Hidden in Plain Bytes

Investigating Interpersonal Account Compromise with Data Exports

Julia Nonnenkamp, Naman Gupta,
Abhimanyu Dev Gupta, Rahul Chatterjee

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

Madison
TECH CLINIC

Content Warning: Descriptions of technology abuse in intimate partner violence.

In **interpersonal** abuse contexts[1]

(intimate partner violence, elder abuse),

abusers often perpetuate control through technology

often by compromising survivors' **online accounts**.

1. Doerfler, 2019

Interpersonal Account Compromise is...

very common

2 in 3 intimate partner violence (IPV) survivors report account "hacking"

Freed et al., 2018

technologically simple

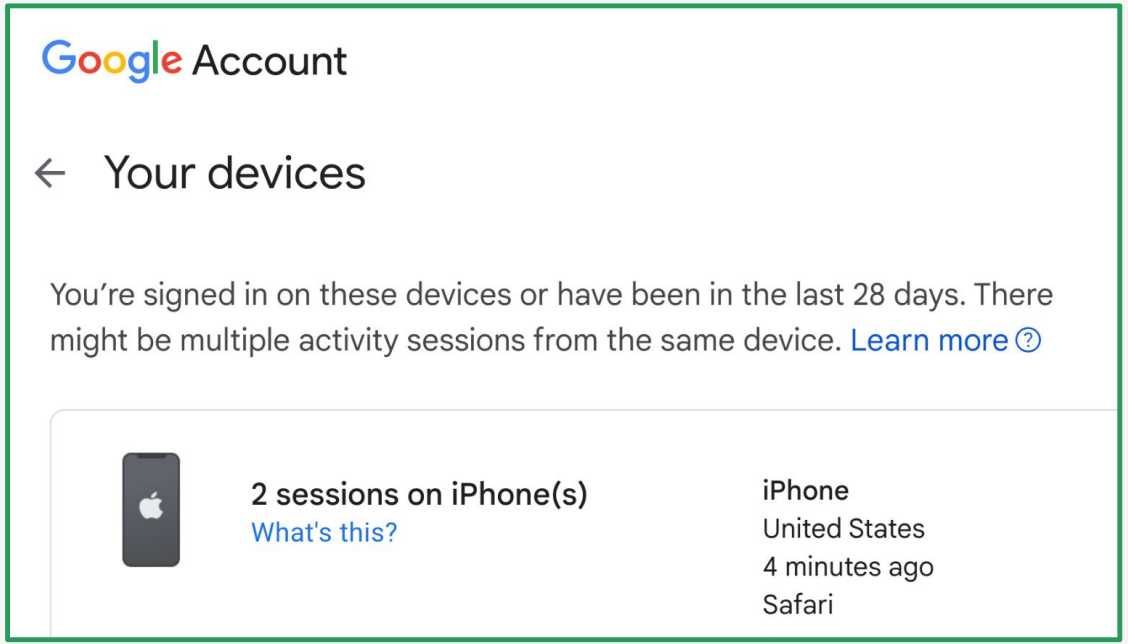
Known credentials

Physical access to devices

Identifying **Account Compromise**

Daffalla et al., 2023:

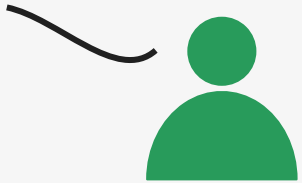
“Account Security Interfaces”



Is my account compromised?

Who did it?

