Mobile Networks and Applications
https://doi.org/10.1007/s11036-022-02048-9

Badoo Android and iOS Dating Application Analysis

Jack Long[1] · Ivan Cvitić[2] · Xiaolu Zhang[1] · Dragan Peraković[2] · Kim-Kwang Raymond Choo[1]

Accepted: 13 December 2021

Abstract
Usage of mobile dating apps has been a rising trend in recent times, including during the COVID-19 lockdown periods. One of the key concerns about the use of such apps is in the amount and types of user data collected (e.g., personal and sensitive information such as sexual orientation, and information about online activities such as intimate messages and browsing behaviors). Since it is relatively easy and inexpensive to setup a man-in-the-middle attack and intercept dating app communication, a natural question is then whether the communication is encrypted and/or how much 'useful' information an attacker can infer from the intercepted communication, for example using freely available tools. Seeking to answer this question, we focus on the Badoo dating applications for both Android and iOS mobile devices (i.e., app version 5.187.0 on iPphone 7 (iOS 14.2), and app version 5.198.1 on Moto G5 Plus (Android v7.0)). Specifically, we explain the types of information an individual could obtain using only a laptop and Wireshark, a freely available network capture tool.

Keywords Dating apps · Online dating · Dating app artifacts · Man-in-the-middle attack

1 Introduction

Dating applications (apps) are increasingly popular, as `old-school' dating platforms like e-Harmony and Match migrate to mobile dating apps. For example, a 2020 Statista study found that the two most popular mobile dating apps, Tinder and Bumble, had reportedly 7.86 and 5.03 million users in 2019 [1]. With so many people choosing to create accounts on mobile dating apps, it is crucial that users understand the risks. Mobile dating apps contain a treasure trove of personal information that can have serious implications when such information falls into the wrong hands. In 2016, for example, a Tinder user was reportedly murdered by another user who they 'rejected' on the app. The rejected individual allegedly broke into the victim's home and committed the murder [2]. There are many more other recent instances of dating app-related criminal activities, and thus mitigating the risks of mobile dating is a key safety concern for the users and broader society.

One would note that dating apps contain a large amount of sensitive information on each user. Almost every app requires users to upload pictures and fill out an extensive user profile. Here, we will focus only on one such (popular) mobile dating app, namely: Badoo. The Badoo user profile contains information on age, gender, occupation, education, hobbies, and daily routine. Many mobile device users routinely connect their devices to a third-party Wi-Fi provider, for example in a shopping mall, at a café, at the airport, or even to an inflight Wi-Fi system. A malicious actor (adversary) can easily carry out a man-in-the-middle (MITM) attack, by impersonating as a legitimate Wi-Fi access point. Hence, in this paper we seek to determine how an adversary, armed with only a laptop and freely available software, could intercept communications from an Android or iOS mobile device / app user and what the adversary could infer about the user from the intercepted communications.

Specifically, we install Badoo dating app versions 5.187.0 and 5.198.1 on on an iPphone 7 (iOS 14.2) and a Moto G5 Plus device, respectively. We then create two dating app profiles (one for each device), and set up a packet sniffer, and capture and decrypt the (captured) network traffic (see Sect. 3). Such a setting is representative of a very simple real-world attack, where an adversary sets up a proxy server to intercept

✉ Kim-Kwang Raymond Choo
raymond.choo@fulbrightmail.org

[1] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

[2] Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia

Published online: 02 November 2022

HTTPS traffic sent by the mobile app user. The findings from the investigation are reported in Sect. 4, for example in terms of the various artifacts obtained by the adversary, where the majority data is found in the HTTPS packets.

Next, we will briefly review the extant literature.

2 Related work

Mobile app forensics is one of the major research areas in mobile forensics, and many researchers have proposed different approaches to faciliate the acquisition of forensic artifacts from mobile apps on smartphones. Since data gereated by a mobile app is usually stored in a well-known directory hierarchy (e.g., App data is store under */data/data/{app_name}* on Android and */Applications/{app_name}* on iOS), analysis could be undertaken on the clear-text/enrypted data found in these locations. For example, the authors of [3, 4] demonstrated how one can acquire evidence from clear-text data in mobile health/fitness apps. The authors had successfully retrieved the user's walking distances, style, speed, and user's health data, geo-locations, and walking paths. To deal with encrypted data such as the encrypted user credencials, privacy, and database, the authors of [5, 6] proposed that an investigator can hijack/leak the decryption keys via reverse engineering of the disambled app or sniffing the network traffic where the decryption keys are exchanged. While these articles were particularly written for vault and social media apps, the proposed methods can be used for analyzing other types of mobile apps (e.g., IoT, social media, bank, malicious). For example, the authors of [7] conducted a conperhensive forensic analysis over Amazon Echo, in which the authors found significant forensic artifacts such as account information and user-Alexa communication data from the Echo's companion mobile app. In [8], the authors examined the mobile apps for IoT devices, namely Insteon IP Camera, Insteon Hub and nest thermostat. In addition to the evidence on the local device, the authors extended data acquisition to the Cloud server of the IoT applications via open Cloud APIs. In terms of social networking and messaging app forensics, the authors of [9] tested 70 iOS apps with a packet sniffing technique and concluded that user privacy such as user's geo-location, user credentilas for social network, email, etc., can be caputered from 15/70 applications and 50/70 were found exchanging unencrypted authorization data through network. Another work outlined in [10] particularly focused on Facebook, Twitter, LinkedIn and Google + on both Android and iOS platforms. The authors successfully recovered user credencials and users activities that are of forensic interest from network traffics, memory and internal storage of the mobile devices. To encapsulate the aforementioned methods to an integrated digital forensic framework, the authors of [11] proposed a design science approach and demonstrated how to apply such a framework while investigating Android IoT applications.

