Kanpur Philosophers
ISSN 2348-8301
International Journal of humanities, Law and Social Sciences
Published biannually by New Archaeological & Genological Society
Kanpur India
NAAGS KANPUR
Vol. X, Issue I(K) : 2023

INFORMATION SECURITY - CYBER-SECURITY IN MOBILE APPS

Ms. Rucha Patil, Assistant Professor, Department of Information Technology, Nirmala Memorial Foundation College of Commerce and Science

Abstract:

Information security is the practice of minimizing information risks in order to secure information. Typically, it entails lowering the likelihood of data theft or other unlawful uses. As well as the destruction, discovery, modification, inspection, or recording of sensitive data. It entails taking steps to avoid such occurrences.

Information security's primary goal is to secure data while retaining its confidentiality, integrity, and availability against cyber attacks and hackers.

Keywords : Cyber Security, Discovery, Inspection, Confidentiality, Integrity, Availability.

Introduction:

Modern security tools can cover all sorts of devices, but mobile devices present threat vectors, privacy issues and security challenges that aren't common elsewhere. For example, device loss and theft can occur much easier with mobile devices than with PCs. Find out what considerations IT must consider when building a mobile security plan.

Mobile device hardware, such as cameras and fingerprint scanners should be used to enhance cyber security in an “always on” world. Some examples include biometric access controls, like facial recognition, fingerprint scanning, and two-factor authentication. Apps should be designed to work without Wi-Fi or cell signals, so as to maintain user productivity even when normal connectivity fails.

Cyber Security

Cyber security is business-critical to prevent data leakage and unauthorized access to sensitive data assets, A compromised mobile app may well give intruders access to these assets or the ability to take users offline. Security vulnerabilities in mobile apps may allow attackers to exploit either the application platform or the mobile app platform’s operating system with the goal of accessing and stealing sensitive information. Security vulnerabilities in the underlying Wi-Fi environment – especially, in “work from home” environments – may also be exploited by cybercriminals to gain access to sensitive business information. Security weaknesses in the underlying mobile apps may also be used to steal authentication information for later attacks on the apps and business systems.

Techniques to be considered include encrypted databases (with stringent management of encryption/decryption keys), and encryption of all data while in transit over public networks. These techniques ensure that, even if a hacker does penetrate the app or the network, any stolen data will be unreadable. Further, appropriate encryption techniques can also be used to sign and timestamp all changes to corporate data, which may be useful for legal purposes, or in the event of rebuilding lost

or damaged databases.
Insecure code is the key cyber security issue with mobile app development. Criminals typically exploit poorly designed or programmed code to infect the underlying mobile apps and to use them for nefarious purposes, including stealing sensitive data or demanding exorbitant ransoms (now in the millions of dollars per successful attack).

During mobile app development, enterprises should always apply best practice security measures, including manual or automated code scanning to identify common security weaknesses, like insecure libraries, unpatched development tools, breaches of development standards, insecure third-party code, and stringent standards for coding, testing and updating of production libraries.

1.1 No code in apps

a) Low-code and no-code mobile app development software can help, especially when creating task- based apps for small business transactional systems, web applications, and analytics apps.

b) Low-code/no-code applications streamline security verification processes by ensuring that security code integration with a system takes place early in the development cycle, with frequent updates.

1.2 Testing

Penetration testing allows developers to discover and mitigate mobile app vulnerabilities, allowing for optimization at different stages of the development cycle. Such testing reveals potential loopholes that may be exploited to compromise different app features and data.

1.3. Using high level authentication methods

The mobile app development industry has been exploring the potential of passwordless solutions, with biometrics and two-factor authentication explored as alternatives for credential validation. Organizations and developers not yet comfortable with the passwordless route should ensure the mobile app is designed only to accept strong alphanumeric.

Security configuration monitoring (SCM) enforces compliance and prevents cyberattacks.

Summary :

Contact one of our product experts to find a solution that meets your security needs and reduces your business risk. Whether you have one or several initiatives to respond to, ensures compliance, security, and flexible risk management solutions.

References

1) The Art of Invisibility: The World’s Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data

2) Hacking : The art of exploitation

3) https://onlinedegrees.sandiego.edu/information-assurance-vs-cybersecurity/

4) https://www.tripwire.com/solutions/compliance