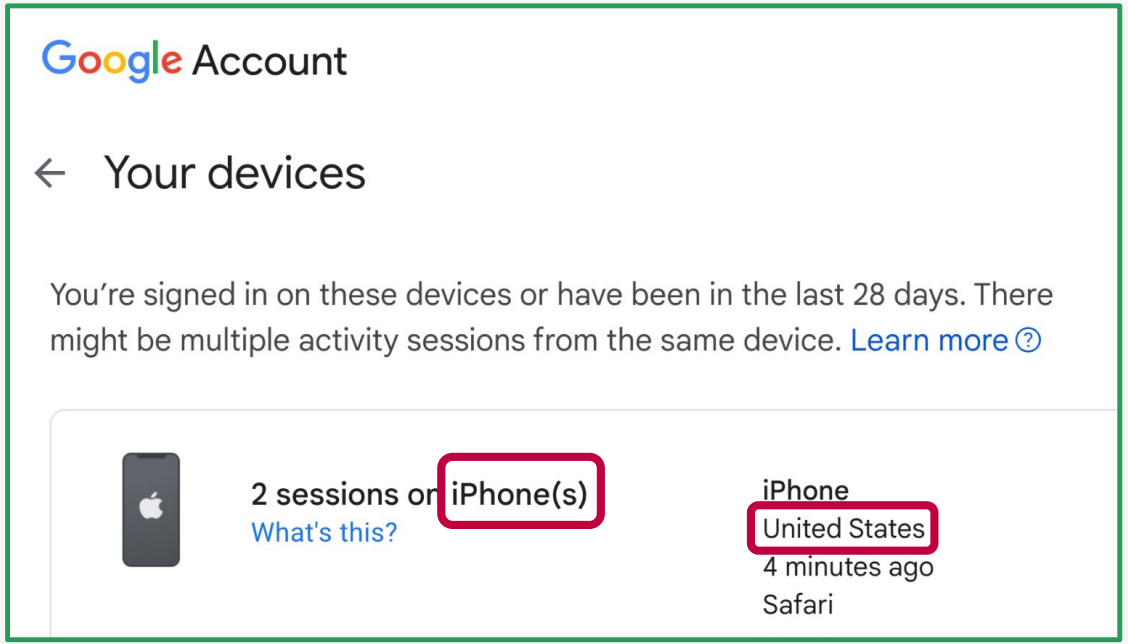
When?



Identifying **Account Compromise**

Daffalla et al., 2023:

“Account Security Interfaces”



Limitations

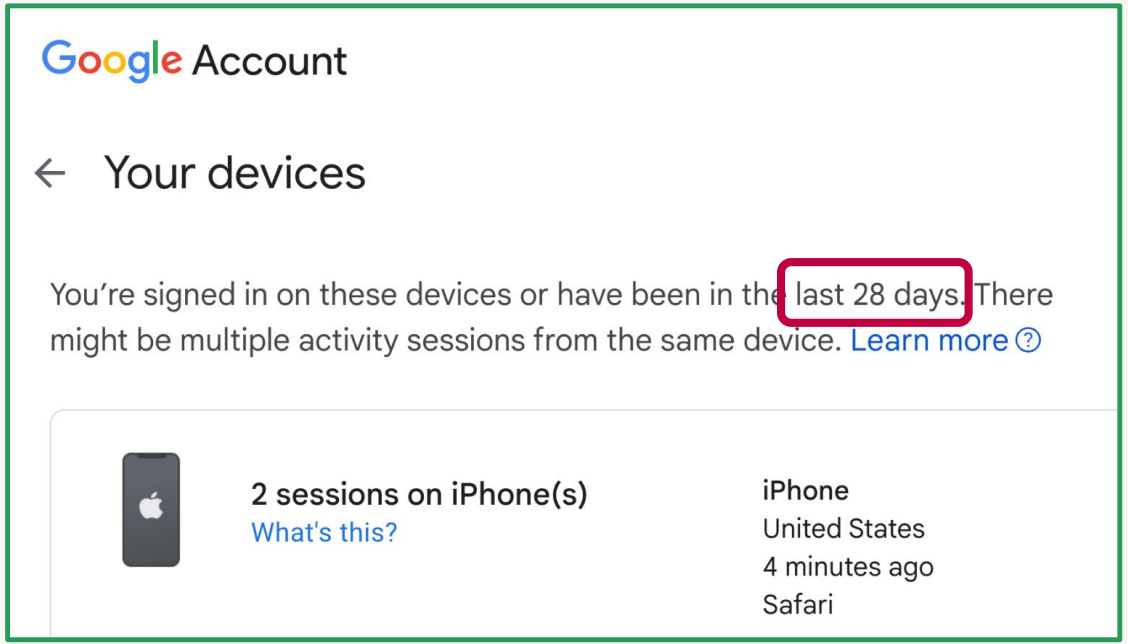
Malicious device recognition

- Device IDs
- Location

Identifying **Account Compromise**

Daffalla et al., 2023:

“Account Security Interfaces”



Limitations

Malicious device recognition

- Device IDs
- Location

Limited time window

But there's **another way** users can access account activity data.

