Codeless Testing Automation

THE IMPORTANCE OF SECURITY TESTING IN MOBILE APPLICATIONS

INDEX

INTRODUCTION

The digital era has ushered in numerous conveniences, literally at our fingertips, thanks to the millions of mobile applications for every conceivable purpose! However, as digital innovation presents newer technologies, cyber criminals too are sharpening their murky skills, to unleash attacks of various kinds. Hence security of mobile applications gains immense importance, as protection of business and individual interests is paramount. Unfortunately, cybercrimes are on the rise both in quantum and form, and a look at some recent trends, is reason to sit up and seriously take note.

One report states that a staggering 5.5+ million Mobile Malware, Adware, and Riskware attacks were blocked in 2024, that too with the year still in progress! Ransomware is responsible for almost 70% of malware violations, and Phishing via emails, messaging apps, social media, and games, is a common route for attacks. Expanding 5G networks have broadened the ambit of attacks, and poorly secured virtualized infrastructure, opens up new vulnerabilities for hackers to have a heyday.

In a world where cybercrime is fast rising, the importance of utmost security of mobile applications cannot be emphasized enough. Mobile applications inadvertently offer hackers an easy platform and very wide reach for their nefarious activities. Besides, many mobile applications deal with very confidential and sensitive information, which makes security non-negotiable. This Whitepaper is therefore a concerted endeavor, to highlight the inherently crucial **Importance of Security Testing in Mobile Applications**, in order to strengthen the hands of those on the right side of the digital divide.

ABSTRACT

The popularity of mobile applications for banking, investment, cryptocurrencies, and other financial and non-financial purposes is rising. The highly sensitive and confidential information that is exchanged, needs to be meticulously protected. Data leakage, theft or manipulation can result in application failure, loss of clients, legal implications and monetary losses too. This Whitepaper will therefore dwell on The Importance of Security Testing in Mobile Applications, scanning it in three different sections, as listed below:

1. **Security – A Key Concern for Mobile Applications – which presents the following:**
   - Mobile Application Attacks in 2024
   - Security Testing – The Proactive Panacea for Mobile Application Threats
   - Importance of Mobile Application Security Testing
   - How Security Testing Enhances the Benefit Quotient
2. **Risk Profile of Mobile Applications:**
   - Risks Common to All Mobile Applications
   - Risks Specific to Android Mobile Applications
   - Risks Specific to iOS Mobile Applications
3. **Making Mobile Applications Hack-proof – comprising of the following:**
   - When should Security Testing Begin?
   - Types of Security Testing
   - Strategy for Proficient Mobile Application Security Testing
   - Steps for Effective Security Testing of Mobile Applications
   - Best Practices in Security Testing

What follows, are valuable insights for ensuring security of mobile applications and all stakeholders too.

SECURITY – A KEY CONCERN FOR MOBILE APPLICATIONS

01 Mobile Application Attacks 2024

Reports reveal that even in 2024, mobile application hacking and data breaches, continue to raise their ugly head ever so often, and have sadly even superseded the previous year's notoriety, causing widespread losses to organizations and individuals. A sampling of some relevant statistics, is presented below, to drive home the point:

- **Cyberattacks Increasing**

  Early 2024 itself witnessed a 15% rise in data breaches, accounting for over 1,500 attacks. Ransomware was the culprit in 30% of the breaches.

- **Menacing Mobile Malware**

  More than 5.5 million mobile malware attacks were blocked in early2024, which shows how active the dark web is. Cybercriminals used Adware as their hacking weapon, in approximately 25% of these cases.

- **Phishing**

  Phishing was the numero uno mode of attack for data breaches, responsible for almost 90% of incidents, where hackers sent scam emails or text messages that looked genuine, but actually contained links to malicious websites.

- **Mobile Banking Trojans and Ransomware**

  As per Securelist, over 11,700 Banking Trojan packages, and 1,990 ransomware packages were detected in early 2024, and these were generally distributed via malicious apps on platforms like Google Play and third-party marketplaces.

