

Examining Leading Pakistani Mobile Apps

Sana Habib¹, Mohammad Taha Khan², and Jedidiah R.
Crandall^{1,3}

¹Arizona State University

²Washington and Lee University

³Breakpointing Bad

Free and Open Communications on the Internet, February
2025



Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology
- 7 Results
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!

Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology
- 7 Results
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!

Motivation: Local Situation

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

ALJAZEERA News - Middle East Explained Opinion Sport Video

Trending > Russia-Ukraine war Gaza Donald Trump ICC

EXPLAINER
News | Imran Khan

Imran Khan vs Pakistan's government: A timeline of political upheaval

As PTI supporters clash with security forces in Islamabad, here's a look back at how Pakistan got here.



02:03

Anniversary of ex-Pakistan PM's arrest: Imran Khan's supporters protest one year on

UPDATED February 08, 2025

By RFE/BL's Radio Mashaal

Pakistan's Opposition Takes To Streets On Anniversary Of Disputed Elections



Supporters of jailed former Pakistani Prime Minister Imran Khan attend a rally in Swabi (file photo)

SWABI, Pakistan -- Pakistani opposition parties, including the Tehreek-e-Insaf (PTI) party of imprisoned former Prime Minister Imran Khan, staged demonstrations on February 8 to mark the first anniversary of the country's general elections, which triggered widespread allegations of vote-rigging.

Motivation: Local Situation

May 20, 2023 9:00AM EDT

Pakistan: Mass Arrests Target Political Opposition

Uphold Rights While Prosecuting Khan Protest Violence



Police detain a supporter of Pakistan's former Prime Minister Imran Khan during clashes, in Islamabad, Pakistan, May 12, 2023. © 2023 W.K. Youssafraji/AP Photo

(New York) – [Pakistani](#) police have carried out mass arrests and detained more than 4,000 people in

MORE READING



February 17, 2025 | Report

China: Right to Leave Country Further Restricted



February 17, 2025 | Dispatches

North Korea's Unrelenting Human Rights Crisis

MOST VIEWED

1 December 15, 2024 | Report
Sudan: Fighters Rape Women and Girls, Hold Sex Slaves



2 February 18, 2025 | News Release
Human Rights Watch Board Announces Leadership Transition

3 May 17, 2021 | Report
"Years Don't Wait for Them"



Motivation: Local Situation

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

MEDIA | PAKISTAN

Press Freedom Day: Why are journalists fleeing Pakistan?

Anas Ahmed
05/03/2024

Acute security risks, intimidation, online abuse and severe financial woes are forcing many media professionals to leave the country.

f X 



Navigation icons: back, forward, search, refresh, etc.

Motivation: Local Situation

WORLD NEWS 2 JANUARY 2025

Pakistan installs China-style firewall, arrests social media users

by PAUL ANTONOPOULOS



Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology
- 7 Results
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!

Research Question

- Is it possible to use leading Pakistani Android apps for spying, monitoring, and targeting vulnerable Pakistani citizens?
- If so, who could potentially misuse these apps, and by what methods could they do so?

Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection**
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology
- 7 Results
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!

App Selection

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!



- **Criteria:** (i) Popularity, (ii) Necessity, (iii) Timeliness, (iv) Personal Data Collection, (v) Local Situation.
- **Government Apps:** (i) Pak Identity, (ii) Pakistan Citizen Portal, (iii) Qeemat Punjab.
- **Telco Apps:** (i) SIMOSA (Previously Jazz World), (ii) My Zong, (iii) My Telenor, (iv) UPTCL.

Government Apps



	App Title	Use	Popularity
1.	Pak Identity	Request, Modify, and Update National Identity Documents.	Downloads: 1M+
2.	Pakistan Citizen Portal	Grievance Redressal System.	Downloads: 5M+
3.	Qeemat Punjab	Get awareness regarding daily prices of agriproducts.	Downloads: 1M+

Telco Apps



	App Title	Use	Popularity
4.	SIMOSA	Manage your Jazz mobile plan.	Subscribers: \approx 71 M, Downloads: 50M+
5.	My Zong	Manage your Zong mobile plan.	Subscribers: \approx 49 M, Downloads: 50M+
6.	My Telenor	Manage your Telenor mobile plan.	Subscribers: \approx 44 M, Downloads: 50M+
7.	UPTCL	Manage your UPTCL mobile plan.	Subscribers: \approx 26 M, Downloads: 10M+

Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities**
- 5 Victim Types
- 6 Methodology
- 7 Results
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!

