Indian Journal of Science and Technology, Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/100190, August 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

# A Systematic Analysis on Mobile Application Software Vulnerabilities: Issues and Challenges

**P. Khurana[1], A. Sharma[1] and Pradeep Kumar Singh[2*]**

[1]Department of Computer Science and Engineering, Amity University, Noida - 201313, Uttar Pradesh, India; pkhurana187@gmail.com, anshikaintegral@gmail.com
[2]Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan - 173234, Himachal Pradesh, India; pradeep_84cs@yahoo.com

## Abstract

**Objectives**: Mobile network, ad-hoc network or Wireless ad-hoc network is the latest networking trend today. In the past fifteen years the no. of Mobile phone users has grown exponentially. The perks offered by this wireless mode of networking are open to all: anywhere, anytime, un tethered access to a huge no. of global users. **Statistical Analysis**: This paper consists of systematic review and analysis of various existing techniques which helps us to cope against such disasters with an actual and sorted representation. In the end, we wind up our results with the merits and demerits of existing methods along with the liabilities of future scope in this area. **Findings:** The review studies have shown various mobile software vulnerabilities with their advantages, disadvantages along with their future scopes. **Application:** The application of mobile software networks is innumerable, from mobile browsers to e-commerce to mobile money, there uses are extensive and important.

**Keywords:** Ad-hoc Network, Authentication, Malware, Mobile Network, Reliability, Vulnerabilities,

## 1. Introduction

A mobile network is a compilation of different nodes which arranges them in a way that they implement a temporary network. The temporary network is then used to carry out the communication process. But there are various methods that hamper the ease of communication in this limited network. Security is the major mission in every aspect of our life, so is the case with wireless mobile network. There are broad number of bugs and weaknesses prevalent in this mode which needs to be corrected and fixed.

Various attacks like Man-in-the Middle attack, Denial-of-Service attack, Jamming attack etc are major cause of misbalance in the wireless environment. This is mainly due to fact that mobile ad-hoc architecture is blessed with limited resources and functionality in terms of processing and computation. There are 2 types of network models available: a) Client-Server, b) Peer-Peer.

A client-server model typically has a centralized approach where one central server processes the requests from the client and returns the response within the specified time.

Peer-Peer architecture on the other hand completely adopts an approach that is different from the Client-Server Architecture, where every peer node communicates with another node in a distributed fashion. The node pursuing the request plays the role of server and other nodes act as clients. Any node can be a client or a server in this approach.

What we need is an efficient environment that provides us with an infrastructure that considers and faces all the attacks and provides an efficient working model.

This review paper is arranged in 4 sections. Section 1 encloses the discussion about the introduction, preceded by literature review in section 2, section 3 covers various security measures that have been proposed and discussed

*Author for correspondence

using various techniques. Finally, section 4 consists of conclusion and future scope.

## 2. Literature Review

In order to do the analysis, we have downloaded almost 250 papers so that we could present a systematic technical analysis of various protection mechanisms regarding the wireless (mobile phones) security, from various digital libraries which include IEEE Digital Library, Science Direct, Google Scholar, ACM and many more. We also tried to formulate three research questions, so that we could find our concluding better at the end of the paper. We went through the paper title, abstract, introduction, experiment and future scope. We have identified most suitable paper for the review. In this review paper we have followed the similar concept as considered in[23-26]. The review for all 20 selected papers has been systematically arranged in this section of the paper:

**RESEARCH QUESTIONS**

**RQ.1** To identify the current problems in Mobile software Technology?

**RQ.2** To discover the most popular techniques in creating secure mobile Software?

**RQ.3** To analyze the scope of improvement and future scope of research in Mobile Software Vulnerability?

Hamieh et al.[1] proposed a method that focused on a specific type of attack called Jamming, which is a type of DoS (Denial of Service) attack. This was done by measuring a statistical co-relation, named as Co-relation Coefficient (CC) and an Error Probability (EP). The experimental work proved that if the CC is larger than the EP then there is the condition of jamming in the network. In order to estimate the correctness of the proposed method, NS-2 tool was used. The disadvantage of the system included in assuming that jammer sends its data only when desired signal is received from the other end. The future work includes application of the same system in different types of DoS attacks and find out appropriate and more reasonable solutions for different jamming attacks.