Personal Data Exports

Right of Access

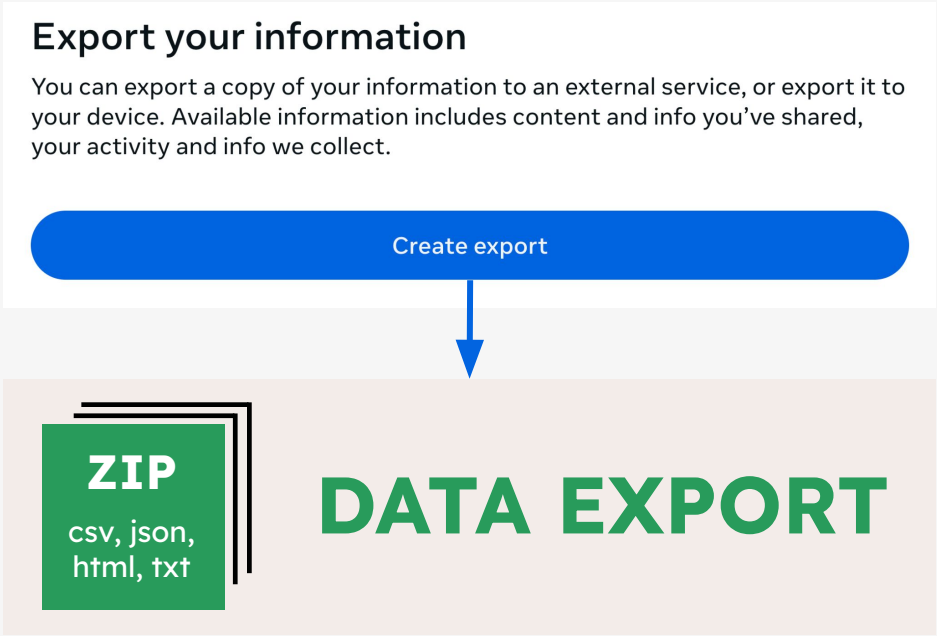
GDPR

LGPD
Lei Geral de Proteção de Dados Pessoais

CCPA

DPDPA

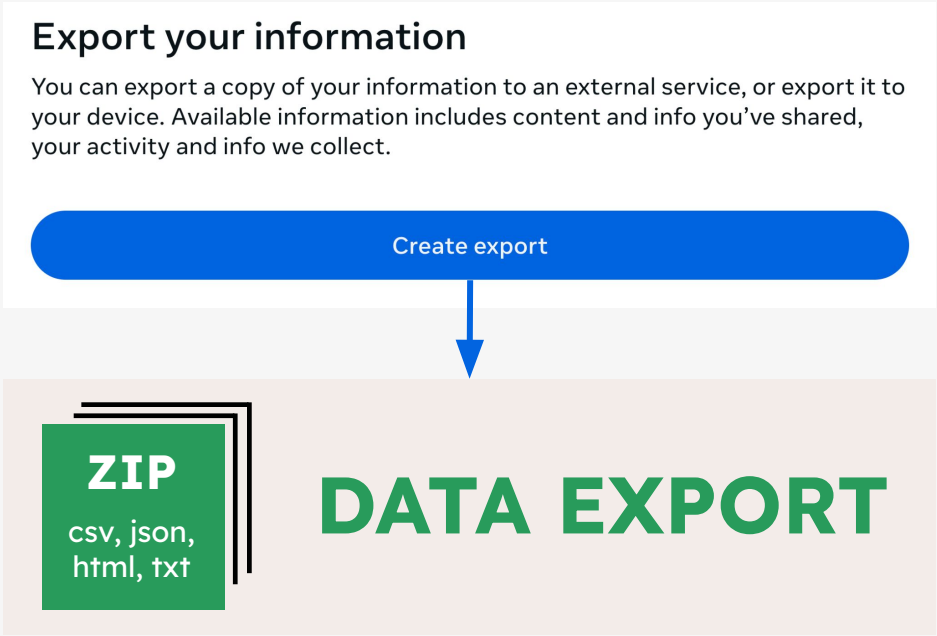
Users request their data



Personal Data Exports

Can we use data exports to **investigate** interpersonal account compromise?

