Brenda Sugey Vega Contreras
CSS545 Mobile Computing

May 19th, 2024
HW4 - Advanced Topics

ENCRYPTION VS ENCODING VS HASHING - TECHNIQUES USED IN MOBILE APPS FOR COMMUNICATION SYSTEMS

Introduction

Mobile applications have become integral to modern communication, with millions of users relying on instant messaging and communication apps for daily interactions. These apps provide users with ways to send messages, share images and videos, and make calls and videoconferences with one or more users. Ensuring the privacy and security of these communications is paramount, and this is where encryption, encoding, and hashing play vital roles. This paper explores how these techniques are applied in mobile apps, with a particular focus on instant messaging apps used for communication systems, to secure user data and maintain integrity.

It's important to clearly understand that encryption, encoding and hashing are used to change the format of data for different purposes [1]. Encryption is a type of encoding technique where the message is encoded using an encryption algorithm so that only authorized persons can access that information. On the other hand, encoding is a technique where the data is transformed from one form to another. Finally, hashing is a technique where the data is converted to hash using different algorithms present there [1].

Industry Trends and Needs for Instant Messaging and Communication Apps

To delve deeper into encoding, encryption and hashing techniques used in mobile apps for communication systems, WhatsApp will be used as an example. WhatsApp is a popular instant messaging (IM) and voice-over-IP (VoIP) service owned by Meta that allows users to send text, voice and video messages, make voice and video calls, and share images, documents, user location, and other content [2].

Some of the major challenges for mobile apps used for communication systems are addressed below:

- **Encryption in Mobile Apps.** As mobile apps handle increasing amounts of sensitive information, encryption has become a critical security measure. Users demand privacy, and regulatory requirements like the Electronic Communications Privacy Act (ECPA) which protects communications during transmission and storage [3]. Encryption ensures that even if data is intercepted, it cannot be read by unauthorized parties.
- **Encoding in Mobile Apps.** Encoding is essential in mobile apps to ensure data is properly formatted and transmitted, preserving data usability during storage and transfer across different systems and networks [1].
- **Hashing in Mobile Apps.** Hashing is used extensively in mobile apps for tasks such as password storage, data integrity checks, and digital signatures. When companies store user data, they can apply hashing algorithms to ensure that the information stays private, even if they suffer a data breach. This technique ensures that data remains unchanged and can be verified for authenticity [4].

Brenda Sugey Vega Contreras
CSS545 Mobile Computing

Current Solutions in Instant Messaging and Communication Apps

WhatsApp, like many other apps used for communication services, mitigates the problem of secure communication and data transmission with end-to-end encryption. Some of the solutions to mitigate this problem are discussed below:

- **Encryption Techniques**

Encryption is an encoding technique that use an encryption algorithm to convert the data to be encrypted, also known as plaintext, into its encrypted representation, known as ciphertext using a secret key called a cipher [1], [4]. Plaintext data can be restored from ciphertext through decryption. Encryption is a two-way function, meaning that something that was encrypted can be later decrypted [5]. Encryption can be symmetric (using the same secret-key for encryption and decryption) or asymmetric (using a public and private key pair). In general, encryption operations do not protect integrity, but some symmetric encryption modes also feature that protection [6]. There's a third option known as hybrid encryption which combines symmetric and asymmetric keys, using the strengths of both and minimizing their weaknesses [4].

Some examples of encryption algorithms are AES Algorithm, RSA Algorithm, and The Diffie-Hellman Key Exchange [1], [4], where AES is the trusted standard algorithm used by the United States government, as well as other organizations [7].

WhatsApp provides end-to-end encryption for all personal messages that a user can send and receive. This makes sure that only the people in the conversation can read or listen to them [2], [8]. Sessions are established via asymmetric encryption with Curve25519 key pair generated at install time. Once a session is established, clients exchange messages that are protected with a Message Key using AES256 in CBC mode for symmetric encryption and HMAC-SHA256 for authentication [8]. WhatsApp employs the Signal Protocol, an advanced end-to-end encryption method, to secure messages [8]. This ensures that only the communicating users can read the messages, and even WhatsApp cannot access the content. In other words, its implementation relies on the idea that each message is encrypted with a unique key, and only the recipient has the key to decrypt it. The keys are generated and stored securely on users' devices.

- **Encoding Techniques**

In the encoding method, data is transformed from one form to another. Encoding transforms data into a form readable by systems or that can be used by any external processes. It can't be used for securing data, but it can be used for data transmission and storage efficiency [1]. Some examples of character encoding/decoding techniques are ASCII, BASE64, UNICODE.

Two of the popular encoding schemes to ensure data transmission through the network and are revisited below:

1. **Base64 Encoding:** This scheme can be used to encode binary data (such as images and videos) into ASCII text, ensuring safe transmission over text-based protocols. It is also used in simple HTTP authentication to encode the credentials [9]. Encoding is used before transmitting multimedia files in the mobile app, they are encoded in Base64, allowing them to be included in message bodies without corruption.

2. **Image, audio, and video encoding**. This type of encoding is performed to save storage space. A media file such as image, audio, and video are encoded to save them in a more efficient and compressed format, so that they can be saved within less space, can be transferred easily via mail, or can be downloaded on the system. For example, a .WAV audio file can be converted into .MP3 file to reduce the size by 1/10 of its original size [9].

- **Hashing Algorithms**

Hashing converts data of arbitrary size into a fixed-size hash using a hashing function, which can be any number generated from a string or text. Hashing is non-reversible and ensures data integrity. The hash table is used for storing data [1]. Some examples of hashing algorithms: MD5 and SHA256.