Papadimitratos et al.[2] coined a method named Dopler Shift Test which helped fighting against adversaries that can cause a client system to reach the fake locations by attacking the GNNS (Global Navigation Satellite Systems) or the GPS (Global Positioning System). The DST (Dopler Shift Test) works in three steps: a) Normal Mode: - system collects all the data when it is reliable, b) Alert Mode: - based on the data obtained in Normal mode, it predicts the future values, and c) Under Attack: - compares predicted values with obtained values. If the value of threshold $t_{relay}$ is higher, there is a greater possibility of attack. In future the authors plan to make the system more cost efficient and implement it for more dangerous attacks.

Sadeghzadeh et al.[3] presented an approach which improves the working of Bluetooth protocols by securing transfer between devices. The proposed approach uses the technique of enhanced pairing using password based EKE and SPEKE. The major advantage with the system is that when some attacker sends a message to the mobile device the MAC and signature fails which causes connection termination. The disadvantage of this scheme is that it only deals at protocol level. Future work includes the security check on each packet and improved encryption standards.

Prieto[4] reviewed the JXME security functionalities used in mobile devices. The JXME proxied version has very poor security standards, causing various attacks like Traffic analysis, eavesdropping, Man in the Middle etc. the JXME proxy less version is comparatively advanced providing a safe communication channel, but still lacks in proper authentication of mobile devices. The future work includes developing a basic security pipeline for the JXME protocols by using encryption and masks.

Mi et al.[5] developed an approach for obstacle avoidance connectivity restoration strategy (OCRS) that solves the problem of network breaking which is caused due to the mobile sensor failure. This strategy requires adjacent information of 2 hops only. The experimental studies show that OCRS gives high results for calculating the complexity of a message and for calculating travelling distance.

Wang et al.[6] proposed a method for security in smart phones against mobile marketing. The method is named as Distributed Privacy-preserving Mobile Access Control (DP-MAC). This is based on Decentralized Attribute based Encryption (DABE) and Identity based Encryption (IBE). It is beneficial against Single Point of Failure (SPOF) attacks.

Aoki et al.[7] discussed a technique which is used for maintaining privacy in mobile phones for community sensing. The technique is named as Multidimensional Randomized response. In this technique the collected sta-

tistical data is processed twice. The scheme discussed here minimizes the monitoring attacks. The drawback with the technique is that it does not process the multidimensional data; also the process is designed to work for the community as a whole and not for an individual. In the future the individual health system will be created while keeping the privacy of the person preserved.

Song et al. [8] presented a Robust Optimized Link State Routing Protocol (ROLSR) for Military domains which overcomes all the loopholes of OLSR Protocol. Various attacks such as Wormhole attacks, Spoofing attacks, and Flooding attacks are removed by using ROLSR. The protocol is based on Strong Control Message Authentication (SCMA) and Comprehensive Neighborhood Trust Model (CNTM). While calculating the performance of ROLSR it was concluded that the overall cost of security processing for a Hello message is 0.9 ms, and for Topology Control message it is 1ms, however the requirement of bandwidth for authentication of messages of strong control environment increases due to the increase in network's size.

Huang et al. [9] implemented the famous (ECC), Elliptic Curve Cryptography algorithm with a new technique named Hidden Generator Point that offers the improvement in the mobile network from Man in the Middle attack, along with these researchers have developed a precise algorithm which is composed of 1's compliment of binary numbers to reduce harming weights in order to minimize the computation power of ECC. The algorithm saves 12.5% of the time as compared to others. In the future researchers will try to induce other methods for implementing Hidden Generator Points.

Wu et al.[10] proposed a new technique for Mobile Phishing attacks which is depended on Optical Character Recognition (OCR) named as MobiFish. The technique solves the problem with heuristic based schemes against phishing attacks since heuristic based methods were depended upon HTML source code and MobiFish which is dependent on the screenshot of the application being tested. The MobiFish attack was tested on Google Nexus 4 which used Android 4.8 Operating System. The simulation results validated that the presented method can wisely fight against Phishing attacks as compared to other Heuristic Based Methods.

Anne et al.[11] presented a technique for the safety of mobile devices which was based on cloud. They used desktop computers that utilized cloud technique to implement security in mobile devices. They have elaborated all the issues that can arise in practicing this technique, including merging of the two different technologies. They have used OzekiNG gateway as an interfacing device, between a mobile device and a desktop computer. The limitation of the paper is in its sole dependence on cloud infrastructure for implementing the security.

