May 2017

Survey and Analysis of Android Authentication Using App Locker

Akshitha Reddy Chintalaphani
University of Nevada, Las Vegas, chintala@unlv.nevada.edu

SURVEY AND ANALYSIS OF ANDROID

AUTHENTICATION UISNG APP LOCKER

By

Akshitha Reddy Chintalaphani

Bachelor of Engineering, Information Technology
Stanley College of Engineering & Technology for
Women, Osmania University, India

2015

A thesis submitted in partial fulfillment of
the requirements for the

Master of Science in Computer Science

Department of Computer Science

Howard R. Hughes College of Engineering

The Graduate College

University of Nevada, Las Vegas

May 2017

UNLV | GRADUATE COLLEGE

Thesis Approval

The Graduate College
The University of Nevada, Las Vegas

March 17, 2017

This thesis prepared by

Akshitha Reddy Chintalaphani

entitled

Survey and Analysis of Android Authentication Using App Locker

is approved in partial fulfillment of the requirements for the degree of

Master of Science in Computer Science
Department of Computer Science

Yoohwan Kim, Ph.D.
Examination Committee Chair

Ajoy K Datta, Ph.D.
Examination Committee Member

Juyeon Jo, Ph.D.
Examination Committee Member

Venkatesan Muthukumar, Ph.D.
Graduate College Faculty Representative

Kathryn Hausbeck Korgan, Ph.D.
Graduate College Interim Dean

ABSTRACT

SURVEY AND ANALYSIS OF ANDROID AUTHENTICATION USING APP LOCKER

By

Akshitha Reddy Chintalaphani

Dr. Yoohwan Kim, Examination Committee Chair

Associate Professor, Department of Computer Science

University of Nevada, Las Vegas

Android Smart phones have gained immense popularity over the years and is undoubtedly more popular than other operating system phones. Following the similar lines android wear was introduced. Steadily android wear is making its way into our daily lives. It helps keep track of the sleep you have, helps you reach fitness goals, keeps track of phone and helps users have easy authentication. Due to the usage of smart lock which enables phone to be unlocked as long as connected to the android wear, this leads to almost no security on both the ends as android wear before Android 5.0 has no lock. We aim to produce the existing authentication methods in android phones and wear and the threats that plague both kinds of devices. As authentication is one of the major building blocks of security, through research we aim at designing a system for android phones which will be able to protect the sensitive data on devices which will be at risk through smart lock using encryption techniques. In this proposed system, the user would be able to decide which applications are needed to be secured when he is using smart lock. This application will enable lock for those user chosen applications as soon as the smart phone device is connected to android wear and similarly disables the lock when connection is disabled between the devices and communication between devices is made secure using encryption algorithms. This application does not interfere with easy phone authentication which users demand but it makes sure data is protected and users are authenticated with the help of multiple authentication layering.

ACKNOWLEDGEMENTS

Firstly, I would like to thank my advisor Dr. Yoohwan Kim, who has offered me immense help whenever I was stuck with my research and with all the equipment needed for the research. He has always been there and never has hesitated to spend time in helping me. I would like to thank Dr. Juyeon Jo, Dr. Ajoy K. Datta, Dr. Venkatesan Muthukumar for agreeing to be on my committee.

I would also like to thank Dr. Ajoy K. Datta, for offering all the help that he could from the first day. I would also like to thank Professor Edward Jorgensen, for being very understanding and helpful with my GA duties for the duration of my thesis work.

I would like to take this opportunity to thank all the people who played an important role in helping me reach this stage. I would like to thank my parents Shravanthi and Sushil Kumar Reddy for giving me the required push to come to the USA and pursue my Masters. My sister Shravya who always had my back and never let me get lost in the madness. My friend Sharath who had an important role to play in me staying and completing my Masters and for always being there when I thought of giving up, would like to thank him for not letting me lose hope when it was required the most. My roommates, Rashmi Niyolia, Priyanka Thota, Sneha Goswami for always inspiring in their own way.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION TO AUTHENTICATON

Authentication can be defined as the process of identifying entities (i. e users) accurately. A person or thing's identity can be attested that they are who they claim to be is defined as the process of identification. Identification can be proved by the process of authentication. This can be achieved by asking particular person for their identification documents or verifying a particular site by checking its digital certificate. Multiple fields use authentication as the factor of identification and is relevant in almost all fields with varying parameters. Authentication in general can be considered to be divided into three categories. The first type of authentication is the category in which a person or a system or a website is identified based on the other trustworthy person or organization and they have first knowledge of the authenticity of the system or person they are endorsing. Generally, this proof of trust can be a family member, friend or a colleague. For organizations, they can trust only the certified bodies that is why organizations follow web of trust functionality that can be used for services like emails. Known trust organizations sign each other's keys. Second category includes type of authentication where comparison takes place between attributes of the element in question and the element which usually is of same kind and similar origin. But this authentication method may fall prey to the forgery attack. Third category includes authentication technique based on documentation facts and checks. In fields related to computer sciences user is given access to certain systems or accounts based on the credentials entered [33].

AUTHENTICATION METHODS	DEFINITIONS
Passwords	Characters are combined and used by user for login attempt and if it matches with the actual secret key then user is logged in.
One-time Passwords	Combinations of characters that can be used only once for logging into resources.
Biometrics	User's identity is proved by using user's physical attributes like eyes detection, fingerprints, palm, voice etc.
Location-Based	User's location is used for authentication.
Two-factor Authentication	Two types of authentication methods are combined.
Smart cards	Hardware which directly communicates with the computer to authenticate user.

Table 1: Types of Authentication

1.1.1 AUTHENTICATION FACTORS

Factors of authentication can also be divided into three categories namely, something user knows, user has or what user is. To authenticate a person or person's identity there are variety of elements involved in different authentication factor before going ahead and giving or granting the user permission to access the resources. The ideal authentication would be where all the three above stated elements are part of the authentication process.

- Factor of knowledge/ something that user knows: examples of this category are passwords, patterns, pins, challenge questions/response, security question, pass phrase.
- Factor of ownership/ something user has: examples of this category are hardware/software token unique to the user, identification cards, security token/cards.
- Factors of inheritance/ something that user itself is: examples of this category are voice identification, fingerprints, face recognition, signature, eye/retina pattern match or any other biometric attribute.

1.1.2 TYPES OF AUTHENTICATION

To authenticate users there has been security level set up mainly by combining one or more factors and often it is two factor authentication that works best.

- One-factor authentication: this can be considered as the weakest authentication form. It will use only one of the factors to authenticate users and this can lead to attackers being able to crack it quicker. This method is considered weak due to the lack of strength and protection. Not recommended in general for high sensitive systems.
- Two-factor authentication: authentication requires two factors to be presented by the user to be able to access resources and authenticate them. For example, a high confidential system's access criteria may include biometric factor and knowledge factor like password or security question [33].
- Multi-factor authentication: this is one of the protected way of authentication. This method uses more than two factors and mixes up authentication factors to build up a strong technique.
- Strong authentication: this definition differs from organization to organization. In general, it uses layered approach of authentication which is dependent on multiple factors to establish user's identity and receiver's identity.
- Continuous authentication process: this method asks users to authenticate themselves for every session and every time they want to access certain resources because most of the systems ask users to authenticate only for the initial time.

1.2 AUTHENTICATION IN DIGITAL PLATFORMS

Communication in today's day and age is via electronic devices. This gives rise to various new found threats like eavesdropping over the network or man-in-the-middle attack where some random third party is trying to access resources or gain some knowledge of sensitive data. To overcome this, a special authentication factor is required like 'key'.

1.2.1 CRYPTOGRAPHY AND ENCRYPTION

To understand key based encryption, it is important to know about cryptography. Cryptography can be defined as a study of methods/techniques or practices that are used when adversaries (third party elements) are present in the network to establish secure communication between genuine users. Cryptography analyzes the methods and algorithms which are used for securing the communications between the two parties and not letting the unwanted third party from accessing private information. There are three basic principles of internet security:

- Confidentiality
- Data Integrity
- Authentication
- Non – repudiation

Encryption can be assumed to be the other name of cryptography. It can be seen as the process of converting readable plain text to some sort of non-readable text and then sending it over the network. This unreadable text is called cipher text. Decryption forms the opposite process of encryption that is converting cipher text to plain text.

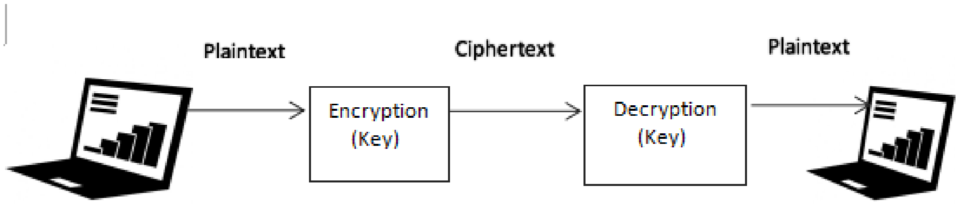


Figure 1: Process of basic cryptography

For converting plain text to cipher text or vice versa what is required is called cipher. Cipher in general is controlled by an instance value called key. Key is generally a string of characters and length can vary. Without key algorithms can be easily broken. Key based cryptosystems can be easily divided into two namely asymmetric key and symmetric key algorithms.

Asymmetric Algorithms	**Symmetric Algorithms**
RSA	DES
Diffie - Hellman	AES
Digital signature algorithm	Triple DES
XTR	IDEA
ECDSA	RC 2, RC 4, RC 6
EIGamal	Blowfish

Table 2: Examples of symmetric and asymmetric algorithms

1.2.2 SYMMETRIC KEY SYSTEM

In this system a single secret key is shared and this one key encrypts and decrypts the plain text and cipher text respectively. These are easy to decode because the key length chosen is small, but works faster due to this. Examples of this system are AES, DES. These algorithms also face threats like man in the middle attack or spoofing attack but with the new age algorithms like Diffie-Hellman these problems can be resolved. Keys can now be authenticated using key distribution center (KDC) or by other protocols like Kerberos.