- **Cyber Risks related to 5G Networks**

  2024 has witnessed increased 5G network activity, which has expanded the attack surface for mobile threats. The fallout is a rise in frequency and complexity of cyberattacks. Nokia's 2023 Threat Intelligence Report, stated that the number of cyberattacks on mobile networks, particularly those involving Distributed Denial-of-Service (DDoS) and malware, has been rising. ENISA identified ransomware and threats against network availability as major concerns in 2024.

- **Cost of Breaches Rising**

  Breaches, besides being messy, also result in huge expenses that include legal fees, rectification expenses, reputational damage, and loss of customers. One report places the average cost of a data breach in 2024 at $4.5 million this far, which is a disturbing 10% increase over the previous year.

- **Human Error**

  Human error or negligence, though unintentional, has also been responsible for around 25% of data breaches in 2024. These stemmed from employees being unwary and succumbing to phishing attempts, using weak passwords, etc.

These facts reveal, that security is indeed a major concern for mobile applications, and a lot more needs to be done to prevent the threats and risks involved.

Security Testing – The Proactive Panacea for Mobile Application Threats
Security testing of mobile applications comprises of actively pre-empting threats and risks, in order to detect and resolve potential security threats, vulnerabilities and loopholes in mobile software applications. This is done through a series of tests that gauge the application's ability to circumvent security threats, unauthorized access, data breaches, and other cyber risks. It's important to simulate real-world conditions, and incorporate best practices in mobile application security, in order to ensure robust and resilient applications that can deflect the attempts of hackers.

02 Importance of Mobile Application Security Testing

- **Allaying Cyber Risks**

  Cybercriminals being consistently on the prowl, security testing is vital to detect and address every vulnerability that has the potential to give hackers unauthorized access, manipulate sensitive information, misappropriate funds, or even unsettle mobile application functionalities in any way.

- **Protecting User Interests**

  There's a host of sensitive information like user names, passwords, and personal data, that pass through mobile applications and must be kept safe from data breaches and leakages. Besides, many mobile applications involve financial transactions where unauthorized access can result in financial losses. Security testing blocks all vulnerabilities, to avert hacking attempts; uphold user interests; and comply with data protection regulations.

- **Protecting Business Reputation**

  In this digital age where so much is online, security testing with its focus on preventing breaches, greatly helps companies maintain good client relationships. Security lapses have the potential to ruin business reputation, result in loss of face, loss of clientele, loss of trust; and also result in financial losses and legal tangles. Security testing aids in averting such situations, and maintaining business credibility.

- **Compliance and Regulations**

  Security testing also ensures that all legal requirements (local and international), as well as all industry standards are met. This is very important for mobile applications as they deal with financial transactions and also have access to personal and confidential information. Meticulous security testing goes a long way in keeping legal and regulatory issues at bay.

- **Proactive Risk Management**

  Shift-left security testing pre-empts and mitigates vulnerabilities right from the start of the Software Development Life Cycle (SDLC), to ensure that security lapses don't escape into production, where implications can be far reaching. This is more so when it results in data breaches, compromises, theft, or loss of confidential information. Apart from this, early detection of bugs, also saves time and money that might have to be spent on late rectifications, which can prove to be substantially high.

It is amply clear that security testing of mobile applications is absolutely vital, and must go hand-in-hand with development throughout the SDLC. Ignoring this truth can be potentially explosive for mobile applications; whereas meticulously implementing security testing, can bring in many benefits as enumerated below.

03 How Security Testing Enhances the Benefit Quotient

- **Protection of Sensitive Data**

  User logins and passwords, are the gateway to very sensitive and confidential data. Any compromisein these can spell potential disaster. Security testing by focusing on keeping user credentials safe and secure, keeps hackers at bay and prevents data leakage and manipulation. Losing sensitive data, such as client information and login passwords, often stem from inadequate mobile application security, which hackers leverage to obtain access to sensitive information.

