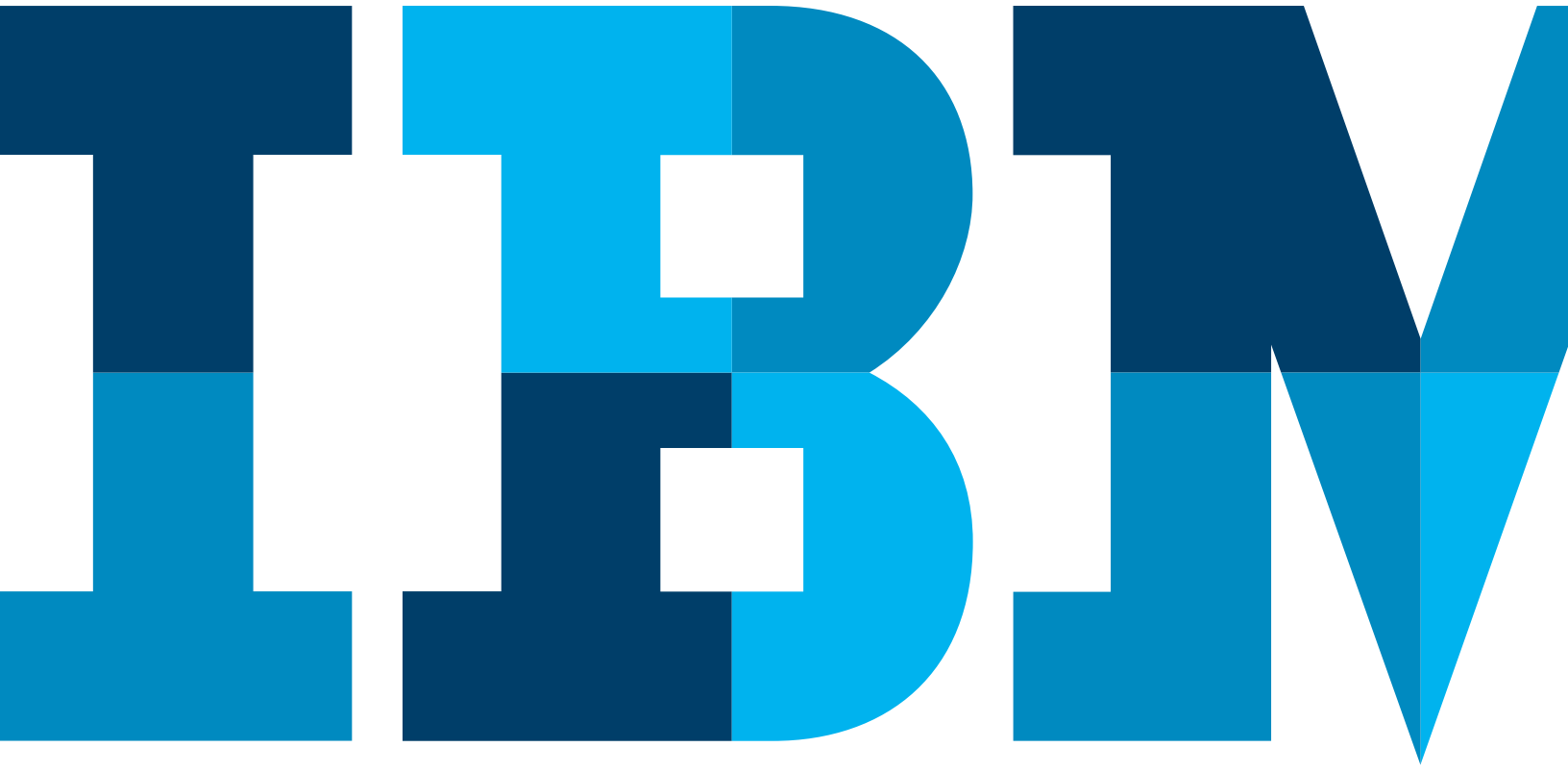
Research Paper

Feburary 2015

IBM Security Analysis: Dating Apps Vulnerabilities & Risks to Enterprises



IBM

Executive Summary

A 2013 Pew Research study revealed one in 10 Americans have used a dating site or app and the number of people who dated someone they met online has grown to 66 percent.[1] To understand the relevance of these statistics from an enterprise risk perspective, one needs to consider our current way of life. There is no longer work, then play. A few years ago, we aimed for a healthy work-life balance. Today, the goal is work-life integration. Employees multi-task work obligations between banking, gaming, tweeting, networking and yes, even dating. All this is made possible thanks in large part to the bring-your-own-device (BYOD) phenomenon.

BYOD has become popular, if not a necessity, for organizations. Employees don't want to be forced to use two phones, one for work, and one for personal, and many businesses save money by not having to purchase mobile devices for employees. Allowing employees to carry one device that combines both personal and work makes their lives easier — for everyone.

The trouble with BYOD is that, if not managed properly, the organizations might be leaking sensitive corporate data via employee owned devices. If a user has the ability to download apps from untrusted third party sites or even apps on traditional app stores, there is the potential for sensitive information such as the employee address book, phone numbers, geo location, and more to be at risk via these devices.