Aziendali et al.[12] proposed a biometric based framework known as FAME (Face Authentication for Mobile Encounters), to handover security in Android mobile devices. The application utilized 4.82seconds in the registration phase and 5.04 seconds in the authentication phase. The future scope of the technique includes, utilizing the framework in determining concentration of students by looking at their faces, training drivers etc.

Ashraf[13] *et al.* discussed an approach using P2P systems in distributed environment in order to provide mobile security, using various encryption and authentication standards. The system maintains all the constraints such as security and reliability keeping efficiency enacted. The approach although is exposed to Denial of Service attack, which can be improved by adding a certain reputation layer[13].

Katsaros et al.[14] studied and presented counter measures against all the techniques which cause attacks in mobile handset technologies. They performed detailed evaluation of various situations like: a code writer tying to get illegal download of an object in a page, free of cost. They analyzed that the techniques for attacking did not relied on huge amount of resources; also the attacking schemes are based on object oriented languages like JAVA and dot net.

Chen et al.[15] proposed an approach which is used to detect abnormally behaving websites using a centralized Client and Server Architecture. Their method helped users from falling prey to these attacks by warning them before they use such hoax websites. The method discussed collected 1000 such websites from yahoo server and produced a precision of 99.476%, Recall of 496%, accuracy 99% and miss rate of just 0.1%.

Stirparo et al.[16] demonstrated a method of stealing a mobile phone user's documents, private data from their android phones by keeping track of how the data is managed in the mobile phone's flash. The project was named as MobiLeak and took the advantage of the poor standards of mobile applications development procedure. The limitation of the paper included in the fact that the software created by them works only in android systems. In

future they plan to work on making a security mechanism against this malware.

Dehghantanha et al.[17] discussed different services and parts of a mobile cell along with various possible threats and attacks to which a mobile phone can fall prey to. In the end they gave a relevant security mechanism which was Data-centralized rather than System-centralized. The application of this approach usually includes Defense Organizations and Government Industries.

Dhaya et al.[18] presented a new technique of analysis of an application's code against malware threats using static analyzing technique. The method used machine learning algorithm that is search based: N-gram analyzing algorithm. CVSS[18] (Common Vulnerability Scoring System) tool to find the loose points in the apk file.

Choyi et al.[19] proposed a scheme which was dependent upon IP Security (IPSec) that described secured communication between two Mobile terminals. Along with this they gave a Mobility Managing technique with route-optimizing algorithm with the help of Mobile IP. They also described the ways of removing latencies in moving a packet from within tunnels of mobileIP in order to generate an actual-time packet transfer delay, by avoiding needless processing.

Sathyan et al.[20] proposed a system which was dependent upon the multilayer collaborating technology in order to provide the adaptable secure infrastructure for mobile networking. In this way they assured that the customer privacy and data both remained enacted. They provide a mobility management criteria based on different requirements of the system. The future work includes in marking the threat against newly generated concept of Mobile Money.

## 3. Analysis on Various Software Security Techniques

In order to make out the analysis of the paper we reviewed all the techniques developed so far thoroughly. We discovered that there are security mechanisms based on different techniques and technologies that can be named as: a) Tool Based, b) Algorithmic, and c) Encryption based.

All the techniques that can be used to provide wireless mobile network based security are shown in Table 1.

## 4. Conclusion and Future Scope

In this paper we have tried to address various security techniques prevalent in mobile environment. There is no second question as to why is this security needed. Our mobile phone roams all around and performs every pos-

