Using a whatsapp vulnerability for profiling individuals

Sebastian Kurowski

Competence team identity management
Fraunhofer institute for industrial engineering IAO
Nobelstr. 12
70569 Stuttgart
sebastian.kurowski@iao.fraunhofer.de

Abstract: This paper aims at raising awareness on the issue of using unfixed vulnerabilities for targeted attacks in order to harness private or even corporate information. We demonstrate an attack by using a well-known, yet not fixed whatsapp vulnerability, enabling us to eavesdrop the cell-phone number of a victim. We identified the concrete states, in which whatsapp leaks the cell-phone number of a victim. By using a volunteering individual, we demonstrate the feasibility of profiling the individual and provide further steps on how to disclose private and corporate information by using the leaked cell-phone number and the profiled information to introduce the adversary into a trust relationship with the victim. Once the victim trusts the adversary, social phishing can be used to retrieve further private or even corporate information.

1 Introduction

The Whatsapp Instant Messenger App[Wh14] has so far provided a working and usable alternative to the short messaging service (SMS). Whatsapp uses the internet connection of a smartphone to deliver short messages free of charge. Due to this advantage, Whatsapp was able to emerge as the most popular instant messaging application for smartphones, and currently delivers 500 million customers[Ec14]. However, this application was in the past not very successful in providing sufficient security and privacy features. Up to 2011, text messages, and cell phone numbers were transmitted unencrypted, despite of the App using the SSL protocol, which could have been used to encrypt the data [Yo11]. Additionally, various attacks were possible on both user authentication, and user data [SFK12]. In a reaction to this finding, Whatsapp implemented encryption of the transmitted data, between the Whatsapp client and the servers, however the cell phone number of the Whatsapp user was still transmitted as plaintext [He12]. In this paper, we describe a way of profiling an individual, taking advantage of the cell phone number being transmitted as plain text.

2 Retrieving the cell phone number

The attack described in this paper, uses a known vulnerability in the Whatsapp messenger. The current implementation of Whatsapp leaks the cell phone number [He12], which can easily be read by using a TCP sniffer, such as Wireshark or TCPDump.

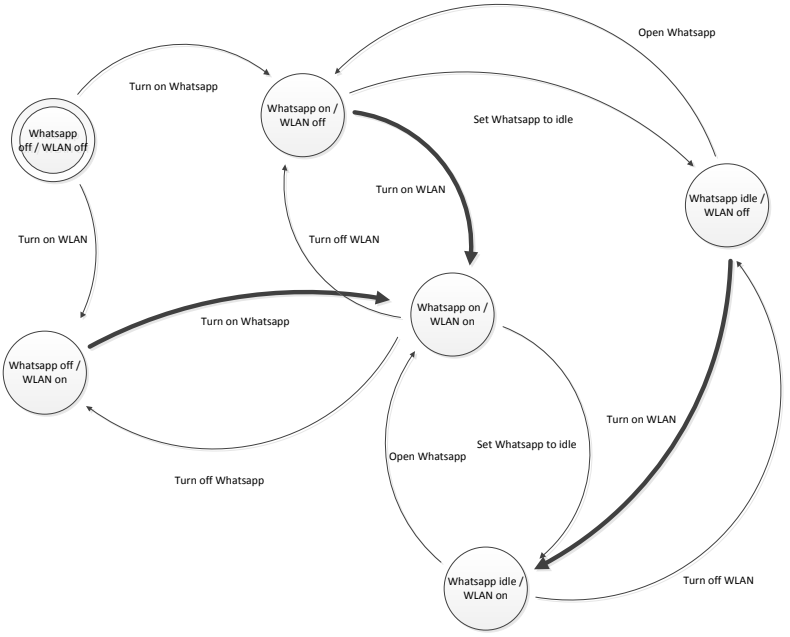

Figure 1 State diagram of the vulnerability analysis. Circles refer to tested WLAN adapter and Whatsapp states, lines depict a state transition (e.g. by opening Whatsapp). The bold lines indicate where the cell phone number is being leaked.

While the vulnerability of the leaked cell-phone number was already reported on, sufficient detail on when exactly this information is transmitted unencrypted was entirely missing. Therefore we conducted an analysis, showing the states in which the Whatsapp messenger leaks the cell-phone number, in order to evaluate the feasibility of retrieving this critical part of information. The test setup included both an iOS Version of Whatsapp (iOS 7.1), and the android version (Android 2.11). The Whatsapp version was 2.8.11. In the testing environment, a laptop equipped with Wireshark was used, to analyze the resulting traffic. All devices were connected with the same wireless LAN access point.