Users request their data



RQ1

What relevant **security information** exists in data exports?

RQ2

How does it **compare** with account security interfaces?

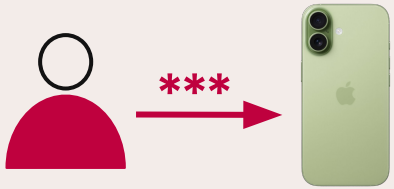
RQ3

To what extent can we **map attacker actions** within data exports?

Method

DATA COLLECTION

Simulate account compromise attacks

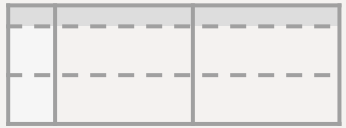


Request data

PREPROCESSING

Clean data

Parse into generic data model



ANALYSES

RQ1 Qualitative Content Analysis

RQ2 UI Walkthrough

RQ3 Targeted Queries *by time & device ID*

Data Collection

6 SERVICES

iCloud

Discord

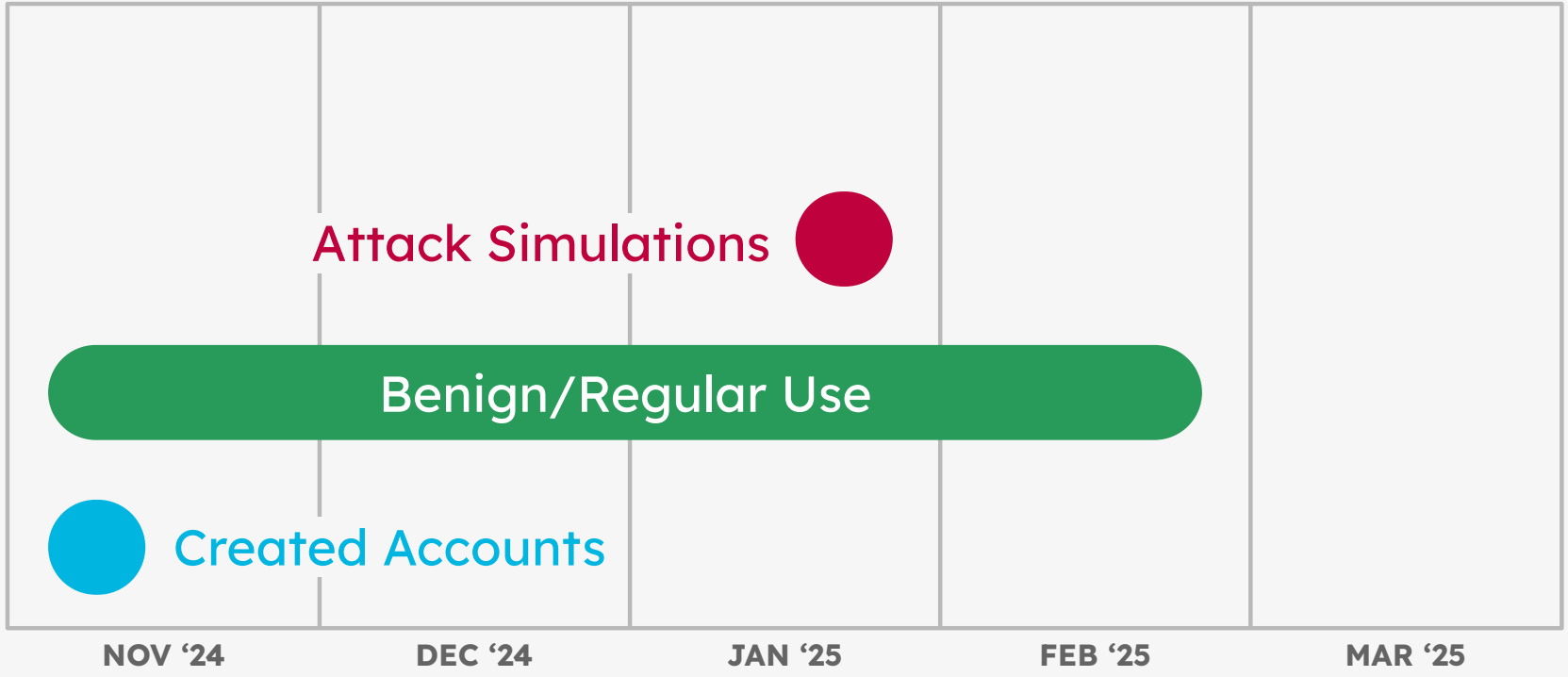
2 USER PERSONAS

with researcher-controlled iPhones & accounts

Target

Attacker

Data Collection



Attack Simulations

technologically simple

