RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -27

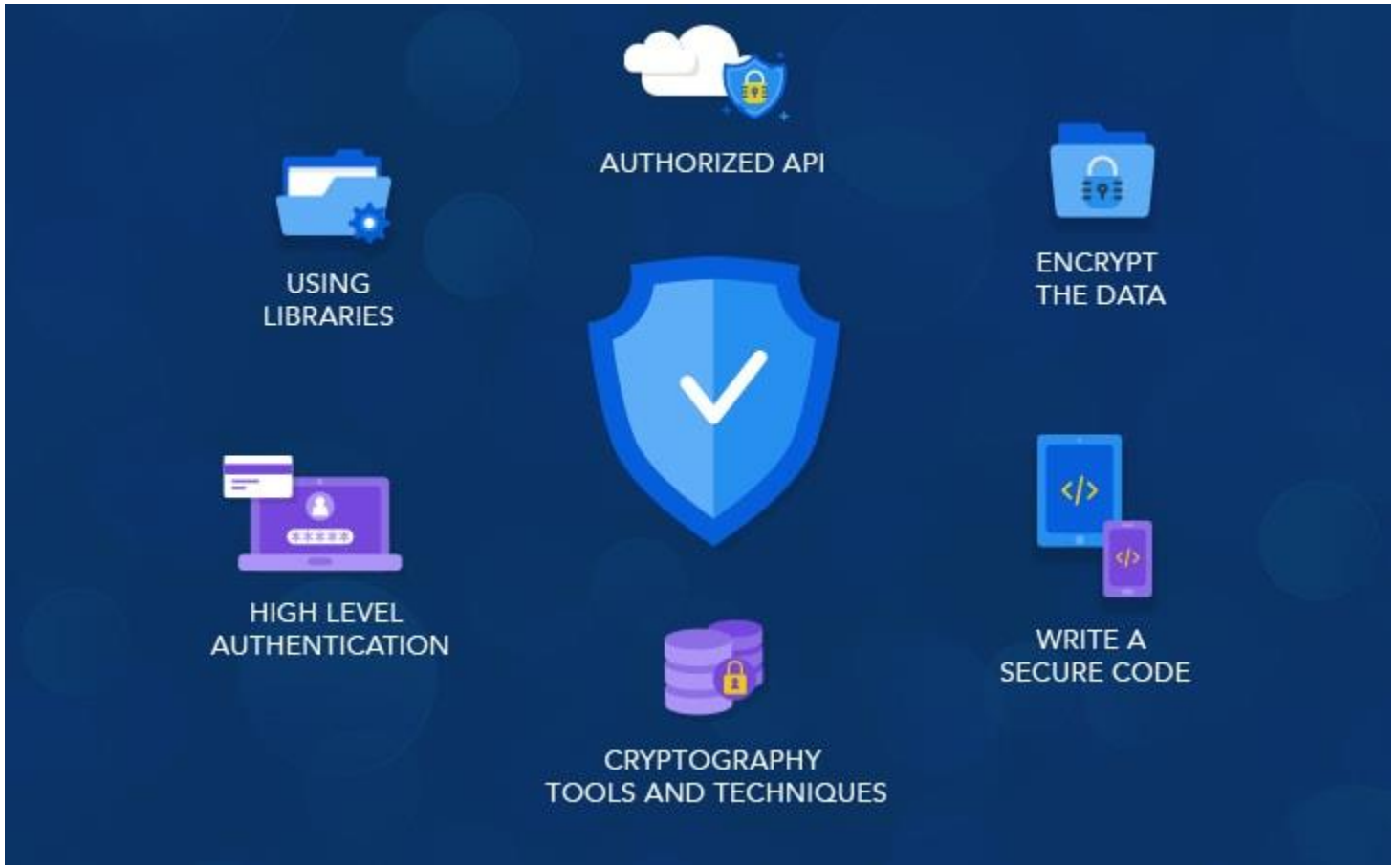
Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- Security issues for mobile app developers
- Some of the ways to build a completely secure mobile app:
- MCQ
- References

Security issues for mobile app developers

Mobile applications are going at par and with this rate of growth it is necessary that mobile app developers not only look at providing new and more features to the customers but also the security aspect of the application..