Using this setup, three different states of the Whatsapp app (on, idle, off), and two states for the WLAN adapter of the mobile devices (on, off) were used. The states for the

Whatsapp messenger app, referred to the app running and currently being opened by the user (on), the app running in background (idle), and the app not running at all (off), while on and off as states for the WLAN adapter, refer to the WLAN adapter of the mobile devices being turned on and off. Tested combinations of these states are shown in Figure 1. During the analysis the state transitions, which are depicted as lines in the diagram, were tested, e.g. the app was turned on and the resulting traffic was analyzed. This test was conducted with all possible states, allowing the exact identification of the states, in which the cell phone numbers are being leaked. These state transitions are marked bold in the diagram. The analysis showed, that the cell phone number was not leaked with every Whatsapp message, but only when (1) Whatsapp was being turned on, or (2) the wireless adapter was being turned on. This yields some restrictions for the described attack, meaning that the cell phone number can only be retrieved, when the app of the victim is not running, or the victim should not be connected to our used WLAN, before we start the TCP sniffing. Yet, the impact of this restriction remains questionable, as e.g. WPA2 secured WLANs require any TCP sniffer to obtain the handshake of targeted devices, before the attacker is able to decrypt the captured traffic. This means, that in WPA2 secured WLANs, the attacker must be sniffing before the victim connects to the same access point anyway.Knowing, when exactly to look for the cell phone number, we are now able to use a TCP sniffer, to obtain this attribute of the victim. In order to identify the cell phone number, we used tcpdump and regular expressions, to search for numbers. Hereby tcpdump runs on a laptop, dumping the captured traffic of the WLAN into a file. This file is then being analyzed by using a short and simple python script, which is searching the TCP dump for german cell phone numbers, using a regular expression.

By using this combination, it was conveniently possible to passively dump the traffic, while analyzing and finding the cell phone numbers, after collection. Therefore, an attacker is able to remain covered, e.g. by hiding the laptop with the TCP sniffer in a bag. The identified cell phone numbers were then parsed into a separate file, allowing easy access.

3 Using the cell-phone number for a targeted attack

Knowing how and when to retrieve a cell phone number from a potential victim, we are now able to use this knowledge for obtaining further attributes. The following describes an attack, which uses feasible and manual profiling, and the cell-phone number in order to establish a trust relationship between the adversary and the victim, and to retrieve private or corporate information by social phishing [QUOTE]. We conducted a small demonstration using a volunteering individual, showing the simplicity of the required profiling.

As we already described the concrete setup required for obtaining the cell phone number in Section 2, we will only briefly discuss this scenario. In this case, the adversary aims at being connected to the same W-LAN, as the victim. Identifying the victim could either be untargeted, or targeted. For instance, an adversary could connect to a W-LAN in a bar, obtaining cell-phone numbers and using the information provided via Whatsapp to

pick a random victim. However, the adversary could also identify possible persons-of-interest, e.g. by observating persons leaving a corporation in the evening and trying to follow them to a bar. In the latter case, the adversary would just simply wait in the same W-LAN for the victim to enter and use its smartphone. As soon as the victim opens the Whatsapp messenger in the W-LAN the adversary is able to retrieve the cell-phone number of the victim as described in Section 2. However, the cell-phone number is a relatively weak attribute. While we could, e.g. subscribe the victim to certain services, we are probably not able to retrieve any further information about the victim, and thus not able to phish for private or corporate information. Luckily for us, Whatsapp users usually use a pseudonym along with a profile picture in their Whatsapp profile (see Figure 2).

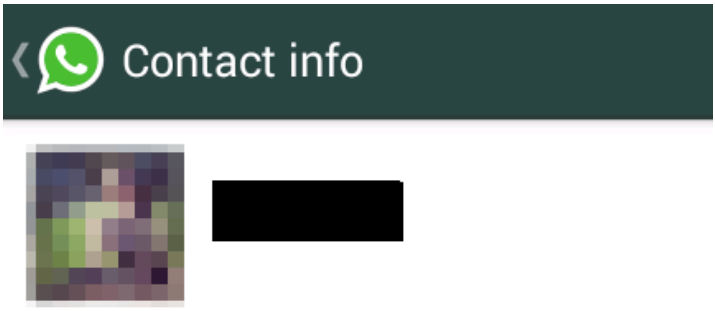

Figure 2 Whatsapp profile of a victim.The name was blanked out, as the screenshot was made after the profiling was finished, and the contact could be included with the real name of the victim