**Table 1.** Techniques providing different types of mobile level security

| Various Mobile Security Techniques Developed So Far | | | | | |
|---|---|---|---|---|---|
| **Sr.no.** | **Technique's Name** | **Ref. no.** | **Sr.no.** | **Technique's Name** | **Ref. no.** |
| 1. | NS-2 Tool. | 1 | 11. | OzekiNG gateway. | 11 |
| 2. | Dopler Shift Test (DST). | 2 | 12. | FAME (Face Authentication for Mobile Encounters). | 12 |
| 3. | Password based EKE and SPEKE. | 3 | | | |
| 4. | JXME Proxyless. | 4 | 13. | Systems in distributed environment. | 13 |
| 5. | OCRS (Obstacle avoidance connectivity Restoration Facility). | 5 | 14. | JAVA and dot net. | 14 |
| | | | 15. | Centralized Client and Server Architecture. | 15 |
| 6. | Decentralized Attribute based Encryption (DABE) and Identity based Encryption (IBE). | 6 | 16. | MobiLeak. | 16 |
| | | | 17. | Data-centralized approach. | 17 |
| 7. | Randomized response. | 7 | 18. | using static analysing technique. | 18 |
| 8. | Strong Control Message Authentication (SCMA) and Comprehensive Neighbourhood | 8 | 19. | IP Security (IPSec). | 19 |
| | | 9 | 20. | Multilayer collaborating technology. | 20 |
| 9. | Trust Model (CNTM). | | | | |
| 10. | (ECC), Elliptic Curve Cryptography algorithm plus Hidden Generator Point. | 10 | | | |
| | Optical Character Recognition (OCR). | | | | |

sible task for us. Apart from our private photographs, audios, and videos, it collects all the data related to our financial accounts like credit card details. Since mobile faults and viruses are separate from others, unique approach to handle these malwares is also required. We came across various modes of security that can be provided to our mobile systems and to the data residing in our cellular systems. Broadly speaking the techniques can be classified as: a) Tool Based, b) Algorithmic, and c) Encryption based.

Tool based techniques such as those dependent upon NS-2 tool provides security mechanism against popular and most hacking jamming attacks. Algorithmic approaches such as Randomized approach deals with monitoring attacks, where one malicious programmer or attacker reads our data without our permission. Third and last Encryption based techniques such as Identity Based Encryption which follows a decentralized approach against Single Point of Failure (SPOF) attacks.

We had addressed three research problems at the starting of our paper. **RQ.1** made us think all the possible problems prevalent in current mobile software techniques. There are many issues that can be thought of today, ranging from security, safety, memory, price and usage. Out of this all security is and has been the major concern of all, the developers. Many software, tools, techniques and algorithms have been generated to raise the solution against this issue. **RQ.2** pointed the affair of identifying the current software technologies, which we can easily address at the end of the paper namely: Dopler Shift Test (DST), Password based EKE and SPEKE, JXME Proxyless, OCRS (Obstacle avoidance connectivity Restoration Facility), Decentralized Attribute based Encryption (DABE) and Identity based Encryption (IBE) etc.

All the techniques discussed in the paper perform under certain determined conditions such as: software requirements, hardware approach (Android, IOS etc), and infrastructure based (Centralized, Distributed, or cloud based), and this leads to their point of limitation.

**RQ.3** aimed at analyzing the future scope and improvements that can be performed in the existing techniques. In future all the techniques will try to implement the security standards outside their architectural scope that is within different infrastructure and different hardware and software requirements. Technique such as multilayer collaborating technology will try and implement security channels in different newer applications that mobile network has started distributing to its users such as Mobile Money. Mobile Money is one of the latest technologies today which demands a great concern in terms of security and protection against malicious attacks.

Various other security providing standards naming Mobileak, OCR, ECC will be worked upon also so that they come out with an efficient, more economical and robust methods than their current standard.

## 5. References


1. Hamieh A, Jalel BO. Detection of Jamming attacks in wireless ad hoc networks using error distribution. Proceedings of International Conference on Communications (ICC); 2009. p. 1–6.
2. Papadimitratos P, Aleksander J. GNNS based positioning: Attacks and countermeasures. Proceedings of Military Communications Conference- MILCOM; 2008. p. 1–7.
3. Sadeghzadeh SH, Seyed JMS, Mohammad M. A new secure scheme purposed for recognition and authentication protocol in bluetooth environment. Proceedings of 12th International Conference on Advanced Communication Technology (ICACT). 2010; 2:1326–31.
4. Prieto MD, Joan AM, Jordi HJ. JXTA security in mobile contrained devices. Proceedings of International 24th Conference on Advanced Networking and Application Workshops (ICCSNT); 2013. p. 1247–50.
5. Mi Z, James YY. Obstacle-avoidance connectivity restoration for mobile sensor systems with local information. Proceedings of International Conference on Communications (ICC); 2015. p. 6395–9.
6. Wang Z, Dijiang H, Huijun W, Bing L, Yuli D. Towards distributed privacy- preserving mobile access control. Proceedings of Global Communications Conference (GLOBECOM); 2014. p. 582–7.
7. Aoki S, Kaoru S. Privacy-preserving community sensing for medical research with duplicated perturbation. Proceedings of International Conference on Communications (ICC); 2014. p. 4252–7.
8. Song R, Peter CM. ROLSR: A Robust Optimising Link State Routing Protocol for military ad-hoc networks. Proceedings of International Millitary Communications Conference (MILCOM); 2010. p. 1002–10.
9. Huang X, Pritam GS, Dharmendra S. Fast scalar multiplication for elliptic curve cryptography in sensor networks with hidden generator points. Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). 2010. p. 243–49.
10. Wu L, Xiaogianj D, Jie W. Effective defence schemes for phishing attacks on mobile computing platforms.