Known credentials

Physical access to devices

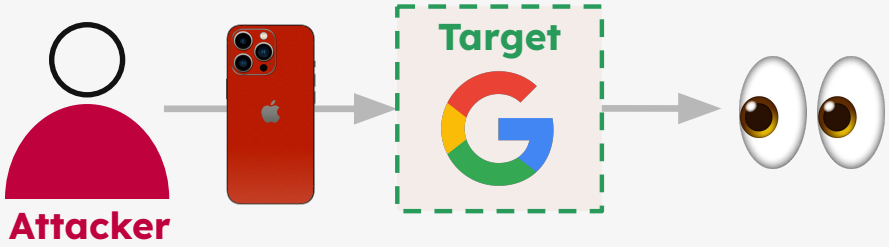
4 Types of ***Interpersonal Account Compromise*** Attacks

Based on Thomas et al., 2021

Attack Simulations

A1. Account Surveillance

Attacker logs into **target account**, browses.



Attack Simulations

A1. Account Surveillance — **Attacker** logs into **target account**, browses.

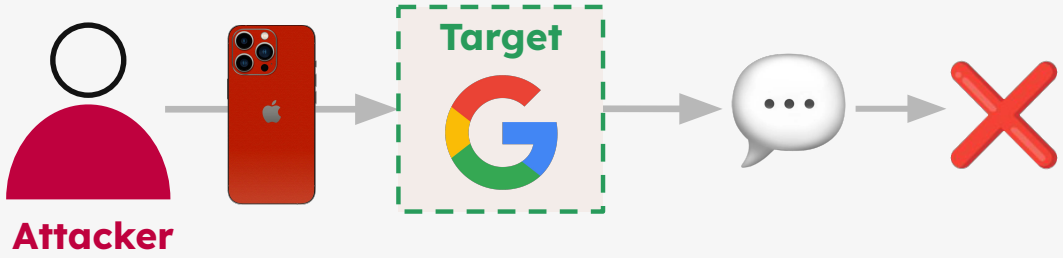
A2. Location Monitoring — **Attacker** accesses **target phone** and shares its live location with **attacker**.

Attack Simulations

A1. Account Surveillance — **Attacker** logs into **target account**, browses.

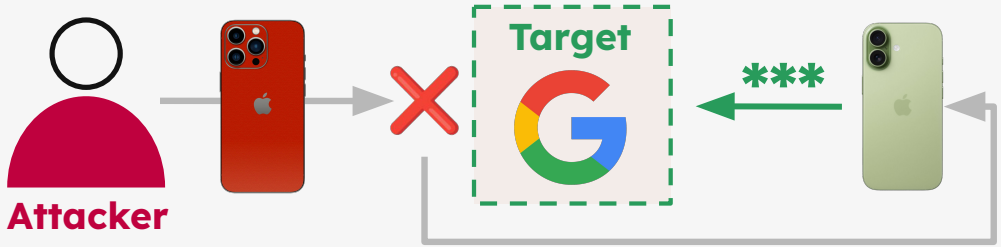
A2. Location Monitoring — **Attacker** accesses **target phone** and shares its live location with **attacker**.