Attacker Types



- **State Attacker:** Actors within local police, district police, and specialized units such as the Federal Intelligence Agency (FIA) and similar organizations.
- **Private Attacker:** Individuals associated with criminal organizations, drug cartels, extremist groups, and perpetrators of domestic abuse.
- **Hybrid Attacker:** Corrupt individuals within government organizations and those who can be influenced or coerced by corrupt actors.

Attacker Capabilities

- **Physical Device Compromise.** All three attacker types can compromise the physical device through:
 - Confiscation.
 - Stealth.
 - Shared device.
 - Usurpation.
- **In-path Network Position.** An in-path network position with access to the server's private key allows attackers to:
 - View data in plaintext.
 - Monitor at-risk users' activities.
 - Extract sensitive information, such as emails and passwords.
 - Intercept and modify data in real time.
 - Fabricate evidence and frame the user.

Attacker Type: State Attacker

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

- Can have access to the **server private key**.
- Can **confiscate** user device.
- Can do **in-path network manipulation**.
- Can **forcefully retrieve user credentials** from the server.



Attacker Type: Private Attacker

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

- Can **steal** user device.
- Can do **in-path network manipulation** (if private attacker controls local network infrastructure—such as a home router).



Attacker Type: Hybrid Attacker

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

- Can have access to the **server private key**.
- Can **confiscate** user device.
- Can do **in-path network manipulation**.
- Can **forcefully retrieve user credentials** from the server.



Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types**
- 6 Methodology
- 7 Results
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!

Victim Types



- At-Risk Members of the Pakistani Media.
- Victims of Domestic Abuse-Passion Offender.
- Protestors, Activists, and Human Rights Defenders.

Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology**
- 7 Results
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!

Methodology: Threat Classification

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

- **Unnecessary Disclosure.**
 - Excessive PII collection.
 - Exposed PII via their storage in plaintext in the Android File System.
- **Login Weaknesses.**
 - Missing Password.
 - Missing Login Detection.
- **Network Security Threats.**
 - Missing TLS.
 - Possibility of Eavesdrop and Modify.

Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology
- 7 Results**
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!

Results: Root Detection and SSL Pinning Capabilities

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

	App Title	Root Detection	SSL Pinning
1.	Pak Identity	×	✓
2.	Pakistan Citizen Portal	×	
3.	Qeemat Punjab	×	✓
4.	SIMOSA	×	✓
5.	My Zong	×	✓
6.	My Telenor	×	✓
7.	UPTCL	✓	✓

Results: Embedded Certificates

	App Title	Embedded Certs (directory inside app package)
1.	Pak Identity	—
2.	Pakistan Citizen Portal	res/raw/pmdu_gov_pk.crt
3.	Qeemat Punjab	—
4.	SIMOSA	assets/jazz_cert.crt, assets/new_cert.der
5.	My Zong	assets/golootlo_key_prod.pem, assets/zong-staging-public-key.pem
6.	My Telenor	assets/cbg_root.cer, res/GX.pem
7.	UPTCL	—

Results: PII Stored by Apps.

Keys: D → Days, Hrs → Hours.

	App Title	Call History (30D,14D,7D,24Hrs)	SMS History (30D,14D,7D,24Hrs)
1.	Pak Identity	×	×
2.	Pakistan Citizen Portal	×	×
3.	Qeemat Punjab	×	×
4.	SIMOSA	✓, ✓, ✓, ✓	✓, ✓, ✓, ✓
5.	My Zong	×, ×, ✓, ✓	×, ×, ✓, ✓
6.	My Telenor	×, ×, ✓, ✓	×, ×, ✓, ✓
7.	UPTCL	×, ✓, ✓, ✓	×, ✓, ✓, ✓

Results: PII Stored by Apps.

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

		Tax Certificate	Location Coordinates
1.	Pak Identity	×	Required.
2.	Pakistan Citizen Portal	×	Required.
3.	Qeemat Punjab	×	Required.
4.	SIMOSA	✓	Optional.
5.	My Zong	✓	Optional.
6.	My Telenor	✓	Optional.
7.	UPTCL	✓	Optional.

