HOW HAS THE NEED FOR CYBERSECURITY CHANGED WITH INCREASED USE OF SMARTPHONES?

Deidre McClellan, Regent University, USA (deidmcc@mail.regent.edu)

Young B. Choi, Regent University, USA (ychoi@regent.edu)

ABSTRACT

Smartphones are being used more often in today's society. They are frequently treated as if they were miniature computers. In some cases, they share the same capabilities. With this increase in the use of smartphones, more personal information is put at risk of being compromised. Smartphones are used for more than just making phone calls. "Devices can be used as consumption points, thus replacing dedicated devices or special media" (Wallin, Jones, Weldin, 2015). There are applications for Office Suites such as Microsoft that are available for download to a smartphone. With these apps, statistics such as location can be viewable to outside audiences. Consumers are storing banking account numbers and have passwords saved into browsers. There is a wealth of data on a smartphone that can be gathered by someone with ill intentions. There is even a risk of trade secrets and other company confidentiality getting into the wrong hands. Many businesses are instituting "Bring Your Own Device" programs at the workplace. With more employees conducting business on their smartphones, companies are leaving themselves exposed to information breaches. All of these factors have contributed to the need for more cyber security. There need to be more methods in place for the protection of consumer information. Private businesses would also find it advantageous to invest in cyber security measures to protect themselves.

Keywords: Cybersecurity, Smartphone, covert channel, jailbreaking, anti-virus software

INTRODUCTION

Unlike older mobile phones, modern smartphones are becoming handheld computing and communications devices that support multimedia communications and applications for entertainment and work (He, Chan, & Guizani, 2015). As a society, we are becoming more dependent on involving smartphones in our everyday activities. Smartphones are used for activities such as online banking, appointment scheduling, video conferencing, and game playing. There are smartphones that even have built in Artificial Intelligence features that serve as a personal assistant to the user. With the sophistication of these devices continuing to grow, so are the security breaches that they can expose us to.

The ease of use that comes with the smartphone also gives those with malicious intent an easy path to your personal information. Popular applications that are downloaded to smartphones can be used against you. Built in features such as location services can turn your phones into a tracking device. Trends such as jailbreaking devices also leave smartphones more susceptible to getting a virus. With more vigilance on the part of smartphone users to protect themselves and more focus put into the development of mobile cyber security, these issues can be avoided.

APPLICATIONS, FRIEND OR FOE

Mobile applications or "apps" as they are sometimes called, can be the most exciting and useful highlight about smartphones. There are apps for productivity and apps that are used just for fun. Both of these can come with their own dangers. For example, many banks now have their own apps. With the Navy Federal app, you can transfer funds, look at your credit score, and take pictures of checks to make deposits (Android, 2017). If you connect your credit card to another app like Android Pay, you can even use your phone as a credit card. Imagine if someone were to still your phone? You would be handing them all of your financial information on a platter.

Losing your phone is not the only thing to worry about because it is not the only way to gather such intel. Applications themselves are becoming compromised every day. Just downloading them onto your phone could be inviting trouble. There can be more than one malicious app on a phone and those apps can "talk" to each other and launch an attack on an unaware user. Android based devices have tried to develop ways to circumvent that kind of threat. "The operating system uses security policy based permission model to provide specific access permissions to shared resources" (Chandra, Lin, Kundu, & Khan, 2014, p. 1). However, there are times where a loophole is found and a smartphone user still falls victim to a cyber crime.

COVERT CHANNELS

A malicious app can retrieve a user's personal information and transfer it to a server over the internet. It can do this by going through another malicious app that existed prior on a user's phone. There could be one app that has requested and been given permission to retrieve the user's personal information but denied access to the internet. Meanwhile, there is another app that has permission to access the internet, but not to store personal information. These two apps can be used to communicate with each other, share records, and override the permissions protocol that the Android OS has put in place. This storing method is virtually undetectable to the user. "The number of malware in apps has increased by 614 percent since 2012" (He, Chan, & Guizani, 2015).