A3. Impersonation — **Attacker** logs into **target account**, sends a message, then deletes it.

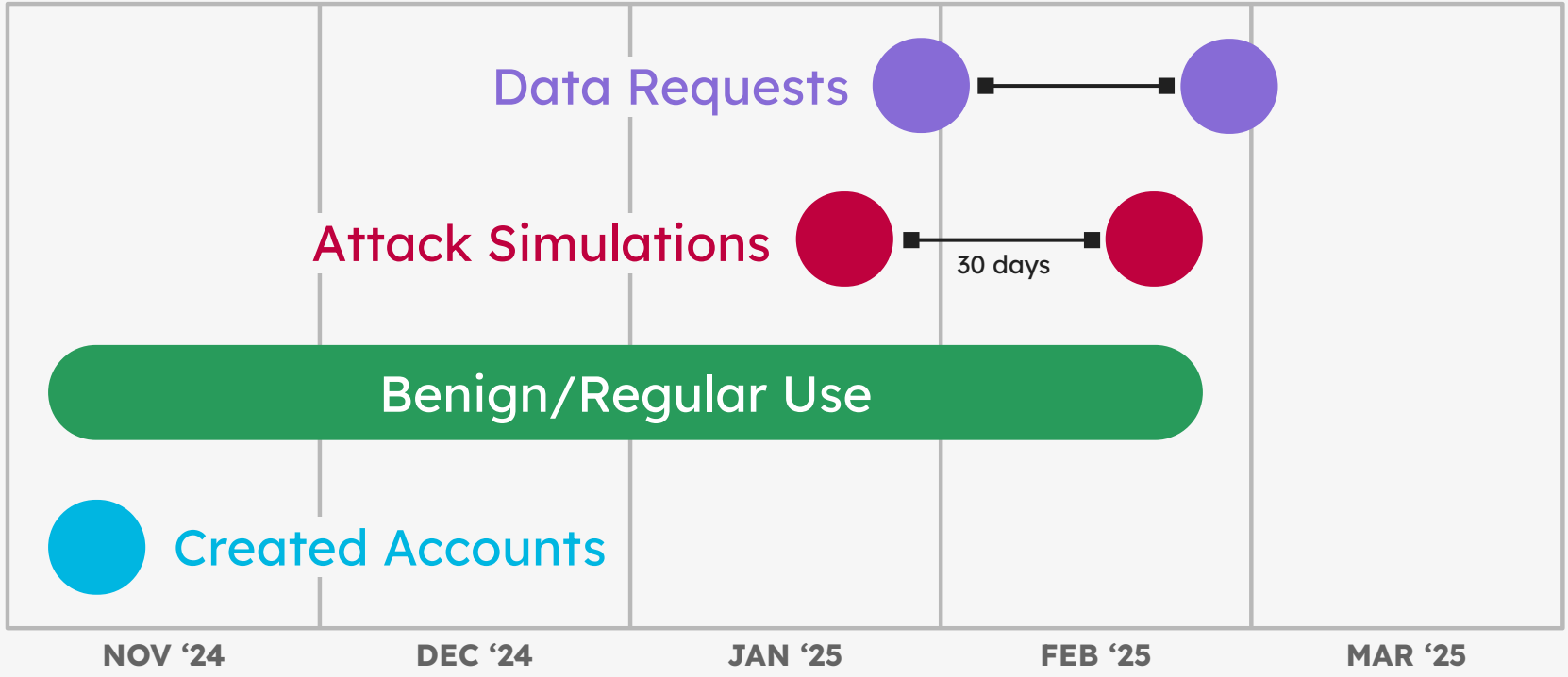


Attack Simulations

A1. Account Surveillance	**Attacker** logs into **target account**, browses.
A2. Location Monitoring	**Attacker** accesses **target phone** and shares its live location with **attacker**.
A3. Impersonation	**Attacker** logs into **target account**, sends a message, then deletes it.
A4. Lockout & Control	**Attacker** attempts to log into **target account**, resets password via **target phone**.



