Technical Review of End-to-End Encryption in Mobile Social Networks

Arturas Bulavko | 05/01/2018
MSc Software Engineering
Faculty of Science, Engineering and Computing, Kingston University
Kingston upon Thames, UK
arturasbulavko@gmail.com

***Abstract*—Mobile social networking is an evolving digital field, allowing peers to socialize and interact freely around the world. Users can create accounts to share textual and visual content with friends and people that have the same interest. The data published online lacks privacy, resulting in various security threats to the users who actively post confidential information. Individuals frequently share data without considering privacy and security aspects, becoming victims of attacks. This paper reviews security threats of mobile social networking and inspects critical user data asset to understand how E2EE is applied to keep the data secure and private in the mobile social networking domain.**

Keywords—mobile social network; security and privacy; mobile risks and threats; cyber security; cryptography; E2EE;

I. INTRODUCTION

Mobile social networking (MSN) is exponentially growing each year. Presently, 2.46 billion people globally use at least one social networking platform [1]. This number is expected to increase continuously because new people are creating accounts daily to stay connected with their colleagues. MSN is actively used to form virtual connections in order to share textual and visual content among peers with similar interests and backgrounds, regardless of their geographical location. Additionally, MSN allows communicating with real life friends to share confidential information. This data is collected and stored on the MSN service provider's servers, which is automatically processed to provide analytics, used to track customers and generate user-centric suggestions.

Numerous social networking platforms have emerged over the years, namely; Facebook, Twitter, LinkedIn, Google+ and WhatsApp. The MSNs are thematically split to accommodate the user needs, which include lifestyle, dating, entertainment, education and business. Each theme is aimed at different user groups and communities, for example; business-oriented MSNs are targeted towards professionals, whereas education-oriented platforms are widely used by students and teachers for the learning purposes. However, lifestyle and entertainment fields are accessed by various people with different interests. As a result of this, MSNs are treated differently in order to provide a better user experience (UX) while neglecting the security and privacy aspects.

In the current market, each MSN service provider aims to increase their market share by frequently offering new functionality and features to their users. This negatively affects the confidentiality of the user's data as new loopholes are introduced into the system, used by the attackers to gain access to the data. People are willing to exchange their personal information for a new social networking feature which enables them to loom from the crowd [2]. A recent Animoji addition by Apple is an example of consumers allowing a system to scan their face by collecting biometric data to create a new type of a graphical symbol which can be used to communicate with peers. The customers are freely using this feature with an assumption that their data is secure and private, without examining this. By publicly storing vast amounts of personal information which is constantly kept updated, the MSNs are becoming a target for attackers to gain access to the sensitive data.

The publicly available information can be used to recover accounts on the other systems, identity theft or gaining access to further sensitive information. An example of this are account security questions. Commonly, users set memorable answers which can be found by looking at the images or posts made by the owner. Once the attacker correctly enters all information, they gain full control of the MSN profile. Such security breaches lead to embarrassment, reputation damage, broken relationships and loss of life in severe cases [3]. There are several preventative measures developed by MSN service providers to aid their customers in keeping their data secure and private.

This paper will review several mobile social networking threats and examine how they are prevented by adapting End-to-End Encryption (E2EE) cryptographic security technique. A WhatsApp case study will be used to illustrate the application of E2EE in the MSN domain.

II. MSN SECURITY CHALLENGES

This section will focus on examining a number of threats which currently exist in MSNs.

In 2016, it was estimated that every minute, 29 million messages are sent through WhatsApp, 3.3 million Facebook posts are published and almost 449 thousand tweets appear online [4]. This creates a pool of data which an attacker can access and use against the user. The data stored on social networks is never secure and private, implying that in a matter of time, an attacker can easily gain access. Because of this, it is vital to understand what types of threats are frequently used to gain access to private data in MSNs. An entree to confidential data can occur due to breaches from service providers, other

users and the third-party applications [5]. These breeches will be reviewed next.

