Jeremy Hellmer
SE 4930 001
12-14-11

Article Review #1

Mobile Attacks and Defense

If you go out on the street and ask anyone what a phone is, they will be able to provide you with an answer. However, their answers may contain slight variations. This is because the scope of the functionality of a phone has been drastically changed in recent years. In the past, a phone was used solely as a communications device. It was a way of talking to people who were not present in the same location. In today's technologically advanced world, however, a (smart) phone can not only be used to place phone calls but can perform many other functions, including functions typically performed by computers.

Because of this advanced level of functionality, they have become a more desirable target for malicious attackers. The added features of the phone provide more avenues for the attacker to exploit. In addition, these additional features place more information which would be desirable to an attacker on the phone. To combat this new attractiveness to hackers, developers of phone operating systems, such as Google and Apple, are forced to take a second look at security and how they are ensuring their systems are secure.

There are two main types of attacks of which phone developers need to be made aware. The first is mobile malware. Both of the operating systems being examined, iOS and Android, provide phone owners with protection against mobile malware. However, the two systems achieve this goal with different approaches.

Apple chose to use an App Store which they have strict control over. All apps must be approved prior to being placed in the store. While it is unsure how closely these apps are inspected prior to approval, this step does eliminate obvious malware. If it is approved, Apple places a code signature in so that the phone running iOS knows this is a safe app and proceeds with the download. This process also restricts users to only purchase apps through the store. Apple also employs the use of sandboxes to run their app, limiting what information a running app can access. However, each sandbox is given the same permissions, regardless of what is running in it.

Google also has a store which is called the Android Market. However, no approval is required to place an app in the store, allowing all developers to directly place their apps into the store. Because the apps do not need to be approved, it is also possible for users to download apps outside of the store. Google like Apple still has the ability to remove an app if complaints are received. Google also uses the idea of sandboxes. However, each sandbox is given a different set of permissions based on what app is running. Users are informed what these permissions will be during installation so that they can cancel if they do not want to divulge that information. However, at that point the user has probably made up their mind about wanting to purchase the app and will simple breeze over that screen.

The second type of attack would be to find and exploit vulnerabilities. This includes exploits similar to those on computers but also on the SMS messaging and GSM radio services that are unique to phones. Different measures have been taken by the operating systems to prevent these attacks.

iOS prevents exploitation by using a layered approach. It uses data execution prevention and address space layout randomization to hinder an attacker from being able to differentiate between data and code, preventing them from being able to find what they are looking for. Restrictions are also put into place to limit the damage that can be done by a successful attack.

Android continues to rely on its sandbox approach in this situation. This prevents an attacker to get to other data on the phone even if they compromise and application. In addition, the fact that most of Android's apps are in Java prevents memory corruption vulnerability type attacks.

From this article, I learned that as phones advance they not only become more functional but also become more vulnerable. For this reason, security is very important. The security concepts and ideas that are often put into place on computer systems need to be transferred over and used on phone systems as well. If this is overlooked, a major security problem could develop.

Works Cited

Miller, Charlie. "Mobile Attacks and Defense." *IEEE Security and Privacy* (2011): 68-70. *Http://www.computer.org/portal/web/security*. Web. 14 Dec. 2011. <http://www.computer.org/cms/Computer.org/ComputingNow/homepage/2011/1011/W_SP_MobileAttacksandDefense.pdf>.