Staqo
Let's Simplify

Mobile App Security Matrix –

Know, Strap, Pre-Empt, Survive

Staqo Editorial

Contents

Staqo
Let's Simplify

Prelude

Mobile applications are at the center of today's digital world. Any innovation in digital technology, more often than not, finds its way to mobility solutions to help enhance their value. Every business, whether made from bricks or clicks, depends on standalone or group of mobile applications for its end-to-end operations.

As history teaches us well, whatever runs the world, catches the eye of the shrewd attacker out there - immediately. Enterprises have been guarding their fragile points since the days of mainframes, and now with the advent of client-servers and through the penetration of "as-a-service" models and cloud. As mobility solutions take center-stage, they present an even more alluring, and an expanded, surface area for adversaries than what traditional data centers or IT infrastructures manifested.

The average time, data, and attention available on these applications is a goldmine for hackers and trouble-makers, in more ways than one. Plus, the gravity of an attack outcome is changing everyday.

The recent stream of constant, and ever-evolving, security attacks on mobile applications serve as a firm reminder to enterprises to put security at the top berth of their application design and management strategy. Here's a compelling and comprehensive view into the loose-ends that can jeopardize any mobile application and what safeguards or response-measures can enterprises take to bolster their security stance.

Security Soft Spots: Key Categories & Concerns

It is not exactly heartening to hear that as much as three-quarters of apps would not pass even a **basic security test**, that 83% of apps have at least one security flaw. Further, mobile security vulnerabilities are found in 91% and 95% of iOS and Android apps.

The frequency, severity and damage of attacks and breaches are getting worrisome with each passing quarter. Their form and types are also expanding consistently. Let's look at some broad areas that we can classify most app-threats into.

The average cost of a corporate data breach is a whopping $3.86 million, according to a 2018 report by the Ponemon Institute. That's 6.4% more than the estimated cost just one year earlier

Cost of a Data Breach Report, 2020

Broad Categorization of Types of App Threats

- Attacks on tech infrastructure
- Hacking or phishing for data
- Client-side injection of malware
- Broken cryptography
- Insecure data storage (cloud infiltration)
- Attacks on Network Security
- Side-channel data leakage and sensitive information disclosure (internal leaking of data)

- Exfiltration of data through redirected requests; Man-in-the-Middle (MITM) attacks
- Malicious applications or Malware attacks that appear safe but steal data or corrupt devices
- Vulnerability attack through reverse engineering
- Threats to DevOps and APIs due to their third-party integrations
- Android attacks: Ex: The libStageFright library
- iOS attack: Ex: : A vulnerability in its mobile app development environment, Xcode

89% of vulnerabilities can be exploited using malware and hackers may not need physical access to a phone or device for their play, as per some recent data from **PTSecurity**. Some cases are caused by weaknesses in security mechanisms (74% and 57% for iOS and Android apps, respectively, and 42% for server-side components).

PTSecurity Report 2019

- Attacks on self-driving cars, connected vehicles, wearables, smart home appliances and IoT Devices
- Client-side **attacks** that can be exploited without administrator rights (jail-break or root)
- Abusing gaps that creep in during the design stage and correcting them requires significant changes to code
- Exploiting the fragility of server-side components
- Hidden apps: Apps that hide themselves and steal precious resources and data - almost half of all malware consists of hidden apps*
- Riskware: Escalated privileges or side loaded software or broad permissions that users grant without checking security aspects
- Spoofing and phishing attacks

**McAfee Mobile Threat Report 2020*

- Ad fraud and fake displays which hog the memory and processing capacity of phones
- Malware monetization where attackers manipulate users into installing adware
- Malvertising and crypto-mining threats

What is worth noting here is that platforms of all varieties are, more or less, equally vulnerable. So organizations should avoid thinking that **investing in one camp puts your enterprise** and its applications behind some garden wall.

High-risk vulnerabilities were found in 38 percent of mobile applications for iOS and in 43 percent of Android applications. Insecure data storage is the most common issue, found in 76 percent of mobile applications. Android applications tend to contain critical vulnerabilities slightly more often than those written for iOS (43% vs. 38%)

PTSecurity Report 2019

We only need to remind ourselves of the damage caused by - and the radical methods applied with - some recent attacks. Orvibo Leaked Database (2 billion), TrueDialog (>1 billion), Verifications.io (808 million), "Collection #1" Data Breach (773 million), Dream Market (620 million), Third-party Facebook App (540 million), Indian Citizens MongoDB Database (275 million) are just some examples that show the versatility that attackers have started to demonstrate in their rampage.

39%
companies suffered a security compromise - as per a recent Verizon report

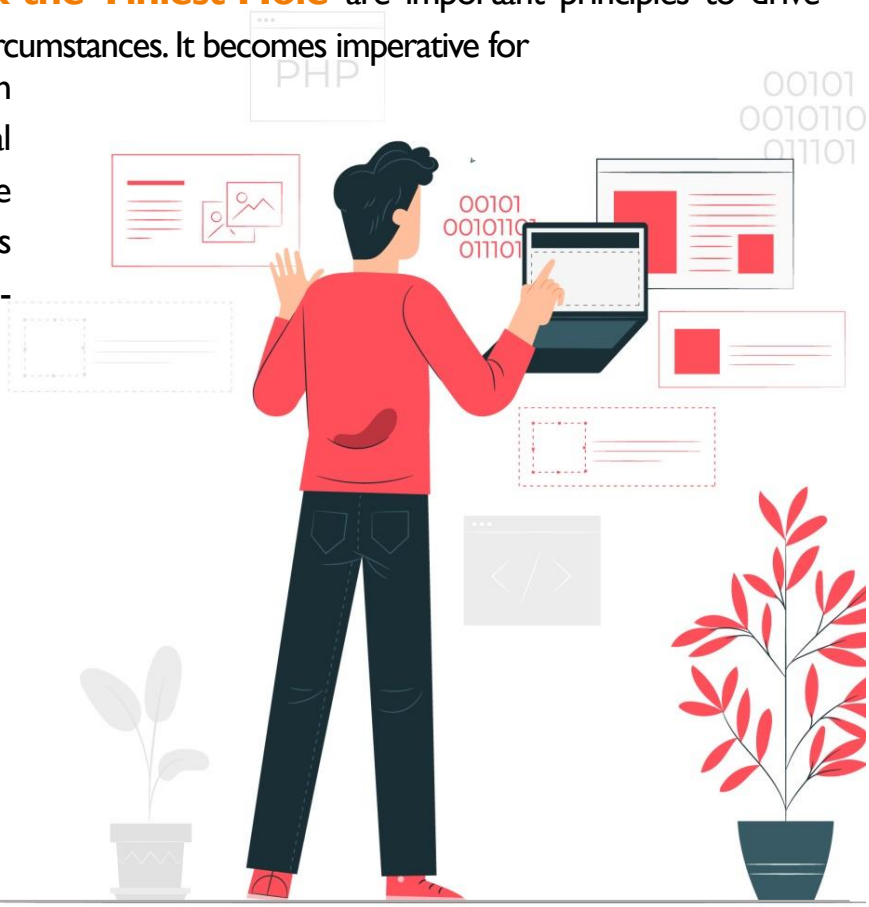
37%
respondents said that the compromise that they experienced was difficult and expensive to remediate

86%
organizations were concerned about malware, and 20% of those don't feel prepared for it

Say Goodbye To Conventional Tactics - Sharpen & Customize Your Defense

The big question is how to protect the app and hence – the user and enterprise? For this, a lot of questions have to be asked at the design and development stages. When an application is created, it entails both the client side and server side. The client runs on the operating system – which can be built on Android or iOS or any other OS. This client gets downloaded to the device and this is where an app distribution platform kicks in and the OS starts using it. On the server – that is hosted by the developer and where data is stored and processed – a web application interacts with the mobile client through an API. Of course, most operating systems are laden with various security mechanisms and sandboxes. But it is those errors that are made by developers in designing and writing code where a lot of room is created for future attackers.

Secure-by-Design and **Fix-the-Tiniest-Hole** are important principles to drive your security strategy in these circumstances. It becomes imperative for an enterprise and the dev team to take care of some fundamental areas if they aim to augment the security of the application. Let's look at a few specific & well-timed measures below.



Staqo
Let's Simplify

- Execute comprehensive security checks for vulnerabilities in the client and server and data transfer areas – do not be assured with just a tick box in one area. Both client-and-server side checks and authentications are important.

- Secure the source code and do not create conditions for it to be available for the wrong eyes.

- Secure the Inter-Process Communication (IPC) parts to avoid attacks via remote access of data.

- Restrict custom keyboard extensions and third-party keyboards that can open new doors for attackers.

- Look at data portability areas seriously. Explore protocols that are in alignment with the latest developments. Like OAUTH, for instance.

- Improve server-side controls.

- Incorporate security in user-testing and other app-performance assessments. Like a test on Input validation can help you to prevent malformed data.

- Try penetration testing with the strongest tools possible to assure you of protection against a wide range of vulnerabilities.

- Secure cryptographic keys, lock down app permissions.

- Make reverse engineering of applications unwieldy and time-consuming. Use third-party tools and software code obfuscation.

- Obfuscate and Strip all that is possible: This will force attacker to traverse the data in the runtime code, decode the binary code, or use advanced methods for mapping application symbol to class names, methods, and function names.

- Incorporate a thorough certificate check on the client-side and secure communications between the client and the backend server.

- Employ mechanisms in advance for anti-debugging, tamper-checking, anti-pharming etc.

- Test cloud applications before implementation – take proper cognizance and coverage of Shadow IT here.

8% of iOS users have jail-broken their devices and 27% of Android devices are running with root privileges. Devices with such privileges are at greater risk, because these privileges can be abused by malware.

PTSecurity Report 2019

- Explore flaws in the implementation of two-factor authentication, as well as configuration flaws around disclosure of sensitive information in error messages, fingerprinting in HTTP headers, and TRACE availability.

- With iOS and Android, specifically, prevent **jail-breaking** loop-holes and root privilege-related issues as much as possible. Ex: Android Debug Bridge (ADB), SSH credentials (root:alpine) on Apple.

- Avoid MITM attacks with certificate pinning.

- Use web application firewall.

- Incorporate proper analysis and monitoring of third-party mobile app risk, including tracking inventory with specific training and AppSec testing tools.

- Follow the latest industry standards and collaborations that are creating stronger blacklists and best practices for the latest slew of threats.

- Be rigorous about Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), National Information Assurance Partnership (NIAP), Common Weakness Enumeration (CWE), and other standards for security.

- Be ready for broken cryptography and ensure fail-proof use of algorithms. Ex- MD5, MD4, SHA1, BLOWFISH, RC2, and RC4.

- Apply encryption at all levels along with strong device-level security. Cover file system, application, database access, and device levels.

- Cover end-to-end data security - at rest on the device, in transit between the device, and servers behind your firewall.

- Provide well against user-side weaknesses – like presence of sensitive data in snapshots, Hash functions with salt (set of random characters) that can be found in the source code.

- Isolate mobile app data with a layer of protection around enterprise-deployed apps, secure network access, authentication mechanisms, network encryption etc.

All this is possible when an organization and the IT team execute platform-health checks and visceral testing-drills with rigor and regularity. Make routine updates and back-ups a habit and an over-arching guideline.

Always deploy every stretch of testing possible – this includes White-box, black-box and gray-box testing. Above all – never compromise security for functionality, speed, performance, uptime or experience. Sooner or later, a loophole in security can wreck the very metrics that you wanted to amplify at the cost of security. An app is only as strong as the slightest chink in its armor. Before you put a bow on it with all the development magic, test it well and keep it amenable for regular checks and updates once it rolls out. The lifecycle value of an app and its revenue-muscle will hinge a lot on its security stronghold.

Conclusion: The Next Frontier - Good Guys vs Bad Guys

As we can surmise from the above information and contemplation, mobile applications would continue to be tempting targets of security attacks. More so with the exponential scale that they get from embracing new technologies around IoT, Artificial Intelligence, Machine Learning, Quantum Computers, Drones, and Robotics. The very fact that applications will start deepening their impact and touching more corners, makes them both easy and attractive for security exploits. The depth, customer intimacy, usage and scale of mobile applications will only grow manifold as we move forward.

As the world gets conversant with connected cars, home, healthcare, voice assistants and bots, there is a bigger playground that is opening for the attackers and monetization thieves out there. On a casual look, this could be just another breach that you can shrug off and move on from. But when you take an aerial view, these attacks are big dents. They cause business disruption, system downtime, and compromise customer trust and privacy. Failing to protect mobile applications will cause customer churn and data leakage along with some bigger compliance and safety costs.

That makes it very critical for enterprises to arm themselves with as many security seat-belts and fail-safes as they can. It is going to become increasingly difficult as attackers will choose the very technologies that application makers are using to defend them. Ex: Adversarial AI and Quantum-based encryption-attacks. The only edge that enterprises can count on then is that of time, discipline, and creativity. Apply the best approach, tool, and stance before an adversary does, and better than how the wrong guy does. There is no rest or pause button here. Keep moving. Keep gaining inches of advantage. That's the only way to stay strong and unscathed in this difficult landscape.

Transform your business & introduce digital acceleration with our Application Services

EMAIL US

www.staqo.com

Staqo
Let's Simplify