The service providers are able to process, analyse and share data stored on their servers in order to gain personal benefit, given that the user provides formal consent. Frequently, personal data is used to personalise content and is shared with research bodies to perform statistical analysis. Similarly, the service providers can collect and store confidential information insecurely, despite stringent regulations. Most MSNs allow personal information access to friends, which is widely exploited by the attackers. By sending friend requests to the victims and upon acceptance, the attackers gain access to the confidential information. The MSN service providers constantly expand their services to offer new functionality, and frequently this is done by third-party developers, who may deploy malicious code. This will enable them to access the system by bypassing security mechanisms that authenticate each user.

Another fundamental security breach is performed by the users themselves, leading to problems with data integrity. People tend to use insecure internet connections to access their accounts or login via public devices, such as tablets, phones or PCs used as displays in the shops. The service consumers generally agree with most consents relating to the data collection, tracking and sharing, just to access their account quicker. In the urge to view the shared content, users click phishing links within the MSN application which lead to fake websites.

The primary goal of computer security is to ensure Confidentiality, Integrity and Availability of the system, commonly known as CIA model. It is built upon three requirements which must be implemented to guarantee a secure system deployment. A security assessment approach is often used to analyse the threats and vulnerabilities of a critical asset. A match between the two enables to study the controls developed to mitigate the threat. A selection of the main MSN threats [6] [7] will now be analysed.

A. Lost or Stolen Mobile Device

In 2016, almost half a million people had their mobile device stolen [18]. By having access to the device, an attacker or an unauthorised person can bypass the device's locking mechanism in order to view, modify or steal user's data asset. This data can be used to gain access to further confidential information, disclosed to third-parties, identity theft and destruction of data. The risk of data loss and disclosure is due to numerous vulnerabilities. 32% of smartphone owners do not secure their mobile phones [18], resulting in absence of biometric and PIN lock screens. Additionally, users do not log-out from MSNs after use, which improves the user experience (UX) and declines the security. As such, by gaining access to an unprotected device, an intruder can access a vast amount of confidential data.

B. Phishing Links as Part of Social Engineering Attack

Phishing links direct the user to a fake website which is cloned prior to the attack. The user is asked to enter confidential information which an attacker requires. This threat is usually achieved by posting a link to an external resource by an attacker within the social network application. As a result of this, an intruder captures the necessary information for identity theft, data disclosure and credit card fraud. The most frequent vulnerability is the user clicking suspicious links, without being aware who it originates from. Furthermore, mobile devices are lacking in antivirus software to scan the links, similarly to the PC version. Such weaknesses lead to risks of identity theft and leakage of confidential information.

C. Identity Theft

By sharing enough personal information online, an attacker can build a profile of the victim, allowing them to bypass various security mechanisms. For example; the birth date can be used as a PIN on the mobile device. By collecting enough information, the intruder can create new social network accounts to target victim's friends, produce fake passports and obtain credit-loans from the bank. This is mainly due to users ignoring the privacy and security settings within the MSNs, making them publicly share personal data by default.

D. Location Leakage

Since most social networking platforms are accessible via a mobile device, users incline to share their geolocation publicly. Generally, people post images with the geolocation enabled to share their holiday destination with peers. Similarly, MSN customers sign-up to various future events which include the location of the event. In critical situations, an attacker will visit such an event to steal the user's mobile device.

Android currently owns the largest market share in the Europe, at 68.9% [8]. Smart Lock was introduced by the Android OS to disable lock screen when the user is in a secure location. This is achieved via geolocations whereby the user selects a location where the device will not prompt for a password to unlock it. This is a major security threat because an attacker can easily get the typical location of the victim via MSN and by traveling to that location, unlock the device, gaining access to all data stored on the mobile equipment.

E. Insecure Data Transfer Protocols

Typically, MSNs operate in a client-server architecture where the client is a mobile device and the server is the MSN service provider. As a result of this, a secure communication channel between the two must be established, allowing data exchange. The man-in-the-middle attacks are very common in this scenario, because the data which is transferred insecurely can be easily red by an intruder using specialised software. An attacker can deliberately monitor the connection in order to view and steal private information. Such a threat is generally possible due to weak encryption, lack of encryption or easily accessible keys.