- **Prevention of Financial Misappropriation**

  The popularity of Mobile Banking and other financial applications, necessitates special protective care of such applications, as they contain sensitive financial information of millions of users – data relating to bank accounts, debit and credit cards, investments etc. A compromised application can also give cybercriminals control over users' phones, to fraudulently siphon off their money and cryptocurrencies. Security testing consistently directs efforts to secure the application and prevent cybercriminals from hacking into it. This is what makes the application safe from financial data theft and prevents misappropriation of user funds, which is extremely important to build confidence in mobile applications.

- **Safety of Intellectual Property**

  Mobile applications are often privy to various kinds of intellectual property like copyrights, patents, source codes, etc. Such applications need detailed security testing, to prevent theft which is detrimental to the business and other interests of the owners of intellectual property. Stealing of intellectual property like source codes by unscrupulous persons, can lead to the creation of duplicate/fake applications through which malware can be spread, or users can be deceived into visiting dangerous sites, that can compromise their interests.

- **Promoting Company's Reputation**

  Security testing, by viewing the application's safety and security from all possible angles, protects the interests and confidential information of users and of the business too. Without meticulous security testing, sensitive data can fall into malicious hands, and be misused or misappropriated, leading to loss of user trust. This in turn will dent the reputation of the company, and result in widespread loss of customers, apart from legal hassles and financial payout by the company.

With this review of security testing, its implications, importance, and benefits; this treatise moves on to the second section, which dwells in more detail on the risks that mobile applications encounter.

RISK PROFILE OF MOBILE APPLICATIONS

'Knowledge is power.' Hence, before getting into how mobile applications can be made secure, it is important to know the risks involved, and then empower the application through targeted security testing. Security lapses like data breaches, injection attacks, Denial-of-Service (DoS) attacks, etc. can have far reaching consequences. This section will therefore dwell on the vulnerabilities of mobile applications, and present the different types of risks that they are exposed to.

Getting down to basics, it must be remembered that there are different types of mobile applications viz. **Web Applications** which are created in HTML and accessed from mobile phones; **Native Applications** that are built to cater to a specific operating system (OS) and hence utilize OS-specific features; **Hybrid Applications** which are built like Native applications but perform like Web Applications, bringing in the benefits of both.

There are also different OS, the most common now being **Android** and **iOS.** While there are common vulnerabilities that need to be addressed, there are also security issues that are typical to specific OS, considering that they have different basic structures and builds. Awareness at all times, of the type of application and operating system, will go a long way in holistically securing mobile applications.

Let's begin with the common risks, and then delve into the OS specific ones.

01 Risks Common to all Mobile Applications

- **Hacking Risks via Application Platforms**

  Platforms like Apple Store and Google Play Store are conduits for downloading applications, and hence provide keychains and platform permissions for secure application development. Hackers try to hack into these platforms' communication systems, to intercept data that is transferred from the platform to the mobile application.

- **Risks related to Insecure Data Storage and Poor Encryption**

  Mobile applications store various kinds of data like cookies, text files, and device settings etc., with the help of storage media like Structured Query Language (SQL) database, information property list (.plist) file, data warehouse, Secure Digital (SD) card, or Extensible Markup Language (XML) file. Meticulous encryption is key to securing this data and protecting the confidentiality of sensitive user information. Systems need to be in place to prevent hacking of the mobile device's operating system, jailbreaking of devices, and other weaknesses in the application's data maintenance framework.

- **Risks via Communication Channels**

  Mobile applications use the client-server route for transferring data via the device's carrier network, and the internet. Any vulnerability in these, can give hackers the upper hand for stealing private and sensitive data. Furthermore, the paucity of internal security systems in the Hypertext Transfer Protocol (HTTP) used for client-server communication, increases the risk of hackers intercepting, modifying, or diverting data. Hence its vital to secure wi-fi and all communication channels, including routers and proxy servers.

