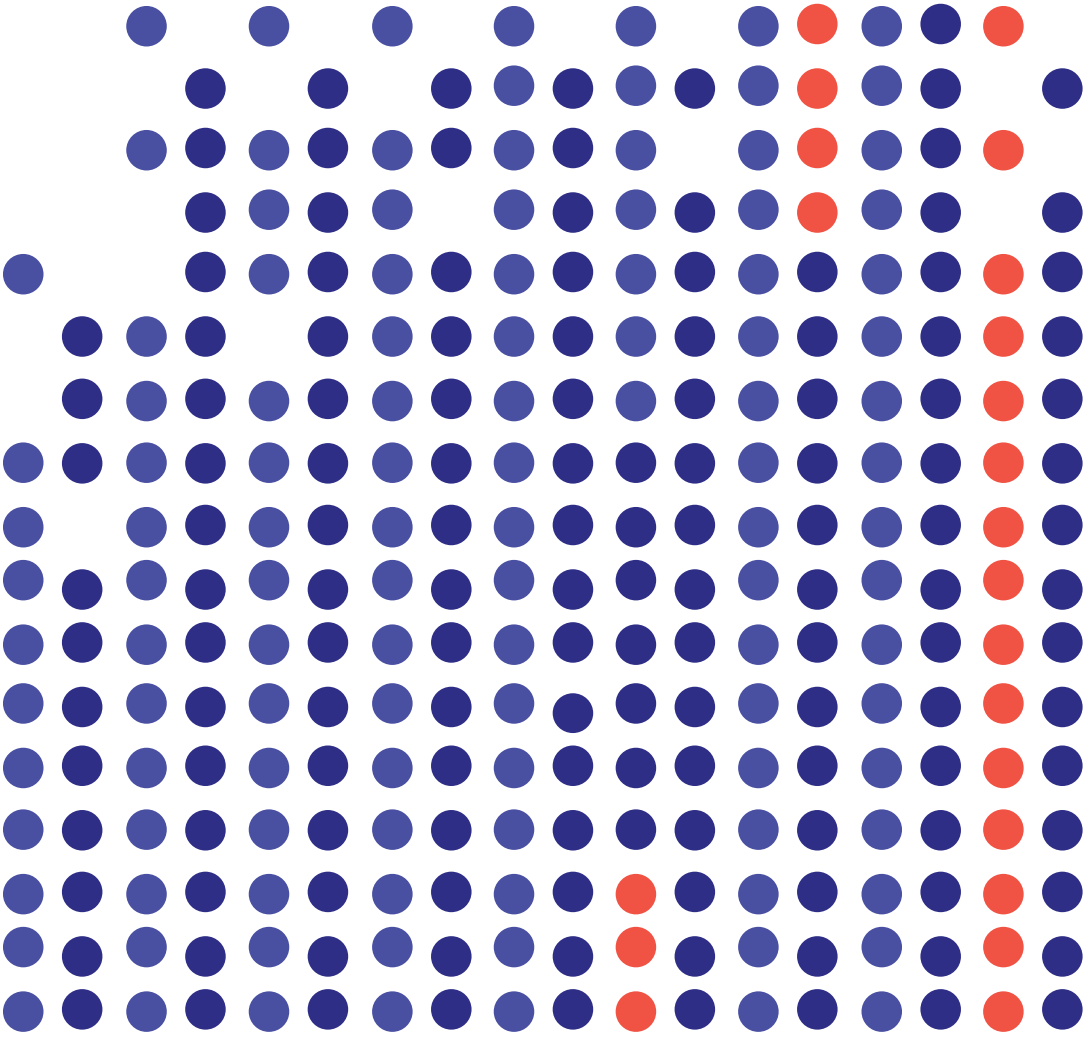
appknox

# Mobile Security Trends For 2021



# Content

# Key Highlights

When we make our way into the ecosystem of security technology and infrastructure initiative, learning about application security trends becomes of utmost importance. The frequency with which applications are being built or integrated by organizations has increased on a large scale, and they are also making strides at adopting DevOps practices along with pushing further for automation. And in order to protect the data of employees, customers as well as citizens, these organizations must strive towards building, integrating, and automating with security in mind.