Results: Tax Certificate



CERTIFICATE OF COLLECTION OR DEDUCTION OF TAX ISSUED UNDER SECTION 164 READ WITH RULES 42 OF THE INCOME TAX ORDINANCE,2001

S.No.: 000000007921164

Original

Date of issue: 21-May-2024

Certified that a sum of Rupees 1040.84/-(one thousand and forty point eight four Rupees) on account of income tax has been collected from:

[REDACTED], Username

Present address [REDACTED] GPO Region PN Country
Pakistan

National Tax Number:

NIC/CNIC No.:

for Mobile Number:

during the period:

under section:

on account of:

on the value/amount of:

[REDACTED]

92321 [REDACTED]

Fiscal Year 2021-2022

236

Telephone usage

Rupees 8929.03/-

Rupees eight thousand, nine hundred and twenty-nine point zero

Results: Transmission of Location Coordinates

Request Response Connection Timing

POST https://shanakht.nadra.gov.pk/authentication/api/v1/authenticate/ HTTP/1.1

authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzZdWI0iJzaGF1aWZzQGZzZD55LWZHU1lCjYpYXQ1OjE3MDg0OEExMDIsImV4cCI6MTc0MDEwMDEwMn0uG8LuU0cqqYvGnGneBgBMGoN_GIiYQ8VB5f5yDXLzW6GYnDzaNNQ8yOtLSGFKOz60jzXJkjPoz6IeyBoY1bJFA

x-app-version: 3.0.1

accept-encoding: gzip, deflate, br

accept: */*

x-device-id: ekBNG559RBW88rfgJdB0_c:APA91bf851oHtsuaJ9IuT8uCBu31SeNmDMS11EJgFdMTzYTgKNPraTEVY8rmhuZoLAGV4LfnJMLMq5rWzWYZq9SFIIIfXuuM7TjFswDHWlmeMmLorXQp3kE1wdo448I9ws3LNUJ3j6km

Content-Type: application/json

Content-Length: 788

Host: shanakht.nadra.gov.pk

Connection: Keep-Alive

User-Agent: okhttp/4.9.2

JSON

```
{
  "email": " ",
  "password": " ",
  "publicKey": "-----BEGIN RSA PUBLIC KEY-----\nMIIBCgKCAQEAvglpYOR/I9YR0PgmY50uyNsdyPP+HGd6/hHyP4g60UzsNeGuN27\n",
  "userLoginMetaInfo": {
    "deviceId": "ekBNG559RBW88rfgJdB0_c:APA91bf851oHtsuaJ9IuT8uCBu31SeNmDMS11EJgFdMTzYTgKNPraTEVY8rmhuZoLAGV4LfnJMLMq5rWzWYZq9SFIIIfXuuM7TjFswDHWlmeMmLorXQp3kE1wdo448I9ws3LNUJ3j6km",
    "deviceName": "29",
    "deviceOS": "android",
    "latitude": " ",
    "longitude": " "
  }
}
```


Results: Unnecessary Disclosure



App Title	PII	Storage Location
Pak Identity	Full Name, Email ID, Password, Mobile Number, Citizen ID, Location Coordinates	cd/ata/data/pk.gov .nadra.pakid/databases/ RKStorage, cd/data/data/ pk.gov.nadra.pakid/databases /RKStorage-journal

(Details are in the paper.)

Results: Login Weaknesses

◆ → State Actor, ▲ → Private Actor, ■ → Hybrid Actor

	App Title	Missing Password	Missing Login Detection
1.	Pak Identity	×	◆ ▲ ■
2.	Pakistan Citizen Portal	×	◆ ▲ ■
3.	Qeemat Punjab	×	◆ ▲ ■
4.	SIMOSA	◆ ▲ ■	◆ ▲ ■
5.	My Zong	◆ ▲ ■	◆ ▲ ■
6.	My Telenor	◆ ▲ ■	◆ ▲ ■
7.	UPTCL	◆ ▲ ■	◆ ▲ ■

Results: Network Security Threats

 → State Actor,
  → Private Actor,
  → Hybrid Actor
   → Respective Attackers can Eavesdrop.

	App Title	Missing TLS	Traffic Interception & Manipulation
1.	Pak Identity	×	  
2.	Pakistan Citizen Portal	×	  
3.	Qeemat Punjab	×	  
4.	SIMOSA	×	
5.	My Zong	×	  
6.	My Telenor	×	  
7.	UPTCL	×	

Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology
- 7 Results
- 8 Exploitation**
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!