Fundamentally, all threats in MSNs lead to data tampering, making it a critical asset in the MSN domain. The access to data by an attacker breaches Confidentiality, modification of data breaches Integrity and destruction of data breaches Availability within the CIA model. This prevents systems from being treated as secure and thus not very popular among the mobile user base. It is therefore important to understand what security mechanisms are used in the industry to combat these threats. The next chapter reviews how the asset securely communicates between the clients via the server using a cryptographic technique.

III. MSN SECURITY SOLUTIONS

Most MSN threats result in data loss, disclosure and leakage. Consequently, a strong security mechanism must be applied to prevent such risks. This section will review end-to-end encryption (E2EE) implemented in MSNs.

Most MSN service providers do not own private data centers and therefore rely on third-parties to store their customers' data [9]. Subsequently, it is vital to hide the information from a range of parties that have access to it. The commonly used practice in the MSNs is E2EE. It is a type of cryptographic technique used to convert plaintext into ciphertext. The ciphertext is the outcome of an encryption algorithm application on a plaintext, converting the data into a string of characters. Such encryption cannot be understood by humans and machines without decrypting it, providing the highest level of data protection.

There are two types of encryption; symmetric and asymmetric [10]. Symmetric encryption uses the same keys to encrypt the plaintext and decrypt the ciphertext which is not very secure. Asymmetric on the other hand, uses different keys which are public and private in order to perform encryption and decryption. Asymmetric encryption performs two functions. It authenticates both parties in a communication channel and encrypts the data, preventing parties without a decryption key from understanding the confidential data.

The primary advantage of E2EE is that only the sender and the receiver are able to decrypt the message, preventing third-parties from accessing the confidential information during the transfer. Figure 1 shows an example of E2EE in a client-server architectural style, widely adopted by MSNs.

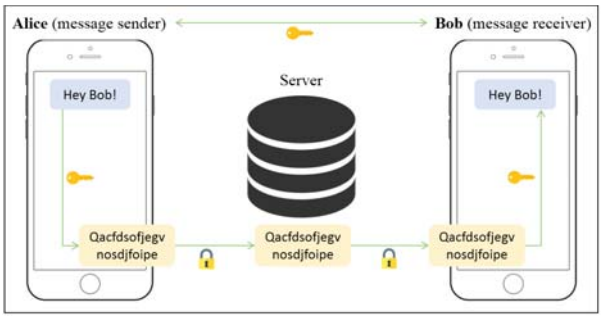

Figure 1. End-to-end encryption example.

During a communication, Alice and Bob both have public and private components of the encryption key. They share the public key components and use the private key in secret to create a shared key that nobody else is able to know. During the first connection, Diffie-Hellman key exchange protocol may be used to securely exchange keys in an asymmetric encryption scheme [11]. It allows the establishment of a secure communication channel via an insecure connection.

The message is encrypted on the sender's device (Alice), which is then transferred to a server and stored in the database encrypted. Since the server is not involved in the key exchange, it therefore can't decrypt the message, ensuring third-parties hosting the MSN data have no access to the confidential information. The message is then routed to the receiver (Bob), who uses the key to decrypt the ciphertext, allowing him to read the message from Alice.

A number of MSNs adopt digital oblivion security measure in which the data expiration time is established [9]. After a specific period, the data is automatically deleted from the server, leaving no traces. Essentially, such strategy accomplishes two conditions. The data is publicly available for a short period of time, preventing several data threats. Additionally, the storage requirements of the data servers can always remain minimal to accommodate the communication. As a result, the MSN vendors are likely to establish private data centres, as oppose to storing the data on the third-party storage services. Digital oblivion is disadvantageous in MSNs where the users are interested to view the communication history.

E2EE has a number of drawbacks which must be considered when using this cryptography method. An attacker is able to gain access into the user's device, which is a particular danger in routed and jailbroken machines. By having access to the device, an attacker can obtain the key which is used to encrypt and decrypt the data. It is therefore critical to store the key securely on the device. Additionally, when an encrypted data is stored on the server, a corrupt employee can make changes to the string, preventing both parties from decrypting the message correctly. For example; if a single character is changed in an encrypted string, the decrypted message will not make sense.