- **Risks related to Inadequate Authentication Procedures**

  Many mobile applications do not have online authentication processes like multi-factor authentication (MFA), resulting in a higher risk quotient. Besides, factors like weak passwords, lack of/ improper session management, etc. can be misused by hackers to manipulate user accounts, gain access to sensitive information or application functionalities, and defraud the user monetarily and in other ways too.

- **Risks related to Servers**

  The server stores and processes very vital information like authentication data, business data, financial or transactional data, and personal data, all of which are pivotal for the smooth functioning of the application. Majority of the communication between the user and application occurs through the server. Hence, any weakness in the server is bound to jeopardize the interests of the application and its users.

- **Risks Associated with Security Misconfigurations**

  Servers, databases, APIs, and cloud services which are not properly configured, pose a risk for mobile applications as there is a possibility that sensitive data will be exposed, giving hackers a field day.

- **Risks Caused by Insecure API**

  APIs (Application Programming Interfaces) too increase the risk quotient of mobile applications due to vulnerabilities like improper or missing authentication procedures, poor data validation, or inadequate access controls. This negatively impacts data integrity as well as confidentiality.

- **Risks Related to Third-Party Dependencies**

  Mobile applications also need to Integrate third-party libraries, plugins, or components, which increase the risk factor for the application, if security checks are not thoroughly done. Insecure third-party integrations have the potential to become backdoor entries through which hackers can gain unauthorized access to the application.

- **Risks Related to Poor Logging and Monitoring**

  Cybercriminals are always at work and hence security testing must be on full alert at all times – even post launch when the application is out in the market. If efficient and active logging and monitoring systems are in place, hacking activitiescan be detected quicker, and necessary steps can be taken to speedily arrest such activities and unauthorized access.

Having dealt with the risks that are common to all mobile applications, this treatise will now train its attention on security issues that are typical to applications on Android and iOS individually. Since applications on these two competitive systems are differently developed and distributed, their security concerns too differ in nature and risk quotient, with applications on Android being exposed to higher risks.

02 Risks Specific to Android Mobile Applications

Android applications have a higher risk exposure, as Android is an open-source operating system, which gives anyone the freedom to use or change Android's source code for developing mobile applications. Furthermore, there is no stringent screening process for applications that are developed on Android, and this too has its negative role to play in increasing security risks for Android applications.

Among the more prominent security issues in Android applications are the following:

- MITM (Man-in-the-Middle Attacks)
- Cryptojacking
- Malvertising
- Phishing and Social Engineering
- Component-related Threats
- Permissions-based Issues
- Rooting

Awareness of these security concerns is the first step in securing them. There are many security testing tools that can identify these issues effortlessly, so that robust solutions can be put in place to avert or fix vulnerabilities.

03 Risks Specific to iOS Mobile Applications

iOS is a proprietary software (except for Apple Public Source License), and this closed environment along with strict screening processes for application development, makes iOS applications comparatively more secure than Android applications. However, even with these processes in place, iOS applications are by no means 100% secure. Cybercriminals have managed to hack into iOS applications too, albeit less frequently. The fact that iOS is largely favoured by high net-worth individuals, keeps iOS applications prominently on the hacker's radar. Security risks detected in iOS applications include the following:

- Storing Data Locally on the Device
- Jailbreaking
- Phishing and Social Engineering
- Permitting 301 Redirects (for permanently redirecting from old to new URLs)
- Stolen Certificates to Host Applications

With this detailed update on the risk profile of mobile applications, this Whitepaper will explore security measures that will help address these risks, in order to make mobile applications safe and secure.

MAKING MOBILE APPLICATIONS HACK-PROOF

Alarming cybercrime statistics infer that security of mobile applications needs to be taken a lot more seriously. Apart from checking known vulnerabilities, testers, and in fact the entire software development team, need to get into the mind of cybercriminals and pre-empt threats, in order to stay ahead of hackers, and secure mobile applications well.