While digital forensics, including mobile forensics, is relatively well-studied, dating application forensics is surprisingly less represented in the research literature, considering the amount of sensitive information in such apps that could impact on the user's physical safety concerns [12, 13]. There are a small number of research articles that focus on forensic artifact discovery. For example, Shetty, Grispos, and Choo [14] studied seven popular Android mobile dating apps, and the Google Chrome browser app. The research results showed that mobile dating apps are, potentially, vulnerable to various commo security risks. Knox et al. [15] investigated the Happen dating apps for both Android and iOS devices, and Stoicescu, Matei, and Rughinis [16] focused on Tinder and OkCupid dating apps. It was also observed that a number of researchers used an adversary model in mobile device / app forensics, such as the one proposed in [17]. An adversary model is a modeling approach in which the roles of the potential attackers are defined and subsequently used to evaluate the target device / app. For example, an dating app 'adversary' is assumed to have the ability to listen, send, reveal, execute, and corrupt data in transit [17], which represents the real-world attacker capability. Ma, Sun, and Naaman [18] studied the temporal component of the Happn dating app, seeking to understand how users utilize information about the location overlap and what benefits and drawbacks location overlap offers to dating app users. Phan, Seigfried-Spellar, and Choo [19] studied issues surrounding dating apps, in terms of the various associated risks of dating app usage such as crimes, mitigation strategies, physiological and psychological impacts on users, assessment on associated cybersecurity risks and potential digital artifacts of interest in a criminal investigation. In an earlier study [20], the authors provided a systematic overview of how mobile dating app investigations should be carried out. The authors also presented forensic techniques on nine proximity-based dating apps and identified what data could be recovered from user devices.

As discussed earlier, dating app forensics and security evaluations appear to be understudied, in comparison to mobile (device) forensics and mobile security (e.g., see [21, 22]). Findings from earlier studies such as [20] may no longer be relevant due to changes in the apps. This reinforces the importance of ongoing research efforts in mobile app forensics and security.

Table 1 provides a snapshot of the related dating app research literature.

3 Research setup and approach

Badoo allows users to create new accounts or link existing accounts such as Facebook and Twitter, through the popular OAuth API. For this experiment, two mobile devices

were used to create Badoo accounts. One iOS device (i-Phone 7) and one Android device (Moto G5 Plus). Unfortunately, Badoo restricts a single mobile device from creating multiple accounts. This means any cell / phone number can only create one associated Badoo user profile. Due to this restriction, only two Badoo user accounts were created in our experiment, one on each device. Table 2 describes the devices and associated accounts.

The iPhone 7 device was used to create the fake Jackson Choo profile and the Moto G5 Plus created Sarah Koo. The two accounts were created at the same time. The profiles were then 'matched' using Badoo's proximity matching feature. This feature enables users to match with other Badoo users who are closest to them. The Jackson Choo account swiped right on Sarah Koo when the user's dating card appeared in the stack. Sarah Koo also swiped right, and the users were matched. Once matched, the two devices could then message each other. Due to privacy considersations, we did not actively search for or interact with other dating app users.

Due to COVID-19 restrictions, the two device owners were not able to run Badoo while on the same network. Due to this restriction, the Jackson Choo profile, running on iOS 14.2, was the main subject of investigation. In other words, the experiment focused on the capturing of forensic artifacts from this device. Jackson Choo will use Badoo to communicate with Sarah Koo, the Android device located in Houston.

3.1 Mobile hotspot packet sniffer

Acting as the 'adversary', the research team began with a packet sniffing operation. The goal was to intercept messages sent from the iPhone (Jackson) to the Android (Sarah) via the Badoo dating app. To capture network traffic, a laptop running Windows 10 would act as packet sniffer. The tools and tactics used to establish the attack were all open-source and publicly available (Fig. 1).

First, the laptop created a mobile hotspot named 'LAPTOP-ADVERSARY'. Jackson connected to this hotspot thinking it was a legitimate Wi-Fi access point. The laptop began to capture all network traffic sent between Jackson and the internet using Wireshark, a free packet sniffer. To gain access to the raw traffic, a Wi-Fi Protected Access Pre-Shared Key (WPA -PSK) was generated. The key was generated using the Passphrase and SSID of the hotspot network, see Fig. 1. The key enabled the packet sniffing software to decrypt IEEE 802.11 wireless traffic sent to and from Jackson's iPhone [24].