IBM scanned 41 of the most popular dating apps available for Android devices including apps helping users find dates via geo location or by simply swiping through different profiles.

The analysis was done based on apps available in the Google Play app store in October 2014. In advance of releasing this research to the public, IBM Security has disclosed all impacted app vendors identified with this research.

To understand enterprise user adoption of these 41 dating apps, app data was analyzed from IBM® MobileFirst™ Protect, formerly IBM MaaS360®. IBM found employees use the identified vulnerable dating apps in nearly 50 percent of the small-to-mid size businesses and large enterprises sampled for this research, leaving users open to potential cyber-attacks and threats.

In addition, the research team analyzed the permissions granted to each app once a consumer downloads it to understand what the app can access on a consumer's device. While the vulnerable apps can leak personal user information, if corporate data is also located on the device it can affect the enterprise.

Dating App Vulnerabilities and Consequences

IBM Security's research found that over 60 percent of the leading dating apps studied are vulnerable to medium and/or severe vulnerabilities that put application data, as well as data stored on the device, at risk. The vulnerabilities uncovered by IBM can affect the use of these dating apps in a number of different ways, including:

- **Integrity**: An attacker could modify data and information stored on the applications.
- **Confidentiality**: Information could potentially be leaked from the device that the application as access to.
- **Availability**: An attacker could deny user access to the application.

The specific medium and high severity vulnerabilities uncovered across the at-risk 60 percent of leading dating apps include:

- **Cross Site Scripting (XSS) via Man in the Middle (MiTM)**: This vulnerability acts as a gateway for an attacker into the app and even into other features on the device. It allows an attacker to intercept cookies and other information from the app via a Wi-Fi connection or rogue access point and tap into other device features such as the camera, GPS, and microphone that the app has access to.
- **Debug Flag Enabled**: If Debug Flag is enabled on an application, it means that a debug-enabled application on an Android device may attach to another application and read or write to the application's memory. The attacker can then intercept information that flows into the application, modify its actions and inject malicious data into it and out of it.
- **Weak Random Number Generator (RNG)**: Some dating apps use encryption with a random number generator, but IBM found the generators in these apps are weak and easily predictable. A hacker can predict the encryption algorithm and gain access to sensitive information through the dating app.
- **Phishing via MiTM**: An attacker can offer up a fake login screen via dating applications to capture your user credentials, so that when you try to log into a site of their choosing, your credentials are disclosed to the attacker without your knowledge. Then, the attacker can reach out to your contacts, pretending to be you, and send them phishing messages with malicious code that could potentially infect their devices.

The vulnerabilities identified can potentially allow a hacker to gain access to a phone's camera or microphone if the app was granted permission to these features when downloaded. An attacker can gain control of the phone's microphone as long as the dating app is running in the background and does not require that the user be logged into the app. This means an attacker can eavesdrop on personal conversations and even confidential business meetings without the user knowing.

An attacker may also be able to access the phone camera and photo library which may include sensitive, personal and embarrassing images of the user and perhaps images of confidential business proposals and plans. If an app has access to the user's camera, the user has the ability to snap a selfie for automatic upload to their profile on the site. This could also allow an attacker to take control of the camera and take unauthorized photos or videos of the user when they are not aware. This could be an enormous personal privacy violation for the user.

When a consumer downloads an application, it will ask for permission to different phone features such as GPS location, camera, media files, and address book, among others. Figure 1 below illustrates the percentage of apps that permit various access or actions to take place. Some applications will even ask for more access than required to use the app, which means consumers may be providing access to unnecessary information. This can leave sensitive information at risk via these vulnerable dating apps.

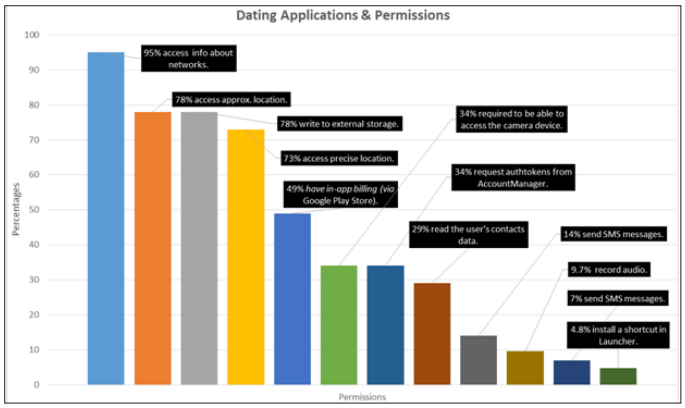


Figure 1: Dating Applications and Permissions.

Threat Scenarios for Consumers and Enterprises

A dating application's primary goal is to connect users, not protect users from cybercrime. While some apps have privacy measures in place, IBM found they are still vulnerable to attacks that can lead to the following scenarios:

In-App Phishing

Dating app users are waiting for that message from their potential love interest. Through the compromised app, an attacker can send out a notification to the user that appears to come directly through the dating app, which the user would trust. Since consumers don't expect malicious notifications from their phones—especially dating apps—an attacker can easily coax a user to share sensitive information through the app. An attacker can also potentially use the fake notification to direct a user to download malicious malware that can infect the device.