These initial attributes can already provide sufficient information to kick-off a profiling of the individual. However, Whatsapp allows users to adjust their privacy settings, e.g. only individuals in the victims contact list are able to see the pseudonym or the profile picture. Yet, as the privacy settings are only retrievable by choosing “Settings”, “Account”, and then “Privacy” and thus relatively hidden, we are quite optimistic that this retrieval maybe promising. Additionally, recent events, such as the reset of the privacy settings due to software updates in Whatsapp to default settings, and thus full disclosure of some attributes [Sü14], allows for further optimism on this issue. As we want to obtain further attributes of the victim, in order to be able to access, e.g. facebook/linkedin/xing profiles, our primary interest is in obtaining the victims name. We used Google image search on the profile picture of the victim. By doing so, we were able to identify a second hand clothing platform, holding a pseudonymized profile of the victim.

By using this profile we were able to identify the city, the victim is living in. Additionally, our victim provided information on the current job position, which enabled us to use this attribute for further information gathering. Using google search with the pseudonym of the victim and the gathered attributes, however did not provide any results, as the victim did not seem to have reused the pseudonym. The clothing platform provided a follower list, showing a total of 20 followers on this particular accoiunt. Out of these 20 followers, only 2 were in the same city as the victim. Additionally we could

identify one of those 2 followers (from hereon refered as friend A) as having the same affiliation as the victim. The profile page of friend A provided us with a picture. As with our initial picture search, we were able to obtain instagram pages related to friend A. However, the privacy settings of friend A, prevented us from viewing the profile directly. Yet, a friend of friend A, from hereon refered to as friend C, used less restrictive privacy settings, enabling us to retrieve an additional pseudonym of friend A. By searching for this pseudoynm, we discovered, that friend A reused this value on a facebook page, enabling us to find a past event, where friend A had participated, by using google on the pseudonym. Having obtained the facebook profile of friend A, which again prevented us from viewing any friends or any contents, due to privacy settings, we were still able to retrieve the groups, to which friend A had subscribed. By searching the publicly available member lists of these open groups, we finally discovered our victim and were able to obtain the full name.

As an attacker, we are now in posession of the victims name, cell phone number, pictures, affiliation, and we know with which persons our victim is befriended or otherwise associated. As our demonstration showed, it was relatively simple to retrieve the cell-phone number, the name of the victim, affiliation, pictures and friends of the victim. These attributes were collected in a relatively short timeframe: In the experiment we required approximately 10 mins, even though the victim had high privacy standards associated with their facebook profile. In the context of social phishing [JJJ07] we could already possess enough knowledge of the victim to obtain private or corporate information. The adversary could now contact the victim and provide a fake identity, e.g. the identity of one of the friends. This introduces the adversary directly into a trust relationship with the victim. As the adversary possesses a trusted attribute of the victim (the cell-phone number), providing a fake identity would result in more credibility of the attacker.

A possible conversation could thus look like this:

> Adversary: "*Hi this is Maria, I have a new cell-phone number but I am still using the old one from time to time.*"

Hereby "Maria" could stand for a friends name, which the attacker could easily obtain via facebook in our previous experiment. Now, let's assume the adversary wanted to obtain private information. In this case it would be feasible for the adversary to fake the identity of e.g. a family member in the same manner. In the case of targeting corporate information, the adversary would fake the identity of a working colleague, or associate of the same organisation. As soon as this message is sent, it is quite likely that the victim associates the adversary with the fake identity, and thus inserts the adversary into a trust relationship.

Finally, in the case of corporate information, this leads the adversary to sending a message to the victim containing a request, such as:

> Adversary: "*Hi, could you send me the last state of your CAD drawings? We require some information in there… Also I somehow cannot access my mails, so could you send it to my private one? adversary@SomeMailProvider.com*"

Et voila. We now have obtained corporate information, by using 10 minutes of manual profiling and retrieving the cell-phone number of a victim. Interestingly, in this attack the cell-phone number is not a strong attribute, as it cannot be used for profiling. However, possessing the cell-phone number allows the adversary to enter a trust relationship with the victim, while remaining anonymous. This offers the opportunity to either stalk the victim and exploit or retrieve private information [My05], or to phish for corporate information. The latter is based on social phishing [JJJ07], [KHH13], which exploits the trust relationship of a victim in order to retrieve information. Hereby this technique can exploit available information, in order to retrieve information, while contacting the victim via trusted channels. Experiments show, that this form of phishing is relatively promising, leading to success rates as high as 76% [JJJ07].