If the device used for MSN communication is not protected itself, an attacker can simply steal the phone using location leakage threat and gain access to the confidential information. Fundamentally, each mobile device allows the user to set secure lock screen, preventing unauthorised access. This is mainly achieved by asking the user to unlock the device using either face ID, touch ID, PIN or a pattern lock. However, face ID, touch ID and pattern lock can be bypassed using a numeric PIN or an alphanumeric code. Frequently, the user selects a number pattern or date of birth as the numeric PIN [12]. Similarly, the alphanumeric code is typically a memorable phrase or word, which can be obtained from an insecure MSN profile or via a brute-force attack to discover the code.

IV. CASE STUDY

One of the most popular MSN service providers who adopts client-server architecture E2EE is WhatsApp. This section will focus on examining WhatsApp MSN. Arguably, the success of this application is due to 'security by default' approach. The users benefit from E2EE in chats, group chats, images, videos, voice messages and file exchanges [16]. Each user is linked to a profile via their unique phone number. General user information, such as; name, phone number, status line and avatar are securely stored on a central server, automatically accessible by other users wishing to establish a communication. WhatsApp also stores public keys associated with the user's identifier in their database, though, at no time WhatsApp is able to fetch the private key, stored on the user's device [16].

To start a communication between the users, an encrypted session is setup which generates a shared key automatically. Each transmitted message is encrypted using 80-byte AES-256 CBC mode and authenticated using HMAC-SHA256 [16]. The encryption key changes after each message, preventing an attacker gaining access to a sole key and decrypting a lengthy conversation. All users are able to verify the keys with people

they are communicating to confirm the identity via scanning a unique QR code or comparing 60-digit number. This eliminates man-in-the-middle attacks by an unauthorised third-parties.

WhatsApp adopts a novel security mechanism, preventing the attackers from seeing the user's history by obtaining a currently used key [16]. Essentially, a new key is generated after a certain period of time. As a result of this, by obtaining the current key, an attacker is unable to decrypt the older messages of the user. However, the communication backups generated by WhatsApp use AES 192 algorithm which can be easily decrypted using a publicly available key applicable to all devices [17]. This is a major security problem as backups contain critical assets and are not thoroughly protected.

WhatsApp is not only available for mobile devices, but is also accessible via the web. Instead of making the user register using an email and password, a QR code is used [10]. During the first use of WhatsApp, a user is asked to verify their mobile number to certify user's identity. As a result, the user can use their smartphone to generate a unique to them QR code, permitting access to WhatsApp web, allowing them to connect freely via E2EE over the web. By using the smartphone as a key, a QR code is used to authenticate and verify the existing user. Such a strategy prevents attackers from accessing the user's web account in order to view the confidential data.

V. CONCLUSION

This paper has reviewed several security threats in the MSN domain. It also critically analysed the implemented E2EE security technique to avoid them. Such security mechanism is widely used to prevent a range of threats used to gain access to user data asset. It ensures that only the authorised parties are able to read the confidential information.

However, the major disadvantage of E2EE comes from a social and ethical point of view, because it serves as a secure communication channel for the criminals. They frequently use MSNs with E2EE to organise and perform terror attacks [13]. While the law enforcement may be granted access to the servers used to store the confidential data, they are unable decrypt it. It is reported that MSN mobile applications were used to plan Paris attacks in 2015 [14] which has killed 130 people, leaving 100 in critical conditions [15]. The criminals were able to facilitate a secure communication using E2EE to organise an attack.

The law enforcements are unable to capture the keys used to encrypt and decrypt data, making it impossible to prevent such attacks. The only feasible mitigation strategy is generating and giving a master key to the high-rank officials, allowing them to decrypt all data stored on the servers. However, this would destroy the privacy and security advantages of E2EE [13]. Because either a corrupt employee can make the master key publicly available or the key can be captured by the intruders by performing a number of attacks. Similarly, this process must be done manually, and the only way to prevent crimes is to adopt an automated system to check for suspicious content in advance.

