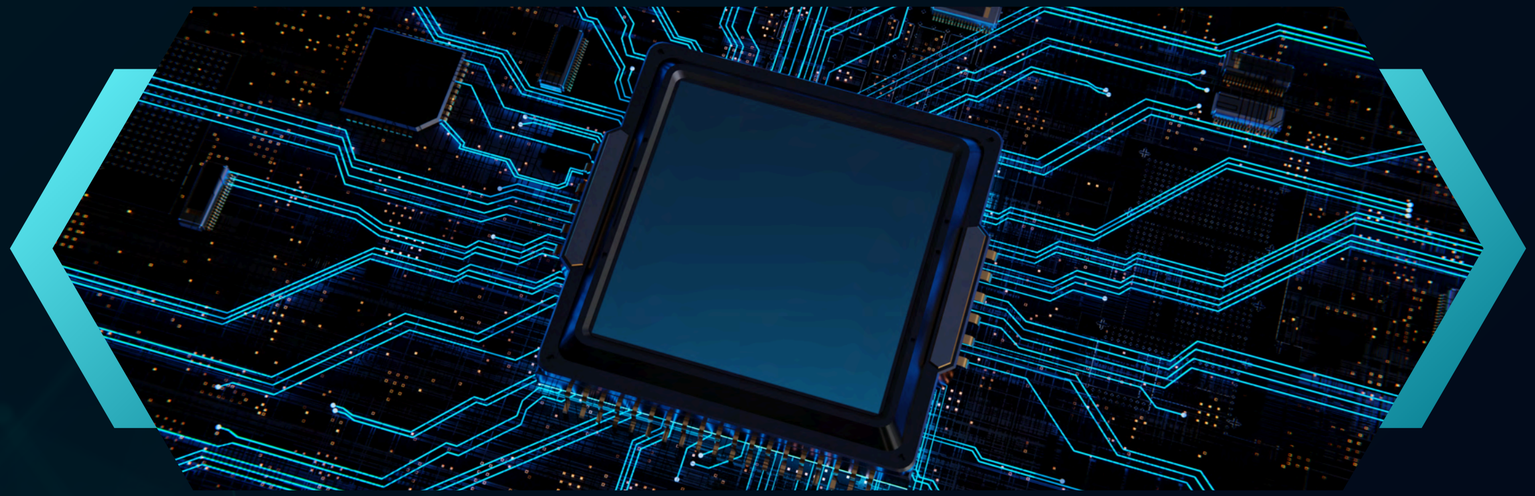
TABLE VI
POPULARITY RATINGS FOR THREADS CONTAINING CODE SNIPPETS.

Programming Task Validity

	secure	apps
Secure Networking Task		
broken hostname verifier	○	19,520
alternative hostname verification	●	214
ICC Task		
service	-	42,193
intent filter	○	8,133
exported=true	○	3,796
permission	◐	3,827
permission, signature	●	86
permission, signature or system	●	15
Secure Storage Task		
filesystem, private	●	120,834
filesystem, public	○	34,183
database, private	●	4,471
database, public	○	154
shared preferences, private	●	130,408
shared preferences, public	○	17,848
Least Permissions Task		
dial, permission	○	3,907
dial, no permission	●	48,832
call, permission	○	5,336
call, no permission	◐	6,157

● = secure; ○ = insecure

TABLE VII
RESULTS OF STATICALLY ANALYSING A RANDOM SAMPLE OF 200,000 ANDROID APPS.



LIMITATIONS

- The low response rate for online survey
- An artificial scenario
- a majority of lab participants were students rather than professional developers
- Stack Overflow threads are limited to only those accessed by lab study participants
- False positives on static code analysis.

PART 4:

DISCUSSION