5 Conclusion

This paper describes an attack, by exploiting a Whatsapp vulnerability, basic Google searches and a small amount of time in order to retrieve private or even corporate information. We showed how to conretely retrieve a cell-phone number and discussed the severity of the adversary possessing an individuals cell-phone number, as being able to integrate itself into an anonymous trust relationship with the victim. We suggested social-phishing to retrieve corporate information, which proved to be quite effective in past resarch [JJJ07]. Other attacks would of course still be possible, once the adversary received details about the victim and its' cell-phone number, e.g. by using the knowledge for a pretexting attack in order to obtain access to a system [Ne08].

An interesting finding throughout the demonstration showed to be the low effort required to profile an individual even with high privacy standards associated with the individuals account. Due to not adjusted privacy settings in Whatsapp, we were able to obtain a picture, and thus collect information of the individual. While the full name of the victim could not be initially retrieved, due to privacy settings, and while privacy settings of befriended accounts of the victim prohibited us from accessing the profiles, a lack of privacy settings at the friends, of the individuals friends enabled us to retrieve enough information to finally obtain the full name. Having access to information rich profiles, such as facebook, could now enable us to extend our attack, and e.g. actively stalk the individual.

Whereas this is mainly a privacy issue, in combination with social phishing for corporate information, the privacy issues of the individual in a private setting, suddenly emerge towards security issues for a corporation.

Another interesting aspect which arised throughout the demonstration lies in the applicability of the retreived attributes in Whatsapp. The google image search, merely produced usable results and completely failed in providing similar images of the individual, except for large amounts of false-positives. Yet, the reuse of the Whatsapp profile picture, led us directly to an associated account which we could easily use for profiling the individual.

Therefore, this contribution raises awareness on the issues of privacy and security and their alignment with regard to corporate information. Whereas the privacy issues may create a risk for the well-being of the individual in this setting [My05], they can also create security issues and the disclosure of sensitive corporate information in combination with social-phishing [JJJ07], [KHH13].

References

[Wh14] WhatsApp Inc, „Whatsapp“, 2014. [Online]. Verfügbar unter: http://www.whatsapp.com.

[Ec14] M. Eckstein, „Whatsapp knackt halbe milliarde“, *connect*, Apr-2014. [Online]. Verfügbar unter: http://www.connect.de/news/whatsapp-nutzerzahlen-rekord-halbe-milliarde-wachstum-2246210.html.

[Yo11] YourDailyMac, „WhatsApp leaks usernames, telephone numbers and messages“, *YourDailyMac*, Mai-2011. .

[SFK12] S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, und E. Weippl, „Guess who’s texting you? evaluating the security of smartphone messaging applications“, in *Proceedings of the 19th annual symposium on network and distributed system security*, 2012.

[He12] heise, „WhatsApp versendet keinen Klartext mehr“, *Heise Security*, Aug-2012. [Online]. Verfügbar unter: http://www.heise.de/newsticker/meldung/WhatsApp-versendet-keinen-Klartext-mehr-1673054.html.

[Sü14] Süddeutsche.de, „Whatsapp-Nutzer plötzlich wieder gläsern“, *Süddeutsche.de*, Sep-2014. [Online]. Verfügbar unter: http://www.sueddeutsche.de/digital/beschwerde-von-nutzern-whatsapp-aendert-online-status-nach-update-automatisch-1.2124693.

[JJJ07] T. N. Jagatic, N. A. Johnson, M. Jakobsson, und F. Menczer, „Social phishing“, *Commun. ACM*, Bd. 50, Nr. 10, S. 94–100, 2007.

[My05] M. Secret Mysterypants, „Stalking for beginners“, *VICE*, Nov-2005. [Online]. Verfügbar unter: http://www.vice.com/read/stalking-v12n10.

[KHH13] K. Krombholz, H. Hobel, M. Huber, und E. Weippl, „Social engineering attacks on the knowledge worker“, in *Proceedings of the 6th International Conference on Security of Information and Networks*, 2013.

[Ne08] J. P. Nehf, „Pretexting: Protecting Consumer Telephone Records from Unauthorized Disclosure“, *Fed Comm LJF*, Bd. 60, Nr. 53, 2008.