Table 1 Dating app research literature: A snapshot

Research	Year	Research focus(es)	Number of dating apps studied, and names of the apps
[13]	2020	User safety	14 Badoo, Bumble, Grindr, Growlr, Happn, HER, Hinge, Hornet, Jack'd, OKCupid, Plenty of Fish, Scruff, Tinder, Wapa
[14]	2017	Cybersecurity	8 Tinder, Happn, Badoo, MeetMe, Skout, Lovoo, Coffee Meets Bagel, Chrome for Android, Facebook
[15]	2020	Cybersecurity, privacy, partially digital forensics	1 Happn (versions 9.6.2, 9.7, and 9.8 for iOS devices, and versions 3.0.22 and 24.18.0 for Android devices)
[16]	2020	Privacy	2 Tinder and OkCupid
[18]	2017	Cybersecurity, privacy	1 Happn
[19]	2021	Crimes, mitigation, physiological and psychological effects, cybersecurity, digital forensics	- - (literature review article)
[20]	2015	Digital forensics	9 Badoo, Grindr, Skout, Tinder, Jaumo, Meet Me, FullCircle, MuiMeet

Table 2 Test devices

Device	OS version	Device location	Badoo app version	Installation date
iPphone 7	iOS 14.2	San Antonio, TX	5.187.0	Oct 20, 2020
Moto G5 Plus	Android v7.0	Houston, TX	5.198.1	Oct 20, 2020

Fig. 1 WPA-PSK Generation [23]

3.2 Fiddler proxy server

A proxy server was created on the adversary Windows 10 laptop. The proxy server was created used *Fiddler Anywhere*, a web-debugging proxy built to inspect HTTP(S) traffic. The tool is free and built to help web-developers quickly spin up and debug web servers. We used the tool for a slightly different, more nefarious purpose, in the sense that the adversary's laptop will use the proxy server to funnel all of Jackson's mobile traffic through *Fiddler Anywhere*.

The proxy server was in a different network environment. Instead of connecting through the laptop hotspot, Jackson and the Adversary would now be peers in the same network. Both devices were connected to the same network gateway. The gateway was a Google Wi-Fi mesh router. Both devices were configured to be 'discoverable' on the network. To verify that the devices could communicate, a ping request was sent from the Adversary to Jackson. The ping was successfully replied to, verifying that the devices could communicate (Figs. 2 and 3).

Several important configuration steps were taken to setup the proxy. The *Fiddler* application was given admin rights on the Win10 box. This enabled *Fiddler* to capture remote connections and not be constrained to only local traffic. In addition, Jackson's iPhone was forced to send all traffic through the *Fiddler* proxy on port 8866 of the local network [25]. The *Fiddler* Root certificate also needed to be downloaded and trusted on Jackson's iPhone. This step was critical to maintain web-access and capture all network traffic. See configuration screenshots from Jackson's iPhone in figures two and three.

Once successfully configured, Jackson's decrypted HTTPS web traffic was visible through *Fiddler Anywhere*. The proxy server was used to track three separate sessions of Jackson's common activity on Badoo. The proxy server also gave the Adversary of tracking Jackson's activity in real time. This meant the Adversary knew when Jackson was on Badoo and could create a profile of Jackson's activity.

4 Results

The network traffic captured sent from Jackson's iPhone to the *Badoo* server. The packet sniffing and proxy server operations were able to capture significant forensic artifacts. The results of the packet sniffing operation will be discussed first followed by the proxy server.

4.1 Packet capture

The freely available and widely used *Wireshark* packet capture tool was able to intercept network traffic between Jackson's iPhone and the Badoo servers. The Domain Name Server (DNS) packets revealed that Jackson was actively using Badoo's iOS app. How do we know that it is the iOS version of Badoo? The DNS traffic also revealed iTunes. So far, the laptop 'adversary' knows that Jackson is using an iPhone to run Badoo's iOS app.

Further investigation with packet capture was thwarted due to HTTPS-TLS encryption. All application layer traffic sent from Jackson's iPhone was encrypted. This information provided little to no information about Jackson's information or activity on Badoo. To overcome this, the research team setup a proxy server. The results of this operation will be discussed next.

4.2 Proxy server

The proxy server captured a large amount of significant data between Jackson and the Badoo servers. Jackson's traffic was captured during three different Badoo sessions. The first session involved Jackson sending two messages to Sarah, the Android in Houston. The proxy server captured network traffic during the session. The traffic contained forensic artifacts that revealed very sensitive information about Jackson and the device he used.

4.2.1 Messaging session

An HTTP/1.1 POST request was sent from Jackson's iPhone7 to Badoo's US based server (us1.badoo.com). The post request body contained detailed JSON (Java Script Object Notation) about Jackson and his mobile device. The JSON included the devices make and model, iOS version, the device ID, network interface type (Wi-Fi), version of the Badoo app and language, free versus premium Badoo subscription, and the Badoo *session_id*. All this information could be used by the Adversary to exploit Jackson. For example, the Adversary could use the Badoo *session_id* to hijack Jackson's connection to Badoo.