PROS AND CONS OF SYMMETRIC SYSTEMS:

PROS:

- It is faster
- Since the key is not transmitted with the data over the network, decryption is difficult.

- To prove identity of the user, passwords are set.
- Decryption of message is only possible when shared key is present with the user

CONS:

- Shared key is at risk as it needs to reach the receiver before the message is sent as it is needed for decryption. Communication over the network is never safe that is why key is unsafe and at risk.
- Digital signature is not provided.

1.2.3 ASYMMETRIC KEY/PUBLIC KEY CRYPTOGRAPHY

In this system there are two keys involved namely public key and private key. Encryption process uses public key and decryption process uses private key. It is a way better way of securing communication than symmetric key. Examples of this system are RSA, ECC.

Spoofing can be done in this system as well because public key is known to all users and any third party can publish their key as some authentic user. To solve this problem certificate authorities and public key certificates were introduced in PKI systems (public key infrastructure). These organizations can act as the trusted third party and provide digital signature to user at both the ends. Problems with this method is any private agency can act as CA and error can be made [32].

Type of Attack	Definition
Birthday attack	Attack in which collisions are found using brute force approach
Brute force attack	All the possible possibilities are tried and tested till its successful
Dictionary attack	It is a type of precomputation attack. Pre computed list of values are checked and tried for passwords
Meet-in-the-middle attack	Two separate keys are used for encryption. A known plain text is used for encryption by the attacker using a key and original cipher text is decrypted with other key and hopes both the values will be same.
Man-in-the-middle attack	When two parties try and communicate their keys, third party adversary sends different keys to both the parties and establishes communication with both the parties pretending to be the actual party.
Precomputation attack	Values in look up table that are pre-computed are used to crack passwords or pins or pass phrases.
Chosen cipher text attack	Attacker has the option of choosing cipher text to be decrypted.
Chosen plain text attack	Attacker can choose the plain text that has to be encrypted.
Known plain text attack	Attacker has the knowledge of both the plain text and cipher text.
Cipher text only attack	Attacker has cipher text and no other information.

Table 3: Attacks faced by cryptosystems

PROS AND CONS OF PUBLIC KEY CRYPTOSYSTEM:

PROS:

- Key distribution is not a problem as keys are not shared between users.
- Private keys need not be displayed or transmitted ever to other users. So it is safe.
- Digital signatures are provided.

CONS:

- It is not as fast as symmetric key encryption algorithms

1.2.4 AUTHENTICATION VS ENCRYPTION

Secret key is used in the encryption process to convert meaningful data into non readable meaningless data. And data is read by the receiver by decrypting the cipher text. Whereas authentication is the process where user identification is proved then access is granted. In general authentication based systems are considered to be less secure than that of those systems which are encryption based but are comparatively more flexible. Passwords are generally used in both encryption and authentication and serves the basic purpose of letting user in the system only when right password is entered.

	Authentication	**Encryption**
Password	Authorization to work on system depends on the user knowing something which usually is a combination of characters	Key is formed by converting what user knows.
Key	Secret key is used as the verifier	Original resources are transformed.
Unlock	Verifier on satisfaction allows user to access resources	Resources which are of value are converted from gibberish values.

Table 4: Authentication and encryption differences

PROS AND CONS OF AUTHENTICATION SYSTEMS:

PROS:

Passwords can be reset

- Data can be recovered if passwords are lost by other methods.
- Access to resources can be controlled like some users may be given only read permissions and other user can be given permission to give permissions to other users.
- Authentication systems can enable remote accessing as it is not locally working as encryption does.
- Once given accesses can be revoked anytime.

CONS:

Gatekeeper sort of entity is required for checking and granting access.

If not encrypted data can be accessed through other ways avoiding the gatekeeper.

Identification entity or often password is used by the user to gain access from the gatekeeper which might be at risk because it is not protected.

PROS AND CONS OF ENCRYPTION SYSTEMS:

PROS:

- Unauthorized access to systems is very limited.
- User's identity is always protected.
- Encryption of data is secure to transmit.
- Can prevent data theft.

CONS:

- Maintenance of the key.
- Generation of keys is expensive.
- Data cannot be recovered if key is forgotten or lost.

1.2.5 EXAMPLES OF COMMERCIAL PRODUCTS FOR ENCRYPTION

- AxCrypt
- Veracrypt
- BitLocker
- GNU Privacy Guard
- 7 Zip
- Launch key [22]

CHAPTER 2

AUTHENTICATION IN ANDROID

2.1 INTRODUCTION TO ANDROID

Android was designed and developed loosely on Linux kernel by Google, as the operating system for mobiles particularly Smartphones and Tablets. Direct manipulation is the main basis on which android user interface is built and the daily gestures are incorporated in the interface and from there comes swiping gestures and tapping gestures which in turn manipulate the objects on-screen like application icon, submit buttons, scrolling etc.

Android OS was initially developed by Android Inc, in 2005 it went on to be bought by Google. An amalgamation of software concepts, efficient hardware and telecommunication designs for mobile devices was brought into limelight through open handset alliance in 2007 by Google. This new concept by Google changed the way mobile devices were going to be used and viewed in the following years to come. Android OS in undoubtedly the most famous and easy to use, what goes in its favor is easy user interface, ease of downloading, affordable prices. Apart from mobile phones android platform has ventured into televisions, tablets, electronics like digital cameras, notebooks, game consoles, android auto for cars, android wear for watches. From 2013 android tablets lead the way in the markets, unbeatably the best till date. Similarly, android has been pioneer of telecommunication and mobile devices industry in most parts of the world [29].

To establish easy access to all the application developers and users who want to use certain applications when and where there is need, Google Play Store was established in 2013. Android application development went on to become one of the sorted job titles and according to surveys over 71% application developers develop for android, 40% developers see android platform as a serious job profile and as of survey in 2015, around 2 million active devices were connected.

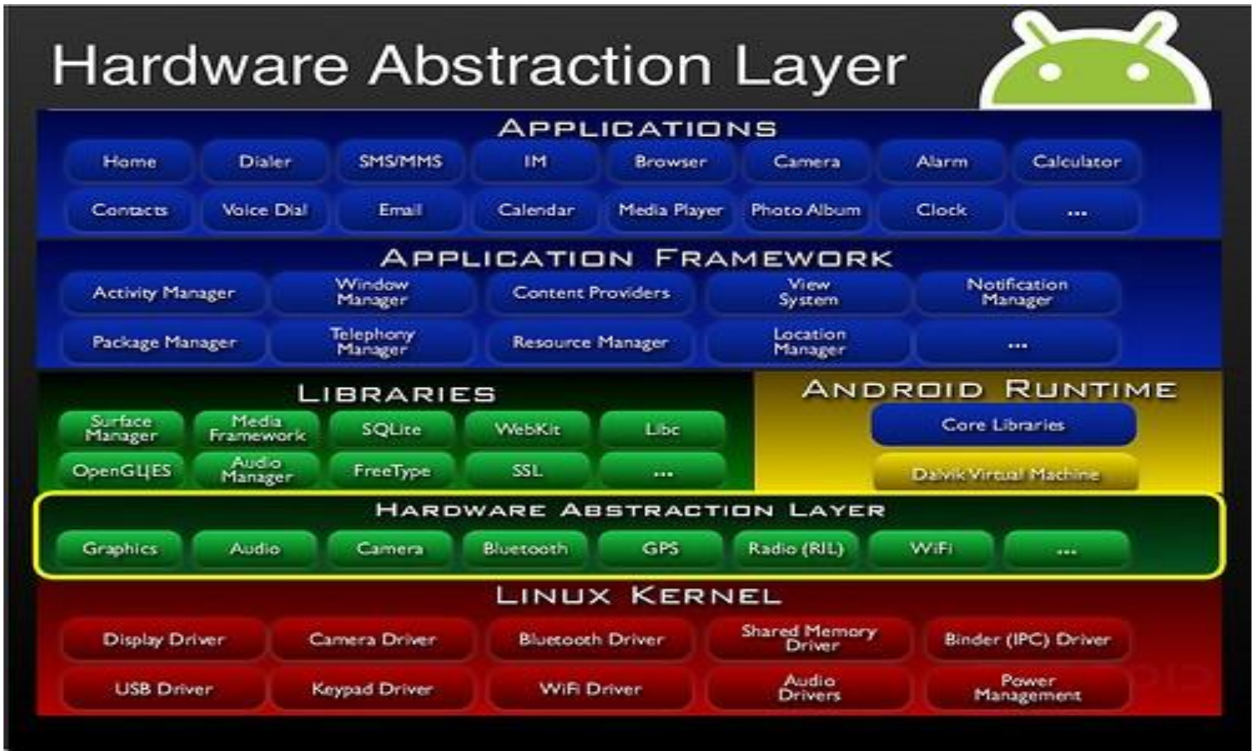


Figure 2: Hardware abstraction layer [20]

2.2 FEATURES

General features of android include messaging, web browsing, internet, voice based search, multi-touch, multitasking, screen capturing, recordings, video recording, multiple language support, accessibility. Android has various connectivity and media features such as Bluetooth, tethering, media and streaming support, external storage extension and has other hardware and software support.

In android over the years there has been inclusion of more hardware devices being able to connect to the android devices such as GPS (used for location based apps), thermometers, accelerometers (used for fitness and driving apps), proximity and pressure sensors etc.

Android also has other software features such as java support, storage, handset layouts as android works for any screen size, any layout and can also be connected to external devices.