When pictures and text messages are sent over the network, images and text may be sent to different servers for efficiency purposes. So, to verify that the images have not been tampered with on the internet, a hashing algorithm like MD5 and SHA256 can be used. MD5 generates a 128-bit hash value, while SHA256 generates a 256-bit hash value. Hence, SHA256 is a relatively complex algorithm with better security than MD5 [10]. Another purpose for hashing is for verifying passwords for login on various websites [8].

Coming back to the WhatsApp example, these are some of the mechanisms that are used to ensure secure messaging:

1. **SHA256:** WhatsApp uses the SHA256 algorithm for various security functions, including generating message authentication codes (MACs) and ensuring data integrity [8].
2. **HMAC (Hash-based Message Authentication Code):** For additional security, WhatsApp uses HMAC along with SHA256 to authenticate messages and verify data integrity. The sender transmits a normal encrypted message to the recipient that contains the encryption key, the HMAC key, a SHA256 hash of the encrypted blob, and a pointer to the blob in the blob store. Once the message is stored, all receiving devices decrypt the message, retrieve the encrypted blob from the blob store, verify the SHA256 hash of it, verify the MAC, and decrypt the plaintext [8].

<u>Critical Analysis - Pros/Cons of current solutions</u>

- Symmetric encryption is better suited for processing large amounts of data, such as messages, because it is computationally less intensive. In contrast, asymmetric encryption, which uses a public and private key pair, is more secure but requires more computational power, making it better suited for smaller amounts of data.
- Encryption is used to protect the confidentiality of data, encoding is used to preserve data usability and presentation, and hashing is used to verify data integrity. Encoding is distinct from encryption and hashing as its main purpose is not to hide data but to ensure it is in a format suitable for use.
- Encryption and encoding can be reversed while hashing cannot be reversed.
- Encryption is the only technique among the three that is specifically intended to protect data during transit. Encoding and hashing do not provide security against unauthorized access during transmission. Hashing is usually used to ensure the integrity of data, primarily when large amounts of it are being stored [4].

Proposed solution

The techniques mentioned before for secure data transmission are concerned with cryptography, which uses encryption to make the message unreadable. An area that would be interesting to explore to find new solutions is steganography, which hides communication traces [11]. Steganography differs from cryptography because the sensitive information is concealed in such a way that this obscures the fact that something has been hidden. For instance, one could hide a Shakespeare poem inside an AI-generated image of a cat [12]. In the context of mobile communication apps, combining steganography techniques with existing encryption methods could provide an additional layer of security by making the existence of the message itself undetectable, providing additional benefits for data compression and storage [12].

Conclusion

To conclude, encryption, encoding, and hashing are crucial for securing mobile communication apps like WhatsApp. By examining current solutions and their applications, it is evident that while these techniques provide robust security, there is always room for improvement. Incorporating advanced techniques like steganography could further enhance the security of mobile communications. Steganography adds an additional layer of security by concealing the existence of the message itself, making it harder for unauthorized parties to detect, intercept and tamper communication. This approach could address current limitations ensuring that user data remains secure in an increasingly interconnected world.

References

[1] “Encryption vs Encoding vs Hashing,” GeeksforGeeks. Accessed: May 18, 2024. [Online]. Available: https://www.geeksforgeeks.org/encryption-encoding-hashing/
[2] “WhatsApp,” *Wikipedia*. May 13, 2024. Accessed: May 19, 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=WhatsApp&oldid=1223569652
[3] “Electronic Communications Privacy Act of 1986 (ECPA) | Bureau of Justice Assistance.” Accessed: May 19, 2024. [Online]. Available: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285
[4] “Hashing vs. Encryption: What is the difference? | NordVPN.” Accessed: May 19, 2024. [Online]. Available: https://nordvpn.com/blog/hashing-vs-encryption/
[5] P. Nohe, “The difference between Encryption, Hashing and Salting,” Hashed Out by The SSL Store™. Accessed: May 19, 2024. [Online]. Available: https://www.thesslstore.com/blog/difference-encryption-hashing-salting/
[6] “Cryptography in Mobile Apps | OWASP MASTG.” Accessed: May 19, 2024. [Online]. Available: https://mobile-security.gitbook.io/mobile-security-testing-guide/general-mobile-app-testing-guide/0x04g-testing-cryptography
[7] “What Is Data Encryption: Algorithms, Methods and Techniques,” Simplilearn.com. Accessed: May 19, 2024. [Online]. Available: https://www.simplilearn.com/data-encryption-methods-article
[8] “About end-to-end encrypted backup | WhatsApp Help Center.” Accessed: May 19, 2024. [Online]. Available: https://faq.whatsapp.com/490592613091019
[9] “Types of Encoding Techniques - Javatpoint,” www.javatpoint.com. Accessed: May 19, 2024. [Online]. Available: https://www.javatpoint.com/types-of-encoding-techniques

[10] "What Is the Best Hashing Algorithm?," Code Signing Store. Accessed: May 19, 2024. [Online]. Available: https://codesigningstore.com/what-is-the-best-hashing-algorithm

[11] "Difference between Steganography and Cryptography," GeeksforGeeks. Accessed: May 19, 2024. [Online]. Available: https://www.geeksforgeeks.org/difference-between-steganography-and-cryptography/

[12] "New breakthrough enables perfectly secure digital communications," ScienceDaily. Accessed: May 19, 2024. [Online]. Available: https://www.sciencedaily.com/releases/2023/03/230307073224.htm