In addition to device information, the packet's JSON data contained artifacts about Jackson's dating profile. The data included user age, gender, and type of communication sent. Interestingly, Jackson's chat message did not appear in plaintext. The JSON data had a *comm_type* variable that showed that it was a 'chat', but the value of field was just a long float number (311.6127500034054).

4.2.2 Swiping session

The second proxy session, the swiping session, involved Jackson using Badoo's swiping and proximity match features. Jackson swiped on user profiles that were presented in his "stack" and viewed Badoo profiles in that were near his current location. This session created a lot of HTTPS traffic, allowing the adversary to intercept considerably more information about Jackson and the profiles he was swiping on.

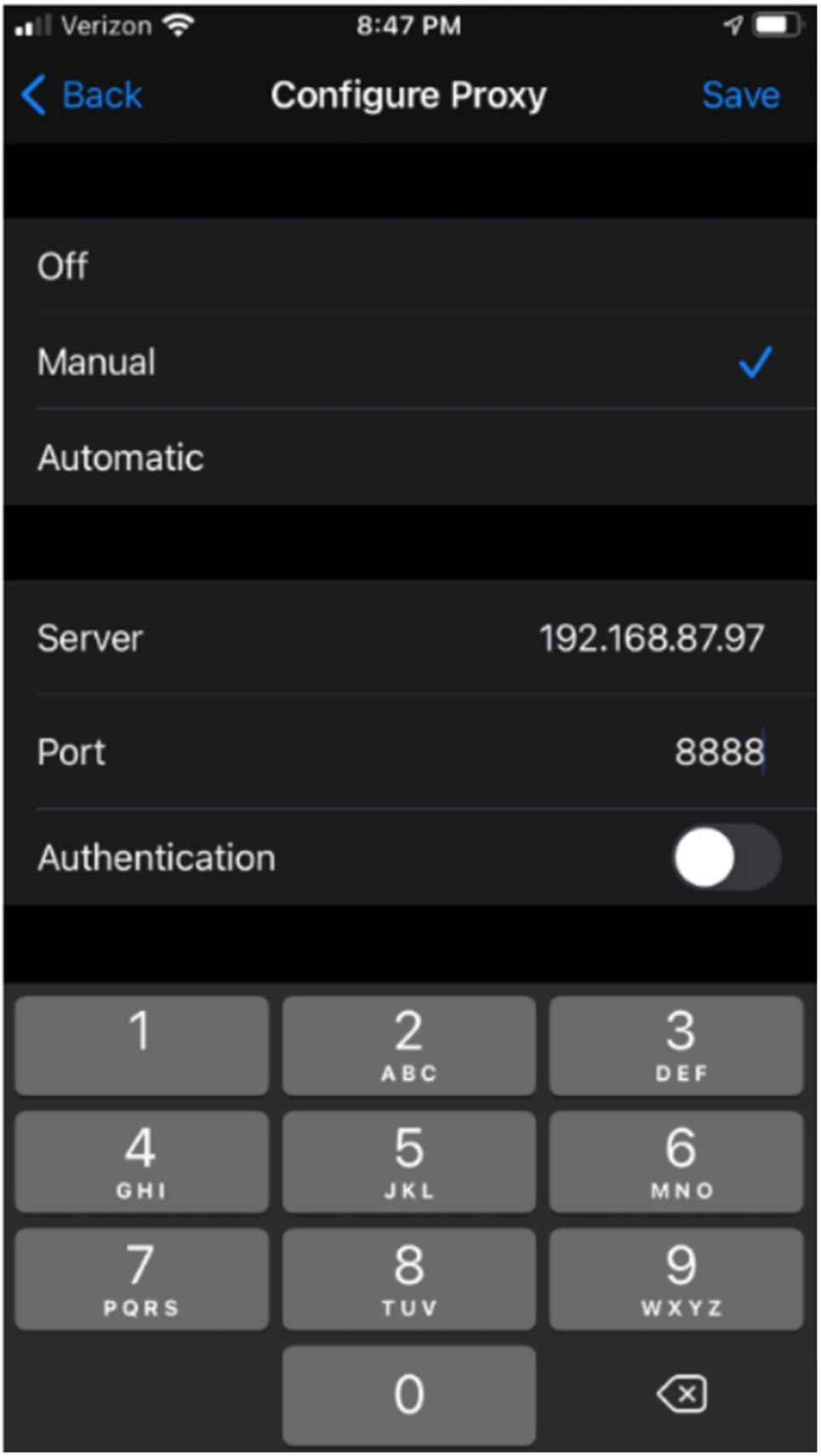

Fig. 2 iOS 14 proxy configuration

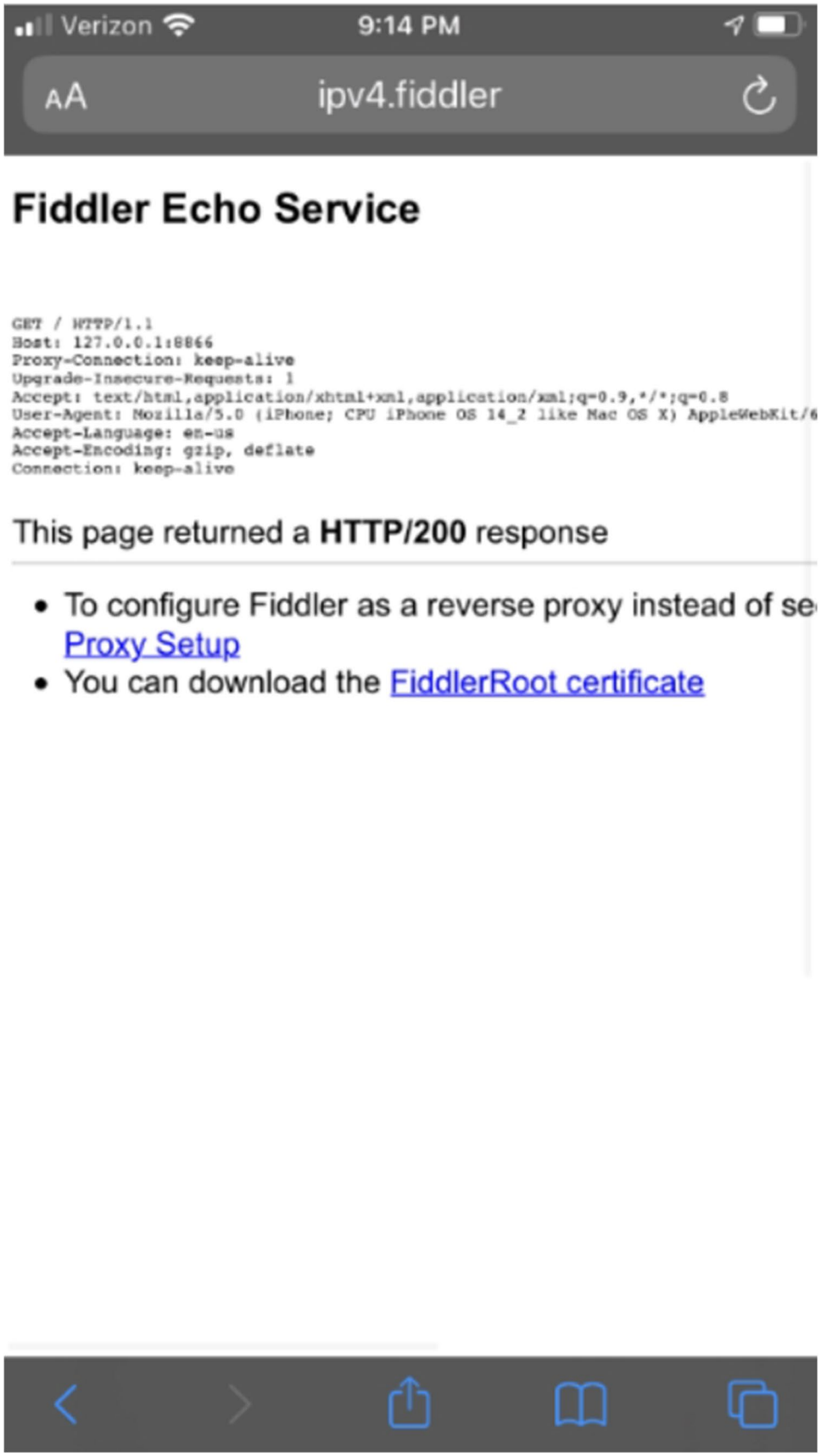

Fig. 3 Fiddler Root Certificate

The Adversary captured every user profile presented to Jackson in his swiping stack. Jackson's device generated a GET HTTPS request to Badoo's content distribution network (CDN). The CDN replied with an HTTP response containing the images and information on the profile card presented to Jackson. From this HTTP response, the adversary was able to capture the JPEG images.

After each swipe, Jackson's device sent a POST request to the Badoo server. This request contained updates to Jackson's profile. It also contained a new variable, *Encounters/vote*. This variable fluctuated between 0.0 and 100.0 based on Jackson's interactions. Before swiping on any profiles, Jackson had an *Encounters/vote* value of 0.09. After swiping on a user and matching, Jackson's *Encounters/vote* value shot up to 65.77. Then, Jackson swiped on another user and did not immediately match. The following POST request showed Jackson's *Encounters/vote* value decrease to 52.92.

The Adversary had access to the pictures Jackson was swiping on as well as the updates to Jackson's profile info. The adversary could easily deduce which user Jackson had liked, disliked, and matched with from the GET and POST request data. These artifacts reveal a detailed account of Jackson and the users he encountered on Badoo.

When Badoo is launched, the app sends an interesting POST request to the remote server. This POST contains JSON with all the user and device info discussed above. In addition, it contains a JSON variable named *measurements*. This variable contains a type and value measurement for the various Badoo services. These services include primary, navigation user interface, and iOS launch. The type and value data are just integers and do not obviously correlate to any user or device info. This data could be an interesting avenue for future research.