2.2.1 MESSAGING

There are two forms of messaging like SMS and MMS. Text message services, video message services, cloud based texting are also available.

2.2.2 VOICE BASED SEARCH

From android 2.2 google search could navigate between applications, perform tasks, can call contacts and send texts.

2.2.3 MULTITASKING

By using a very unique way of allocating memory, multitasking is made possible. Multiple processes are run and can produce results at almost same time.

2.2.4 SCREEN CAPTURE

Android lets its users take screen shot of their applications and data by pressing power button and home button in few device and by swiping in few devices.

2.2.5 VIDEO CALLING

By default, android has no video calling setup but some mobile manufacturing companies use their own operating system to enable video calling on their devices.

2.2.6 MULTIPLE LANGUAGE SUPPORT

Android over the years has established itself to cater to all kinds of people thereby bring in customized set of languages available for the device.

2.2.7 BLUETOOTH

Bluetooth is basically used to send files, contacts, data between phones. It also supports voice dialing.

2.2.8 MEDIA AND STREAMING SUPPORT

RealPlayer supports the concept of live streaming on android. Android also supports most of the major image, video, audio and document formats such as MPEG, AMR, DOC ,PDF ,MP3 ,NTFS etc.

2.3 HARDWARE FOR ANDROID

ARM architecture (namely ARMv7, ARMv8), X86, MIPS (in later versions of android) are the main platforms for android. After the android version lollipop 65-bit is also being supported apart from the usual 32-bit. Android requirements for RAM are quite simple like 512MB for screens with normal density and 1.8GB for screens with high density. Some new age technology like GPU is also present.

Android also incorporates additional hardware devices like video camera, GPS, sensors, controls (for gamming) etc. Android can be run on PC apart from being run on phones and tablets. Android SDK, emulator are run on PC for programming applications for android.

2.4 ANDROID DEVELOPMENT

Google develops android in private till the new changes and updates in the software are available for release. Once the updates are released the source code is made open source. Even though the code is made public, all the drivers are not available which are needed for specific hardware components.

Updates are done by Google every six to nine months, with new version name which most of the high end device receive through air. As android platform is used in many devices the updates reach devices at different times unlike IOS. This is because of hardware variations of the devices for which the updates need to be uniquely tailored.

Linux kernel is one of the main building blocks. Android uses Linux kernel and kernel versions depends on the hardware of the device. Linux for android has various additional components like binders, wake locks etc.

Apart from Linux kernel there are other software stacks responsible for proper working of android namely, middleware technologies, APIs, libraries, application software and framework. Dalvik which is a virtual machine with JIT compiler was used in android till 5.0 version to run dex-code. Each time an application is launched Dalvik performs compilation and local execution. Ahead of time compilation has been in use from android 4.4 which uses application byte code.

2.5 ANDROID SECURITY AND PRIVACY

Android devices are one of the devices which allow investigating agencies to access user data, here data encompasses all the communication that takes place from SMS, chatting apps, social networking sites. Apart from this privacy risk, android faces certain security threats like malware which sends advertising clips or messages to other users without any knowledge of the user and in turn the personal information is shared to some third party. Android platform has been seeing the rise of security threats exponentially over the years as compared to IOS, but engineers beg to differ saying its advertising gimmick by security companies [23].

Security related issues regarding downloaded applications is taken care of by the android engineers as all the applications in the devices are stored in the sandbox which is isolated from other system resources. If an application requires special access or permission, then it is mentioned while downloading generally from play store.

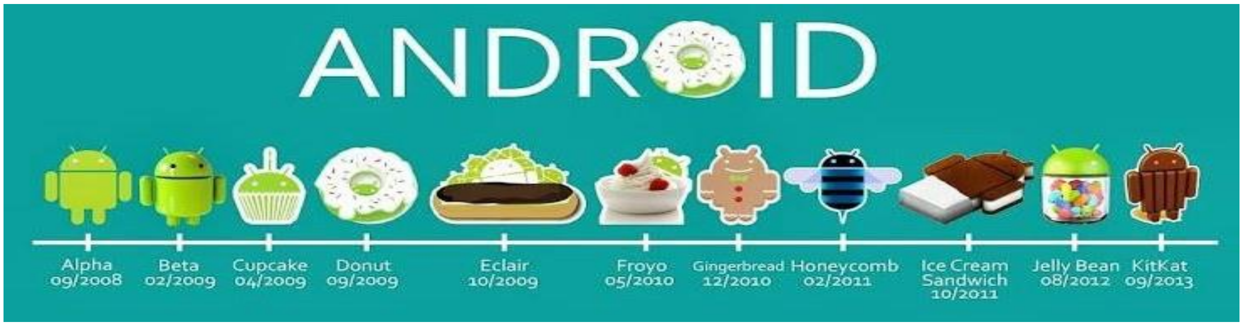


Figure 3: Android versions

2.6 INTRODUCTION TO ANDROID WEAR

Operating system by Google which will is integrated on to wearables like smartwatches. Wearables work by connecting to the android phones with version 4.3 or newer. Some of these devices are compatible with iOS phones as well but with limited features and support. Android wear supports certain application features through Bluetooth, Wi-Fi or mobile data. These applications can be downloaded through android market like Google play store. By the reports in 2015, 10% of market share was of android wear in all the smartwatches.

On 24th March 2014, android wear platform was launched. Along with the platform developers preview was released. At the time of launching the most successful android mobile devices producing companies were declared as partners. Companies included Samsung, HTC, LG, Motorola. The first watch which was launched and then shipped was LG G watch. Moto 360 followed suit. The next android update gave new watch face API and added new features in December 2014 via lollipop version.