The unpredictable COVID-19 situation has made global businesses more vulnerable than ever to cyberattacks and breaches. Be it the Zoom data breach (500k records stolen) or the Marriott (5.2 million records breached), hackers don't seem to miss opportunities to exploit vulnerabilities and gain access to business infrastructures and public records. The major aim of this guide is to pave a way into understanding the core concepts related to application security, be it people, processes, or technology which is required at every step in order to plan out an excellent application security strategy. These procedures are further embedded into application types and their respective platforms. A precise application security process can help in mapping several types of application security techniques, be it wholly or partially.

## How Appknox has Revolutionized Application Security?

Be it the early birds or the giant Fortune 500 companies, Appknox has ever been instrumental in building a safe and secure mobile ecosystem for businesses all over the globe by utilizing its system plus human approach to beat the hackers at their own game. Appknox offers one of the most advanced plug-and-play security solutions embedded with smart vulnerability assessment and penetration testing tools which help security experts and developers in building the safest mobile applications.

## Companies Appknox has Worked With

We have had the pleasure of working with some of the most revered brands across several industry verticals and from across the globe including Xiaomi, Flex International, Heathmont, Decathlon, Euphoria Digital, Unilever, DCB Bank, First Bank of Nigeria and several others. Appknox has always proven its ability to focus on the core client needs and delivering the best possible security solutions.

# Securing Mobile Apps

In the global diaspora consisting of several information algorithms operating all at once, mobile devices have gained more popularity as compared to desktops or laptops. They are embedded with several advantages right from taking your zoom calls to your major work-related tasks like scheduling meetings, project management can be done via mobile applications from the concerned tools. Apart from being handy at use, they are also capable of performing all those functions which desktops can and much more.

Mobile app security is one of the major techniques to protect applications from external threats which basically consist of malware and other types of digital frauds that make the personal and financial information of users vulnerable to hackers. Any kind of breach in mobile app security can result in disclosing personal data of users like current location, banking information, etc. which are highly vulnerable to attack by cybercriminals. Undoubtedly, the security of mobile applications becomes a must for organizations who want to stay competitive in the market and maintain a healthy relationship with their users.

Now let's look out for some of the trending approaches related to mobile application security.

## Introduction to Foundational Security

Foundational security is one of the most critical as well as impactful aspects of application security for the majority of organizations. Investments done in these resources will lead to amplification of security and similar advances across IT projects within organizations. The major endpoints of foundational mobile app security are:

- **CI/CD and DevSecOps:**

CI and CD (Continuous Integration and Continuous Delivery) have the ability to bring an end-to-end integration in a seemingly haywire software development and deployment process. With the help of CI/CD, developers actually have more time to focus on the development side of the things and improve the features instead of focussing on the tricky deployment process.

However, the one thing which is missing from the scene here is security. CI/CDcan actually accelerate the whole process, but not security. DevSecOps, on the other hand, pushes security into the software development process and creates a unique blend of development, security and operations. With the introduction of DevSecOps, security assessment is done much earlier in the SDLC and thus, the impact of discovering a security vulnerability is reduced massively.

