Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.7, No.6, 2017

Comprehensive Overview of Security Issues in the Internet and Mobile Applications

Saif Uldun Mostfa Kamal
Department of Technical Computer engineering, Iraq University College, Basra, Iraq

Abstract
The popularity and advanced functionality of mobile devices have made them attractive targets for malicious and intrusive applications. Although strong internet security measures are in place for most mobile systems, the area where these systems often fail is the reliance on the user to make decisions that affect the security of a device. In our prime example, Android relies on users to understand the permissions requested by an application, on which depends its installation decision on the list of permissions. Previous research has shown that this reliance on users is ineffective, as most users do not understand or considerate permission information.
Keywords: Internet Security, Mobile Applications, Mobile Security, Security Issues

1. Introduction

People who rely on the Internet do so for different reasons. However, many enjoy the opportunity to quickly and cheaply keep up with friends and loved ones via e-mail, while others love the vast oceans of information or the rush they get from playing Internet games [1]. Whereas, the most Internet users do not think about computer security. Although this is understandable, it can be a costly mistake. When you log onto the Internet, you step into a public arena. Thus, it is important to remember that surfing the Internet comes with certain inherent risks. However, in recent years, smart mobile devices have become pervasive. More than 50% of all mobile phones are Smartphone's, and this statistic does not account for other devices, such as tablet computers that run similar mobile operating systems [2]. According to Google, more than 400 million Android devices were activated in 2012alone [3]. Android devices have widespread adoption for both personal and business uses. From children to the elderly, novices to experts, and in many different cultures around the world, there is a varied user base for mobile devices. However, the ubiquitous usage of these mobile devices poses new privacy and security threats.

Our entire digital lives are often stored on these devices, which contain contact lists, email messages, passwords, and access to files stored locally and in online databases. Possible access to such personal information by unauthorized parties puts users at risk; and this is not where the risks end. These devices include many sensors and are nearly always with us, providing deep insights not only into our digital lives but also our physical, offline lives. The GPS unit can tell exactly where you are, the microphone can record audio, and the camera can record images. Additionally, mobile devices are often linked directly to some monetary risks, via SMS messages phone calls and data plans, which can affect a user's monthly bill. Moreover, mobile devices can also be used to authenticate bank access or directly link to a financial account through a "digital wallet." This easy access means that any application (henceforth called "app") running on these devices has the potential to tap into certain private information. In the benign case, the access is performed to provide useful functionalities, but in other scenarios, it may be used to collect a significant amount of personal information and even as a means to have some adverse impact on a user. Furthermore, the line between benign and malicious is often fuzzy, with many apps falling into gray areas where they may be overly invasive though not malicious [4]. Compared with desktop and laptop computers, mobile devices have a different paradigm for installing new applications [5]. For computers, a typical user installs relatively few applications, most of which are from reputable vendors, with niche applications increasingly being replaced by web-based, or cloud services [6] . In contrast, for mobile devices, a person often downloads and uses many apps from multiple unknown vendors, with each app providing some limited functionality. Additionally, all of these unknown vendors typically submit their apps to a single, or several app stores [7], where many other apps from other mobile security vendors may provide similar functionality, different commercial services as shown in Figure 1. Therefore, the different paradigm requires different approach in dealing with the risks of mobile devisees well as offers distinct opportunities.