When Should Security Begin?

It's a no-brainer that security of mobile applications is vital and everyone is amply aware of this. However, reality begs to differ. Truth be told, serious efforts for mobile application security testing should be flagged off right at the start of the SDLC, and go hand-in-hand with development. The problems arise when this is not done, and testing is pushed to the end – just before the application is sent to production... And in worst case scenarios, security testing may even be sacrificed on the altar of time!... However, this is sure to backfire sooner or later, and by then, the backlash is great. This section is therefore dedicated to understanding the Types of Security Testing, Strategy for Proficient Mobile Application Security Testing, Steps for Effective Security Testing of Mobile Applications, and Best Practices in Security Testing.

TYPES OF MOBILE APPLICATION SECURITY TESTING

- **Static Application Security Testing (SAST)**

  Static Application Security Testing is a type of testing that is performed on the source code of the application. It is performed by analyzing the code for potential security vulnerabilities. SAST is a powerful tool for identifying security issues early in the development lifecycle. It helps to reduce the cost of fixing vulnerabilities, which will be excessively high, if detected in later stages.

- **Dynamic Application Security Testing (DAST)**

  Dynamic Application Security Testing is a type of testing that is performed on a running application. It is performed by simulating an attack on the application to identify potential vulnerabilities. DAST is a useful tool for identifying vulnerabilities that SAST cannot detect.

- **Mobile Application Penetration Testing**

  This is a type of testing that is performed by simulating an attack on the application, to identify its vulnerabilities. Penetration testing is a useful tool for early identification of vulnerabilities that attackers can exploit.

- **Mobile Device Management (MDM) Testing**

  This is a type of testing performed to ensure that the mobile device is secure. It is performed by checking the device configuration, policies, and encryption. MDM testing is a useful tool for ensuring that the device is secure from various threats..

STRATEGY FOR PROFICIENT MOBILE APPLICATION SECURITY TESTING

Before moving into the security testing process, it's important to have the right approach, keeping in mind the various factors that need to be addressed. Frist and foremost is **Risk Management** which must be effectively thought through. The second concern is **Cost Containment** which can be addressed via a good security testing strategy that optimizes resources, without compromising on testing quality and application security. Thirdly, Security testing must focus on meeting **Legal/Statutory Compliances and Industry Standards,** more so because there is so much of sensitive information at stake. Fourthly **Vulnerability Assessment** must be active throughout the SDLC for timely detection and fixing of all vulnerabilities. Last but not the least, is the **User Confidence** angle of doing security testing from users' viewpoints, to boost user trust and satisfaction. This is vital because if user confidence is shaken, the application can even die a premature death.

STEPS FOR EFFECTIVE SECURITY TESTING OF MOBILE APPLICATIONS

1. **Defining Scope of Testing**

   There are various aspects to be kept in mind, to fully decide the scope of testing. – The type of mobile application, the platform on which it will run, the types of security risk exposure that the application is likely to face, regulatory requirements – whether legal or industry standards, or security directives that are specific to the organization's area of operation.

2. **Setting Up the Testing Environment**

   The real world is a combination of various components and therefore security testing must be done in environments that closely mimic reality. This includes incorporating the various mobile devices the application will be used on, all the relevant operating systems, network configurations, and other related tools and software.

3. **Following Threat Modeling Practices**

   Threat modeling consists of ascertaining and analyzing potential security threats, attack vectors, and vulnerabilities associated with the application's architecture and functionality. This enables identification of possible attack surfaces, entry points, and other security weaknesses in the application, thus guiding the security testing personnels' efforts in the right direction. One important parameter that needs scrutiny, is whether logs are stored within the app store, and the possible threat to user data if credentials are stored. Good encryption is vital to counter this threat. Connectivity with other apps or third-party services also need securing.