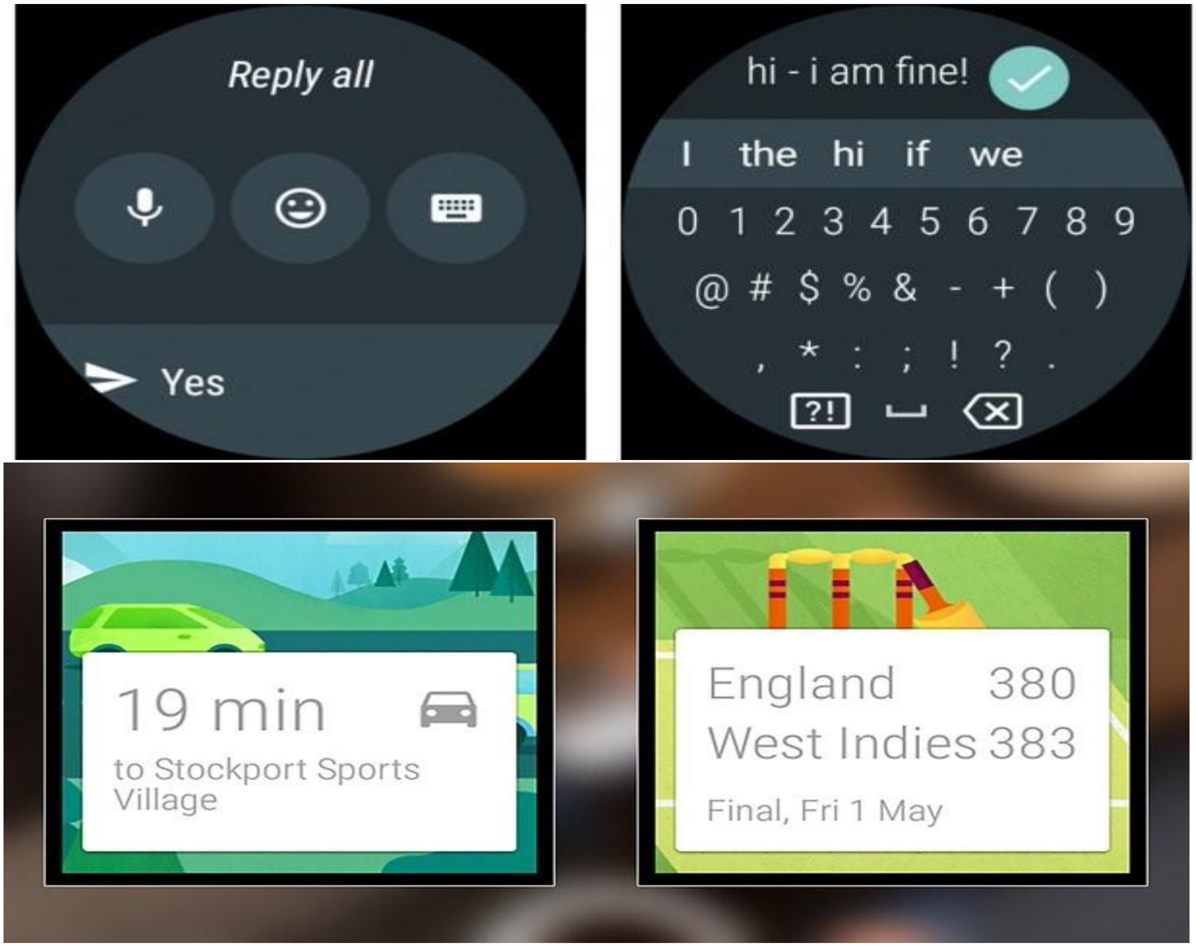


Figure 4: Android wear special features

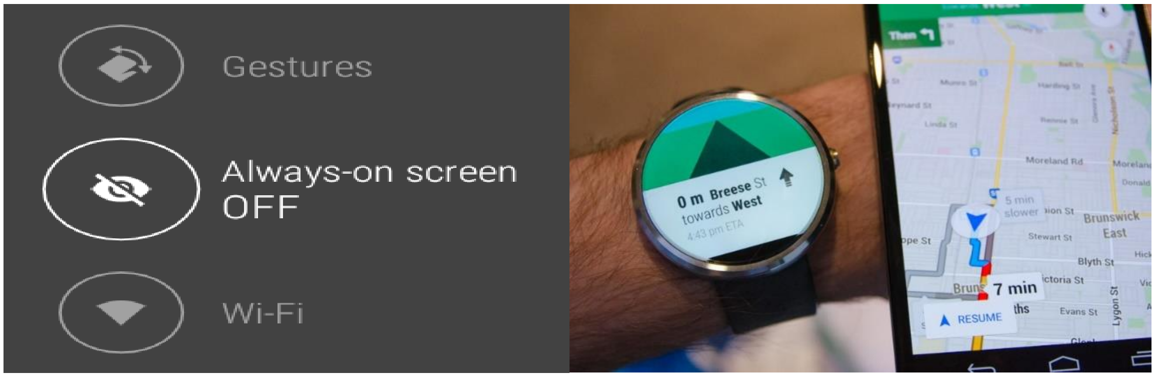


Figure 5: Always on display feature and navigation on android wear

2.6.1 FEATURES OF ANDROID WEAR

Like android phones android wear also had features like always on, tilt to wake the screen and get directions from phone. This application which provides direction also allows user to start journey as well as update it in the log and the app also gives turn intimation. Similarly, there exists a fitness app in the watch and phone as well. This app tracks running, walking, sleep, food, time to bed notifications, calorie count, step count. These applications sport sensors and work well with Google (say Ok Google) search. Watch also gives notifications of the goals reached like fitness, sleep etc. At the end of week summary of the collected data is presented to the user. Android wear can control the phone like playing music, calling, taking pictures, finding the phone and seeing the notifications. User gets notifications from selected notifications on the watch through vibration engine. Google Voice can also be used to reply messages and emails using dictating response and Google hangout notifications can also be replied to with the help of voice messaging. Also Google Now notifications specifically intelligent notifications like check-ins, bookings, flight timings, traffic updates, weather and stock updates are also supported. Okay Google makes it easy for users to set up alarms. New SMSs can also be initiated from android wear. Artificial intelligence is used in android wear from version 5.1.1 which lets users to draw responses. And the same technology helps users to draw emoji and also Google search is supported. Camera on the phone can be activated to relay to the watch and through it camera features can be controlled. If any third party application uses camera, then phone's camera is used for streaming instead of watch's camera. Notes, appointments, check lists and Google keep is supported completely [24].

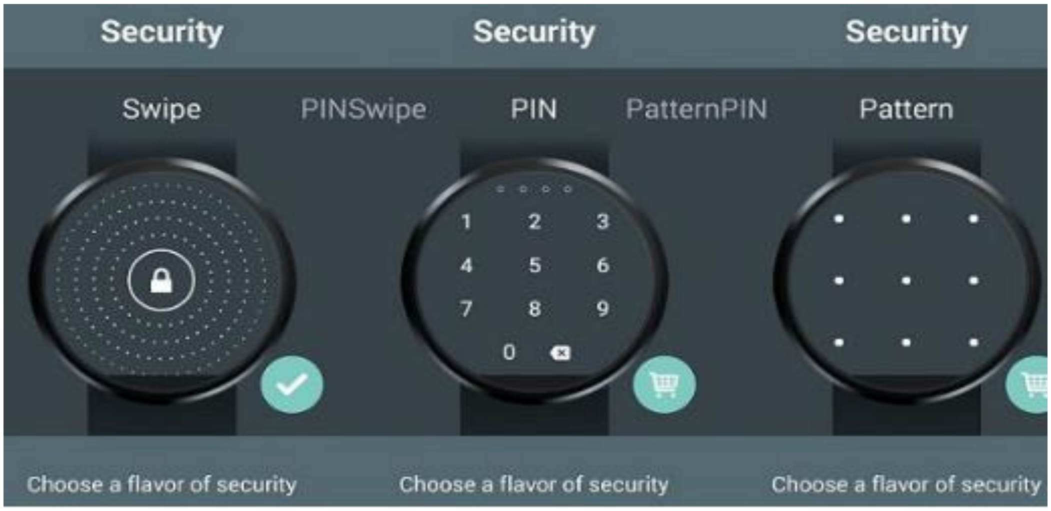


Figure 6: Screen lock on android wear

2.6.2 ANDROID WEAR VERSION HISTORY

June 2014 saw the initial release of the android wear with base version 4.4(W1). In the same year platform saw the new update version 4.4(W2) with features like playing music over Bluetooth with better music player user interface and GPS support. In December 2014 itself version 5.0.1 was released with some new popular interest updates. Updates included sunlight and theatre mode, ability to undo notifications that were cancelled earlier, just completed actions log, battery usage statistics. Next year in 2015, Google released android wear version 5.1.1. This update supported Wi-Fi, drawable emoji, pattern lock screen, notifications heads up. Also allows user to change font size, in order to access app drawer swipe left on watch screen. This update saw many hand gestures added and now applications could be on always. In 2015 itself there was a new update which had added features like Google translating to android wear and now faces of watches were more interactive. Version 6.0.1 was released in year 2016 in which the wrist gestures were improved. Additionally, speaker of the watch was also improved and directly from the watch messages could be send. Next update version saw the comeback of restart the watch option out of many. Bugs were fixed and security level for the screen was added. Early 2017 will probably see the release of android wear version 7.x and the tech gurus are estimating certain improvements like built in keyboard for texting, smart notifications, better user interface, Google play store on the device.

CHAPTER 3

ANDROID SECURITY

3.1 INTRODUCTION TO ANDROID AUTHENTICATION

Authenticating phones at present is one of the most important and necessary measure. As internet is at fingertips, sensitive data is at risk. As there is an increase in the usage of mobile phones for online shopping, online banking, the user's privacy is at risk. Smart-phone encompasses literally all the data that hackers look for like passwords, details like credit card information, contacts, emails. All the applications on phone require a user to allow the application to access certain information that can be sensitive, and this information is stored in cloud which makes it available at another avenue for hackers to access. Authentication of applications may not be covered in this paper but plays major role in understanding the vulnerabilities we face. As all this data can be accessed easily through it is very important to have the authenticated users access it, which forms the basic security layer. Wearable technology is on all time high but security is being left behind. We will concentrate on smart-watch as our smart wear technology in this paper as our experiments will be held on it. According to the survey held by HP on the smart-watch Security the results were "disappointing but not surprising". The major vulnerability found in this survey is lack of authentication apart from lack of encryption and privacy issues. This opens doors to new threats to sensitive data. Notifications are pushed onto smart-watch from phones and lack of authentication can lead to information being handed-over to wrong groups [35].

3.2 THREATS AND ISSUES FACED BY ANDROID

Mobile computing has recently seen a lot of increase in usage so did the threats that the smart phones face and users too. Therefore, concept of mobile security has gained immense importance due to the amount of threat faced by android devices. Smart phones are being used for more business purposes to plan business arrangement and organize their work. Apart from business smart phones have taken over private lives of people too. In companies these new technologies have caused changes in information systems and these changes lead to rise of new sources of threat. Privacy of users need to be protected as users are increasingly using the smart phones and android devices to share and store sensitive data whose access needs to be limited to protect it. Smart phones, android wear are like new age computers therefore under attack. There are various weaknesses on android devices that attract the attackers. In android phones even simple services like Short Message Service and Multimedia Messaging Services can be attacked. Wi-Fi, Bluetooth, GSM are also targeted as a lot of data is been transferred through these services. Browsers and operating systems on whole are also not safe from these attacks. When there are attacks there are counter measures, which are being developed to counter the ever growing threats.

3.2.1 THREATS FACED BY ANDROID MOBILE PHONES

When a user is using a phone he is exposed to various threats, according to a survey by ABI the threats of new kinds have grown tremendously at the rate 261%. On this basis it is safe to assume that the data can be transmitted or modified by the attackers who rise the threats. It is of high importance at this time for all applications to be able to provide privacy to its users and take care of the security concerns. Attackers target weak points like, using GPS location, blocking the user address book, billing users for the services which were not used by the user.

Attackers mainly have the following targets:

- Data: What attracts attackers to data is its sensitivity. Smart phones with internet have made life easier for users to access online resources like online shopping, social networking sites etc. These can lead to the users saving or transferring sensitive data like credit card numbers, passwords, social security number, private information, contact list, activity logs.

- Identity: When owner of the smart phone is targeted attacking the phone is easy to gain information about that person as phones today can highly be customizable and it can reveal a lot of information about the owner.
- Availability: Owner can lose the control over the device and can end up getting restricted use.
- Attackers can be grouped into the following three categories:
- Professionals: Sensitive data is stolen by professionals from general public. Even military is not safe from the attacks by them. They can use the sensitive data gained from one attack to execute another attack.
- Thieves: These attackers produce threats to gain money. They get income from the attacks made, identities stolen or through sensitive data collected.
- Black hat hackers: Availability is the basis on which attacks are made. Main purpose is to make viruses, which are potent enough to cause damage to the device and steal sensitive data.
- Grey hat hackers: They don’t believe in stealing information or damaging devices. They just show the vulnerabilities that the device faces and gets them noticed.

3.2.2 CONSEQUENCES OF THE THREATS

The phone that was attacked will not be owned by its owner anymore, it will end up being the zombie machine of the attacker. Once it is controlled by the attacker it can be used to send spam messages via

SMS or email. Not only email or messages but phone calls can also be made by the attacker by going through the contact list or by accessing the phone directory and this can lead to extra charges for the owner or sometimes attacker can congest the network of the emergency service numbers by calling. Privacy concerns arise when a device is compromised and this can lead to the conversations being recorded or heard by the third party and this could lead to business damage. User's identity is always at risk when security issues arise, mainly the identity can be stolen when the device is compromised and this can be done by as simple technique as hacking the user's sim card. Security and privacy issues are on all time high due to the options of online orders, online transactions, bank account details. Not only the applications or the identity is at risk even he basic phone performance can be degraded when compromised. They can achieve this when attackers keep running one or more applications in the background which will drain the battery life. Mobile computing is anyway considered less performance oriented when compared to the traditional computers. Attacker is also in the position to stop users from using the devices or not letting devices function properly. Operating system of the device can be can be disabled to work by deleting the boot script files. Or the attacker can install an application that would discharge the entire battery at once. Attacker can also steal the private information of the user like pictures, contacts, videos, messages, music and business details alike.