4.2.3 Proximity session

Next Jackson used Badoo's proximity feature. This feature presents the user with numerous profiles of users who are close to device. The average proximity observes on the app was 1–10 miles. The Adversary captured Jackson's traffic during this session using the same proxy server from earlier sessions. The Adversary found artifacts that revealed information about Jackson and the users who were closest to him at the time of the session.

To active the proximity feature Jackson's device sent GET and POST requests to Badoo's US and European servers. The POST request to Badoo's European server contained the most information relevant to Jackson and the other user profiles. The body of the POST contained a 1000+line JSON file with information on all Badoo users presented to Jackson. The data included multiple user ids, encoded names, a full list of user profile information, and information on if they had liked Jackson or not. In addition, the JSON contained the same *Encounters/vote* variable found before in Jackson's profile (Fig. 4).

This is clearly a significant amount of data on all Badoo users that Jackson encountered. However, some of these artifacts were less revealing. For example, the profile information only contained metadata about what the user had filled out. The Adversary could see if the proximity users had filled out the job and education fields, but he/she did not have access to the value of this fields.

4.2.4 Looking through profiles

During Jackson's final Badoo session, we took a closer look at the profiles Jackson had been matched with. Badoo enables users to view the photos and profile descriptions of other users. The users do not need to be matched to view


```
{
  "body": {
    "view_profile": {
      "job_shown": false,
      "encrypted_user_id": "1580148339",
      "crush_badge": false,
      "restored": false,
      "mutual_badges_count": 1,
      "liked_you_badge": false,
      "common_interests_shown": false,
      "interests_shown": true,
      "lifestyle_badges_count": 2,
      "activation_place": 2,
      "education_shown": false
    }
  }
}
```

```
{
  "body": {
    "vote_profile": {
      "gesture": 3,
      "encrypted_user_id": "1474236176",
      "crush_badge": false,
      "vote_result": 3,
      "mood_status": false,
      "activation_place": 2,
      "liked_you_badge": false
    }
  }
}
```


Fig. 4 JSON Profile Information on close-proximity users

each other's profiles. Jackson viewed the profiles of users he matched with and those he found in the proximity session. Like earlier sessions, the Adversary used the Fiddler proxy server to capture and decrypt all network traffic between Jackson's device and the Badoo servers.

The Adversary was able to intercept all profile pictures viewed by Jackson. The pictures were intercepted via the GET HTTPS response sent to Jackson's iPhone when he viewed each profile. However, the Adversary was limited to the same JSON data found in Fig. 4. The profile name was not available. Instead, the JSON contained an encrypted user id and profile description variables. Overall, this session did not provide the Adversary with any new or significant artifacts.

5 Discussion and research limitations

Our preliminary research results presented in this paper raise several questions, firstly on users' safety, dating apps' cybersecurity, user privacy, and the help that such applications can provide to the investigators. Dating apps significantly negatively impact user safety, which has already been raised by other researches [13, 19]. Like every other application, dating apps are also vulnerable to various cyber threats and can be targeted to facilitate a broad range of nerfarious activities (e.g., user privacy violation). Such actions can have a negative impact on a user in a virtual or physical context (e.g., cyber / physical stalking, sexual assault, and/or murder). Nevertheless, this research indicates that investigators can retrieve user information and activities in the Badoo app, such as user ID and other relevant information that can be of great help during a legitimate and court-authorized (criminal) investigation.

The primary limitations in this study were due to Covid-19 restrictions. The iOS and Android devices, owners were never able to operate their devices in the same network after the initial setup. This meant that the investigation had to focus on the iOS device, Jackson, and only used the Android device, Sarah, as a sender and receiver of messages. From this point on the investigation was limited to only traffic sent and received by the iPhone7 running iOS 14.2.

There were several limitations with the iOS device. Researchers were unable to locate app data when the device was backed up with iTunes. The iTunes backup contained no application data. The only artifacts found were system data and pictures/videos from Jackson. The *Happn* investigation, discussed earlier in the literature review, used iTunes backups to acquire data on the user's dating profile [15]. Badoo's data was not accessible through the iTunes backup. This limited the Adversary's ability to gain information on Jackson.

Research was also limited by the OS restrictions on the Android and iPhone. The owner of both devices specified that they should not be permanently altered in anyway. This meant that the iPhone could not be jailbroken, and the Android could not be rooted. Both operations could cause irreparable damage to the device. Mobile rootkits can permanently hinder a device's performance and make them more suspectable to malware [26]. Also, rooting a phone almost always voids the warranty. Since major alterations to the devices were not permitted, most of the research was restricted to network traffic.

6 Conclusion

Our preliminary research focused on the Badoo dating app, where we attempted locate and record sensitive user data sent by a Badoo user using a simple MITM attack. We demonstrated how easy it is to intercept network traffic that contains sensitive information about the target user, and users communicating or interacting with the target user. The Adversary gathered personally identifiable information relating to our target user, which includes age, gender, sexual preference, and personal pictures. The Adversary also gained access to our target user's *Encounters/votes* score. This variable is not meant to be seen by users and is meant to score users based on how many likes they have received. The Adversary used this number while our target user was swiping in real-time to determine if (s)he matched with the users our target user encountered. In addition to our target user's information, the Adversary gained information on other Badoo users. The HTTPS traffic captured during the *4.2.3 proximity session* contained sensitive information about Badoo users who were within 10 miles of our target user. Profile pictures, user ids, and profile metadata were all captured. Overall, the Adversary collected information on 50+Badoo user profiles during the MITM session.