4. **Evaluating Vulnerability**

   Vulnerability assessment must begin at the start and be done throughout the SDLC, to scan the mobile application and identify potential security weaknesses. Security testing automated tools greatly aid this process. Proactive vulnerability assessment helps timely detection and patching of mobile applications, thus preventing monetary losses and damage to reputation.

5. **Penetration Testing**

   Penetration testing which is ethical hacking, consists of creating real-world simulated attacks on the mobile application, to identify vulnerabilities that may have escaped vulnerability assessment. There are different techniques, tools, and methodologies that can be used to manipulate vulnerabilities and gain unauthorized access to the application's systems, in order to check the efficacy of its defence mechanisms. Penetration testing helps identify security lapses

6. **Risk Assessment**

   Risk assessment identifies assets, assesses vulnerabilities, estimates threats and evaluates the level of impact as well as the probability of occurrence for each security threat. This helps prioritize security testing, to target the most critical risk areas first.

7. **Security Audits**

   Security audits are important to ensure that the application is security-ready, with security controls, policies, and procedures in place. It also checks that best practices, legal and statutory compliances, and industry standards are met. Security audit is done by reviewing security documentation, interviewing stakeholders, and performing technical assessments to pin-point gaps in security governance, access controls, data protection mechanisms, and incident response procedures.

8. **Holistic Redressal of Vulnerabilities**

   The results of security testing must be addressed totally and comprehensively, whether it involves setting up the network, updating the application code, altering the settings on mobile devices, or any other remedy. It's important to think like hackers and holistically plug all vulnerabilities, to ensure the application is secure.

9. **Re-testing the Application**

   Once vulnerabilities have all been addressed, the next step is to re-test the application to make certain that no vulnerabilities exist, and certify that the application is indeed secure.

10. **Documenting the Results**

    Documentation of the security testing process is important. It must record the results of security testing stating the vulnerabilities found, their severity, the corrective actions taken, and also specific recommendations for future security testing. Meticulous documentation can greatly reduce future security testing time, and improve its quality.

11. **Continuous Monitoring and Redressal**

    Since cybercriminals are always on the prowl looking for novel ways to hack into mobile applications, security testers too need to consistently be on alert, monitoring systems, identifying threats, looking for any untoward activity; and ensuring swift action to plug any security vulnerabilities. Regular vulnerability scans, security assessments, and incident response readiness, are proactive ways to stay ahead of cybercriminals, and ensure timely redressal of evolving security threats that may surface despite best efforts.

Having reviewed the various steps for efficient security testing, this Whitepaper will conclude by presenting best practices for mobile application security testing. These practices will go a long way in enhancing the security of mobile applications and building the confidence of all stakeholders.

BEST PRACTICES IN SECURITY TESTING

- **Integration of Security Testing into SDLC**

  A shift-left testing approach is important to ensure security testing begins right at the start and is meticulously integrated into the SDLC, progressing along-with development. This proactive approach secures the application through all stages of the SDLC including planning, requirements gathering, design reviews, code development, and of course testing. It proves to be cost-effective too.

- **Securing User Authentication**

  User identities and passwords must be well protected via robust access control systems, to prevent identity thefts. The level of authentication controls will vary depending on the sensitivity of mobile application data, and the legal and reputational damage that breaches can cause. It pays for mobile applications that are highly sensitive in these areas, to use authentication server solutions that are conducive for incorporating various types of two factor authentication, and other identity protection processes.

- **Verifying Security of the Software Supply Chain**

  Mobile applications incorporate components of third parties, hence ensuring security of the entire supply chain, is vital. The choice of libraries and frameworks must therefore be governed by their reputation for safety, and security.

- **Securing Data**

  Robust encryption is important for securing data in mobile applications. Encryption changes data into an unreadable format, which helps protect data even if anti-social elements chance to intercept it.