3.3 DIFFERENT KINDS OF ATTACKS

3.3.1 SMS AND MMS ATTACKS

Binary messages cannot be handled by few phones, this conditioned can be achieved by sending blocks which force the phone to restart and this can lead to the denial-of-service attacks. Example of such scenario is when a Chinese character is sent to the phone Siemens S55, this would lead to denial-of – service attack. Internet can the breeding grounds for these kinds of attacks, SMS that is sent from internet can be the source of Distributed denial of service attacks. Network will be overloaded by the message requests thus causing delay along the way.

Apart from SMS, MMS can also be the source of risk. When a user gets an MMS attached in a message, the user can choose to download the attachment and if he does then the virus that is present in the MMS infects the device when forwarded to the other contacts virus spreads thus infecting major number of devices. Sometimes without the knowledge of the user the malicious software can be downloaded with the MMS and send messages or MMS to the other contacts [44].

3.3.2 WIFI BASED ATTACKS

Information can be gained when eavesdropping can be done on the Wi-Fi network. This kind of attack can take place on any device but smart phones are more vulnerable than others as Wi-Fi is used as the main means of accessing internet and communicate through it. Thus making security of the wireless networks an important concern. Initially WEP keys were used to maintain security of wireless networks but then the shortcoming of this method was encryption key which was short and was same for all the clients that were connected. WPA is the current method used to protect wireless networks and is based on TKIP protocol. It is based on the fact that all the previous devices connected and protected by WEP will have a smooth transition to WPA. Dynamic encryption keys are seen as the improvements in this protocol and when it comes to smaller networks WPA has a pre-shared key which is similar to shared key. Short encryption keys are vulnerable to attacks more than a decent length key. Mobile device's keyboard has limited options for users to set the key, users tend to choose numbers for short length keys, this puts the network at high risk that can lead to attacks by using brute-force technique. Just like GSM where breaking the identification key guarantees successful attack not only on an individual phone or device but can extend to an entire network. Wireless LAN are mostly remembered on the smartphones which lets users not to identify themselves each time they want to connect to the network this gives less scope to attackers to crack the key, but when attacker duplicate the network with same characteristics then the device may get confused and connect to the attacker's network. Data transferred on this network can be intercepted by the attacker if the encryption protocols are not implemented on the network. Worm named lasco infects the device as it makes the device believe that the file being downloaded is from a trusted source.

3.3.3 ATTACKS BASED ON BLUETOOTH

Attacks on Bluetooth differ from device to device and different devices have different security issues. Major security threat is the services that are not registered and don’t seek authentication, virtual serial ports are dedicated to control the cellular devices. Once the attacker has the control over the port then they can gain complete control over the entire device. For files to be transmitted phone's Bluetooth must be in range to the other device and it should be discoverable to other devices. Attacker can send file through the Bluetooth and when the recipient accepts the request virus can be transmitted over. Even without the knowledge of the user the virus can search for the other discoverable devices and then transmit the virus over and damage the device.

3.3.4 ATTACKS ON WEB BROWSERS

Web browsers in general have been the grounds of attacks likewise mobile browsers also work and navigate similarly with plugins and widgets. Vulnerabilities in web browser can be used to attack the device or the system. Attack can be based on a frequent occurring problem like stack overflow. Vulnerable libraries can also form the vulnerability in android. But due to the android sandbox architecture the damage was restricted to the browser only. Due to the lack of strong antivirus mechanisms devices face phishing, malicious software and websites.

3.3.5 ATTACKS ON OPERATING SYSTEM

When attackers modify operating system then the safeguarding rules and criteria become null. When bytecode is being bypassed then operating system can be on the attacker's radar. Change of firmware results in operating system and system on whole being compromised. Even though OS stored in ROM in mobile devices and malware cannot alter it, in some devices and in some circumstances, it is possible. Certificates play an important role in verifying the source of downloaded application. Certificates can be faked and added to the list of recognized certificates.

3.3.6 HARDWARE VULNERABILITY BASED ATTACKS

Simple hardware like headphones can also be a vulnerability. When headphones are plugged in to the device through audio-output jack and spoofed audio commands to control the device and make it perform functions wanted by the attacker. USB port has a dual use. By using malicious charging set ups in the public places viruses can be installed into the device.

3.3.7 PASSWORD CRACKING ATTACK

Smudge attack can possibly help the attacker crack the password. This attack works by attacker following the victim's finger smudges on the screen. Whereas in public shoulder surfing can result in attacker knowing the password or patterns by following the finger strokes.

3.3.8 MALWARE ATTACK

Malware can compromise mobile devices like personal computers as they form the single major point access to internet. A program whose only purpose is to damage the system in which it resides is called malware. Examples of malware are worms, Trojan, virus [44].

- Worm: when multiple computers are connected over a network the program which multiplies on all those screens is called a worm.
- Trojan: smart phones when running a program that allows external systems or users to connect to the device discreetly is called Trojan.
- Virus: it is a software that is designed to damage other systems by inserting themselves into the other system and run parallel programs.
- Ransomware: mobile users are generally less conscious about the security thus leading it to be one of the most attacked platform. Ransomware has grown as a threat in recent years strongly. It is like not letting the user unlock their device and asking money for allowing them to unlock and use their own device. This is a big threat to users whose business is mobile dependent. It can mean sensitive data being gained and asked for ransom to not leak it.

- Spyware: this is a program that sends whatever data is gained to a server called flexispy.
- Malware attack works in phases. It has three phases namely infection of host, accomplishment of goals, spread of malware. Malware uses all the resources that the infected device has to offer for example, the output port like Bluetooth or the stored resources like contact list or email list. As users trust each other when part of the contact list malware exploits this trust.
- Infection phase: by using faults or vulnerabilities malware gets into the device. This is infection phase where device is infected. Depending on the degree of infection it can be categorized into explicit permission, implied permission, common interaction, no interaction. In explicit category user is asked if it can possibly infect the device or not. Implied category is based on how users can
- be attracted and tempted into installing certain applications like games which carry malware. Common interaction probably is the most used for victimizing users, it is sent via email or MMS.
- No interaction category has smartphone being infected without contact.
- Accomplishment of goal: once the device is infected the attacker would want their goals to be achieved like damage the device or the data present.
- Spread to other systems: when a smartphone is infected or damaged, it will certainly spread it to other devices through Bluetooth, Wi-Fi, emails etc.

3.4 COUNTER MEASURES FOR ATTACKS

Threats can be countered if good measures are taken. As all threats, cannot be countered at the same level measures are also categorized based on counter level. On a bigger picture user knowledge is important to counter threats. User should have knowledge of careful surfing and downloading. At the same time manufacture surveillance is also required. Usage of software, protecting OS can be considered as good measures to combat threats.

3.4.1 MEASURES FOR PROTECTING OPERATING SYSTEMS

Operating system forms the first level of security so it is important to protect it from threat. One of the measures is rootkit development. Rootkit inclusion in the mobile device is as dangerous as it is on other device. Due to programs like these securities can be partially or completely compromised. Therefore, it is important to stop such intrusions. For countering this certificate check can be made and if the result is not satisfactory boot stops. As every user name is assigned to every function it is important that there is no malicious software in the system as it does not let the proper functioning of the system. So sandbox approach can be followed and blocked from interfering with the system. Permissions are required for users to edit and make any changes to any file. This permission mechanism helps to keep the restrictions on who is being able to view, edit or update which file. Memory protection takes care of the scenario where one process gets to memory that is allocated to other processes and can change the data.

3.4.2 SECURITY SOFTWARE

Software built for combating security issues and threats. Security software forms the second layer of protecting mechanism after operating system. Examples of such software are:

- Firewall / anti-virus: this software protects the device from known threats. It will scan for infectious programs or applications; signature check is usually done. Large companies protect their networks through firewall. Firewall scans the traffic in the network and ensures no malicious program enters the network.
- Visual notification: this helps users deal with actions which were not initiated by them. For example, call being made or messages being sent. What this does is how the notification or any action that is taking place on the device.
- Turing test: this is used to differentiate between real users and virtual users.
- Identifying via biometric: morphology is used in this biometric technique to authenticate users like eyes, voice, fingerprints.

3.4.3 MONITORING RESOURCES

When certain actions are triggered on the device it is easy to detect any malicious software on the device. One such parameter is battery usage, if battery is draining way too quickly it can safely be assumed that there is some malicious code in the device. If one application uses more memory than generally required, then it is suspicious. If any application is using more bandwidth in the network than usual, then it has to be checked. When different services are active when not really in use then there has to be a check done.

3.4.4 SURVEILLANCE OF NETWORK

Network routing points can be checked if the network is safe or not. The mobile network usage is predictable, if it deviates too much then it need attention. Spam filters are used in the network to try and detect spam messages. Encryption can be used to safeguard any information stored, transferred or maintained. Network behavior for services like SMS, MMS can be predictable when compared to protocols used on computers. When heavy traffic is generated by an application then it can be scanned to make sure it is safe.

3.5 CURRENT AUTHENTICATION METHODS AND TRENDS

3.5.1 PASSWORD/PASSCODE/PINS/PATTERNS

These are one of the oldest methods of authenticating. But sadly with growing technology the hackers have also grown smart, there are many apps in market right now to break a password or pattern. Shown in. Considered the least level of authentication. Shoulder surfing is one big threat to this method. People have similar patterns set for ease of remembering, which makes it easy for hackers to break through.

