e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

A Survey on Communication for Smartphone

Reshma Raj[1], Anishamol Abraham[2]
[1]*Department Of CSE, Amal Jyothi College Of Engineering Kanjirappally , Kottayam, India*
[2]*Department Of CSE, Amal Jyothi College Of Engineering Kanjirappally , Kottayam, India*

Abstract-Nowadays security and privacy issues are getting more and more important for people using state of the art communication tools like mobile smartphones or internet.As the power and feature of smartphones increases,so has their vulnerability.By using short range wireless communication smartphones commu-nicates each other.But the data confidential-ity is not guaranteed.In barcode and Near Field Communication enabled devices the smartphones exchange information by simple touch.The main drawback of Near Field Com-munication and barcode systems is the vul-nerable nature to attack since they are using key exchange then encrypt techniques.In the smartphones with android platform,it is possi-ble to provide security against all the attacks by securely exchanging message or data with-out using key exchange protocol.PriWhisper is an technique that enables keyless secure acous-tic communication for smartphones and pro-vides better security as well as data confiden-tiality.

I. INTRODUCTION

Androids are the most common platform on which smartphones are built.It is an open source operat-ing system.Android applications can use advanced level of hardware and software,as well as local and server data,exposed through the platform to bring innovation and value to consumers.Smartphones must have high security mechanism to ensure se-curity of user data,information,application and net-work.Smartphones are not secure as it appears.There are many security problems faced by the smartphones that are being based developed on android operating system.Some of them are they have no security scan over the application being uploaded.There are even some applications that can exploit the services of another application without permission request.The main advantage of smartphones is the fastest way of communication that is through simple touch.The smartphone communicates through short range wire-less communication.This short range wireless commu-nication have been used in many security sensitive smartphone applications and services such as contact-less micro payment and device pairing.

The common approach of the short range wire-less communication in smartphones is through key exchange the encryption.Here the sender and the re-ceiver has to first utilize Difie-Hellman key exchange protocol to set up a common secret key at the be-gining of each session.But this requires some time for message exchanging.Sometimes this may dominate the entire communication session.Thus this is not much eective.It is always better to have keyless communi-cation.

Most of the transactions using smartphones are tak-ing place in public.Thus data confidentiality is not guaranteed.This is the most highlighted vulnerability while using Near Field Communication and barcode system.Due to its fundamental design principles,the visual nature of barcode based short range communi-cation makes them extremely vulnerable to shoulder snifing.The availability of the cameras in the public place even helps the attacker to hack the system.So it is very much needed to provide security against this defect.One of the security enrichment that is used to increase the privacy protection during pervasive net-work use is by using Priwhisper.This provides bet-ter security than Near Field Communication and bar-code system.The main advantage is that it can with-stand eavesdropping,shoulder snifing etc.Priwhisper uses a keyless secure acoustic communication.It is purely based on aerial acoustic communication.It is realized by system that oers great compatibilities

to various smartphone platforms without any additional hardware requirement.Priwhisper can be implemented in any smartphone that contains a speaker and micro-phone.

II. LITERATURE SURVEY

Barcode System

Barcode system is a network of hardware and soft-ware consisting of mobile computers,printers,handled scanners,infrastructure etc.It is used to automate data collection where hand recording is neither timely or cost eective.They are not radio frequency identi-fication (RFID) system.Unencrypted barcodes poses threat.Barcode system can be easily hacked through value cloning,value overow and code injection.Public Key infrastructure and digital signature helps to in-crease the eficiency of bar code system but their ex-pense and cumbersome infrastructure have found lim-ited acceptance,roll out to remote and diverse loca-tions is not always feasible due to expense or infras-tructure requirements and there are lingering uncer-tanities about positive orginator identification.

