The Security of Tinder

A Mobile App That May Be More Intimate Than We Thought

Author:

Margaret Feltz

Mentor:

Ming Chow

December 15, 2015

Contents

1 Abstract

Tinder, owned by The Match Group, is a Geosocial mobile application for dating and social discovery that offers a quick and simple way to meet singles nearby. The location-based service renders 40 profiles of potential matches of which the user can shuffle through and if the attraction is mutual, they are prompted to begin a conversation. Tinders use of location-based networking presents significant vulnerabilities, exposing users to privacy concerns that many are unaware of. Without responsible use of a users location, an attacker can use trilateration to pinpoint a users exact location with very high precision. In addition, users are not privy enough to the personal information they allow their social networks to use, in turn, putting their privacy at risk. This paper will discuss the relevant security issues within Tinder and what users can do to protect their privacy.

2 Introduction

2.1 What is Tinder?

In the rapidly growing world of mobile dating apps, Tinder has certainly claimed its position as a top contender, potentially reaching 58 million active users worldwide in 2016.[5] The location-based service renders 40 profiles of singles nearby of which users can shuffle through and swipe right if they like the potential match, or left if they dont. When someone you like, swipes right on you, the app notifies you that you have matched and prompts both parties to start a conversation via the private messaging platform in the app.

2.2 Features

Some newer updates to Tinder include a paid service that allows users to undo a swipe, have access to unlimited swipes, and change their current location to discover singles in different locations all around the world. Being able to change their location, an attacker can more easily narrow down the position of their victim. The simple convenience of a users location can lead to a false sense of security. Tinder has also integrated a feature that allows users to share their Instagram photos on their profile with potential matches.

2.3 Relevant Security

Released in 2012, Tinder hit one million users in a little over a year; one million people liberally sharing their location and personal information across Tinders servers. In July of 2013, an engineer in San Francisco discovered that the Tinder API returns much more personal information than the user is aware of. Tinder was exposing information, as well as calculating the distance between matches on the client side of the app. Once corrected later in July, researchers at Include Security exposed and reported an issue found in the fix. The new fix revealed that the API was returning the extremely high precision distance between two users. Using a method called trilateration, an attacker or stalker can located the exact position of a user with very little technical skills involved. Although the distance was adjusted to a much lower precision, Tinder and many other Geosocial applications present many privacy concerns that can link a general location to much more intimate information about its users.

3 To The Community

With nearly 10 million daily active users as of November 2015[3], Tinder is the fastest growing mobile dating app right now.[4] Tinder and many other dating applications promote intimate relationships and connections which can also create more hazardous relationships, such as stalking. With such a massive customer base making millions of matches per day, it is important for everyone to be aware of the privacy concerns they face as well as the steps they can take to defend themselves. Nowadays, people constantly use new technologies without fully understanding the privacy and security risks they are at. For the community, this paper intends to better inform users and urge Geosocial and other social networking platforms to further educate their users about protecting their privacy.

4 Vulnerabilities

4.1 First Vulnerability

The first location vulnerability was discovered and reported by Mike Soares, an engineer in San Francisco in early July 2013.[1] Tinder's API was returning exact and very high precision latitude and longitude data for each user as well as their Facebook ID and exact birthdate in lat, lon, fbId, and "birth_date" fields, respectively.

4.1.1 Latitude and Longitude

According to Quartz, the lat and lon fields marked the most recent location where a user was using Tinder. It goes without saying that returning a users exact location through latitude and longitude is about as vulnerable as it gets. An attacker can easily query the server a number of times to look for patterns of the user's location to narrow down where the victim may be at any given time.

4.1.2 Facebook ID

The Facebook ID returned in the API response correlates to the specific profile of any Tinder user. A Tinder profile only reveals a user's first name, allowing them a much higher level of privacy than if their last name were visible. However, with a Facebook ID, an attacker can find a user's Facebook profile by simply adding the fbId data into the id field of the url:
https://www.facebook.com/profile.com/profile.php?id=123. A Facebook profile can

expose a user's last name and a whole lot more depending on the privacy settings on the user's Facebook account. Discovering a Facebook profile can give the attacker access to information such as place of work, school, recently visited places, friends of the victim and much more personal information. With enough information, an attacker can find patterns in their victim's activity and narrow down details about their positional habits. Unfortunately, Tinder doesnt currently allow users to activate an account without authenticating with a Facebook account. However, with Facebook possessing so much personal and vulnerable information, omitting the requirement of authenticating with Facebook, while also verifying the integrity of a user, would be ideal.

4.1.3 Fix

This vulnerability highlights one of the more obvious don'ts of location-based mobile apps. The first step in fixing the vulnerability is to completely remove the Facebook ID, latitude and longitude from the API and find another more secure way of rendering potential matches nearby. Data such as the Facebook ID, latitude and longitude of the victim should be encrypted and undiscoverable. The calculations that decide the proximity of matches is something that should happen behind the scenes. Later in July, Tinder released an update, no longer returning the three pieces of data.

