Security / Encryption in Mobile applications

Introduction:

In the past few years, the increase of smartphones and the fast progress of mobile technology have drastically changed the way we use digital services. From banking to social networking and from shopping to healthcare, mobile applications have made the processes of doing things easier and have also improved our lives in ways that were never before possible. Through the taps on our screens, we can carry out the financial transactions, get to see our personal health records, and talk to people from all over the world. However, as the use of mobile applications is increasing the more, the concern for security and privacy is growing also. The main features that make mobile apps indispensable are also the ones that make them susceptible to the manipulation by the bad people. Cybercriminals are always on the lookout to find the loopholes in mobile app security to get unauthorized access to the data, such as personal information, financial details, and confidential communications. Thus, the encryption becomes a major protective measure. Encryption is the process of concealing data in a way that only the authorized persons with the proper decryption key can access or decipher it. Through the encryption of confidential data in mobile applications, developers will be able to stop unauthorized access and hence, the user privacy will be preserved. No matter if it is encrypting the communication channels, protecting the stored data, or verifying users, encryption is the basis of the mobile app security. This research paper is dedicated to the analysis of the complicated security and encryption landscape in the mobile applications. Through studying of today's industry trends, recognition of the most common security problems and a rigorous analysis of the present encryption solutions, we intend to expose both the advantages and the shortcomings of the current methods. In addition, we are suggesting new ideas and improvements in order to go for a roadmap for a much stronger and stable mobile app security environments. In the subsequent parts, we will investigate the industry trends and the needs and analyse the current encryption solutions, critically discuss their advantages and disadvantages, and finally we will suggest new strategies to enhance the security posture of the mobile applications. By considering different points of view and using multifaceted approaches we aim to assist in the discussion of mobile app security and thus create a safer and more secure digital world for everyone.

Industry Trends:

Nowadays, the mobile applications industry is undergoing a paradigm shift with the constant development of the mobile applications that are becoming the part of almost everything in the modern life. From the way to the mobile apps have changed the lives of the users from managing finances to communicating with friends and colleagues to getting health care services, they have become the most essential tools that give the users with the convenience and the accessibility that they have never had before. Nevertheless, the fact that mobile technology has been deeply embedded into our everyday lives also bears security issues which cannot be overlooked.

The paramount necessity in the software industry today is the introduction of tight security mechanisms in the mobile applications because they are the basis of primitive life. This demand is especially important in those industries where it is impossible to share the information without facing risks such as banks, healthcare, and communication.

Mobile banking applications, for instance, have become a basic part of the modern banking services that have been introduced to the customers, giving them the opportunity to perform different financial transactions, for example, through the palm of their hands. Yet, the frailty of these applications, which deal with the financial data like account numbers, transaction history, and payment credentials, makes them the most sought-after targets by the cybercriminals. A potential breach of a mobile banking app can lead to the severe financial losses for users and the irreparable damage to the reputation of the financial institutions. Besides, healthcare applications have also seen a sharp increase in use, providing the patients with the opportunity to get to their doctors, to book appointments, to get telemedical consultations, and to monitor their health using the technology. However, the huge amount of private medical data that is kept inside these applications which includes the medical history, the treatment records and the personal health information, make them the most targets for the bad people who want to use this data for financial gain or to steal the identity of the owner of the data. In addition, communication apps, including messaging platforms, email clients, and social media applications, sit at the heart of the world-wide connection and the exchange of information. Nevertheless, the full-fledged transmission of confidential communications that could be from a personal to a business conversation, demands to have tight security procedures to protect the whole process from the interception, eavesdropping and data breaches.Basically, the fact that mobile applications are now available in almost every field proves the importance of strong security measures to be taken in order to protect the private information and keep the user's privacy. The dependency on mobile technology is increasing and it is necessary for the software developers and the industry representatives to concentrate on the security and encryption of the mobile applications in order to protect the user from the changing threats and to maintain the user confidence and trust.

