**Mobile App Security Assessment Framework**

In order for the proper controls for mobile apps to be developed and tested, developer team should first identify the layers of risk. As given in below table, there can be multitudes of layers, but the basic risk segments can be divided into five main mobile app security categories these are:

* Mobile devices
* Mobile app web servers
* Mobile app databases
* Mobile app management
* Mobile networks

Although the testing framework controls mentioned below does not encapsulate all complementary controls, it focuses on the key controls required to have a basic maturity level around strengthening mobile apps security.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mobile App Security Assessment Framework – Mobile Device** | | | | |
| **Category** | **Controls - Domain** | **Controls (Need to be verified)** | **Controls** | **Risk Mitigated** |
| Mobile Device | Data storage | Data are stored securely to prevent malicious extraction from the app when data are at rest | Encryption of the data at rest in the mobile device (app) is set to Advanced Encryption Standard (AES) as per the best Industry practice. No sensitive data should be written to application logs | Data loss and disclosure |
| Mobile Device | Data transmission | Mobile app data transmission is  encrypted when data are not at  rest (transferred). | Encryption of data is enforced  for data in transit using Secure  Sockets Layer (SSL) and strong  security protocols such as:  • Web access—HTTPS vs. HTTP  • File transfer—FTPS, SFTP,  SCP, WebDAV over HTTPS vs.  FTP, RCP  • Security protocols—Transport  Layer Security (TLS). | Data loss and  disclosure |
| Mobile Device | Reverse engineering  of app code | App code is protected from  modification from unauthorized  intruders through use of binary Protections. | Binary protections are standard  protocol for app development  life cycle and enforced by the  development team at time of  app coding and maintenance. | User experience  compromise,  unauthorized  access, data loss |
| Mobile Device | App access  management and  security | App is configured to limit access  and configured appropriately for  limited authorized use. | Mobile application management  is utilized to manage access and deployment of the app. Additionally, proper whitelists (approved) and  blacklists (noncompliant) are  maintained. | Unauthorized  access and fraud |