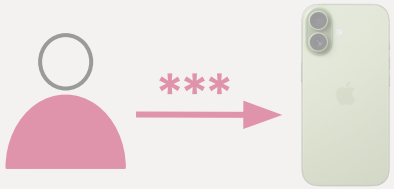
Data Collection



Method

DATA COLLECTION

Simulate account compromise attacks

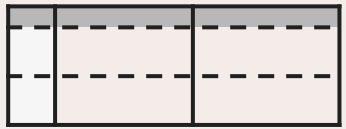


Request data

PREPROCESSING

Clean data

Parse into generic data model



ANALYSES

RQ1 Qualitative Content Analysis

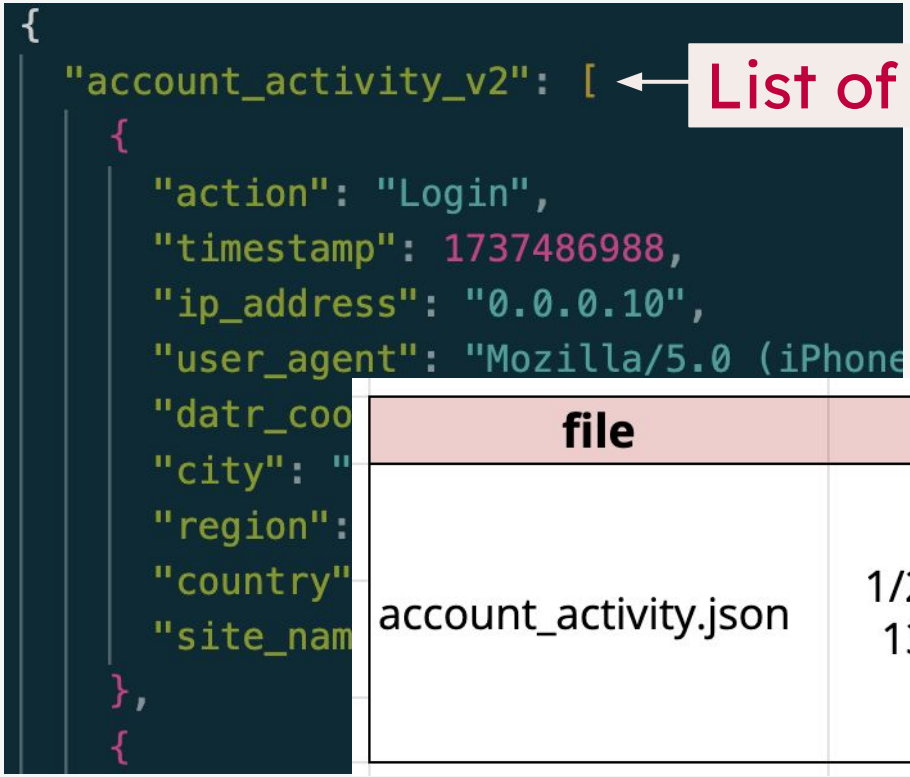
RQ2 UI Walkthrough

RQ3 Targeted Queries *by time & device ID*

Preprocessing

List of data elements

Preprocessing



List of data elements

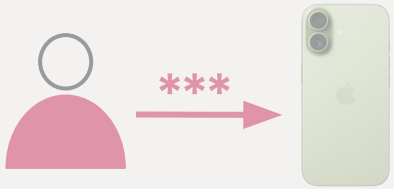
Generic Parser

file	ts	attribute	value
account_activity.json	1/21/2025 13:16:28	account_activity_v2. **action**	*Login*
		account_activity_v2. **ip_address**	*0.0.0.10*
		....	

Method

DATA COLLECTION

Simulate account compromise attacks

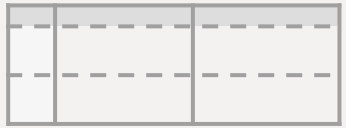


Request data

PREPROCESSING

Clean data

Parse into generic data model



ANALYSES

RQ1 Qualitative Content Analysis

RQ2 UI Walkthrough

RQ3 Targeted Queries *by time & device ID*

RQ1

What relevant **security information** exists in data exports?