- **Ensuring Safe and Effective Sessions Management**

  Sessions timeout processes should be conducive to user safety, and work effectively too, and hence using industry-standard technologies for issuing security tokens and session management, is advisable. Banking and other high risk mobile applications should ideally have session time-out of just around 15 minutes. This time frame can be relaxed to even an hour for applications that don't deal in sensitive information.

- **Applying the Principle of Least Privilege**

  The principle of least privilege augments security of sensitive user information, by restricting authorization only to those that need access to execute jobs. Demanding more than required permissions is detrimental to mobile application security, as it widens the surface area for attacks.

- **Improving Testing Strategy**

  Continuous testing strategy is better than periodic testing. Testing can be further strengthened via automated testing and threat modeling, to ensure ongoing scanning that helps keep cyber risks at bay.

- **Incorporating App Shielding Techniques**

  App shielding prevents tampering, reverse-engineering, etc. of mobile applications. By segregating the application's data from the runtime environment, it protects the data inside applications. Runtime Application Self-protection (RASP) keeps a check on the application's internal state, inputs, and outputs, thus helping developers detect flaws during mobile application security testing, before or after deployment.

- **Striving for Continuous Improvement**

  A continuous improvement mindset learns from past security experiences, testing results, and industry trends, to improve and fine tune security processes, tools, and strategies. This attitude helps testers quickly counter upcoming threats.

- **Collaborating with Security Experts**

  Collaborating with experts will help gain from their knowledge and expertise. Security concerns are better addressed when well experienced security professionals are employed, as their proficiency in detecting vulnerabilities, awareness of attack vectors, and assessment of security controls, provide timely valuable insights.

- **Leveraging Automated Testing Tools and Frameworks**

  Security testing tools and frameworks that automate vulnerability scanning, penetration testing, code analysis, compliance checks, etc., are necessary to ensure quick and effective security testing, and better security test coverage too; both of which are vital in this current age of speed, volatility, and rising cybercrimes.

In a nutshell: Although cybercriminals are continuously looking for weaknesses in mobile applications that they can exploit for their nefarious purposes, yet with the right security testing strategies; meticulous following of the comprehensive steps for security testing; and incorporation of best practices detailed herein; mobile applications can be kept safe and secure. It is imperative that security testing begins at the start of the SDLC, moves consistently along-with development throughout the SDLC, and continues beyond – as long as the mobile application exists. It is hoped that this treatise will benefit testers and greatly enhance the efficiency of security testing in mobile applications.

CONCLUSION

The Importance of Security Testing in Mobile Applications is amply clear, in the face of intensifying cyberattacks. The increasing complexity of malware, ransomware, and phishing attacks, makes it incumbent on mobile application development and testing professionals, to ensure that every known vulnerability is sufficiently addressed. Security personnel need to go even further, to pre-empt the actions of cyber criminals, to protect the interests of users and build confidence in mobile applications.

Users and organizations alike, need to take utmost care to incorporate every security measure, including patching vulnerabilities, using mobile security apps, implementing strong authentication methods, etc., to counter the increasing risks. Mobile application security testing must therefore start right at the beginning and be meticulously followed along-with development, and in fact continue even post deployment.

The distinction between secure and risky mobile applications, lies in the quality of security testing. We take this opportunity to introduce you to BOTm – a high-tech automated platform for all your mobile and web app testing needs. BOTm keeps abreast of the latest in the software world, and has mastered the art of staying ahead of cybercriminals too. Secure your applications on our tried and tested platform, that offers error-free and effective security testing, and in fact the entire gamut of testing needs. Visit us at **www.botmtesting.com** and avail of our free trial, to experience peace in testing, thanks to the power of our AI and ML driven holistic app testing platform.

GET IN TOUCH

☎ 022 4050 8200

✉ sales@botmtesting.com | www.botmtesting.com

BOTm is the accelerator BOT for automated and manual testing of Mobile and Web applications - developed for both Android and iOS devices.