- **Application Security Testing:**

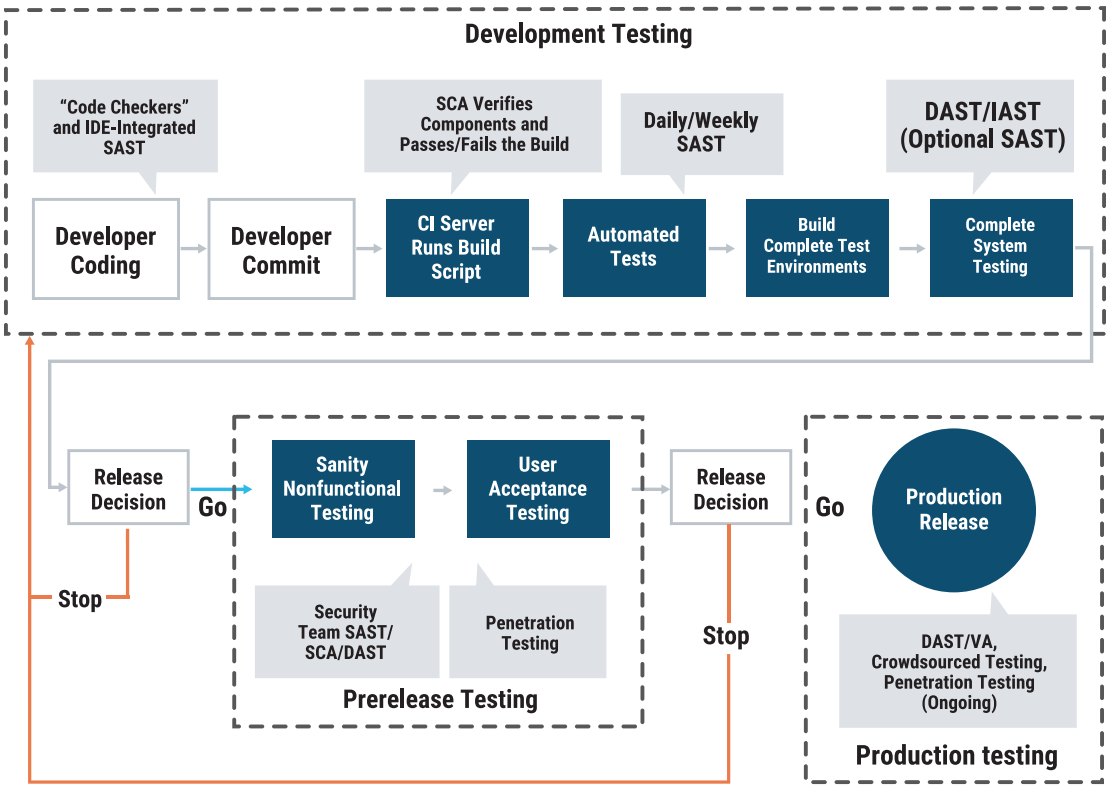
Any approach to security can't be complete without application security testing. Finding security threats early in the software development life cycle can reduce risks on so many levels and that is why mobile app developers follow these approaches to application security testing:

1. Static Application Security Testing (SAST) decides the analysis procedure of an application's source, binary code and bytecode in order to check for security vulnerabilities, preferably during the programming and testing phases of the SDLC.

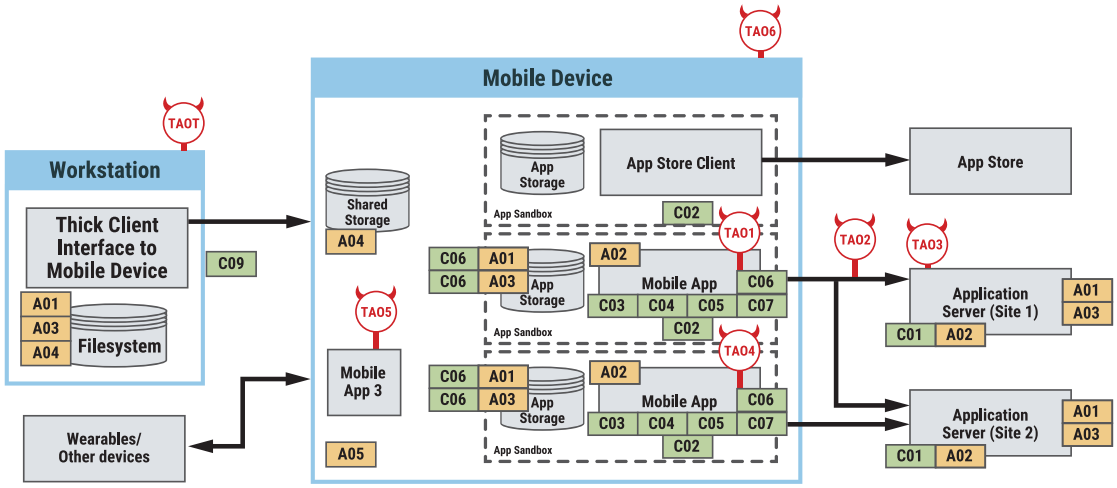
2. Dynamic Application Security Testing (DAST) helps in analyzing applications during their testing or operational phase, precisely in their dynamic or running state. It also acts as a catalyst in simulating attacks against web-based applications, services, and APIs. This technology also helps in analyzing the reactions related to the application and decides the level of its vulnerability.