BUILT IN FEATURES CAN GO ROGUE

A new disturbing trend in smartphone related cyber crime is surveillance attacks. A surveillance attack happens when "a specific user is under surveillance by means of his/her infected smartphone, making use of the built-in sensors" (He et al, 2015, p. 139). Smartphones are equipped with elements such as GPS sensors, cameras, and microphones. If targeted by the wrong person, those elements can be used against the owner of the smartphone, thus putting that person under surveillance. Any expectations of privacy are lost. Aggregation of GPS data alone "permits a third party to discover his or her eating preferences, political agendas, religious beliefs or even sexual habits" (McKinnon, 2014).

CAMERAS CAN BE A GATEWAY

Even if you do not have your camera in use, it is still not safe to assume that it is turned off. "Researchers demonstrated how an attacker can use reflections in the user's face to perform keylogging with a smartphone's front camera" (Storm, 2014). A hacker can use this to their advantage to see what it is that you are typing into your phone. They can figure out what your password is to your email or other sensitive accounts. A pin number to your bank account or could also be easily retrieved. All of this can be collected because you held your phone too close to your face when you used it.

Phone brands such as Samsung use the rear facing camera to take your pulse through a finger scan. A cyber criminal could just as easily use that same rear facing camera to steal a copy of your finger print scan. That stolen scan can be duplicated over and over for their own purposes. Just think of the far-reaching consequences if this happened to someone with a high-level security position that involved the use of finger print scans. Small breaches like this can lead to bigger payoffs later for a cyber hacker.

The camera on a smartphone can also be used to take pictures without your knowledge. In 2012 the military demonstrated how easy that could be by creating an Android app called PlaceRaider. "The sensory malware covertly taps into the phone's camera to capture photos which attackers can stitch together to recreate a 3D image of the victim's surroundings and then steal any sensitive information in view" (Storm, 2012). More companies are instituting "Bring Your Own Device" like policies. With malware like PlaceRaider, you are setting your own company up to be bugged and put under surveillance. The consequences of the uses for such would be endless and devastating. Employees of a bank could inadvertently provide blue prints for the building so that it could be robbed later. Executives could have trade secrets stolen because pictures of prototypes and contracts were taken.

JAILBREAKING AND ROOTING CAN LEAD TO EXPOSURE

Smartphones come with pre-existing limitations. Jailbreaking removes restrictions on iOS devices while rooting is the process to remove restrictions on Android devices. "Jailbreaking allows root access to system files that can be manipulated to enable installation of apps, themes, and extensions that are not supported by Apple or unavailable for download on Apple App Store" ("Jailbroken Device", 2017). Rooting Android phone does the same thing, by getting to the root of your system. This may seem like a clever way to get the most out of your phone, but it is very dangerous. "Jailbreaking smart phones bring vulnerabilities to the operating system" (He, Tian, & Shen, 2015, p. 3).

When you jailbreak or root your phone, you are taking away some of the protections that the manufacturer had in place for you. Not only are you removing restrictions for yourself, you are removing the restrictions that would have protected you from worms, viruses, and other hacking techniques. Any privacy that you had before is taken away.

Hackers can easily pull files right out of your phone. There are even tools that have been created to scan Wi-Fi networks and search for jailbroken iPhones (Castillo, Matos, Chavez, Figuera, Cordon, & Pons, 2014, p. 3).

LACK OF ANTI-VIRUS SOFTWARE

There are apps available that may appear to have anti-virus software, but they do not. For example, companies like McAfee, Symantec, and Trend Micro have apps but they are not there to provide virus protection. Instead, "they focus on helping you find lost devices, backing up your data, securing your web browsing, and protecting your privacy" (Costello, 2017). While the service these companies provide is valuable, more needs to be done. With this lack of basic protection, users need to be more vigilant about how they use their phones. It would not be a good idea to do anything to a smartphone that would leave it more vulnerable to getting viruses.