3.5.2 FINGERPRINT VERIFICATION

Finger print verification is one of the most-effective authentication methods. This method possesses three stages: enrollment, searching and verification. This method always has secondary authentication generally a pin in-case of failure of fingerprint recognition. The unlocking attempts are limited; after last attempt the user is asked to enter the pin for unlocking. Many online applications are using this method for authentication of their users.

3.5.3 GENERATION OF QUESTIONS

One of the systems implemented is where authentication questions are generated based on data collected by smartphones which in general is location information. Location-based profiles are built for all the users based on the data periodically collected like WIFI points the user is connected to. This method was tested on 14 individuals some in sets of two and others individually. Two sets of questions are presented to the user: one based on user's own data and the other set chosen randomly. This method implements algorithm based on Bayesian classifier to authenticate legitimate users. First step in this implementation is to calculate user's score for every authentication session, every incorrect option is penalized so that users will not attempt to compromise the system [2].

3.5.4 ONE TIME PASSWORD GENERATION

The other popular method used by many online services is the usage of one-time password(OTP). Services like banking, online transactions, chatting websites etc. use OTP to authenticate users. Any chatting application these days like WhatsApp, hike, WeChat requests the user to enter the OTP before being able to start the application to make sure that authorized user is only using the application with the given phone number. To lower the risk of passwords being stolen, shoulder surfing, phishing used passwords can be volatile. GPS nowadays is precise and this ca help implement this method without any problem. This method is comparatively easy to implement when compared with other methods. This method requires only the in-built GPS system and no special designs or interfaces which makes it cost effective. OTP is generated based on time and location which will be difficult for the hackers to know the exact details [44]. In-case of a misjudgment where a legal user is not allowed to access the service, SMS service can be used [18].

3.5.5 POLICY BEACON

A small device called policy beacon is placed in an area to draw a boundary in which the policy is in effect. It has an area location service discovery implementation and it can be used by mobile devices. If mobile devices are equipped with policy beacons protocol, then they will be able to sense the active policy beacons in that area. Foot print of the beacon's communication signal determine whether the device is in the vicinity or out. Policy Beacon authentication mechanism checks the proximity of the policy beacon on a mobile device. If a device is being able to be detected and verified it is considered successful.

3.5.6 TWO FACTOR AUTHENTICATION

This method follows two factor authentication which means it has two different authenticating mechanisms combined together. Here location and Biometric are combined. GPS tracking is used to know the location of a particular user. GPS gives longitude and latitude coordinates and send them to the local server for authentication. Fingerprint is used as the biometric here. Fingerprint identification algorithm is used. This method uses encryption for exchange of data after authentication

3.5.7 LOCATION REGISTRATION

This protocol has two level implementation. In the first level registration algorithm is used. Registration by users is allowed only once, when the user is joining the system. Next level is authentication. Authentication is performed for every session unlike registration phase. In this protocol, taken information which is based on location is typically divided into two major types namely, static and dynamic. Static location is the information that has the standard/static location of user that was logically captured during user registration and is stored in location based ID database. This location information is not changed till the user explicitly changes it. Dynamic location Information is gathered when the user requests for the authentication. Here authentication server sends some authenticating challenges to the users when they want to access the system. Response to the challenge question is given by the user by giving the security credentials. On success of this step the server authenticating the user sends location information for verification and the request is raised to the client application, which resides on the user's smart-phone. User is prompted to enter the PIN and then this PIN is sent to location based ID database and encryption is performed [7]. Results are sent to the server by location authorization policy and then finally user is authenticated by the server (authenticating server) [6].

3.5.8 SMART LOCK

Android version 5.0 saw the rise of smart lock option and over the years it saw some good evolution. Now there are more options through smart locks which can secure the mobile phones. Smart lock is preferred to be used when user knows apart from him no other person will have access to the phone. Smart lock's advantage lies in the fact that user does not have to undergo the pain of authentication every time he is trying to access the phone at specific locations, when connected to devices or with face and voice [27].

PROS:

- No need of remembering passwords, patterns
- Simple
- Convenient
- Smart compatible

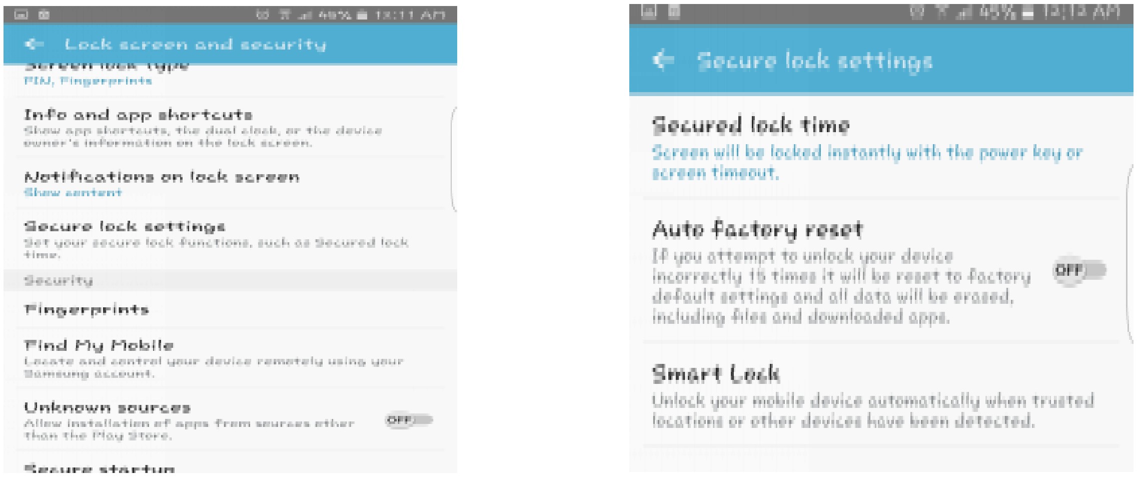
CONS:

- Vulnerable
- Limited distance

- Limited time activation
- Security trade-off for convenience

Process of enabling smart lock is as follows:

- In order to use the smart lock, user needs to go to settings and select smart lock.



49% 12:11 AM

Lock screen and security

Screen lock type
PIN, Fingerprints

Info and app shortcuts
Show app shortcuts, the dual clock, or the device owner's information on the lock screen.

Notifications on lock screen
Show content

Secure lock settings
Set your secure lock functions, such as Secured lock time.

Security

Fingerprints

Find My Mobile
Locate and control your device remotely using your Samsung account.

Unknown sources
Allow installation of apps from sources other than the Play Store. OFF

Secure startup

45% 12:12 AM

Secure lock settings

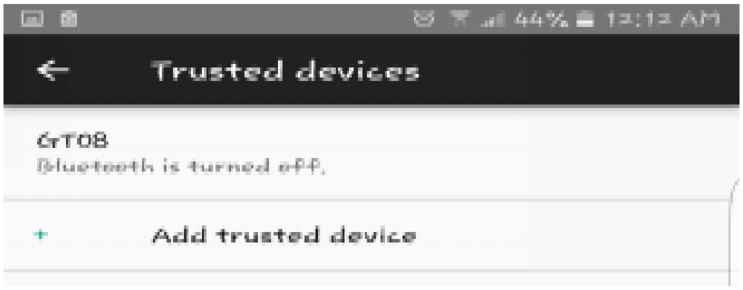
Secured lock time
Screen will be locked instantly with the power key or screen timeout.

Auto factory reset
If you attempt to unlock your device incorrectly 15 times it will be reset to factory default settings and all data will be erased, including files and downloaded apps. OFF

Smart Lock
Unlock your mobile device automatically when trusted locations or other devices have been detected.

Figure 7: Android security features

- Once user selects smart lock, options available on smart lock are displayed. User can select any feature suitable. Examples of features are like following:



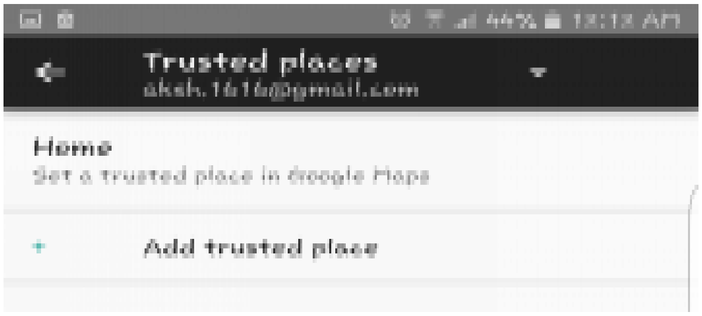
44% 12:12 AM

Trusted devices

GT08
Bluetooth is turned off.