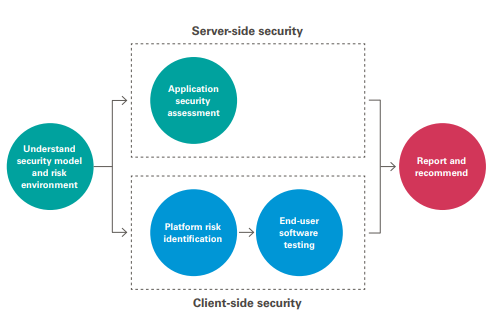
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mobile App Security Assessment Framework – Web server** | | | | |
| **Category** | **Controls - Domain** | **Controls (Need to be verified)** | **Controls** | **Risk Mitigated** |
| Web server | Operations patch  management | A process is in place to identify and apply critical system security patches and updates | Processes exist for the  deployment of system patches  for all applicable systems.  Processes exist for identifying  new patches or for notification  of new patches from vendors.  If any vulnerability scans have been performed, patches have been applied to address any identified issues. Missing patches are identified and compared against documented formal exceptions from security team. | Data loss and  disclosure,  unauthorized  access |
| Web server | Access management | Roles and responsibilities  for ownership have been established, documented and  communicated. | All applicable web servers have  been assigned both technical  and business system owners, as  required. The defined roles and  responsibilities are adequate,  especially for internal and third party personnel. All default  accounts and passwords are  disabled by enforcing strict  password controls. | Data loss and  disclosure,  unauthorized  access |
| Web server | Brute-force attack | Management of denial of- service (DoS) strategy encompasses proper programs  to lock out unauthorized protocols. | Lock-out protocols are enabled  for accounts with multiple  incorrect password attempts.  Utilization of CAPTCHA (program  that distinguishes between  humans and computers) is  recommended to avoid DoS. | Unauthorized  access and fraud,  availability of app |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mobile App Security Assessment Framework – Database** | | | | |
| **Category** | **Controls - Domain** | **Controls (Need to be verified)** | **Controls** | **Risk Mitigated** |
| Database | Privileged access | Elevated accesses to databases are properly secured utilizing best practices | Access to database is limited  to appropriate individuals, and  proper access reviews and  documented system accounts  are kept on file. All default  accounts and passwords are  disabled by enforcing strict  password controls. | Unauthorized  access and fraud |
| Database | Structured Query  Language (SQL)  Injection | Back-end database access is properly secured from  vulnerabilities utilizing proper input validation techniques | Input validation technique is in  place; specifically defined rules  for type and syntax against key  business rules exist. | Unauthorized  access and fraud |
| Database | Validation of app  (client) input | Data coming from mobile apps have to be vetted prior to  trusting it to pull or push data to the database layer | Sanitization of app user data  coming from the mobile app  is properly protected through  embedded logic checks  within the application. Proper  implementation of logic checks  is enabled at the server side | Unauthorized  access and fraud |
| Database | App database  Services | Database server software is updated to current secure versions. | The database server is properly  tested and hardened against  malicious attack. Login forms  have HTTPS required. SSL  connections are mandatory. | Unauthorized  access and fraud |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mobile App Security Assessment Framework – App Management** | | | | |
| **Category** | **Controls - Domain** | **Controls (Need to be verified)** | **Controls** | **Risk Mitigated** |
| App  management | App deployment  administration | App store updates are properly governed utilizing a life cycle management methodology. | A governance structure is in  place for mobile app life cycle  management, specifically, the  release of mobile apps to the  app store and modification of  future releases. | Unauthorized  access and fraud |
| App  management | App deployment  source code  management | Source code management  is properly assigned prior to release. | App is signed and provisioned with valid certificate | Unauthorized  access and fraud |
| App  management | Rooted device | Ability to warn user if installed on rooted device | App detects whether it is being executed on a rooted or jailbroken device. Depending on the business requirement, users are warned, or the app is terminated if the device is rooted or jailbroken. | Data loss and  disclosure,  unauthorized  access |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mobile App Security Assessment Framework – Mobile Network** | | | | |
| **Category** | **Controls - Domain** | **Controls (Need to be verified)** | **Controls** | **Risk Mitigated** |
| Network | Wireless connectivity | Encryption is enforced when Wi-Fi connection is activated. | Transmission of data utilizes, at  a minimum, SSL or TLS—both  cryptographic protocols for  Secure transmission of data. | Data loss and  disclosure |
| Network | Session hijacking | Prevent hijacking of a session due to insecure connection  protocol. | Connection protocols for the  uniform resource locator (URL)  via TLS are through HTTPS  rather than HTTP to securely  connect to a URL. | Data loss and  disclosure,  unauthorized  access |
| Network | Domain Name  System (DNS)  Spoofing | DNS is secured to avoid  rerouting of data to another  Internet Protocol (IP) address. | Proper packet filtering setup is  built in to verify source address  and blocking packets with  conflicting source address.  Utilization of TLS, Secure Shell  (SSH) and HTTPS is enabled for  secure communication protocol. | Data loss and  disclosure,  unauthorized  access |

**MOBILE APPLICATION SECURITY TESTING APPROACH**



**Application Mapping:**

The initial step in the Mobile application security assessment is the mapping of the application for each type of the Operating System architecture. This will provide a detailed understanding of the application and the data flow, within the application as well as to the server.

* Application understanding
* Dataflow mapping

**Client Side Attacks:**

In this stage, the focus of the testing is to understand the weaknesses on the client side. This includes the analysis of temporary storage, sensitive information and client side encryption

* Binary Analysis & Identification of insecure APIs
* File system analysis for identification of sensitive files & weak encryption implementation
* Memory & Process analysis

**Network Attacks:**

In this stage, the communication channel between the client and the server undergoes the review and attack. Sensitive plain text traffic is retrieved by analyzing

* Installation traffic
* Run time traffic

**Server Side Attacks:**

The final phase of a mobile application security assessment is to assess the security of the server. In this, the server-side application would be tested to find out how it responds to various malicious requests.

* TCP attacks are performed to identify vulnerabilities such as Buffer Overflows
* HTTP Attacks are performed to identify application vulnerabilities such as XSS, SQL injection and other OWASP listed vulnerabilities

In addition to the basic testing framework laid out in this document, it is recommended to use a OWASP mobile testing framework that applies to all mobile apps prior to official release. This reduces the risk of external and internal vulnerabilities that can result in the compromise of data.