Going forward, we plan to investigate other popular dating apps. *Do other popular dating apps, such as Tinder or Hinge, better protect their network traffic?* This investigation revealed that simply using HTTPS-TLS encryption may not be enough. An adversary could setup a Wi-Fi hotspot that routes all users traffic though a proxy server like Fiddler Anywhere. *Do widely used dating apps have in-place additional level(s) of encryption to protect user pictures and information?*

In addition, we plan to explore the use of other tools, such as the recently developed "DC3 Advanced Carver, a modular software package for the salvaging of corrupted data files from almost any digital device" [27] and perform an empirical evaluation of both commercial and open-source forensic tools in terms of the range and types of information that can be obtained from a forensic analysis of the devices and proxy servers. To share the findings and the forensic artifacts of Badoo in a standard form with the digital forensic community, we plan to create a schema (a form that can represent how to find the important forensic artifacts from a significant amount of data, but does not include any real/sensitive data) on ForKaS [28], which is an automated knowledge-sharing

forensic platform that can automatically suggest schemas during forensic investigation.

The goal of connecting users is a noble one, but it should not sacrifice the privacy of those users to accomplish it. Findings from the Pew Research Center, for example, show that dating app use continues to grow every year [29], including during COVID-related lockdowns [30]. It is also known that such applications can be abused to facilitate a broad range of nefarious activities [31]. For example, a male accused person was reportedly sentenced to seven years' imprisonment after being found guity of 'raping and sexually exploiting teenage girls he met on Instagram and Tinder' [30]. In addition, given the sensitive nature such apps, there may be attempts to obtain and/or exfiltrate data from these applications. In other words, the larger the pool of exposed information grows, the more likely a criminal enterprise will try and exploit it. Dating applications can give users a false sense of security by keeping the like system double blind. However, the true threat to users may not be from inside the applanation, as demonstrated in this study. The findings reinforce the importance of both security- and privacy-by-design principles in future app developments. Also, *can we integrate crime prevention theories such as the Routine Activity Theory* [32] *and security- and privacy-by-design principles in future app developments?* For example, can we align security and privacy-preservation measures with the three constructs of the Routine Activity Theory, specifically in terms of increasing the effort required to offend (by reducing opportunity), increasing the risk of getting caught (by enhancing guardianship), and reducing the rewards of offending (by reducing motivation).

Authors' contribution Conceptualization: J. Long and K.-K.R. Choo; Methodology: J. Long, X. Zhang, K.-K. R. Choo; Formal analysis: J. Long; Investigation: J. Long; Supervision: D. Peraković, K.-K. R. Choo; Writing – original draft: J. Long and K.-K.R. Choo; Writing – review & editing: I.Cvitić, X. Zhang, D. Peraković, K.-K. R. Choo.

Funding This work was partially supported by National Science Foundation CREST under Grant HRD-1736209.

Data availability Not applicable.

Code availability Not applicable.

Declarations

Conflicts of interest/competing interests Not applicable.