In future work, it would be advantageous to evaluate peer-to-peer (P2P) MSN communications for comparison purposes. It would be beneficial to examine which paradigm introduces more security and privacy for the users.

REFERENCES

[1] Statista. Number of social media users worldwide from 2010 to 2021 (in billions). [Internet]. 2017 [cited 2017 December 18]; [1 page]. Available from: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

[2] Barnes S.B. A privacy paradox: Social networking in the United States. First Monday 2006 September 4; 11(9).

[3] Clarke C, Pfluegel E, Tsaptsinos D. Confidential Communication Techniques for Virtual Private Networks. 12th International Symposium on Distributed Computing and Applications to Business, Engineering & Science 2013 September; vol.2013: 212-216.

[4] Allen R. What happens online in 60 seconds?. Smart Insights. [Internet] 2017 February 6 [cited 2017 December 18]; [1 page]. Available from: https://www.smartinsights.com/internet-marketing-statistics/happens-online-60-seconds.

[5] Hongyu G, Jun H, Tuo H, Jingnan W, Yan C. Security Issues on Online Social Networks. IEEE Internet Computing 2011 July-August; 15(4): 56-63.

[6] Sadeghian A, Zamani M, Shanmugam B. Security Threats in Online Social Networks. 2013 International Conference on Informatics and Creative Multimedia 2013 September; vol.2013: 254-258.

[7] Fire M, Goldschmidt R, Elovici Y. Online Social Networks: Threats and Solutions 2014; 16(4): 2019-2036.

[8] Statcounter. Mobile Operating System Market Share Europe. [Internet]. 2017 [cited 2017 December 18]; [1 page]. Available from: http://gs.statcounter.com/os-market-share/mobile/europe.

[9] Rathore S, Sharma P.K, Loia V, Jeong Y, Park J.H. Social network security: Issues, challenges, threats and solutions. Information Sciences 2017 December; vol.421: 43-69.

[10] Neha S, Surendra Y, Brahmdutt B. A review of Data Encryption Techniques Userd for Social Media on Internet. International Journal of Advanced Computational Engineering and Networking 2016 September; 4(9): 64-68.

[11] Rittinghouse J, Hancock W.M. Cybersecurity Operations Handbook: The Difinitive Reference on Operational Cybersecurity. Elseview Science; 2003.

[12] Pinola M. The Most (and Least) Common PIN Numbers and Numeric Passwords. Is Yours One of Them?. LifeHacker. [Internet]. 2012 [cited 2017 December 18]; [1 page]. Available from: https://lifehacker.com/5944567/the-most-and-least-common-pin-numbers-and-numeric-passwords-is-yours-one-of-them.

[13] Titcomb J. What is encryption, how does it work and what apps use it?. The Telegraph [Internet]. 2017 March 29 [cited 2017 December 18]: Technology. Available from: http://www.telegraph.co.uk/technology/0/encryption-should-using/.

[14] McDonough M. Emerging Threats: End-to-End Encryption (E2EE). Law Enforcement Cyber Center. [Internet]. 2016 April 25 [cited 2017 December 18]; [1 page]. Available from: http://www.iacpcybercenter.org/emerging-threats-end-to-end-encryption-e2ee/.

[15] BBC News. Paris Attacks: What happened on the night. BBC News [Internet]. 2015 December 9 [cited 2017 December 18]: Europe [1 page]. Available from: http://www.bbc.co.uk/news/world-europe-34818994.

[16] WhatsApp. WhatsApp Security. [Internet]. 2017 July 6 [cited 2017 December 18]; [10 PDF pages]. Available from: https://www.whatsapp.com/security/.

[17] Cosmino A. Forensic Anslysis of WhatsApp Messenger on Android Smartphones. Digital Investigation 2014 Sptember; 11(3): 201-213.

[18] Pham M. Nearly half a million Brits had phones stolen last year. Mobile News [Internet]. 2017 March 13 [cited 2017 December 18]: News [1 page]. Available from: http://www.mobilenewscwp.co.uk/2017/03/13/nearly-half-million-brits-phones-stolen-last-year/