Near Field Communication

Near Field Communication is a type of contactless wireless technology used for sending information or making payments.This enables low power radio com-munication between two Near Field Communication enabled devices by simple touch.By embedding an NFC chip inside a smartphone a company can cre-ate a virtual wallet where user store credit card in-formation and can pay at store simply by waving their smartphone over credit card reader.The small NFC chips inside the smartphone generates an elec-tromagnetic field.This field is received by an NFC tag found in a card reader,a smart poster etc.The tag contains information and using the electromag-netic field as its power supply,sends this information to the smartphone.Security problem faced are eavesdrop-ping, data manipulation or corruption, viruses.NFC compactable devices can only communicate when they are within 4cm of each other.NFC tags never power themselves.NFC is similar to bluetooth but oers faster and easier connection between smartphones.The main disadvantage is that it does not provide any pro-tection against eavesdropping.

Eavesdropping occurs when a third party inter-cepts the signal sent between two devices.Data ma-nipulation or corruption occurs when a third partyintercepts the signal being sent,alters it and sends it on its way.The information the receiving party gets moy not want to steal the information.The at-tacker simply wants to prevent the correct informa-tion from getting through.This is also known as de-nial of service.Near Field Communication allow users to store valuable bank account and credit card infor-mation on their smartphone thus making them a tar-get.Near Field Communication secure channel ensure Near Field Communication security is to use an Near Field Secure channel.It uses a standard key agreement protocols such as Diee- Hellman because of the in-herent protection has against man in the middle at-tack.Here shared key can be used to derive a symmet-ric key which can be then used for near field commu-nication secure channel.

Near Field Communication is an intriguing innova-tion.Some of its advantages are

- convenience
- versatility
- safety
- NFC enabled credit cards are much more secure than a credit card magnetic strip
- Requires PIN

The main disadvantage is the security itself.It is ex-pensive to implement.

Priwhisper

This overcomes all the defects of Near Field Com-munication.A keyless acoustic communication is be-ing used.The reason for using aerial acoustic is that it does not require line of sight,computational power is suficient enough to modulate/demodulate acous-tic signal using acoustic modem .Inorder to achieve keyless secure communication,friendly jamming tech-nique from radio communication is used.The inseper-ability of data signal and jamming signal is checked by using blind signal segmentation technique.PriWhisper is implemented in smartphone environment.Materials required are microphone and a speaker.Similar to Near Field Communication is achieved by using simple touch.PriWhisper automatically initializes the keyless acoustic communication when two smartphones are close to each other.The two devices must be placed within 0.5 cm.Both the sender and receiver need to send a audible acoustic signal during secure communi-cation and its length is 1-2 seconds.The eavesdropping can be done even through multiple or single sensors.To provide better data confidentiality and to provide se-curity against the eavesdropping PriWhisper is devel-oped.The attacking can be done through either ofiine or online phase.In online phase the mixture signal are collected by attackers multiple microphones through the air medium.Ofiine phase hacker tries to estimate the data signal using blind signal segmentation.

Priwhisper provides secure communication in the presence of both passive eavesdropping and its se-curity against active adversaries.The multiple sensor eavesdroppers try to separate the data signal from his or her recorded mixture signals.The eavesdrop-pers are allowed to place their sensors at any fixed locations in priori to the acoustic short range com-munication.Priwhisper is also evaluated based on the blind signal segmentation.Blind Signal Segmentation is nothing else but the technique that aims to separate several simultaneously active source signals from a set of mixed signals without any additional knowledge of the source signal.The results show that it is very much dificult to separate the data signal and the jamming signal.ICA is one of the most successful Blind Signal Segmentation.

Priwhisper architecture consists of aerial acous-tic communication.The narrow sense Bose,Chaudhuri and Hocquenghem error correcting code is used as the channel coding algorithm.The signal is transmitted by the senders speaker and collected by the receivers mi-crophone through the air medium.The received acous-tic signal is demodulated by the demodulator and then channel decoded.Priwhisper uses a jamming signal in-order to protect the original data signal.The jamming signal strength should be selected such that it will be within the decibel level of the receivers speaker hard-ware.To guarantee the confidentiality of the transmit-ted data the system has to adjust the data signal strength of the sender adaptively.The optimal decibel level of the data signal should be merely strong enough for the legitimated receiver to demodulate it without error.Once the system bit error rate performance for dierent signal to noise ratio is known,the sender can adaptively select the optimal signal strength according to its current environmental noise level.