3. Interactive Application Security Testing (IAST) basically consists of elements embedded in DAST simultaneously with the instrumentation procedures of applications under surveillance. These elements are typically implemented as agents within the runtime of a test environment (for instance, instrumentation of the Java Virtual Machine [JVM] or .NET CLR) which plays a vital role in observing operations or attacks along with identifying vulnerabilities.

**Application Security Testing in the Phases of an SDLC**



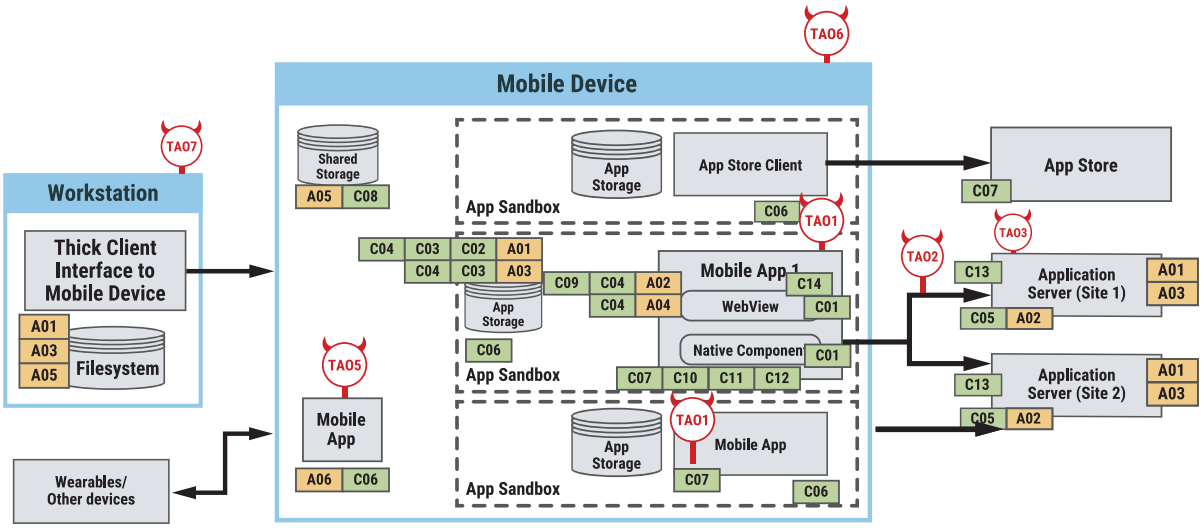
- Automated Vulnerability Assessment and Penetration Testing




**Assets**
A01: Application Data
A02: Application Functionality
A03: Authentication Tokens/Credentials
A04: Users Private Data
A05: Device Functionality

**Controls**
C01: User Authentication / Authorization
C02: App Sandboxing
C03: App Store Verification
C04: Binary Hardening
C05: Root/Jailbreak Detection
C06: TLS / Certificate Verification / Certificate Pinning
C07: App Permissions Enforcement
C08: Data Encryption
C09: Application Backup Configuration

**Threat Agents**
TA01: Malicious App Users
TA02: Network Attackers
TA03: Malicious Servers
TA04: Malicious App (Sandboxed)
TA05: Malicious App (Root Privileges)
TA06: User with physical access to device
TA07: Malicious app on user's workstation




**Assets**
A01: Application Data
A02: Application Functionality
A03: Cookies/Authentication Tokens/Credentials
A04: DOM Objects
A05: Users Private Data
A06: Device Functionality

**Controls**
C01: TLS / Certificate Verification / Certificate Pinning
C02: Cache Directives
C03: Data Encrpytion
C04: Same Origin Policy
C05: User Authentication / Authorization
C06: App Sandboxing
C07: App Store Verification
C08: App Permissions Enforcement
C09: Javascript Obfuscation
C10: Binary Hardening
C11: Root/Jailbreak Detection
C12: Application Backup Configuration
C13: Input Validation/Output Encoding
C14: Whitelist of Sites Accessible Through WebView