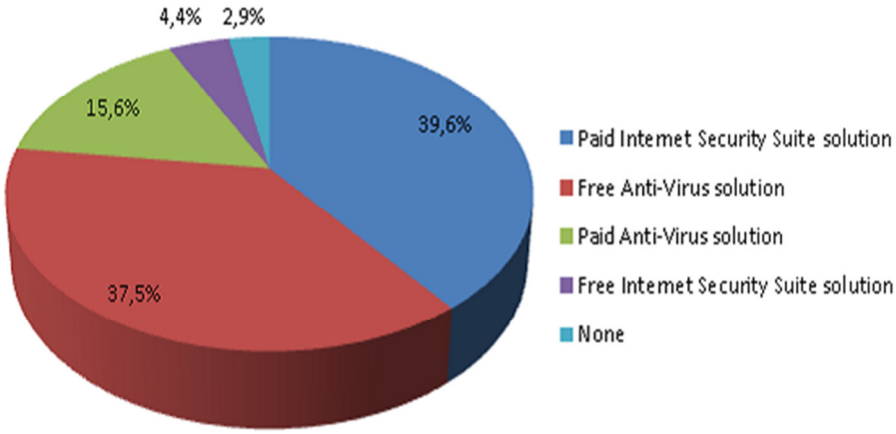

Figure 1: Mobile Security Solution

2. Internet security

A decade ago, the Internet was something just "techies" discussed. It was new boundless wellspring of data, with not very many users [8]. Today, the Internet has as of now turned into a vital piece of our lives. It's the place we get to our saving money records, financial records, expense forms and other profoundly delicate individual information [9]. Before this current decade's over, more than 2 billion individuals will be joined with the Internet that is about a large portion of the world's present populace. On the other hand, with all the great things the Internet offers us, it additionally opens the way to genuine, conceivably destroying dangers. Not at all like corporate and government PC frameworks, have couple of PCs had any shields past essential infection insurance. That implies at whatever time you're on the web, you are a potential focus for online hoodlums and programmers. What's more, in the event that you have fast Internet get to, your PC is online more often than not, making Internet crooks and programmers a 24-hour-a-day, year-round danger to you, your own data, and your family. Treats, pop-ups, and adware are devices that track your online conduct, and are utilized to advance different items. Numerous treats are innocuous online data assembling and following apparatuses. The dominant part of adware comprises of pop-up advertisements that are only spontaneous irritations. The issue is that programmers and online hoodlums are progressively utilizing treats and adware to unobtrusively sneak onto your PC and to get to your own data without your insight. This "spyware" watches and records all that you do internet, leaving your passwords, private record data, and other individual and delicate data defenseless. Once caught, this data can be sent back to online hoodlums for utilization in getting to your private data, taking your character, and your cash. It can likewise be utilized to highjack your PC for unlawful purposes. Spyware finds its way to your PC through:

- Web sites you browse on the Internet.
- Adware and pop-ups that load onto your PC.
- Results of your Internet searches.
- Unusual ecommerce sites you visit.
- Software you download onto your PC from the Internet.
- Weaknesses within the operating system software you are utilizing.

Clearly, the great majority of users are interested in on-demand malware file detection rate tests, followed by the Whole-Product Dynamic “Real-World” Protection Test, as well as proactive/retrospective tests that evaluate heuristics and behavior-blocking capabilities, to name a few, when offline. However, if product does not include a file detection capability then we would not test that product for it. Over half of the survey participants found both performance testing, and malware removal to be valuable. However, IPSec also incorporates an anti-replay mechanism. According to IPSec, a unidirectional security association can be established between any two computers in their network (source and destination) [10]. The source keeps a counter for the sequence numbers used for sending messages, and includes the current value of the sequence number with any messages sent. The destination uses a sliding window to determine whether a received message is a normal or replayed message. If the sequence number of the received message is less than the number represented by the left edge of the window, the message is regarded as a replayed message and is discarded by the destination. If the sequence number of the replayed message falls inside the window, the destination can determine whether the message is a replayed message or not by checking the information kept in the window. If the sequence number of the received message is larger than the number represented by the right edge of the window, the message is accepted as afresh message and the right edge is made equal to the received sequence number. This method, although effective, can result discarding of good messages.

Table 1: Summarization of Internet Security Attacks

Category	Type	Attacks	Solutions	Remarks
DNS hacking	All	All	DNSSEC [11]	Assumes secure client/server, no security against leakage
Routing table poisoning	Link	Interruption	Acknowledgments [14, 15]	Attack has limited significance
		Modification/fabrication	Digital signatures [14]	Excessive overhead in distance vector protocols, assumption that PKI exists
		Replication	Sequence numbers [14, 15]	Updates within the same time period can be replayed (limited effect)
	Router	Link state	SLIP [19]	Assumes symmetric network and no collusion
			JiNaO [7]	Not scalable
		Distance vector	Consistency checks [8]	Unable to detect consistency attacks
Packet mistreatment	Link	Interruption	WATCHERS [9], packet profile [20]	Not scalable
		Fabrication/modification	IPSec [21]	High complexity
		Replication	IPSec	Unnecessary dropping of good packets
DoS	All	All	Filtering [10, 23]	Can prevent limited attacks
			Link testing [12]	Not scalable, may be a tool for DoS attacks
			Logging [13]	Not scalable
			ICMP traceback [24]	May be used as DoS attack
			IP traceback [25, 26, 27]	Not complete, still evolving

