RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -15

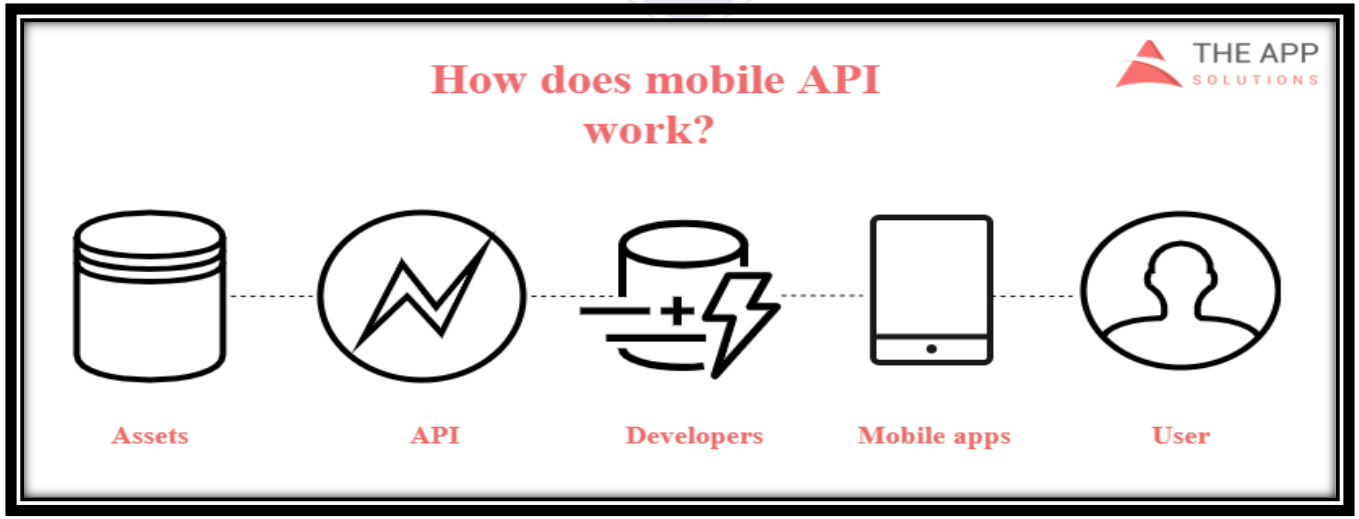
Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- Reliable Third-Party Library Detection in Android and its Security Applications
- What is the 3rd party API?
- Three main API use cases
- How to Secure an Android App
- MCQ
- References

What is the 3rd party API?

- When you come to a restaurant and want to order, you need a waiter who will deliver your order to the kitchen and bring it to your table.
- In this case, API performs as a waiter. It sends the request from your mobile app to a third-party system and delivers the result back to your app.
- Also known as an application programming interface, API is a defined method of communication between various software components with a set of subroutine definitions, tools, and protocols that allow your mobile app borrowing functionality and data from other apps or services.



Three main API use cases

The integrated API could perform the following actions:

Using other services features

- One example is apps that use PayPal's Braintree API as the payment gateway or our project Spotnews, an app with integrated Spotify API allowing users to listen to music while reading news.