Current Solutions:

Mobile applications employ various encryption techniques to address security concerns and below are some of them which I feel are the current solutions:

1. End-to-End Encryption (E2EE): WhatsApp and Signal messaging apps use E2EE which makes sure that only the recipient can decrypt the message so no one else can access the information.

2. Transport Layer Security (TLS): The TLS protocols enable data transmission over networks with encryption so that eavesdropping and tampering are not possible, thus, they provide protection for the communication channels between the client devices and the servers.

3. Advanced Encryption Standard (AES): AES is used to encrypt data which is stored on devices; thus, it protects the sensitive data from unauthorized access by transforming plaintext into ciphertext.

These encryption methods and protocols strengthen the mobile app security; hence they protect the user privacy and the mobile apps from security breaches in the digital world.

Critical Analysis:

1. End-to-End Encryption (E2EE):

Limitation: Relies heavily on trust in app providers, making user data vulnerable to hacking through backdoors or vulnerabilities.

Pros:

Provides strong protection for data during transmission and storage.

Ensures that only the sender and intended recipient can access the encrypted data.

Cons:
Vulnerable to attacks if implemented incorrectly or if there are flaws in the encryption protocol.
Can be challenging for users to verify the authenticity of encryption implementations.

2. Transport Layer Security (TLS):
Limitation: Weaknesses in data protection can lead to man-in-the-middle attacks, compromising data integrity.
Pros:
Widely used protocol for securing communication over networks.
Provides encryption and authentication, ensuring data confidentiality and integrity.
Cons:
Vulnerable to attacks such as protocol downgrade attacks or implementation flaws.
Requires regular updates and patches to address newly discovered vulnerabilities.

3. Advanced Encryption Standard (AES):
Limitation: Complex encryption algorithms like AES can slow down applications due to their computational intensity.
Pros:
Widely regarded as a highly secure encryption standard.
Provides strong protection against brute-force attacks.
Cons:
Resource-intensive encryption and decryption processes can impact system performance.
May not be suitable for all applications, especially those with strict performance requirements.

In summary, while these encryption solutions offer significant benefits in terms of data security, they also come with their own set of limitations and challenges. It's essential for organizations to carefully evaluate their security needs and select encryption solutions that strike the right balance between security, usability, and performance. Additionally, regular updates and adherence to best practices are crucial for mitigating the risks associated with these encryption methods.

Proposed solution:

To address current limitations, a hybrid encryption approach is proposed as below based on my readings and understanding of the topic.

Hybrid Encryption: The advent of the hybrid cryptography method that employs both, symmetric and asymmetric cryptography, thus, facilitates the efficient data transmission and security key exchange. Symmetric encryption like AES encrypts data while asymmetric encryption like RSA handles key exchange.

Homomorphic Encryption: The use of homomorphic encryption allows for the computation of encrypted data without the data being decrypted, thus, more privacy and security is ensured in data processing.

Thus, my thought is to have a hybrid style of mobile applications, which is based on homomorphic encryption, can be used to secure the apps more and to protect the privacy of the users without the compromise on the performance.

Citations:

1) Munjal, K., & Bhatia, R. (Year of publication). A systematic review of homomorphic encryption and its contributions in the healthcare industry. (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9062639/)
2) Z. Zhou, C. Sun, J. Lu and F. Lv, "Research and Implementation of Mobile Application Security Detection Combining Static and Dynamic," *2018 10th International Conference on Measuring Technology and Mechatronics Automation (*https://ieeexplore.ieee.org/document/8337376*)*
3) Ali Balapour, Hamid Reza Nikkhah, Rajiv Sabherwal, Mobile application security: Role of perceived privacy as the predictor of security perceptions,International Journal of Information Management,Volume 52,2020,102063,ISSN 0268-4012 (https://www.sciencedirect.com/science/article/pii/S0268401219309041)
4) Paul, Prantosh and Aithal, P. S., Mobile Applications Security: An Overview and Current Trend (October 10, 2019). Proceedings of National Conference on Research in Higher Education, Learning and Administration, 1(1), pp. 112-121. ISBN No. 978-81-941751-0-0., Available at SSRN: https://ssrn.com/abstract=3484091