**Threat Agents**
TA01: Malicious App Users
TA02: Network Attackers
TA03: Malicious Websites
TA04: Malicious App (Sandboxed)
TA05: Malicious App (Root Privileges)
TA06: User with physical access to device
TA07: Malicious app on user's workstation

- **Advanced Security**

Once the basic aspects of application security, i.e. foundational security are taken care of, it becomes essential to ensure that no other stones are left unturned and focus on the advanced aspects of security. The components of advanced security include:

● Mobile Application Security: Mobile applications are one of the most critical aspects of the presence of any business online since almost all types of businesses are dependent on users that are connected online and via mobile applications. The area of mobile application security primarily puts focus on the software security concerns of mobile applications that are run on Android, iOS, Windows phone, and similar platforms.
This also includes applications that are compatible with running on tablets as well as phones. These basically involve application assessment for security issues and within the context of the platform on which they have been designed to run on and the frameworks which have been used to develop them along with its anticipated set of users (employees, end-users, etc.).

● In-App Protection: In-App protection is one of the most observable security solutions which is implemented within applications in order to protec them from attacks. This, in other words, means that when the distribution of a security-critical app is done to the consumers or enterprises, users want to be assured that the app is secure and is not vulnerable to attacks or data stealing. This is possible when users are able to make use of some kind of technological advances inside the app that ensure app protection. The possible features may include code obfuscation, threat detection, encryption, etc.

● JavaScript Security: JavaScript security is basically about prevention investigation, protection, and resolving issues inside applications pertaining to security at places where JavaScript is used. Malicious codes, man-in-the-middle attack, cross-site scripting (XSS), exploiting vulnerabilities inside the source code of web-based applications, are some of the most common vulnerabilities related to JavaScript.

● Runtime Application Self-Protection (RASP): RASP is basically a kind of technology that runs on a server and gets accelerated whenever an application runs. It is comprehensively designed to detect attacks that affect an application in real-time. Whenever this app protection approach is incorporated on a server, it brings about consistent security. RASP intercepts all types of calls from the app to the system, thereby making sure that all applications are secure and data requests are validated directly inside the app. RASP can play a major role in protecting both the web as well as non-web-based applications.

● Secrets Management: Secrets management is one of the best practices in cybersecurity which digital businesses can adopt in order to enforce security policies in a consistent manner for non-human entities. Secrets management plays a major role in assuring users about resources included with tool stacks, platforms,

cloud environments, etc. that are available for access by authenticated and authorized organizations and entities. The steps given below are subsequentl included while deciding a secrets management initiative. A number of these approaches as well as techniques are also used to protect all kinds of privileged access by users in general.

- Authentication of all types of access requests that make use of non-human credentials.
- Application and maintenance of the principles of least privilege.
- Regular maintenance of rotation of secrets and credentials which also focus on enforcement of role-based access control (RBAC).
- Application of reasonable policies in a consistent manner and automation of secret information management.
- Maintenance of a comprehensive source of audit and tracking of almost every access

- API Security and API Gateways: Security remains one of the topmost priorities of organizations, government agencies, institutions, and similar enter prises, and when we talk about API Security, it is important to know that companies that are ready to ramp up their existing efforts towards security should consider bringing more investment into their API infrastructure.

One of the most optimized security drivers for API gateway technology is access control, which goes a long way in serving as a governor of sorts where organizations are able to access as well as manage an API and maintain regulatory norms around data maintenance and handling of data requests. IT security experts are bound to feel more confident in situations where all traffic is routed through a specific gateway and this also makes them keep a check on the pulse of an organization.

# Key Security Trends and Forecasts for the Year 2021

After getting to know the trending approaches to security in 2020, we can now discuss what security trends and forecasts will shape the landscape of mobile and general appli-cation security in 2021. Some of the key trends include:

- In the coming days, large business units would prefer the services of organizations that adopt automated and customized security solutions and are capable of solving immedi-ate

customer needs with visible COST/ROI/SPEEDING UP SDLC, whenever the need arises.

● The market segments that are bound to witness high demand in the near future consist of cloud-based endpoint protection platform (EPP), assess management (AM), privileged access management (PAM), secure web gateway (SWG), and cloud access security broker (CASB). The chances of these segments getting impacted by COVID-19 remains relatively low.