References

1. Statista (2019) Most popular online dating apps in the United States as of September 2019. https://www.statista.com/statistics/826778/most-popular-dating-apps-by-audience-size-usa/. Accessed 18 May 2021
2. Awford (2017) Tinder stalker stabbed date 11 times, then doused her in gasoline. http://nypost.com/2017/02/16/tinder-stalker-stabbed-date-11-times-then-doused-her-in-gasoline/. Accessed 23 Aug 2021
3. van Zandwijk JP, Boztas A (2019) The iPhone Health App from a forensic perspective: can steps and distances registered during walking and running be used as digital evidence? Digit Investig 28:S126–S133
4. Hassenfeldt C, Baig S, Baggili I, Zhang X (2019) Map my murder: A digital forensic study of mobile health and fitness applications. In Proceedings of the 14th International Conference on Availability, Reliability and Security, pp 1–12
5. Zhang X, Baggili I, Breitinger F (2017) Breaking into the vault: Privacy, security and forensic analysis of Android vault applications. Comput Secur 70:516–531
6. Al Barghouthy N, Said H (2013) Social networks IM forensics: encryption analysis. J Commun 8(11):708–715
7. Li S, Choo KKR, Sun Q, Buchanan WJ, Cao J (2019) IoT forensics: Amazon echo as a use case. IEEE Internet Things J 6(4):6487–6497
8. Meffert C, Clark D, Baggili I, Breitinger F (2017) Forensic State Acquisition from Internet of Things (FSAIoT) A general framework and practical approach for IoT forensics through IoT device state acquisition. In: Proceedings of the 12th International Conference on Availability, Reliability and Security, pp 1–11
9. Bhatt AJ, Gupta C, Mittal S (2018) Network forensics analysis of iOS social networking and messaging Apps. In: 2018 Eleventh International Conference on Contemporary Computing (IC3). IEEE, pp 1–6
10. Norouzizadeh Dezfouli F, Dehghantanha A, Eterovic-Soric B, Choo KKR (2016) Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google + artefacts on Android and iOS platforms. Aust J Forensic Sci 48(4):469–488
11. Zhang X, Liu CZ, Choo KKR, Alvarado JA (2021) A design science approach to developing an integrated mobile app forensic framework. Comput Secur 105:102226
12. Pooley K, Boxall H (2020) Mobile dating applications and sexual and violent offending. Trends and issues in crime and criminal justice 612. https://doi.org/10.52922/ti04862
13. Cvitić I, Peraković D, Periša M, Husnjak S (2018) Application possibilities of digital forensics procedures in vehicle telematics systems. Zesz Nauk Wyższej Szk Tech w Katowicach 1(10):133–144
14. Shetty R, Grispos G, Choo K-KR (2017) Are you dating danger? An interdisciplinary approach to evaluating the (In) security of android dating apps. IEEE Trans Sustain Comput 6(2):197–207. https://doi.org/10.1109/tsusc.2017.2783858
15. Knox S, Moghadam S, Patrick K, Phan A, Choo KKR (2020) What's really 'Happning'? A forensic analysis of Android and iOS Happn dating apps. Comput Secur 94. https://doi.org/10.1016/j.cose.2020.101833
16. Stoicescu MV, Matei S, Rughinis R (2019) Sharing and privacy in dating apps. In: Proceedings – 2019 22nd International Conference on Control Systems and Computer Science, CSCS 2019, pp 432–437. https://doi.org/10.1109/CSCS.2019.00079
17. Do Q, Martini B, Choo KKR (2019) The role of the adversary model in applied security research. Comput Secur 81:156–181. doi: https://doi.org/10.1016/j.cose.2018.12.002
18. Ma X, Sun E, Naaman M (2017) What happens in happn: The warranting powers of location history in online dating. Proc. ACM Conf. Comput Support Coop Work. CSCW, pp 41–50. https://doi.org/10.1145/2998181.2998241
19. Phan A, Seigfried-Spellar K, Choo K-KR (2021) Threaten me softly: A review of potential dating app risks. Comput Hum Behav Rep 3:100055. https://doi.org/10.1016/j.chbr.2021.100055

20. Farnden J, Martini B, Choo KKR. Privacy risks in mobile dating apps. May 2015, [Online]. Available: http://arxiv.org/abs/1505.02906
21. Rodríguez E, Otero B, Gutiérrez N, Canal R (2021) A survey of deep learning techniques for cybersecurity in mobile networks. IEEE Commun Surv Tutor 23(1):1920–1955
22. Sequeiros JB, Chimuco FT, Samaila MG, Freire MM, Inácio PR (2020) Attack and system modeling applied to IoT, cloud, and mobile ecosystems: embedding security by design. ACM Comput Surv 53(2), article no. 25
23. Wireshark. WPA PSK (Raw Key) Generator
24. Spy Traffic From Smartphone with Wireshark (2019). https://null-byte.wonderhowto.com/how-to/spy-traffic-from-smartphone-with-wireshark-0198549/. Accessed 21 Mar 2021
25. Velikov K (2019) How To: Capture iOS Traffic with Fiddler. https://www.telerik.com/blogs/how-to-capture-ios-traffic-with-fiddler. Accessed 18 Jan 2020
26. Green E (2020) Why root Android phones? The pros and cons explained. https://nordvpn.com/blog/why-you-shouldn't-root-android/. Accessed 26 Nov 2020
27. DC3 advanced (2021) https://techlinkcenter.org/technologies/dc3-advanced-carver-suite-for-digital-forensics-content-recovery/92b523e1-6859-4f17-92b0-961f825500a8. Accessed 8 Nov 2021
28. Zhang X, Choo KKR, Beebe NL (2019) How do I share my IoT forensic experience with the broader community? An automated knowledge sharing IoT forensic platform. IEEE Internet Things J 6(4):6850–6861
29. Anderson M, Vogels E, Turnet E (2020) The vitures and downsides of online dating. https://www.pewresearch.org/internet/2020/02/06/the-virtues-and-downsides-of-online-dating/. Accessed 25 Mar 2021
30. Wu Y (2021) Tinder, bumble and hinge show surge in Americans looking for love Online. https://www.wsj.com/articles/tinder-bumble-and-hinge-show-surge-in-americans-looking-for-love-online-11613246400. Accessed 26 Oct 2021
31. Garga S, Thomas M, Bhatia A, Sullivan A, John-Leader F, Pit S (2021) Geosocial networking dating app usage and risky sexual behavior in young adults attending a music festival: cross-sectional questionnaire study. J Med Internet Res 23(4), article no.: e21082
32. Cohen LE, Felson M (1979) Social change and crime rate trends: A routine activity approach. Am Sociol Rev 44(4):588–608