4.2 Second Vulnerability

The new fix however was a large vulnerability itself. In October of 2013, researchers at Include Security found that the fix Tinder made was that its API now returns the distance to a match with extremely high precision; mileage to 15 decimal places, accuracy to 100 ft.[2] Although this solution seems much better than returning a users latitude and longitude, it isnt a significant improvement. An attacker can draw a circle around themselves with the distance from the API to see the potential positions their victim might be. This may seem a little more vague, but with a method called trilateration, an attacker with a serious intention can find a victims exact location with a few more steps and very little technical knowledge. [6]

4.2.1 Trilateration and Tinder Finder

Include Security used trilateration which is a method by which the exact location of a user can be determined using a minimum of three distances as radii from different locations of the attacker. To demonstrate this, Max Veytsman from Include Security created an unreleased web application, Tinder Finder, to simulate the attack. Finding a Tinder user ID is easily done by sniffing the phone network traffic.[6] Within the application, a user's ID is entered and three fake Tinder accounts locate the victim. From this, Tinder Finder has access to the three distances from the fake accounts to the victim. All the attacker has to do is draw three circles with radii of the corresponding distances around the locations of the false accounts. The point at which all three circles intersect is the exact location of the user with the high precision of 100 ft, which is more than enough precision

to draw conclusions about a victims whereabouts.

The ease of making a simple API call makes this vulnerability overly accessible to attackers. And, with a some minimal geometry, trilateration doesnt require any immense hacking abilities. The convenience of trilateration exists across most, if not all, location-based applications. Even without explicitly listing the distance between matches, with enough accounts to find the victim, the victim can be located. To date, there is no approach to rendering location-based data without the ability to perform trilateration. The most practical way improve the privacy of users while also preserving the location-based essence of the product is to provide much the lowest effective precision of the data. The position of the user should still be encrypted with the low precision data calculation also on the server side.

4.2.2 Fix

On January 1, 2014, Include Security reported that they could not reproduce the high precision data. Although Tinder did not respond to Include Security or issue a statement on a fix, Include Security claims that Tinder now rounds the distance returned by the server side to an integer instead of the high precision floating point value.[6] With this new fix, Tinder has increased the privacy of its users, but hasnt made their location completely undiscoverable. The fix has only made the task of using trilateration more laborious. The lower precision data only requires a greater number of fake accounts to increase precision of the discoverable location.

5 Action Items

5.1 Awareness

In terms of action items, there is little people can do without stopping the use of apps like Tinder all together. One of the more important things people can do, is make themselves aware of the risks they are putting themselves at by using location-based apps. With more knowledge of the vulnerabilities of Geosocial apps, people can become more confident in which services they choose to share their location or personal information with.

5.2 Facebook Privacy and Tinder's Privacy Policy

Because a Facebook account is required to create a Tinder account, users should be very aware of their Facebook privacy settings. If they are not, users should do a thorough overhaul; reviewing all of the information their Facebook profiles possess. According to the Tinder privacy policy, "the service may collect and store any personal information you provide while using our Service or in some other manner".[7] The vagueness of this statement allows Tinder rights to literally *any* information a user may provide the service throughout their use.

6 Defense

6.1 Being Mindful

Unfortunately, there is no fool-proof defense of your location in Tinder or any location-based app. There are, however, techniques people can use to put up their best defense against attackers. Attackers are very receptive, so they will be looking for patterns in locations their victim might travel to, to draw conclusions about their positional habits. Users should be much more mindful of when and where they decide to open their location based apps. Opening Tinder out of boredom with no real intent to use the app allows the service to update a user's most recently visited location, making them more vulnerable to an attacker.

6.2 What Can Tinder Do?

There are a few tactics Tinder can use to provide a higher level of security for its users. Their safety notices and guidelines explicitly say that Tinder does not perform any kind of background check on its users.[8] Without a background check, attackers can easily create fraudulent Tinder profiles in order to perform an attack. Tinder can improve its defenses by making it harder for attackers to create dummy accounts by using phone code verification or by monitoring the number of requests coming from a certain user, which can restrict the amount of information an attacker can gain from a victim.

In addition, Include Security was able to locate a user by entering the Tinder user ID that each user is assigned upon creating an account. Include Security sug-

gests that the Tinder user ID can be found by sniffing a phone traffic. In addition, the API, written by Rich Taylor, contains an endpoint that returns the list of recommended potential matches of a user.[9] The response of the recommendations endpoint contains a field named _id, which is the Tinder ID of the user. Data such as this should be encrypted and more secure across the servers to prevent attackers from being able to pinpoint specific users.