+ Add trusted device

Figure 8: Trusted device feature

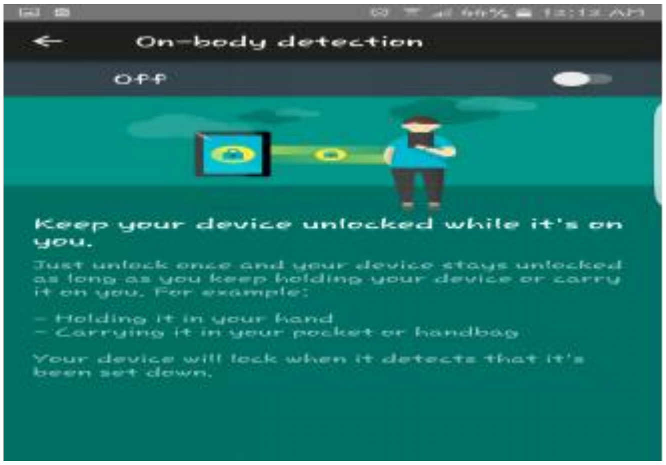


Trusted places
aksh.1616@gmail.com

Home
Set a trusted place in Google Maps

+ Add trusted place

Figure 9: Trusted place feature



On-body detection

Off

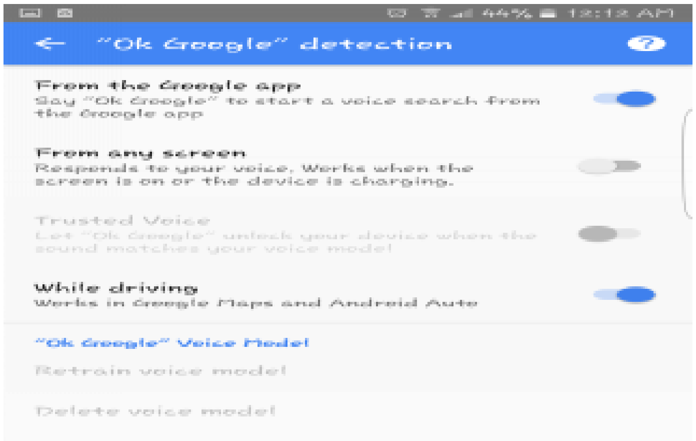
Keep your device unlocked while it's on you.

Just unlock once and your device stays unlocked as long as you keep holding your device or carry it on you. For example:

- Holding it in your hand
- Carrying it in your pocket or handbag

Your device will lock when it detects that it's been set down.

Figure 10: On-body detection feature



"Ok Google" detection

From the Google app
Say "Ok Google" to start a voice search from the Google app

From any screen
Responds to your voice. Works when the screen is on or the device is charging.

Trusted Voice
Let "Ok Google" unlock your device when the sound matches your voice model

While driving
Works in Google Maps and Android Auto

"Ok Google" Voice Model

Retrain voice model

Delete voice model

Figure 11: Trusted voice feature

- TRUSTED VOICE: By following in the footsteps of 'OK GOOGLE', Google has added a similar feature in smart lock. 'OK GOOGLE' feature is available on most of the phones and works even when is locked and keeps track of what user is talking and act according to user's command. Similarly trusted voice works, meaning it listens to the user and when the voice matches automatically the phone unlocks. Disadvantage of this feature is that any voice close enough to the user's voice can unlock the phone at a very low battery discharge. Therefore, not considered to be the secure option [27].
- TRUSTED FACE: Android version 4.0 saw the introduction of the trusted face feature. Unlocking a phone without the need to enter the password was a real thing and was done by phone remembering user's face and unlocking. Major disadvantage of this method is that it makes easy for attackers to pass through any security that is there. Feature introduction saw the spoofing attack as the major threat in the initial days. Spoofing was possible with just the user's photograph. After much improvements this feature saw the additional security feature in which user has to blink eyes while setting up this feature which showcases the liveliness of the user. Disadvantage of this feature was the amount of time required to spend looking at the camera before it unlocks. After the feature was added to the existing bundle of smart lock it has improved drastically and notifications can be taken from lock screen. If the phone does not unlock by face detection then, password or other security feature will be activated [27].
- TRUSTED PLACES: This is one of the easiest feature on user as it requires no input from user's end. This feature runs in the background without interfering in any other process. This feature uses phone's GPS. GPS has to be turned on for this feature to work and is very much customizable. Home address or office address can be entered and once in that location phone will be kept unlocked with just swipe screen as security, once out of the places mentioned phone will be locked.

- ON-BODY DETECTION: This feature helps people who cannot or do not prefer carrying phone around. Phone will be unlocked in all the times where it is stationary for example kept on a desk or in a bag. Once the phone is touched or unlocked by the user, it keeps the phone unlocked till the phone is in user's hand or pocket, basically as long as it is on user's body it is unlocked. Sensors are activated and feature heavily depends on them. Comparatively it is safer.
- TRUSTED DEVICES: Simplest way to use smart lock is by using trusted devices feature. This feature requires either Bluetooth or NFC to be turned on. Using Bluetooth is recommended as scanning NFC tags take much longer time than unlocking phone through normal security feature. When any new device is connected smart lock pops up a message asking if user wants to add that device as a trusted device. Then as long as the phone is connected to the selected trusted device phone is unlocked. But one big disadvantage of this feature is that it keeps the phone unlocked for nearly four hours even when there is no interaction taking place. After four hours it reactivates the security lock [27].

3.6 ANDROID ENCRYPTION ON PHONES AND WEARABLES

Android phones do not have their entire disk encrypted. It is usually how applications encrypt their data. Every application has its own server and can be stored on any other third party sever, so encryption and privacy is not guaranteed. Communication over Bluetooth is encrypted but is considered to be breakable. In general user has an option to encrypt the entire device by using encrypt security feature. Android manufacturers can alter the software at certain levels and use different components apart from what Google releases. Therefore, there arises security issues which can not be controlled by Google. Due to performance issue manufacturers have revoked default encryption feature. Passwords or other security feature will act as the guarding aspect when the device and information on it are encrypted [28].

Android wear has its share of security issues. As android wear is connected to smartphones it is even more important to know how well it is abled enough to handle threats. These two devices connect through only Bluetooth and this opens up new avenues for attackers as Bluetooth is always on. Plain text messages can be taken over from the Bluetooth. Data is always stored on smartphone and just projected on smart watch, which limits the risk. There is no specific encryption algorithm that is used to encrypt the device but applications can.

CHAPTER 4

PROPOSED ENCRYPTED APP LOCKING SYSTEM

4.1 MOTIVATION BEHIND THE SYSTEM

As discussed in the prior chapter, the smart lock has become the easiest way of authentication for users but with the kind of disadvantages that this method has per feature is tremendous. We will be using the trusted device feature of the smart lock. Typically, this is one of the secure ways of smart lock but with certain disadvantages which can compromise the security at the very basic level. This feature can be activated by either connecting it through Bluetooth or NFC tag. In general, the trusted device is either a smart watch or any device that can be connected to the phone via Bluetooth. Traditional features like passwords, pins, patterns are not secure enough, as we have already established and can be hacked but is stronger than swipe screens and no locks at all. Similarly, Bluetooth connection is prone to attack so inevitably trusted device falls prey to it as well. All the other features of smart lock are. So our aim is to propose a system which can utilize the strength of the old, new, strong and weak systems. Which is secure but does not take away the ease from the user. Security in the android can be made stronger when the application being used is having it own cryptosystem. Encrypting the communication between the devices can ensure that certain threats can be avoided. Having kept all these strong point in mind the proposed system combines the strength of password, ease of trusted device and security of encryption [36].

4.2 SYSTEM DESIGN

The proposed system uses three security features encryption, trusted device, password. Two entities are used for us to implement our proposed system. Firstly, a connected has to be established between the android wear and the android smart phone. User needs to turn on the Bluetooth and connect the smartphone to the android wear. Before the connection, the application needs to be installed on both the devices which will run in the background [40]. The basic functionality of the application on the watch end would be to identify itself to the phone. On the other hand, application on the phone end will be in-charge of checking the credibility of the watch connected by using the encryption technique and keeping the user chosen applications locked as long as the watch is connected to the phone via Bluetooth [41].

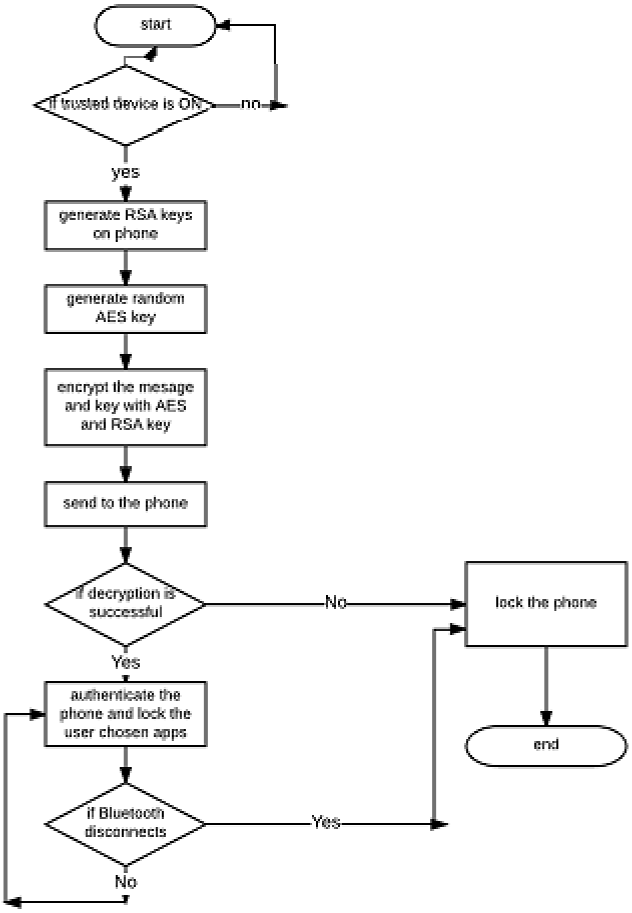
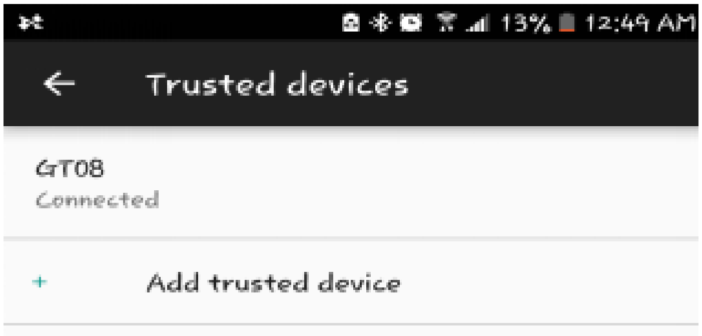

start
if trusted device is ON
no
yes
generate RSA keys on phone
generate random AES key
encrypt the mesage and key with AES and RSA key
send to the phone
if decryption is successful
No
lock the phone
end
Yes
authenticate the phone and lock the user chosen apps
if Bluetooth disconnects
Yes
No

Figure 12: Flow chart of the proposed system

Functionality of the system:

- User installs the application and selects the applications to be locked.
- And sets a passcode
- User connects the smart watch and smartphone via Bluetooth and enables trusted device feature.