Receiving other's services information

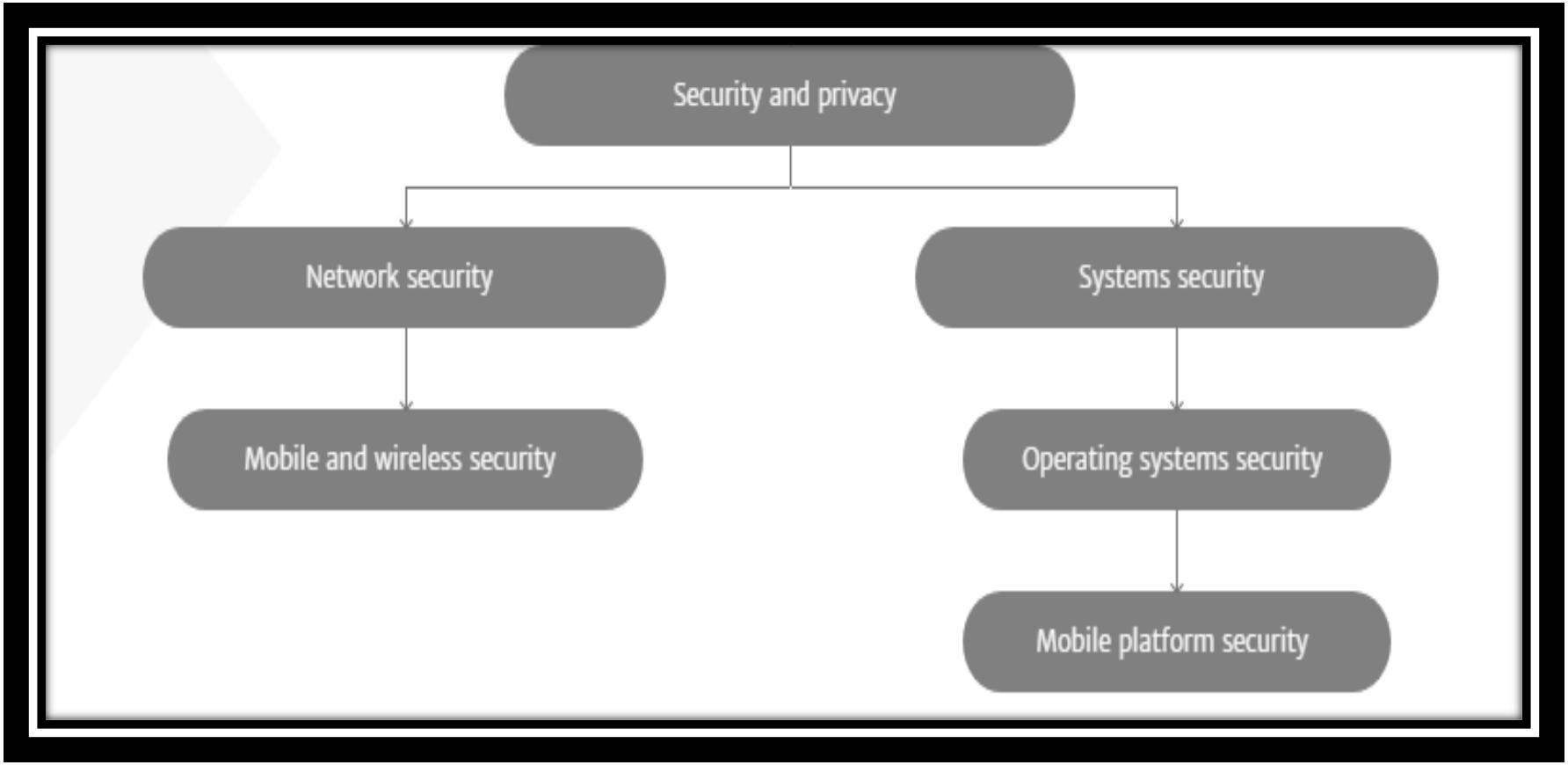
- For instance, by integrating New York's subway system API, you can provide your app users with real-time travel data, like the schedule of trains, arrival and departure.

Getting access to mobile app device functions

- Examples of such API integration are apps like Snapchat and Instagram which use the phone's camera API to take pictures. At the same time, Google Maps can define the user's location by using the phone's geolocation API.

In a nutshell, by using API, you can add new features to your app, get access to other services data or mobile device features, without spending a fortune on developing those features from scratch.

Reliable Third-Party Library Detection in Android and its Security Applications



How to Secure an Android App

The Android operating system has lots of built-in security features, such as application sandboxing, protection against buffer and integer overflow attacks, and segregated memory areas for program instructions and data. As a result, simple Android apps that don't perform any file system or networking operations can often be considered secure by default.

- **Use Internal Storage for Sensitive Data**

```
File myFile = new File(getFilesDir(), "myfile.dat");
```

- **Encrypt Data on External Storage**
- **Use Intents for IPC**
- **Use HTTPS**
- **Use GCM Instead of SMS**
- **Avoid Asking for Personal Data**
- **Validate User Input**
- **Use ProGuard Before Publishing**

MCQ

6. The full form of EDR is _____

a) Endpoint Detection and recovery

b) Early detection and response

c) Endpoint Detection and response

d) Endless Detection and Recovery

7. _____ technology is used for analyzing and monitoring traffic in network and information flow.

a) Cloud access security brokers (CASBs)

b) Managed detection and response (MDR)

c) Network Security Firewall

d) Network traffic analysis (NTA)

8. Compromising confidential information comes under _____

a) Bug

b) Threat

c) Vulnerability

d) Attack

9. Lack of access control policy is a _____

a) Bug

b) Threat

c) Vulnerability

d) Attack

10. Possible threat to any information cannot be _____

a) reduced

b) transferred

c) protected

d) ignored

REFERENCES

- https://code.tutsplus.com/articles/how-to-secure-an-android-app--cms-26385
- https://theappsolutions.com/blog/development/third-party-api-integration/