TOP 10 MOBILE SECURITY RISKS

METOVA

MOBILE DEVICES AND APPLICATIONS ARE NEVER DEVOID OF VULNERABILITIES.

When new features are added, so are new openings for potential threats. In order to continue to create mobile applications that our customers rely on and that we can be proud of, our developers stay on top of changes in operating systems and current best practices.

APP SECURITY

1. Clone Wars

Do you have Instagram on your phone? Pokemon Go? Counter Strike? Breadwallet? All of these applications have been the target of malicious app cloning. In order to do this, hackers create similar applications designed to trick a user into downloading them. Users blindly give the app permission to access the device as if it were the original app. Then it becomes easy for the application can commence its dirty deeds.

The types of damage these apps can do vary. The Pokemon Go clone included a remote access trojan that allowed hackers remote access to the device and users' personal information. Apple has seen an influx of counterfeit currency management applications that are created to steal users' money. Sometimes the applications only collect personal information that will then be sold at a later time.

How do you protect yourself? While not foolproof, it is likely safer to download an application from a reputable app store than a third party source. Niantic staggered the release of the Pokemon Go application to the store which prompted users to download the APK file from alternate, and sometimes malicious, sources.

2. Android “Instant App” Vulnerabilities

The idea of instant apps was introduced at Google I/O 2016 and has since been slowly rolled out. Instant apps give the user the ability to use just a piece of functionality without needing to wait and download the entire application.

Users just have to click on a link to run it. Contextual clues like developer, description, screenshots, url, etc that normally give insight into whether or not the install is trustworthy are unavailable. Even once it is installed it could be difficult to recognize abnormalities since it is all new to the user.

Instant Apps will be available on devices running Jelly Bean 4.1 and up, although older devices may have trouble displaying them. In October 2017, almost 50% of compatible devices were running pre-Marshmallow, which means that they don’t have the flexibility to pick and choose app permissions. In addition, users running older versions are missing out on security updates and patches that could protect their device.

The way that applications can be updated to work with Instant App downloads could also cause trouble. Because the applications will need to be modularized, there is a new opportunity for backdoors and malicious code to be added. Since many applications are already in the Play Store, the approval process for updates may be more lax, allowing for malicious additions to enter unnoticed.

3. Mobile Ransomware

Mobile ransomware was in our list of top mobile security threats last year. This year, it is still a top vulnerability. People live their lives on their phones. They are used for everything from social interactions to shopping to working. Ransomware expects that your device stores large amounts of important information- information you would willingly pay large sums of money to get back if it became unavailable.

Ransomware holds devices hostage by locking the user out and demanding a payment to be made before access is granted. The best way to avoid it is to download applications from a trusted source and keep your applications and system updated.

4. SMS-based Attacks

Up until recently, two-factor authentication via SMS has been a recommended option for safer login. After entering a username and password, a user must then submit a code sent to them via text to complete authentication. It is unlikely that a person's username, password AND physical device would be compromised at the same time. Unfortunately, now through redirection or interception, hackers can access an SMS without needing the actual device. Because of this, NIST (the National Institute of Standards and Technology) is considering removing out-of-band authentication using the SMS from their guidelines.

While SMS is not as safe as it once was, there are still multiple viable alternatives for two factor authentication. Applications like Google Authenticator or dedicated hardware tokens are good options. These work by constantly changing the password based on an algorithm shared with the server. The site or application you are logging into gives you a key that can then be transformed into a token via the authenticator. Both options are far less likely than SMS to leak an access code to a third party.

5. Improper Platform Usage

Operating systems come with security features and best practices. iOS has a keychain feature that assists applications in the storage of passwords and any other bits of secure data. Others may focus on payments, permissions, or communication. These features are there to guard against a variety of vulnerabilities. When these are overlooked, misunderstood, or blatantly ignored, it makes an application vulnerable. Use a developer who is familiar with the ins and outs of the platform to ensure your application takes advantage of these features.

DATA VULNERABILITY

It's commonplace to keep the information a user enters in an application around for the next time it is needed. This keeps the user from needing to enter the same information multiple times and reduces friction. In order to offer this type of user experience, the data has to be securely stored from session to session.

6. Insecure Data Storage

Developers should always protect their users' information. One example of insecure data storage is keeping data in an unencrypted format. Even though the Average Joe won't know one way or the other, a hacker or nefarious app will. If personal information is in plain sight in the code, it can be very easily stolen. This can include anything from location data to passwords to credit card numbers.

7. Insufficient Cryptography

Encryption is standard operating procedure and needs to be done correctly. In order for data to be encrypted, an algorithm (cipher) is used to transform the data into a seemingly nonsensical format. Using an inappropriate cipher or an encryption key that is short or obvious, such as user ID, weakens the encryption and allows for easier theft.

8. Insecure Communication

Devices and applications are constantly sending and retrieving data: websites, passwords, messages, media, etc. If you need Wifi or a data connection to use it, your device is communicating with a server to offer it. These communications should be done using TSL (transport layer security), which is colloquially still referenced by many as SSL. When communication is insecure, it opens your device up to man-in-the-middle attacks and network sniffing. This means third parties could potentially intersect communication or disguise themselves as a trusted source.

9. User and Device Authentication

Before displaying personal information or communicating with a server, an application needs to verify the authenticity of the person or device. Without this check, everything is exposed for the taking.

Passwords are required for just about everything. The difficulty in creating a password, strength, and type of information that is being stored behind the login wall must all be weighed to ensure a user's information is kept safe without becoming too much of a hassle. Many applications require long complicated passwords with a minimum number of characters, numbers, non alphanumeric characters, uppercase, and/or lowercase. Users tend to make obvious exchanges such as 3 instead of E or ! to replace an i, reducing the efficacy of the requirement.

It has been determined that the improved security received from these sorts of requirements is greatly outweighed by frustration it causes the user. In order to strike the perfect balance, the NIST recommends that **user generated passwords** be user-friendly.

They should be a minimum of 8 characters with a maximum of 64. Although it was previously thought best to rotate passwords every 60-90 days, now it is recommended to only change them when required or compromised. To minimize breaches, the number of incorrect login attempts permitted should be restricted. Applications should compare new passwords to a blacklist of previously hacked passwords, dictionary words, and other likely options such as the name of the application. If a match is found, the user should create another.

10. Timed Sessions

Not only should an application have rules around acquiring access but also severing it. Understandably, forcing a user to log in every single time they access the application can impede use. Sometimes however, more controlled access is necessary. When an app contains highly sensitive information, it is important that the developer require authentication more often to reduce the chance of compromisation. The exact timeframe should be contingent on how long it takes users to complete their tasks and the sensitivity of the information exposed. This is often seen with banking applications and websites where users are automatically logged out after only a few minutes of inactivity.

STAY SAFE

Threats are everywhere. The best thing you can do to counteract them is to be aware of the possibilities and stay proactive. Be cognizant of what applications you use, where you get them from, and what permissions they require. When it comes to building your own application and putting your name on it, use a development team that knows the platform. Go with a reputable company that can develop not only a good-looking application, but one you know will care as much about your users' security as you do.

LEARN HOW METOVA CAN SECURE YOUR MOBILE APP

Contact us to get started on making your company's app more secure.

CONTACT US TODAY

METOVA