● The market share as well as the demand for solutions that are cloud-based is bound to grow. Endpoint Detection and Response (EDR), managed detection and response (MDR), and other similar cloud-oriented detection and response solutions will successively expand their reach.

● Since more and more businesses are undergoing a rapid digital transformation and are moving from offline to online through mobile applications across industries like consumer goods and services, FMCG, on-demand delivery services, the market share for vulnerability assessment solutions and mobile application security is also bound to increase across these sectors.

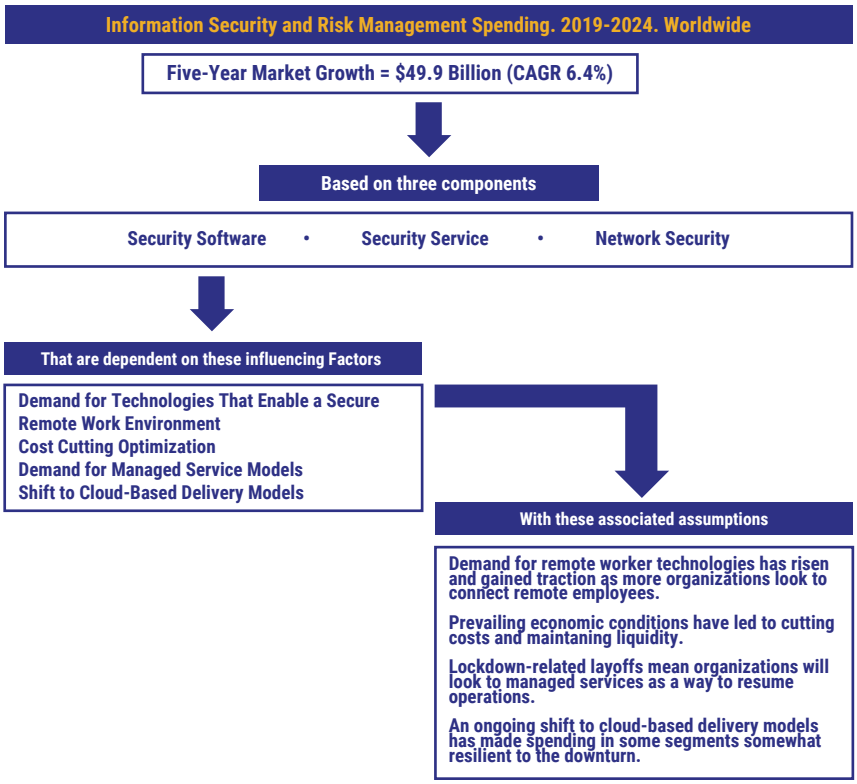
● One of the major focus areas of cybercriminals in the upcoming future will be remote workers across organizations. Cybercriminals are bound to follow potential users and launch attacks on them that exploit their inherent behaviors.

● There is a rising debate over making the ransomware payments illegal in the cybersecurity world. Countries like the US might introduce laws to introduce penalties for those who pay ransomware money to the cybercriminals.

● MFA or Multi-Factor Authentication is set to become the strongest weapon in the cybersecurity arsenal. With business processes and applications moving swiftly to the cloud, the best possible way to protect corporate and personal data is to introduce multiple layers of authentication.

● As attack surfaces continue to expand, developers will be more inclined towards DevSecOps in order to tackle threats from different perspectives. Automation of DevSecOps pipelines will be a real game changer as dev teams would like to get security issues fixed as soon as they arise.

# What Factors will Influence Information Security Spending in the Years to Come?




## Influencing Factor: Cost-cutting and Optimization

● Forecast Assumptions: Organizations have consistently been moving towards cost-saving mode through a greater part of 2020, primarily seeking out security tools that can cause less cost burn on the workforce productivity and give higher ROI, in order to cope up with an uncertain environment.

## Influencing Factor: Cloud-based delivery model for security solutions

● Forecast Assumptions: A visual shift to cloud-based delivery models which is ongoing in security software segments is primarily a result of the upheaval caused by the COVID-19 pandemic in the current scenario. In order to keep up with security solutions and steadiness in terms of delivery, SaaS has become a preferred delivery method.