3. Mobile Security

Smartphone's are changing into a lot of integrated and prevalent half of individuals' daily lives because of their highly powerful computational capabilities, like email applications, on-line banking, on-line searching, and bill paying. With this quick adoption of good phones, imminent security threats arise whereas communicating sensitive personally identifiable data (pii), like checking account numbers and master card numbers used when handling and performing those advanced tasks. Traditional attacks (worms, viruses, and Trojan horses) caused privacy violations and disruptions of important software applications, for instance, deleting lists of contact numbers and private information. Malware attacks on Smartphone's were typically "proof of concept" makes an attempt to interrupt to the phone's system and cause harm. However, the new generation of Smartphone malware attacks has increased in sophistication and is intended to cause severe monetary losses (caused by identity theft) and disruption of important software applications. As a result of Smartphone's are turning into a lot of various in providing general purpose services, for instance, instant messaging and music, the impact of malware might be extended to incorporate draining batteries, incurring further charges, and bringing down network capabilities and services. Theoretical framework smart phones are rapidly becoming enriched with confidential and sensitive personal information, such as bank account information and credit card numbers, because of the functionality and powerful computational capabilities built into those mobile devices. cyber criminals, in turn, launch attacks especially designed to target Smartphone's, exploiting vulnerabilities and deficiencies in current defense strategies built into Smartphone's' operating systems indicated that because mobile app security refers back to the extent of protection of mobile device apps from malware, also because the activities of crackers and different criminals [11]. The term will additionally check with varied technologies and production practices that minimize the danger the chance of different entities exploiting the mobile devices through their apps. A mobile device has various elements, they all susceptible to security weaknesses [12]. The elements are created, distributed and utilized by multiple players, every of whom plays an important role in making certain the safety of a tool. Every player ought to incorporate security measures into mobile devices as they're designed and designed and into mobile apps as they're conceived and written; but, these tasks aren't perpetually adequately administered. Common vulnerabilities for mobile devices embrace architectural flaws, device loss or theft, platform weakness, isolation and permission issues, in addition to application weakness [13]. When evaluating mobile devices and apps for security, developers should ask themselves the following questions:

- How do clients get a specific application?
- Should a firm produce its own particular application store?
- How is an application verified before it's offered for sale?
- How is an application protected against malware?

- Was a specific application written and shipped in an excessive amount of a rush?
- How will clients tell the distinction between a genuine application and a pretend one?
- How simply will automatic update options get hijacked?
- What measures exist to manage the danger of device jail breaking?
- What sort of permissions ought to a specific application request?
- Can any of the functions and capabilities distinctive to mobile devices (like geo location) enhance application security?

However, to illustrate the security application for mobile. Figure 2 shown the most security applications.

