River Kelly
CSCI-445
February 11, 2022

Problem Overview

As the level of online activity has increased, so too has the concern for privacy protection online. Anyone who uses the internet is aware, to some extent, that their online data is being tracked. Everyone knows not to login into secure accounts, like their online banking portal, while connected to an unsecured network, like one at a coffee shop. But this best practice only scratches the surface of what users endure to ensure that their privacy is protected. Those who are aware of what's really going on have turned toward the use of services like VPNs. But for the everyday-Joe, online privacy protection is not given much thought at all.

With the release of iOS 14.5, Apple introduced a new feature to allow users to disable app tracking. This new feature was a first of its kind. Built-in functionality geared toward protecting its users from third-party apps. But how monumental was this new feature? Well, during Facebooks 2021 Q4 earnings report, CEO Mark Zuckerberg directly faulted the $10 billion revenue hit to Apple's iOS changes. It can go without saying, that Facebook shareholders were not very happy with Apple. These new iOS features were just a small step towards adding further privacy protection for iPhone users. (Peterson)

Malicious apps continue to steal users' data without their permission. The newest and fastest-growing app Tiktok is being accused of doing exactly this. According to two separate audits, Tiktok has been found guilty of circumventing Apple and Googles' privacy protections. In fact, it was found that the app can completely access full user's data regardless of the user's settings specifications. (Siu)

With the ever-growing threat of attacks on users' privacy, the need for an all-encompassing solution has never been so great. Something that will once and for all stop third-party apps on mobile devices from abusing users' sensitive and personal information.

Redesign

Permission descriptions and rulesets are a crucial foundation to any computer system. It is desirable for applications to have limited access to only the information that is necessary. For example, the photo-sharing app Instagram needs permission to access the photos which are saved on your device. But, it would not be desirable for the photo-sharing app to access all of the stored photos on a user's device, or for that matter, allow the app to access a user's contacts, email, or call logs. Apple has integrated a feature for users to set specific permission for which an app can access certain photos. But what if, as previously mentioned, the app has malicious intent and circumvents the user's wishes? Currently, there is no available option for a user to completely control an app's privy information to user data on their device.

When it comes to best practices in information security it is essential to clearly establish permission accessibility and boundaries. This can be done by isolating a program's (or apps) modular components. This is exactly how my solution would attempt to tackle the problem of bad-faith actors and malicious apps. To ensure that a user's personal information is protected, that app would be isolated from the private data stored on the device. Not physically, of course, but virtually. Imagine that when opening an application on your iPhone, a virtual container is created and the program is executed within this container. Essentially creating a barrier between the running application and the data on the device. This practice is already commonplace in many areas of the computing industry.

When a developer is working with potentially harmful software, they can install a Virtual Machine (VM) container to safely execute any application. This limits the worst-case scenario to be; the software exploits the Virtual Machine container without affecting the core system in any way. Another benefit to this implementation is that the user can completely shut off the applications container at any time. This is useful because this would eliminate any background application activity that may be taking place. For example, who knows what the Facebook application is really doing in the background when the app is not actively in use. It may be constantly recording your location.

Measurement Strategy

To determine the improvement of efficiency, health/safety, and worker satisfaction, two separate examinations would need to be completed; objective and subjective studies. The results would be compared to before the user installed the new software features, known as the baseline.

Objective

Data analysis would be done to examine the privy information available to the app running within the virtual container. First, the direct data would be examined. This would determine exactly what information the app can access. This would entail an analysis of exactly what permission is granted to the virtual container. The second would be an analysis to examine the network data. Typically, any useful application is supported by a backend, where database information is stored. This analysis would be to examine what information is contained within communication between an application and the backend server. The success of these two analyses would be such that only the exact personal information, to which the application is provided permissions, is accessible.

Subjective

The user of such a software feature would be given a survey before and after installing the app container integration. A user would be asked how safe they felt their personal information is,

how much they trust certain applications on their phone, and to what extent they are knowledgeable of privacy protections. The users would then be informed of how previously their device did not support such protection and provided an explanation of how the new feature worked. A follow-up survey would be given asking the user if; they felt safer with the new integrations, if they were unaware of how vulnerable they previously were without the new software, and if they believe that such technology is desirable.

Human Tech-Ladder

Physical: To implement this solution, iOS developers would need to integrate this functionality into the core system itself. Essentially, upon launching each app installed on the device would then create a new container and execute the app within this container. Therefore, creating separation between a user's personal data and the running application.

Psychological: The most likely scenario is that the majority of users are unaware of the danger to thier private information. The psychological goal would be 'peace of mind'. Society has likened ease of use over protection. The primary example of this would be confirmation everybody has agreed to: "I have read the terms and conditions". These agreements have become so long, it has become too time-consuming to thoroughly read and the user actually has no idea what it is they are agreeing to.

Team: One of the main issues with trusting applications is that you have to trust the authority of the organization that provides such systems. For a successful implementation of this software integration, it would need to be open-source. This way, everyone has the ability to be knowledgeable of the softwares potential. If such a feature were accessible to the public, malicious intent could be identified and addressed.

Organizational: The maintenance of such a service would be similar to that of a free-to-use Linux distribution. There would be a specified organization that oversees implementation and distribution, but similar to many Linux kernels, open to contribution from the public.

Political: The political implication of this is massive. The government is always creating new laws. Laws typically exist to provide protection to its citizens. Currently, the scope is very broad considering laws protecting online privacy. With the integration of such a feature, new laws outlawing certain malicious practices would not be necessary. This is because these potentially illegal actions would not be possible if they were eliminated at the source.

Works Cited

Peterson, Mike. “Facebook will take $10 billion revenue hit in 2022 because of App Tracking Transparency.” *AppleInsider*, 3 February 2022, https://appleinsider.com/articles/22/02/03/facebook-rebuilding-ad-platform-due-to-app-tracking-transparency-data-laws. Accessed 14 February 2022.

Siu, Antoinette. “TikTok Can Circumvent Apple and Google Privacy Protections and Access Full User Data, 2 Studies Say (Exclusive).” *The Wrap*, 14 February 2022, https://www.thewrap.com/tiktok-circumvent-privacy-protections-user-data/. Accessed 14 February 2022.