Profile Take-Over

Using stolen credentials, the attacker could log into a user's app and change their profile, send compromising messages to users and expose the user's history. If the user has any personal information regarding dating status, location, sensitive photos, or other potentially embarrassing information on their profile then the hacker can take this information and share it broadly. This could potentially affect the reputation of the true user's identify. For example, if a CEO using a dating app is hacked, then the personal messages between potential love interests or even opinions they have on other people can be leaked and lead to embarrassing press around the CEO and the company.

GPS Stalking

These apps have potential for a user to become stalked by a hacker using the geo location details. As highlighted in Figure 1 above, IBM found that 73 percent of popular dating apps studied have access to current and past GPS location information. Some apps enable very specific geo location details and they have access to determining where the user sleeps every night, works, their daily routine, etc. An attacker could cross reference this information with public data and the data in their profile and other social networks (which users can link to in their profiles), to uncover their identities. Using leaked GPS data, the attacker could re-trace a user's movements or pinpoint their current location. If someone from the C-suite had a compromised phone, and the GPS location regularly showed this individual at another company, there could be speculation of an acquisition or merger or a big deal in the works.

Fraudulent Billing

IBM found that 48 percent of popular dating apps studied have access to a user's billing information saved on their device. Many consumers save billing information into their digital wallets to make in-app purchases simply and quickly. An attacker can potentially gain access to this information through the vulnerability in the dating app and steal the information to make unauthorized purchases elsewhere.

Recommendations & Mitigations

In today's connected culture, dating apps have become a regular way to meet new love interests, but consumers looking for love have their guard down about potential cyber threats in their dating applications. People are cautious of suspicious messages in their email, but don't necessarily think twice about messages on their phone. Hackers are taking notice and looking to phone mobiles to capture information. For this reason, BYOD is an area where both security policy decision makers within the organization and employees have equal responsibility to protect personal and corporate information.

What Can Employees Do?

- **Don't divulge too much personal information on these sites**: Your work, birthday, social media profiles, etc. should remain private information.
- **Use unique passwords for every online account you have**: Using the same password for multiple sites, accounts, and platforms can leave you open to multiple attacks if one account is compromised.
- **Always apply the latest patches to your apps and your device**: This will patch any identified bugs in your device and applications, resulting in a more secure experience.
- **Conduct regular permissions analysis**: Each time your app updates, it can gain additional permissions on your mobile device. Check what all of your mobile apps have access to on a regular basis, and if you see something alarming, unclick it or delete the app entirely.
- **Review your contacts & notes on your device**: Check for things that don't belong such as passwords or notes about personal and business contacts.

What Can Business Do?

- **Put the right enterprise solutions in place**: Leverage Enterprise Mobility Management (EMM) offerings with mobile threat management capabilities to enable employees to utilize their own devices while still maintaining the security of the organization.
- **Restrict access to at-risk applications**: Understand which applications are vulnerable to attacks and take action to blacklist at-risk applications from running on a device with corporate data.
- **Educate your workforce**: Educate employees on the dangers of downloading third party applications and highly recommend employees only download applications from authorized app stores.
- **Ensure you have the right steps in place in case of a threat**: Adopt company-wide policies to take automated action and send immediate notifications to both the user and internal IT if malware is detected on a corporate device.

About This Research

IBM Security analysts from the IBM Application Security Research team used its new IBM AppScan Mobile Analyzer tool to analyze the top 41 dating apps available on Android devices to identify vulnerabilities that can leave users open to potential cyber-attacks and threats. These apps were also analyzed to determine the granted permissions, unveiling a large number of excessive privileges. To understand enterprise user adoption of these 41 dating apps, app data was analyzed from IBM MobileFirst Protect, formerly MaaS360. In advance of releasing this research to the public, IBM Security has disclosed all impacted app vendors identified with this research.

To try a free 30-day trial of IBM AppScan Mobile Analyzer, click here: http://ibm.co/1zNBl6u

For a free 30-day trial of IBM MobileFirst Protect (formally MaaS360), click here: http://bit.ly/1DG5AtF

About the author

Michelle Alvarez is a Threat Researcher and Editor for IBM's Managed Security Services; she brings more than ten years of industry experience to her role. In this role, she focuses on communications efforts regarding threat research and mitigation. Michelle joined IBM through the Internet Security Services (ISS) acquisition, where she served as an analyst on the X-Force Vulnerability Database team.

Contributors :

- Roee Hay
- Caleb Barlow
- Diana Kelley
- Michael Montecillo
- Eitan Worcel
- Neil Jones

References

Manifest.permission | Android Developers
http://developer.android.com/reference/android/Manifest.permission.html

IBM BYOD: Bring your own device
http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2015

[1] Online Dating & Relationships, Pew Research Center, Aaron Smith and Maeve Duggan, October 2013

XXX00000-USEN-00