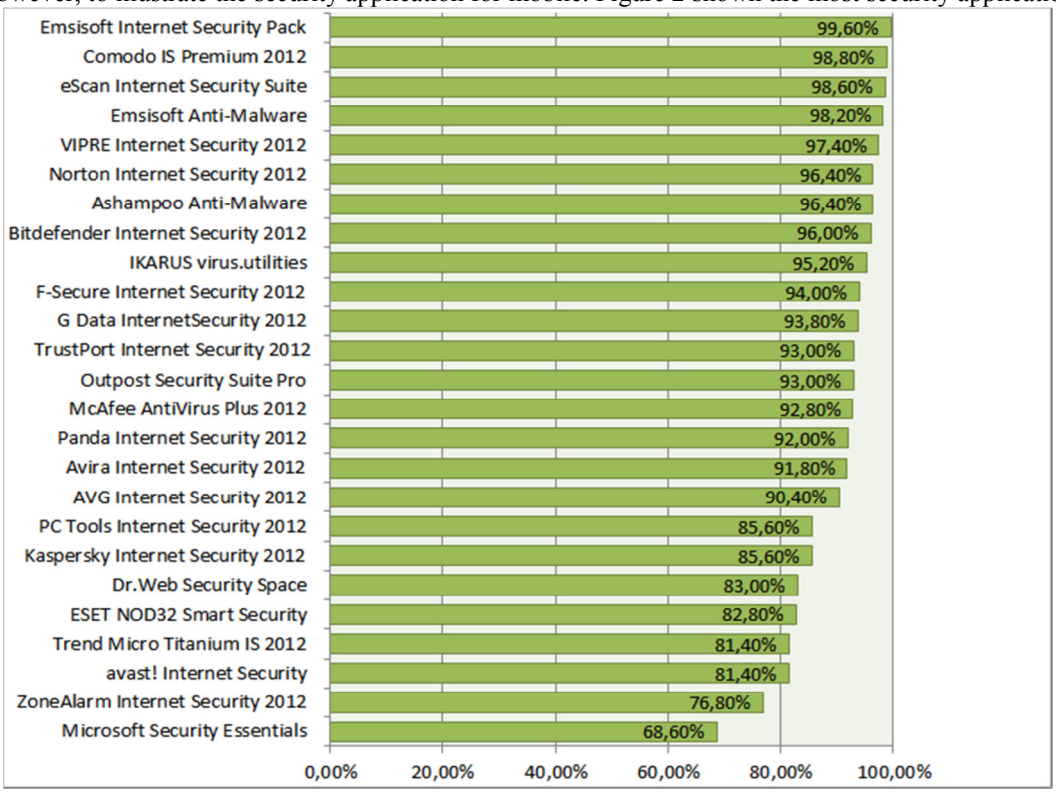

Figure 2: security software trend for the mobile apps

Meanwhile, the biggest concern of the mobile apps security can summarized at figure 3. Not surprisingly, usability, scalability, reliability, and performance are considered more important than application security. This may reflect both the importance organizations place on performance of all applications and the level of management that does not yet appreciate the consequences of non-secure applications. Next, we need to look at what organizations are doing to ensure the security of their systems, data, and users. The security practices are fairly evenly split among the various phases of the software development lifecycle (SDLC), with a secure lifecycle being the highest chosen among them overall. No more than 50% chose another practice; but for those developers, or the organization that supports them, they are evenly focused on dealing with security issues during coding and development.