7 The Future

The future of location-based apps and their security is still a heavily uncharted field with no current approach to eliminate the threat of trilateration. However, does high security of user location on these apps create less of a use case for them? With location as the basis of Geosocial apps, there exists a tradeoff of security and privacy over a better social experience. As it stands now, Tinders low precision distance between matches still presents vulnerabilities of being discovered. The future of Tinder's security and privacy concerns also lies in the hands of the third-party apps it chooses to integrate.

7.1 Third Party Apps

Currently, Tinder users have the option to add Instagram photos to their profiles which, when enlarged, show the users Instagram username. This is another example of where users need to be aware of their privacy settings. If their Instagram profile is public, an attacker can see much more information about where theyve been, who their friends are, and what they like to do. Users have also been discovering the photo map that Instagram has, which can pinpoint the exact location of a user when they upload a photo.[10] Tinder and its partner apps should make a strong effort to inform users of the strides they can take to protect their privacy.

Although Tinders efforts are headed in the right direction, the privacy of users certainly goes beyond the precision of their distance from a match. With so many social apps today using other apps for authentication or features, it becomes up

to the user's awareness and discretion about privacy settings and which apps to use. In today's world, privacy is no longer a question of being visible or invisible. Now, it is more-so a question of how users can sufficiently protect their privacy while still creating the best social experience they can.

8 Conclusion

Tinder has grown itself into a Geosocial giant that has developed into a much more intimate app than we think it is. The buzz of new technology, and especially new mobile dating apps, dilutes the priority of privacy. Users are not privy to the amount of personal information they may be broadcasting about themselves. Without encrypting the more personal details of users and connections to other social media platforms, Tinder is allowing attackers to easily investigate and gather more than enough information to draw conclusions and pursue their victims. Companies like The Match Group must determine whether it prioritizes their users privacy and security or the enjoyable social interactions Tinder creates, while users must also be mindful of the information they are sharing and the social platforms they choose to participate in.

References

[1] Seward, Zachary M. "Tinders Privacy Breach Lasted Much Longer than the Company Claimed." Quartz. Atlantic Media, 14 July 2013. Web. 15 Dec. 2015. ¡http://qz.com/107739/tinders-privacy-breach-lasted-much-longer-than-the-company-claimed/¿.

[2] Summers, Nick. "New Tinder Security Flaw Exposed Users' Exact Locations for Months." Bloomberg.com. Bloomberg, 19 Feb. 2014. Web. 15 Dec. 2015. ¡http://www.bloomberg.com/bw/articles/2014-02-19/new-tinder-security-flaw-exposed-users-exact-locations-for-months¿.

[3] Kokalitcheva, Kia. "Tinder's Parent Company Makes an 'Oops' Filing with the SEC." Fortune Tinders Parent Company Makes an Oops Filing with the SEC Comments. Fortune, 18 Nov. 2015. Web. 15 Dec. 2015. ¡http://fortune.com/2015/11/18/tinder-match-ipo-interview-filing/¿.

[4] Dave, Paresh. "Tinder Matchmaking App Evolves to Moneymaking." Los Angeles Times. Los Angeles Times, 6 Nov. 2014. Web. 15 Dec. 2015. ¡http://www.latimes.com/business/technology/la-fi-tn-tinder-plus-20141106-story.html¿.

[5] Freier, Anne. "Tinder Mobile App Statistics and Revenue - Business of Apps." Business of Apps. Business of Apps, 21 May 2015. Web. 15 Dec. 2015. ¡http://www.businessofapps.com/tinder-mobile-app-statistics-and-revenue/¿.

[6] Veytsman, Max. "How I Was Able to Track the Location of Any Tinder User."Include Security Blog. Include Security, 19 Feb. 2014. Web. 11 Dec. 2015. ¡http://blog.includesecurity.com/2014/02/how-i-was-able-to-track-location-of-any.html¿.

[7] Tinder Inc. "Tinder - Any Swipe Can Change Your Life." Tinder. Tinder, 15 July 2015. Web. 15 Dec. 2015. ¡https://www.gotinder.com/privacy¿.

[8] Tinder Inc. "Tinder - Any Swipe Can Change Your Life." Tinder. Tinder, n.d. Web. 15 Dec. 2015. ¡https://www.gotinder.com/safety¿.

[9] Taylor, Rich. "Tinder API Documentation." Github. Github, Apr. 2014. Web. 15 Dec. 2015. ¡https://gist.github.com/rtt/10403467¿.

[10] Hatmaker, Taylor. "Is Instagram Making a Secret Map of Where You Live?" The Daily Dot. The Daily Dot, 20 Feb. 2015. Web. 15 Dec. 2015. ¡http://www.dailydot.com/technology/how-to-remove-instagram-geotags/¿.