GETTING PROACTIVE ABOUT CYBER SECURITY

"556 million people each year become victims of internet crimes" (Kohar, Riadi, & Lutfil, 2015, p. 2). That kind of substantial number cannot be ignored. Smartphone users need to educate themselves and become more aware of how cyber crime on smartphones can occur. They need to know what can specifically leave themselves open to attacks. In the case of malicious items running in the background, they may be leaving themselves open to repeat attacks.

Smartphone users also need to be more familiar with what access rights their applications have. When downloading anything new, users should carefully review the permissions that the application is asking for and deny those they do not feel comfortable with. They should also be sure that they are downloading from a trusted source. To protect against the fallout of a malicious app, one should "systematically analyze the properties of various shared resources on an Android system and evaluate their use as possible covert channels for establishing communications between two malicious apps installed on the same device" (Chandra et al, 2014, p. 3). It would also be ideal to do periodical malware checks on their devices.

One of the most important things that a user can do is use strong passwords. Complex passwords should be used on all email accounts, financial websites, and even the physical phone itself. To stay ahead of keylogging attacks, users should also get into the habit of changing their passwords on a regular basis. Another way to prevent smartphones from being used as a surveillance tool is to get into the habit of turning off location reporting. "Location Reporting feeds your location data to various apps, while Location History stores your whereabouts for future use in searches and software like Google Now" (Aciman, 2015).

Even Google Maps store a history of where you have been and the locations that you frequent. While turning off location reporting is helpful, it is by no means a cure all. Wi-Fi networks and cell phone towers can still track your whereabouts and report it back to companies like Google and Apple ("Disable Tracking", 2013). This makes it even more imperative to use secure Wi-Fi networks, unlike some of the unsecured ones that are available to the public.

It may be an attractive idea to jailbreak or root your phone, but you should refrain from doing that. To preserve the maximum amount of protection on a smartphone, the user should not alter it. iOS and Android devices have systems in place to protect their consumers. When a user tries to bypass the restrictions that have been put in place, they destabilize the system that was designed to safeguard them. Not to mention it is also an effective way to void your warranty, thus finding yourself without an additional backup in case something should go awry on your phone.

CONCLUSION

Smartphones are a great piece of technology to have in your arsenal. Gone are the days of phones only being able to make calls. They are now mobile computers that we can take anywhere and use for almost anything. Various smartphone brands and models are flooding the market. Newer phones are constantly being released. Operating systems are updated on an almost weekly basis.

The availability of these constant improvements has not deterred those with malevolent objectives. Such people have ramped up their efforts to stay on top of infiltrating modern technology. There are now more ways than ever to have your personal information that of those around you to be stolen. Applications that are downloaded to smartphones from the iTunes Store or Google Play Store can be infected with worms and Trojan Horses. The seemingly innocent software on your phone can collaborate and lower your defenses. They can work together to launch an all-out assault on your phone and your records.

Built in features such as location services can turn our phones into a trailing device. There is a mounting appeal in jailbreaking phones and getting around precautions set by phone manufacturers. The accessibility of directions on how to do it only encourages this rise. This trend toward jailbreaking and rooting only leaves smartphones more susceptible to getting a virus. The more access you seek to have on your phone, the more access you are granting to someone from the outside that should not have it.

Phone manufacturers and anti-virus companies are trying to stay ahead of the game. Ultimately the responsibility falls on the user to protect their own data. You cannot protect yourself against what you do not know about. Staying abreast of current viruses and methods of using smartphones for corrupt purposes is important. It would do well for a user to be familiar with what their apps do and what permissions they need to do it. Just like you need a regular checkup, so does your phone. You should make it a routine to check it for viruses and other hazardous content.

Passwords should not be easy letter and number combinations. Nor should they be the same for everything that you use. Passwords should be difficult to figure out. They should also be updated on a regular basis. In many cases, an excellent password is your first line of defense.

Users should make it a practice to regularly turn off what they are not using on their phones, such as Location Reporting. They should also continuously clear items such as location histories, voice histories, and search histories. Just as crucial is being mindful of what Wi-Fi network you are on. Not all public hotspots can be trusted. Many of them are used to specifically find and exploit weak devices.