SECURITY ISSUES FOR MOBILE APP DEVELOPERS

Security issues for mobile app developers

Mobile application security is one of the primary concerns as the data residing within the app can be at danger if proper security controls are not applied while designing an application also due to the mass usage of apps in today's world mobile application vulnerabilities has increased a lot.

Hackers nowadays are targeting mobile applications to gain access over consumer personal information and details and maliciously use it. Hence developers need to be extra cautious while they build an app for both ios and android platforms.

Some of the ways to build a completely secure mobile app:

- ✓ Try to write a secure code
- ✓ Encrypt the data
- ✓ Be careful while using libraries
- ✓ Use authorized API
- ✓ Use high level authentication
- ✓ Develop tamper detection techniques for your app
- ✓ Provide least privileges
- ✓ Have proper session management
- ✓ Use of good cryptography tools and techniques
- ✓ Test repeatedly

SECURITY ISSUES FOR MOBILE APP DEVELOPERS

❑Try to write a secure code

- ❑ Code is the most vulnerable feature of any mobile application which can be exploited easily by the hackers. Hence it is essential that you write a highly secure code. According to research about 11.6 millions devices are being affected by malicious code.

❑ Encrypt the data

❑Encryption is the way to convert the data transmitting in to such a form that it cannot be read by anyone else without decryption. This is an efficient way to save the data from being used in a malicious way.

❑ Be careful while using libraries

❑Often the mobile app code needs the third party libraries for the code building. Do not trust any library for your app building as most of them are not secure. When you have used various kinds of libraries always try to test the code. The flaws in the library can allow the attackers to use malicious code and crash the system.

SECURITY ISSUES FOR MOBILE APP DEVELOPERS

❑Use authorized API

- ❑ Always remember to use authorized API in your app code. It always gives hackers privilege to use your information for example authorization information caches can be used by the hackers to gain authentication on the system.

❑ Use high level authentication

❑Authentication mechanisms are the most crucial part of the mobile application security. Weak authentication is one of the top vulnerabilities in the mobile apps. As a developer and a user authentication should be considered important from security point of view.

❑Develop tamper detection techniques for your app

❑This method is to get alerts when your code is being modified or changed. Often it is essential to have log of code changes of your mobile app so that the malicious programmer do not inject bad code in your application. Try to have triggers designed for your application to keep logs of activities.

SECURITY ISSUES FOR MOBILE APP DEVELOPERS

❑Provide least privileges

- ❑ The principle of least privilege is often necessary for your app code security. It is preferable to give access to the code to only those who are intended to receive them rest all should not be given the privileges keeping it minimum. Try to keep the network as less as possible.

❑ Have proper session management

❑Session handling is an important feature in app building which needs extra precaution as the sessions on mobile are usually longer than the desktop session. Hence session management should be done to maintain the security in case of stolen and lost devices and it should be done with the help of tokens rather than identifiers.

❑Use of good cryptography tools and techniques

❑Key management is an important step when it comes to encryption of your data so make sure that you do not hard core your encryption keys.

❑Use good protocols for encryption such as AES and SHA256 and never store your keys on local devices. Use the latest and trusted encryption methods.

SECURITY ISSUES FOR MOBILE APP DEVELOPERS

❑Test repeatedly

- ❑ A very simple solution for the app is to test repeatedly for the new changes as security aspects are changing day by day and so you need to be updated with the security trends in order to protect your application.

MCQ

Q 6 - What is log message in android?

A - Log message is used to debug a program.

B - Same as printf()

C - Same as Toast().

D - None of the above.

Q 7 - How to fix crash using log cat in android?

A - Gmail

B - log cat contains the exception name along with the line number

C - Google search

D - None of the above.

Q 8 - Fragment in Android can be found through

A - findByID()

B - findFragmentByID()

C - getContext.findFragmentByID()

D - FragmentManager.findFragmentByID()

Q 9 - What is the purpose of super.onCreate() in android?

A - To create an activity

B - To create a graphical window for subclass

C - It allows the developers to write the program

D - None of the above

Q 10 - What is anchor view?

A - Same as list view

B - provides the information on respective relative positions

C - Same as relative layout

D - None of the above

REFERENCES

- https://www.peerbits.com/blog/security-issues-in-developing-mobile-app.html