Gartner, prior to the COVID-19 pandemic, had made a prediction that SaaS-based delivery models would be preferred over other models and would consist of over 80% of new security purchases globally by the year 2022, an increase of almost 30% from 2018.

## Influencing Factor: Demand for Technologies that Enable a Secure Remote Working Environment

● Forecast Assumptions: With a worldwide market size of almost $18.5 billion in 2019 and an annual growth of 13% during 2019-2023, according to IDC, collaborative applications, which include emails, enterprise social networks, team collaborative applications, conference applications, etc. are in successive demand. Among these, conference and team collaborative applications are inherently capable of growth at 15% in 2020 along, as per predictions of IDC.

# Mobile Security Pitfalls that Must be Avoided in 2021

Mobile security breaches are a major source of fraudulent activities for enterprise data of clients. They are considered one of the most tangible problems since information bypassing risks increase among customers and organizations. The major security challenges among these include:

● Sensitive data losses such as fraud, non-compliance issues, exposure of infrastructure logs, PII, etc. take place because of mobile application security failures.

● Numerous limitations in security functionality are determined by the design and architectural decisions made in the early stages of software development which are available to the security leaders.

● Every industry is undergoing rapid digital transformation and a number of security attacks and vulnerabilities are one common problem faced by mobile applications. Hence, it becomes inherently important for developers to revisit and prioritize concerns related to security at each stage of the software development cycle

Mobile applications are created in a manner so as to run in a hostile environment prone to frequent attacks. Automation systems need to be implemented by security and risk management (SRM) leaders in order to reduce threats and evolve better in terms of digital transformation. Let's discuss some of the best security practices that can necessarily reduce pitfalls.

**1. Do Not Hardcode Credentials**

It has frequently been seen that available credentials are put to hardcore by mobile app developers. Also, rather than waiting for users to authenticate credentials for applications, here credentials and services used by the applications are put to authentication.

**2. Reduce App Permissions**

Apps are empowered by permissions, but this also results in creating a number of risks. Unnecessary permissions, even in a legitimate app can result in causing privacy and compliance hazards, along with becoming a target for attackers.

**3. Certificate Pinning Should be Used Wherever Possible**

Most of the time, mobile applications get connected from unsecured networks, rather than from protected web applications. This is certainly because these apps are always used on the go. One of the best techniques to counter attacks such as man-in-the-middle attacks that can take place over these networks is through the process of certificate pinning.

**4. Perform Security Testing of Applications**

Security testing on the application should be conducted by enterprises, in order to vulnerabilities present in the application along with ensuring best coding practices that are secure as well.

# Recommendations by Appknox on Creating a Secure Mobile App

One of the major sources of breaching and internet fraud for organizations is mobile applications. In order to avoid attacks on infrastructure and data leakage from mobile devices, best practices on mobile security need to be followed by security and risk management leaders. There are a number of ways through which you can ensure the security of mobile applications, which we recommend below:

- Early input on the performance-security trade-offs needs to be provided whenever a mobile architecture (native, hybrid or mobile web) gets selected because of its involvement from the beginning of the process.

- Best practices of application security which put a special focus on mobile and its associated backend infrastructure along with possible API security practices should be

implemented and put to use.

- App permissions, sensitive or PII data, hardcoded credentials should be minimized or eliminated, and certificate pinning should be put to use, wherever possible.

- At every stage and phase of development, security testing should necessarily be performed for every major and minor release cycle.

- Obvious application controls such as application of high-end security measures such as reverse engineering attempts or protecting mobile applications against tampering, code obfuscation, etc. need to be kept under check and you must go beyond these encryption controls.

# Conclusion

One of the most tangible problems that enterprises face today is ensuring the security of mobile applications. Although the problem of preoccupation and breaches has not necessarily been seen in mobile device security but is frequently prevalent and increasingly responsible for enterprise breaches as well as fraud in terms of application security failures. Moreover, most of these applications are public-facing and the chances of them being the primary source of interaction between partners and their organizations are increasingly high. The security trends of present times, as well as the future, require a close watch so as to avoid any kind of pitfalls in security and keep the available applications ready for the current market.