APP SECURITY AUDIT

Presented By: VIKRAM GHADGE

APPS SECURITY AUDIT INDEX

Security of the application is depend on many factors.

NETWORKS

The network plays a very important role in app security. Most threads for app security is from the network.

DEVICES

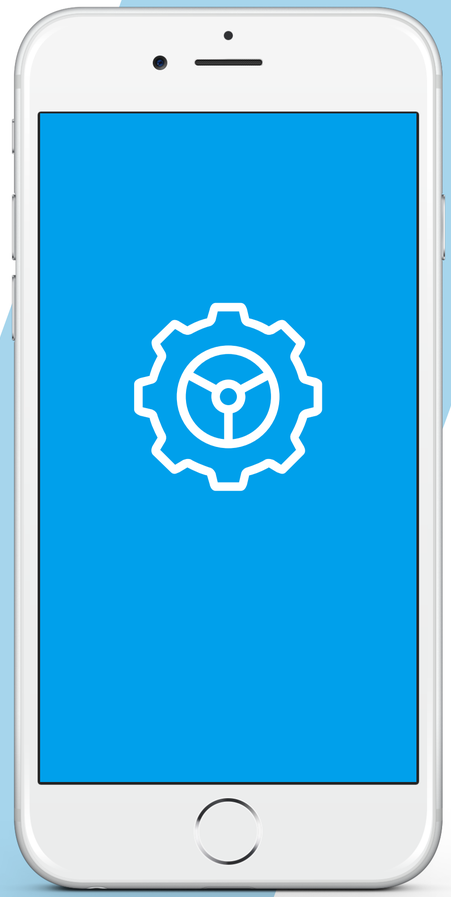
Mobile devices are very personal for every person. As every content in the device connected to personal data.

APP DATABASES

Having offline application gives very good user experience. But with the same feature comes threats for local storage.

APP WEB SERVERS

App performance is a key issue for many users. For making good performing app we need to focus on web servers.



NETWORKS

The network plays a very important role in app security.

Risk	Control Objective	Expected Control	Assessment Approach
Having bad connectivity will cause user experience as well as data loss and disclosure.	To ensure security and app performance connectivity must be enforced with encryption	Timeout strategy and SSL/TSL certificates SSL or TLS—both cryptographic protocols for secure transmission of data. The policy, its associated procedures, and standards include: • having timeout rules for all API connection • Test cases which are specific targeted to connectivity and timeouts • App encryption document with SSL certificate • Text cases for testing SSL and TSL security	Confirm that the managing agent has: i) A written connectivity strategy documentation validation document approved by management with an appropriate degree of challenge and oversight in its development as evidenced through discussions. ii) Written documentation supporting how to prevent data theft using SSL and TSL iii) Details description for monolithic or micro-app architecture usage. • communication of the encryption policy, associated procedures and standards to the relevant stakeholders and individuals responsible for ownership and management of architecture used in the internal model. • Test cases related to all connectivity and encryption
Weak authentication over any network can be hazardous for any apps.	To ensure the security of the application, standard authentication practice need to be implemented	Authentication policy related to accessing application must be defined. The policy, its associated procedures, and standards include: • Authentication framework document • Policies related to recovering user access after theft. • Documents which support Preventing unauthorised access. • Allowing user to Enforcing two factor auth.	Confirm that the managing agent has: i) A written strategy to providing authentication approved by management with an appropriate degree of challenge and oversight in its development as evidenced through discussions. ii) Test cases to about authentication and unauthorised access.

DEVICES

Mobile devices are very personal for every person. As every content in the device connected to personal data.

Risk	Control Objective	Expected Control	Assessment Approach
Data loss and disclosure of app to unauthorised user.	To prevent malicious extraction from the app when data are at rest we should store data securely.	An policies or document which enforces developer to store data in particular way to avoid unauthorised activity. The policy, its associated procedures, and standards include: • define a strategy to store data and retrieve in the application. • Policies to verify unauthorized access to avoid man in middle attack. • Third party verification to test all features for finding out loopholes. • Test cases to verify these strategies been implemented.	Confirm that the managing agent has: i) A written document about storing and accessing data from app approved by management with an appropriate degree of challenge and oversight in its development as evidenced through discussions. ii) Verified third-party agency to do security testing specific for data theft. iii) Test cases to verify strategies.
User experience compromise, unauthorized access, data loss	To ensure that app will not be reverse engineered developer should protect build with varies encryption and app security tools.	The development team should encrypt build with protected software with a licensed copy The policy, its associated procedures, and standards include: • Strategy to protect build from hackers to reverse engineer build. • Build a protection policy for every build • Third party service to protect app build.	Confirm that the managing agent has: i) Complete technical documentation avoids reverse engineer approved by management with an appropriate degree of challenge and oversight in its development as evidenced through discussions.

APP DATABASES

Having offline application gives very good user experience. But with the same feature comes threats for local storage.

Risk	Control Objective	Expected Control	Assessment Approach
1. Choosing the wrong DB framework or library will open ways for malicious attacks	To ensure that our DB is protected we must use the latest strategies and standard practices while storing local data.	Detailed technical document with function comments. The policy, its associated procedures, and standards include: • The policy, its associated procedures, and standards include: • DB storing policies • Library selection and comparison document with the DB model used in the app. • Test cases to test DB storage and negative testing document to test malecisu attack.	Confirm that the managing agent has: i) A library decision document approved by management with an appropriate degree of challenge and oversight in its development as evidenced through discussions. ii) All data storage strategies with a document to support this decision. iii) Test report with relevant DB access files.

APP WEB SERVERS

App performance is a key issue for many users. For making good performing app we need to focus on web servers.

Risk	Control Objective	Expected Control	Assessment Approach
DOS attach are very common for the various app and web servers	To ensure our IP and sockets are not been exposed we should place proxies and policy to ensure it become secure for these kinds of attacks.	Detailed document to keep our IP protected from outside attack. The policy, its associated procedures, and standards include: • Policies to securely accessing our API or third-party access to our system. • Standard architecture document to avoid direct access to business login • Third party verification from verified authority	Confirm that the managing agent has: i) Standard practice document to avoid access to our production keys or IP. ii) DOS protection services on the production server and test cycle to confirm. iii) Third party DOS attach verification from the verified agency. iv) Test Report to support all attach.