Exploitation: Exposed PII via Government Apps



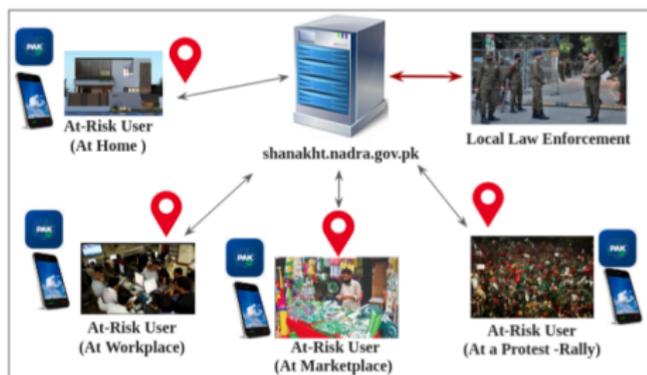
- 1 An at-risk user installs and uses the government apps on their phone.
- 2 An attacker confiscates or steals user device.
- 3 The attacker gains root access to the device and retrieves **sensitive personal information (PII)**.



Exploitation: Exposed PII via Government Apps



Real-time geo-location tracking.



Exploitation: Network Security Threats via Government Apps (Planting Fake Location Coordinates)

The screenshot shows a network traffic analysis tool interface. At the top, it indicates a '-bq email' session. Below that, there are tabs for 'Resume All' and 'Intercept'. The main view shows a 'Request' tab selected, displaying a POST request to 'https://shanakht.nadra.gov.pk/authentication/api/v1/authenticate/'. The request headers include 'authorization: Bearer eyJhbGciOiJIUzUuMiIsImVudCI6IjEwLjZaGFjZWZ6dSS1ZmU1LjIyYXQ1OjE3MDg4OTc0MzImInV4cCI6MTcxMDQ5MzQzM30uEhEaGndrCyx9XQEVd-f4pZMQTMRFTuGVf6VuCCOK4tCsaeZX117k_s6tEtKvh1k9505916E19AnJGyMaq'. The request body is a JSON object with the following structure:

```
Content-Type: application/json
Content-Length: 768
Host: shanakht.nadra.gov.pk
Connection: Keep-Alive
User-Agent: okhttp/4.9.2
```

The JSON body contains fields for 'email', 'password', 'publicKey', 'userLoginMetaInfo', 'deviceId', 'deviceName', 'deviceOS', and 'location'. The 'location' field is highlighted with a red box and contains the following values:

```
"location": {
  "latitude": 0,
  "longitude": 0
}
```

Exploitation: Exposed PII via Telco Apps



- 1 An at-risk user's device is confiscated or stolen.
- 2 The attacker, having knowledge of an at-risk user's mobile number installs the app and retrieves PII.



Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology
- 7 Results
- 8 Exploitation
- 9 Disclosure**
- 10 Conclusion
- 11 Thank you!

Disclosure

Motivation

Research
Question

App Selection

Attacker
Types and
Capabilities

Victim Types

Methodology

Results

Exploitation

Disclosure

Conclusion

Thank you!

	App Title	Email/Complaint Date
1.	Pak Identity	Mar 14, 2024; Apr 13, 2024
2.	Pakistan Citizen Portal	Mar 14, 2024; Apr 09, 2024
3.	Qeemat Punjab	Mar 14, 2024; Apr 13, 2024
4.	SIMOSA	June 24, 2024
5.	My Zong	Nov 03, 2024
6.	My Telenor	Nov 04, 2024
7.	UPTCL	July 30, 2024

Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology
- 7 Results
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion**
- 11 Thank you!

Conclusion

- There are significant security and privacy issues with the leading Pakistani Android apps.
- Users must exercise caution when using the app.

Outline

- 1 Motivation
- 2 Research Question
- 3 App Selection
- 4 Attacker Types and Capabilities
- 5 Victim Types
- 6 Methodology
- 7 Results
- 8 Exploitation
- 9 Disclosure
- 10 Conclusion
- 11 Thank you!**

Thank you!

- Contact: shabib3@asu.edu.
- This work was supported by Sana Habib's fellowship with the [Open Technology Fund's Information Controls Fellowship Program](#) and the [National Science Foundation](#) under Grant [CNS-2141547](#).
- Sana Habib gratefully acknowledges [Pakistan's non-profit digital rights foundation](#) for hosting her and the anonymous contributors whose insights were instrumental in the app selection process.
- We also sincerely thank the [anonymous reviewers](#) and [Shepherd](#) for their constructive feedback, which greatly enhanced the quality of this work.
- Image Credits: [LEGO.com - Shop, BrickLink - LEGO Minifigures](#).