SECURITY INFORMATION

1. Authentication Records
2. Changes to Security Settings

POST-AUTHENTICATION ACTIVITY

e.g., notifications, messages, clicks

RQ2

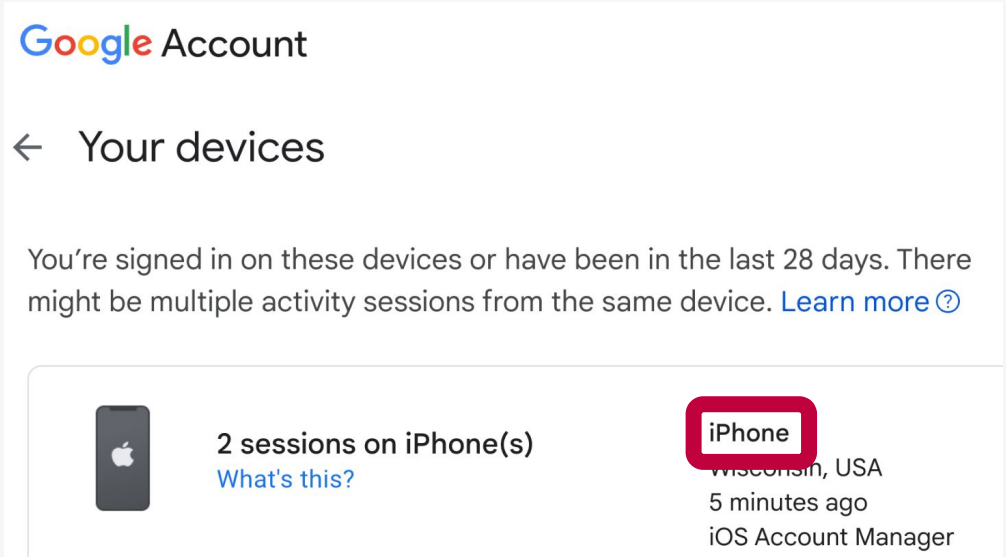
How do exports **compare** with account security interfaces?

Event	Interfaces	Data Exports
📲 Active Sessions	✅ All services	✅ All services
🕰️ Historical Logins	⚠️ 1/6 - full history 3/6 - time limit, “risky”	✅ All services
📩 Email Changes	⚠️ 1/6 - full history 1/6 - time limit	✅ All services
🔐 Password Changes	⚠️ 1/6 - full history 3/6 - time limit	✅ 5/6 services

RQ2

Exports contain **more granular device IDs** than interfaces

NOTE
Most device IDs are likely *not* robust against spoofing



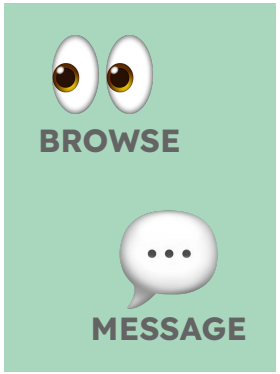
Google: SubscriberInfo.html

```
<td>2024-11-15 23:04:51 Z</td>
<td>0.0.0.6</td>
<td>Login</td>
<td>false</td>
<td></td>
<td>US,Wisconsin,Madison</td>
<td>
  "com.google.Gmail/6.0.241027
  iSL/3.4 iPhone/17.7.1
  hw/iPhone11_8
  (gzip),gzip(gfe)"
</td>
```

RQ3

To what extent can we **map attacker actions** within data exports?

Attack steps we could attribute to the origin device

ATTACKS	AUTHENTICATION	POST-AUTH ACTIVITY	
A1. Account Surveillance			
A2. Location Monitoring			
A3. Impersonation			
A4. Lockout & Control	✅ All services	✅ Google, Discord	❌ None

Takeaways

1. **Method:** We simulated 4 account compromise attacks on 6 platforms and analyzed data exports from the target account.
2. **Exports > Interfaces:** Exports provide strictly more historical authentication data. Discord & Google's exports enable attribution of other activity to the attacker's device.
3. **Impact:** Survivors can identify attacks & plan for their safety.

Questions?

JULIA NONNENKAMP
PhD student
nonnenkamp.com – *she/her*
WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON