Picture credit: Unsplash

HAVE APP WILL TRAVEL

Alan Bavosa *highlights five cyber attacks developers need to know about when it comes to travel booking apps*

With the new year approaching, many are starting to give consideration to their holidays using booking apps such as Skyscanner to plan and book their getaways. According to TravelPerk, the use of these apps is growing rapidly in the UK. In 2022, over 50 percent of travellers used them, with this number expected to grow to 60 percent by 2025. The immediacy of mobile booking has made it the preferred method for travellers who need to organise a trip on short notice. It allows users to find precisely what they need quickly and easily, with the added convenience of being able to do it from their mobile phone. Additionally, travel booking apps allow users to compare prices from different providers and read reviews, ensuring they are getting the best deal and the most reliable service.

As the travel market continues to grow, so too will the number of hackers and fraudsters targeting travellers and travel booking apps. And given the increasingly sophisticated nature of today's cyber attacks, it's more important than ever for mobile brands to prioritise security and protect users and themselves. With so much sensitive data being exchanged during the travel planning and booking process, it is essential to take steps to protect this information from cyber criminals.

However, mobile app security is often overlooked in the booking app industry, increasing the likelihood of successful attacks. A recent study conducted by Security Affairs researchers on top travel booking apps found a wide variety of security issues which exposed sensitive data and personally identifiable information (PII), including home addresses, credit card and bank account numbers, phone numbers, usernames, passwords and session tokens. These security issues could pose both a financial and physical risk to users. For example. If a hacker were to gain access to a user's credit card details and use these to make unauthorised purchases.

With the implications of poor security clear, let's look at the five most common cyber-attacks on travel booking apps and how to solve them.

It is vital that mobile app developers implement an automated cyber-defence system that powers continuous building, testing and monitoring of mobile security features

DATA STORAGE SECURITY AND INADEQUATE DATA ENCRYPTION

Insecure data storage and inadequate data encryption are two of the most common security weaknesses in mobile apps, which allow attackers to steal sensitive data by harvesting the valuable information stored and handled by mobile apps if the app is not sufficiently protected. For example, booking apps often store sensitive data in cleartext, which means that it is not encrypted and can be easily read by anyone who can access the data using many different methods.

Alternatively, they may use weak encryption algorithms or implement the technology incorrectly, which can make it easier for attackers to break the encryption and steal the data. For instance, by using open-source tools, such as Frida, hackers can reverse engineer apps to figure out where this important data is stored in the code and then freely read the data if it's not encrypted. App developers should implement data encryption, such as AES 256, for data stored in the app as well as information stored in the source code as text-based strings.

It's also important to encrypt data in transit as well as in memory. This protects the data while it is being transferred to another, this is especially important when data is being transmitted over public networks. The more sensitive the data, the stronger the encryption should be, especially with travel booking apps when information such as passport details are being shared over multiple platforms.

REVERSE ENGINEERING – DYNAMIC & STATIC ANALYSIS

Hackers employ a variety of techniques to analyse applications, including both static and dynamic analysis to comprehend the inner workings of applications and manipulate them in many ways. Static analysis is a method of analysing an application's code without actually running it whereas dynamic analysis is a method of analysing an application by running it in a stimulated environment. They utilise debuggers and emulators to observe how applications behave in, while disassemblers and decompilers aid in extracting source code and gaining insights into its execution. There exists a plethora of freely available tools for nearly every task a hacker desires to undertake.

IT IS VITAL THAT APP DEVELOPERS IMPLEMENT A DECENT AUTOMATED CYBER-DEFENCE SYSTEM

Leveraging the insights obtained through these tools, hackers can understand how the app works, create clones or fakes, all of which they can use to devise tailored attacks to exploit these weaknesses or figure out how to attack the app's backend.

This can cause serious issues for app providers, not least because apps are required to comply with PCI DSS (Payment Card Industry Data Security Standard) – a set of security standards designed to protect businesses from becoming targets of cyber criminals as payments are usually made through a credit card.

The very first layer of defence in any mobile app security strategy should consist of hardening or 'shielding' the app by implementing basic runtime application self-protection (RASP) measures like anti-tampering, anti-debugging, anti-reversing and jailbreak/rooting prevention. Next, it's important to protect the source code of mobile apps using multiple methods of code obfuscation, such as obfuscating the code, libraries and logical flows of the app so that hackers can't easily understand how the app works by decompiling and analysing the source code.

CONNECTION INSECURITY AND MITM ATTACKS

Another common attack vector is to compromise the connection between the app and the server, through man-in-the-middle (MitM) attacks. MitM attacks occur when an attacker secretly intercepts a communications session between two parties and takes control over the session. There are many ways to achieve MitM attacks, including using malicious proxies, fake certificates, session or cookie hijacking and much more. Businesses can tackle this by protecting their app's connections using a combination of methods such as certificate pinning, certificate validation, enforcing a minimum version of TLS and detecting malicious proxies. These are all effective ways to protect users' sensitive information.

OVERLAY ATTACKS, ACCESSIBILITY MALWARE AND PERMISSION ABUSE

Malware is on the steady rise as a key weapon in attacking Android and iOS apps. Attackers leverage malware, key injection, method hooking and overlay attacks to steal or harvest data used in mobile app transactions or even to falsify mobile transaction data. Overlay attacks in mobile apps occur when malicious actors, typically with the assistance of malware, superimpose a fake graphical interface (overlay) on top of a legitimate app screen to deceive users into performing unintended

actions. Fraudsters are also increasingly abusing legitimate mobile app functions, such as tricking users into approving permissions which malware then abuses, or intercepting accessibility events to take control over apps and achieve account takeovers. These attacks are often used to steal sensitive information, such as log-in credentials, credit card info, loyalty points, *etc*. or to trick the user into enabling features that the attacker can later use to weaponise the app, escalate administrative privileges or plant a backdoor through which they can send payload updates to malware resident on the device. By protecting devices from overlay apps, hackers are blocked from even reaching the app, preventing any data being tampered with or stolen.

AS THE TRAVEL MARKET GROWS, SO TOO WILL THE NUMBER OF HACKERS TARGETING TRAVELLERS

COMPROMISED APIS

Booking apps connect with multiple systems to provide seamless user experiences. These systems often communicate with each other using APIs which allow different applications to communicate with each other and exchange data. APIs can be vulnerable to attack for several reasons. Firstly, each API represents a separate attack vector, if one API is not properly secured, it could be exploited by hackers to gain access to sensitive data or disrupt the app's functionality.

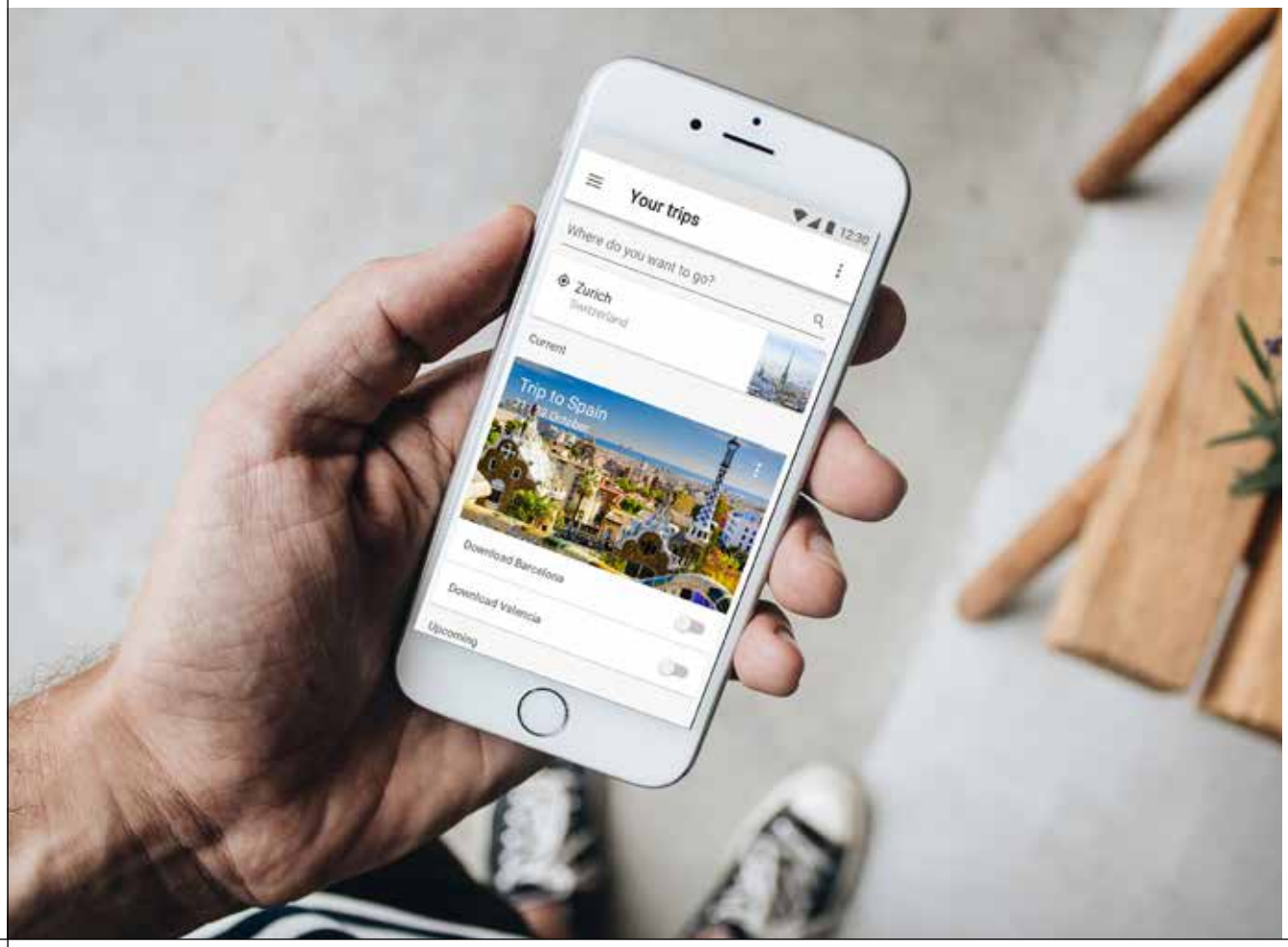
In addition, backend APIs are often targeted by malicious bots and botnet networks which attempt to compromise backend APIs as part of various automated cyber attacks, such as credential stuffing, DDoS and account takeovers (ATO). If your travel processes transactions, then APIs are certainly a target. To protect your backend APIs, it's important to consider a bot detection solution that has been designed to protect against threats in the mobile channel (which is where most of the users are). Your bot detection solution should also consider the mobile user experience and not impose a burden on dev teams to make changes to the app's source code.

Since cyber criminals are constantly evolving their tactics, it is now more important than ever that mobile app developers implement an automated cyber-defence system that powers continuous building, testing, and monitoring of mobile security features within the CI/CD pipeline. This way, apps can continue to serve users without adding additional work, resources or time to their releases.

With travel on the rise and mobile apps a top choice for not only booking, but checking in, tracking, sharing, saving, storing and spending money on any travel journey, it is vital that app providers and developers are taking the necessary steps to help to prevent attacks and protect users' data. This guide outlines the key steps that developers can take to implement an automated cyber-defence system for their mobile apps ●

Alan Bavosa is VP Security Products at Appdome.

By protecting devices from overlay apps, hackers are blocked from even reaching the app in the first place



Picture credit: Unsplash