Jamming signal generation is very much important because this generated signal needs to protect the data signal.The length of each communication session is specified.But this is expensive for the smartphone en-vironment.Also it is impossible to adopt the jamming signal cancellation technique that is used in many ex-isting friendly jamming based radio communication systems.The security level of Priwhisper largely de-pends on the distance between the senders and receivers speakers.

III. RELATED WORK

Friendly jamming technique was first proposed by Negi and Goel in 2005. In their work the jamming signals are generated from the null space of legitimate receivers channel vector and thus the jamming sig-nal does not eect the receiver but others eavesdrop-pers at dierent locations.Gollakota et al.first extend friendly jamming technique to a single duplex receiver in 2011.Their system uses a specialized hardware and thus limits its application in many scenarios.The se-curity analysis in here is hand waving without any quantitative evaluation.But there is a chance for at-tack.PriWhisper is capable enough to overcome this
defect.

	Priwhisper	NFC
Additional hardware	not required	required
Smartphone	supported	not supported
Security	oer	does not oer
Communication	simple touch	simple touch
Transmission rate	high	suficient

IV. CONCLUSIONS

PriWhisper enabled keyless secure acoustic commu-nication in smartphones and is capable of providing data confidentiality for all kind of short range com-munications taking place in the smartphones.It over-comes all the defects of NFC.Since acoustic signals is used as it travels in air medium the signal fades thus the eavesdroppers received mixed signal will not be the same as that being sended by the sender.The jam-ming signal is initated by the receiver thus it will be very much dificult for attacker to remove the exact jamming signal.

REFERENCES

[1] PriWhisper: Enabling Keyless Secure Acous-tic Communication for Smartphones Bingsheng Zhang, Qin Zhan, Student Member, IEEE, Si Chen, Student Member, IEEE, Muyuan Li, Stu-dent Member, IEEE, Kui Ren, Senior Member, IEEE, Cong Wang, Member, IEEE, and Di Ma, Member, IEEE
[2] Shklovski I.,Mainwarning S.D., Skuladottir, H.H., Borgthorsson H., Vej R.L.,Leakiness and Creepiness in App Space:Perceptions of Privacy and Mobile App Use, in ACM CHI Conference on Human Factors in Computing Systems.
[3] W.Stallings,Cryptograohy and Network Secu-rity:Principles and Practice,Fifth edition Pearson Education,Inc 2011
[4] A.J.Menezer,P.C van Orschot ,S.A Vanstone Handbook of Applied cryptography,CR press LCC 1997
[5] J Guerrieri and D Novotny,HF RFID eavesdrop-ping and jamming tests,Electromagnetic Div,Electronics and Elec-trical Lab,National Inst.Standards and Technol-ogy,Tech Rep 818-7-71,2006
[6] M.Erol- Kantarci, H T Mouftah, and S F Ok-tug,A survey of architectures and localization techniques for underwater acoustic sensor net-work, IEEE Surveys Tuts
[7] R.Headrick and L.Freitag,Growth of under-water communication Technology in the U.S Navy,IEEE Commun.Mag.,vol 47
[8] R.Jurdak, C. V Lopes and P.Baldi.Software acoustic modems for short range mote basedun-derwater sensor networks,in Proc. IEEE Oceans Asia 2006
[9] S.Goel and R.Negi.Guaranteeing secrecy using artifical noise,IEEE Trans.Wireless Commun,vol 7,Jun 2008
[10] J.Cardoso,Blind Signal Seperations:Statistical principles,Proc IEEE,1998
[11] R.Negi and S.Goel,Secret communication using aritifical noise,in Proc.IEEE Veh.Technol.Conf 2005
[12] S.Gollakotta,H.Hassanich,B.Ransford,D.Katabi and K.Fu,They can hear your heartbeats:Non-invasive security for implantable medical de-vices,in Proc SIGCOMM 2011