Phones and the software that they come with should not be manipulated. They should not be altered, especially if you are not sure about what you are doing, or you are unprepared for the future calamities. Jailbreaking and rooting phones just leaves the door open for trouble. It is just one messy incident that is waiting to happen. Being content with what your phone can already do and sticking with that can help you to avoid a huge problem later.
Smartphones are not going anywhere and they should not. They have enhanced our lives in many ways. They make it easier to keep in touch and stay productive. We can continue to enjoy them if we stay aware of their potential to be used to do harm. As long as we take the right precautions, smartphones will continue to enhance our lives and make them easier.

REFERENCES

Aciman, A. (2015, February 20). How to Stop Your Phone From Tracking Your Location. Retrieved August 11, 2017, from http://time.com/3716950/location-tracking-turn-off/

Android™ Mobile Banking App. (n.d.). (2017) Retrieved August 10, 2017, from https://www.navyfederal.org/mobile/android.php

Castillo, A., Matos, R., Chavez, W., Figuera, L., Cordon, P., & Pons, A. (2014, August) Mobile Malware.

Chandra, S., Lin, Z., Kundu, A., & Khan, L. (2014, September). Towards a systematic study of the covert channel attacks in smartphones. In *International Conference on Security and Privacy in Communication Systems* (pp. 427-435). Springer, Cham.

Costello, S. (2017, July 13). Can iPhones Get Computer Viruses? Retrieved August 11, 2017, from https://www.lifewire.com/is-it-possible-iphone-virus-1999742

Disable tracking settings on phone: How your phone's operating system buries ad, tracking settings. (2013, November 27). Retrieved August 11, 2017, from http://www.abc15.com/news/science-tech/disable-tracking-settings-on-phone-how-your-phones-operating-system-buries-ad-tracking-settings

He, D., Chan, S., & Guizani, M. (2015). Mobile application security: malware threats and defenses. *IEEE Wireless Communications*, *22*(1), 138-144.

He, W., Tian, X., & Shen, J. (2015). Examining Security Risks of Mobile Banking Applications through Blog Mining. In *MAICS* (pp. 103-108).

Jeannot, C. (2016, July 14). Mobile Security vs Computer Security. Retrieved August 10, 2017, from https://www.linkedin.com/pulse/mobile-security-vs-computer-c%C3%A9dric-jeannot-phd

Kohar, A., Riadi, I., & Lutfi, A. (2015). Analysis of Smartphone Users Awareness Activities Cybercrime. *International Journal of Computer Applications*, *129*(2), 1-6.

McKinnon, A. (2014). Sacrificing Privacy for Convenience: The Need for Stricter FTC Regulations in an Age of Smartphone Surveillance. *J. Nat'l Ass'n Admin. L. Judiciary*, *34*, 484.

Storm, D. (2014, August 20). New attacks secretly use smartphone cameras, speakers, and microphones. Retrieved August 11, 2017, from http://www.computerworld.com/article/2598704/mobile-security/new-attacks-secretly-use-smartphone-cameras--speakers-and-microphones.html Wallin, L., Jones, N., & Weldon, L. (2015, March 20). Mobile Is a Critical Component in a Digital Business Strategy: Use This Framework to Identify Opportunities and Threats. Retrieved June 30, 2017, from https://www.gartner.com/doc/3011418?ref=ddisp

Storm, D. (2012, October 04). Visual malware remotely exploits Android camera, secretly snaps pic every 2 seconds. Retrieved August 11, 2017, from http://www.computerworld.com/article/2473131/malware-vulnerabilities/visual-malware-remotely-exploits-android-camera--secretly-snaps-pic-every-2-.html

What is a Jailbroken Device & What Does Jailbreaking Mean? (2017, June 06). Retrieved August 11, 2017, from https://www.cleverfiles.com/howto/what-is-jailbroken-device.html