Proceedings of Transactions on Vehicular Technology; 2015. p. 1–13.
11. Anne VPK, Venkata R, Rajashekhara RK. Enforcing the security within mobile using cloud and its infrastucture. Proceedings of CSI 6th International Conference on Software Engineering (CONSEG); 2012. p. 1–4.
12. Barra S, Maria DM, Chiara G, Daniel R, Harry W. FAME: Face Authentication for Mobile Encounter. Proceedings of Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS); 2013. p. 1–7.
13. Ashraf K, Rachid A, Behzad B. File management in a mobile DTH-based P2P environment. Proceedings of 26th International Conference on Advanced Information Networking and Applications; 2012. p. 415–22.
14. Katsaros I, Martin I, Honary B. Threats to next generation mobile application software. Proceedings of The 2nd IEEE Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN, IET, 2004. p. 10/1–10/3.
15. Chen CM, Ya HO. Secure mechanism for mobile web browsing. Proceedings of 17th International Conference on Parallel and Distributed Systems (ICPADS); 2011. p. 924–8.
16. Stirparo P, Igor NF, Marco T, Ioannis K. In-memory credentials robbery on android phones. Proceedings of Conference on World Congress on Internet Security (WorldCIS); 2013. p. 88–93.
17. Dehghantanha A, Nur IU, Ramlan M. Towards data centric mobile security. Proceedings of 7th IEEE Conference on Information Assurance and Security (IAS); 2011. p. 62–7.
18. Dhaya R, Poongodi M. Detecting software vulnerabilities in android using static analysis. Proceedings of International Conference on Advanced Communication Control Computing Technologies (ICACCCT); 2014. p. 915–18.
19. Choyi VK, Michel B. Low-latency secure mobile communications. Proceedings of International Conference on Wireless and Mobile Computing, Networking and Communication (WiMob'2005). 2005; 2:38–43.
20. Sathyan J, Manesh S. Multi-layered collaborative approach to address enterprise mobile security challenges. Proceedings of 2nd Workshop on Collaborative Security Technologies (CoSec); 2010. p. 1–6.
21. Anane R, Steven M, Behzad B. Trusted P2P group interaction. Proceedings of the 2nd International Conference on Computer Science and its Applications (CSA 2009), Korea; 2009 Dec. p. 1–8.
22. Ali A, Pavol Z, Dale L, Ron R. A new CVSS-based tool to mitigate the effects of software vulnerabilities. International Journal for Information Security Research. 2011; 1(4):178–82.
23. Singh PK, Sangwan OP, Arun S. A systematic review on fault based mutation testing techniques and tools for Aspect- J Program. Proceedings of 3rd IEEE International Conference on Advance Computing Conference (IACC), India; 2013. p. 1455–61.
24. Singh PK, Rajan P, Sangwan OP. A critical analysis on software fault prediction techniques. World applied Science Journal. 2015; 33(3):371–9.
25. Singh PK, Dishti A, Aakriti G. A systematic review on software defect prediction. Proceedings of INDIACom-2015: 2nd International Conference on Computing for Sustainable Global Development, India; 2015. p. 1793–7.
26. Sharma A, Pradeep KS, Palak K. Analytical review on Image Segmentation and Recognition. Proceedings of 6th International Conference on Cloud System and Big Data Engineering(Confluence); 2016. p. 524-30.