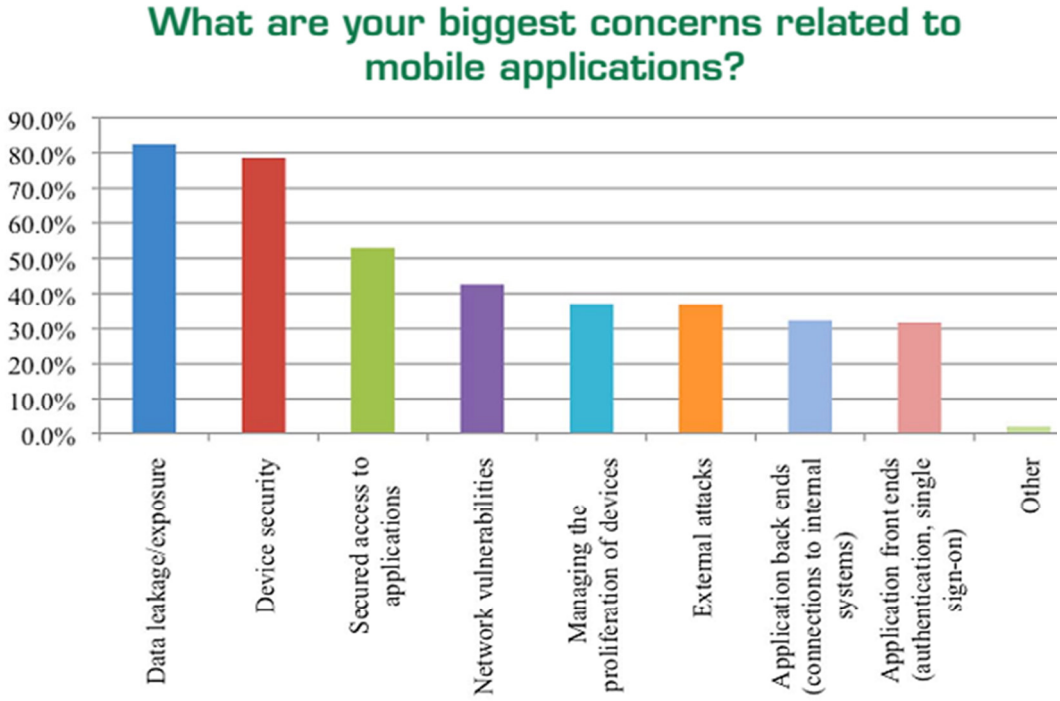

Figure 3: Mobile apps security concerned

4. Conclusion

Sensitive Information Leakage (inadvertent or aspect channel)-This refers back to the explore for references of sensitive information that's then utilized in network communications; alternatively, it refers to observe network traffic to work out what information are being sent. But, Unsafe Sensitive Information Transmission- This refers back to the explore for sensitive information being transmitted in HTTP requests or over SMS/E-mail, that appearance for insecure ways of making communication channels, like disabling certificate checking. And hardcoded Password/Keys- This refers back to the explore for variables or strings that seem for use for authentication or authorization functions. Validated authentication procedures don't use hardcoded values or cryptographic information (keys/salts). While, as organizations and their workers still rush down the trail of implementing and using mobile devices and apps, security wants| to continue to concentrate on our implementations. This is turning into each easier however a lot of troublesome as time goes by. The rush to implement or build mobile applications exacerbates the complexity of security problems that IT personnel should address. This suggests that account able workers members must be on high of the most recent threats and controls offered to the attackers and defenders. Proactive security throughout development and deployment ought to become a best observe.

References

[1] CASEY, W., MORALES, J. A., NGUYEN, T., SPRING, J., WEAVER, R., WRIGHT, E., METCALF, L. & MISHRA, B. 2014. Cyber Security via Signaling Games: Toward a Science of Cyber Security. Distributed Computing and Internet Technology. Springer.

[2] ROBERTS, J. R. 2014. Mobile Tech Report 2014: Technology news from 2013 and predictions and insights about 2014, Mind warm Incorporated.

[3] DESHOTELS, L., NOTANI, V. & LAKHOTIA, A DroidLegacy: Automated Familial Classification of Android Malware. Proceedings of ACM SIGPLAN on Program Protection and Reverse Engineering Workshop 2014, 2014. ACM,

[4] ZHOU, Y., ZHANG, X., JIANG, X. & FREEH, V. W. 2011. Taming information-stealing smartphone applications (on android). Trust and Trustworthy Computing. Springer.

[5] BROWN, J., HRUSKA, M., JOHNSON, A. & POLTRACK, J. 2014. Educational Standards for Mobile Learning and Mobile Application Development. Increasing Access, 17.

[6] DE, S., MISRA, A. & DE, S. 2014. An Improved Approach of Decoupling in Mobile Cloud Computing. Distributed Computing and Internet Technology. Springer.

[7] MARTÍNEZ-PÉREZ, B., TORRE-DÍEZ, I. D. L., LÓPEZ-CORONADO, M. & SAINZ-DE-ABAJO, B. 2014. Comparison of Mobile Apps for the Leading Causes of Death Among Different Income Zones: A Review of the Literature and App Stores. Journal of Medical Internet Research, 16.

[8] ROBERTS, J. R., DROST, C. A., HYDE, G., LANDESMAN, B. & MATTHIES, B. 2014 Internet Reviews. College & Research Libraries News, 75, 48-49.
[9] GRITZALIS, D. 2014. Holistic Information Security: Human Factor and Behavior Prediction using Social Media.
[10] HUTTUNEN, A., SWANDER, B., VOLPE, V., DIBURRO, L. & STENBERG, M. 2005. UDP encapsulation of IPsec ESP packets. RFC 3948, January.
[11]SINGH, A. 2014. Forensic analysis for massive mobile applications using data mining. The International Journal of Big Data, 1.
[12]KIM, M., PARK, N. & WON, D. 2014. Security Analysis on a Group Key Transfer Protocol Based on Secret Sharing. Mobile, Ubiquitous, and Intelligent Computing. Springer.
[13]DYE, S. M. & SCARFONE, K. 2014. A standard for developing secure mobile applications. Computer Standards & Interfaces, 36, 524-530.