- The application works as long as the connection between both the devices is stable.
- Once connection is set, phone will remain unlocked and the applications chosen will be locked.
- After getting connected to the phone, the application will be launched on the two devices and this will push the watch to ping the phone stating that it is connected the same watch.
- Phone will receive the message through the application and will carry a check to authenticate the watch.
- If watch fails the test, the phone will be disconnected to the watch and prior security feature on phone will be activated.
- If the watch clears the check, then the application makes sure connection is maintained and will keep the phone unlocked and apps will be locked till the devices are connected by not interfering in the push notifications.

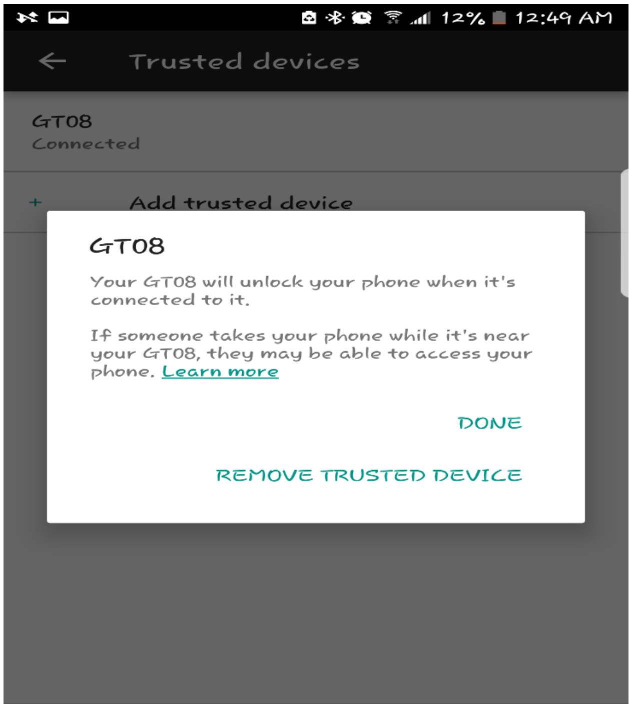


Trusted devices

GT08
Connected

+ Add trusted device

Figure 13: Connecting the android wear as trusted device



GT08

Your GT08 will unlock your phone when it's connected to it.

If someone takes your phone while it's near your GT08, they may be able to access your phone. Learn more

Figure 14: Phone stays unlocked due to smart lock feature

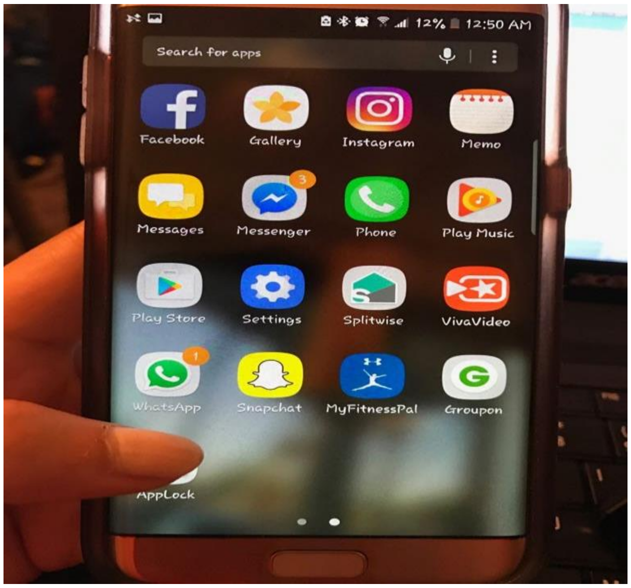


Figure 15: App locker

4.2.1 CRYPTOGRAPHIC DESIGN

As the system functionality section already stated, the watch needs to get authenticated to have the apps locked and smart lock feature to be secured. To authenticate, cryptography system is used. Here we will be using both RSA and AES algorithms [39].

- FORMAL DEFINITION OF RSA:

RSA is an example of public key encryption which is generally used for transmitting data securely over network. Encryption and decryption keys varies in these kinds of algorithms, like public key is used for encryption and for decryption private or secret key is used. What makes this algorithm strong is factoring prime numbers which are large and different [54].

In general, four key steps form the integral part of this algorithm:

- Key generation
- Key distribution
- Encryption
- Decryption

Algorithm:

- The process of key generation requires users to select two large prime numbers (p, q), which is encouraged to be generated randomly and which are a secret.
- Next step is to compute product of p and q which acts as a public key;

$$n = p*q$$

- Calculate Ø(n), which again is a secret

$$Ø(n)= (p-1)\ (q-1)$$

- Select a prime large number 'e' which is a public key that is usually preferred to be less than (p-1) or (q-1) and 'd' which is a private key. Condition is that e should be prime (relatively) to Ø(n);

$$1 < e < Ø(n)$$

- 'd' acts as a private key that needs to be calculated by using the following formula:

$$d = e^{-1}\ mod\ Ø(n)$$

Which is taken from the formula:

$$d*e = 1 \text{ mod } (n)$$

- Public key can be represented as k_s = {e, n}
- Private key can be represented as k_s^{-1}= {d , n}
- Key distribution is done by first entity sending public key Ks = {e, n} to the other entity and secret/private key is not distributed ever.
- Most of the calculation lies on the following formula:

$$C = M^x \text{ mod n}$$

- Where M is the plain text or the message being sent or encrypted, C is the result

For encryption process, key e is used and plain text is, M < n

$$\text{Cipher text} = C = M^e\text{(mod n)}$$

- For decryption key d is used. Calculation is required:

Calculate: C^dmod n

$= M^{ed}$mod n = M

RSA formula in general is written as: X^{y} % n = $X^{(y \, mod \, \emptyset(n))}$ % n

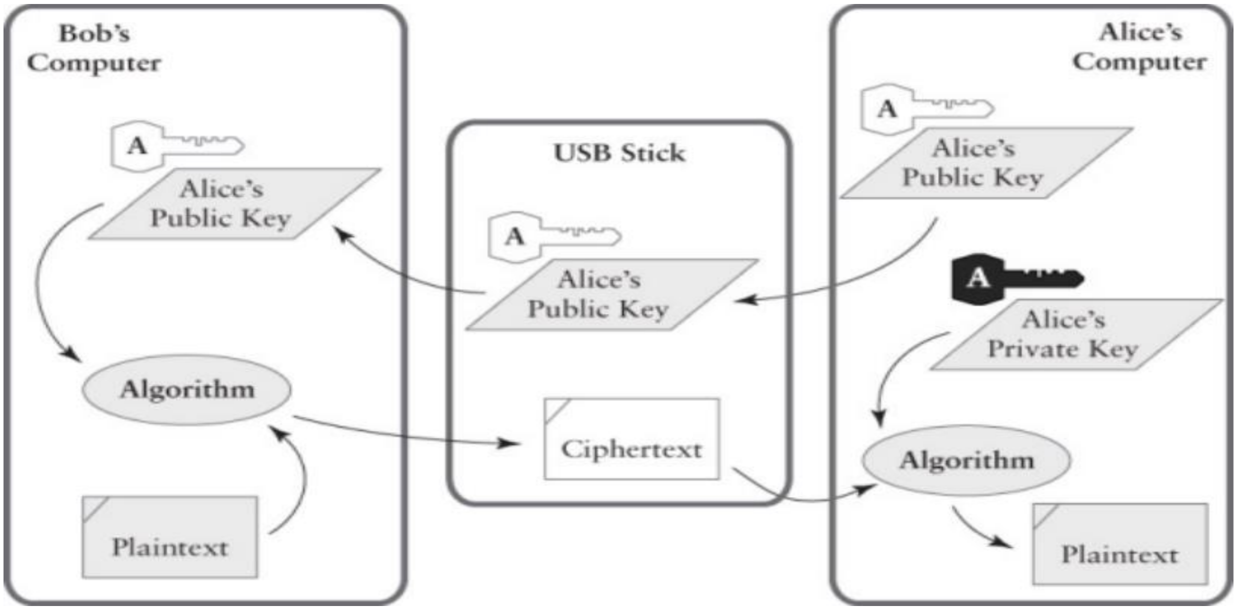


Figure 16: RSA example

- FORMAL DEFINITION OF AES: AES is an acronym used for Advanced Encryption Standard, which is used for encryption and is a block cipher. It helps in electronic data encryption. Mathematical concepts like substitutions and permutations form the basis of this algorithm. It has a fixed block size (128 bit) and key size (128 or 192 or 256) contrast from its predecessors like DES [42].

  Algorithm:

  - Initial step is key expansion, where cipher key is used to derive round keys. In AES there are rounds with 128 bits for each and every round and plus one always.
  - Initial round encompasses a function called AddRoundKey where bitwise XOR is used to combine state byte with round key of the block.
  - Every bite is replaced with another byte ideally by following a look up table.

- Shifting of the last three rows take place by using transposition concept.
- Columns are operated, where four bytes of every column are combined. Then the initial function is executed on the matrix
- Rows are shifted and bytes are replaced in the matrix after which the round key is added again.
- This process continues for cycles of 10, 12, 14.

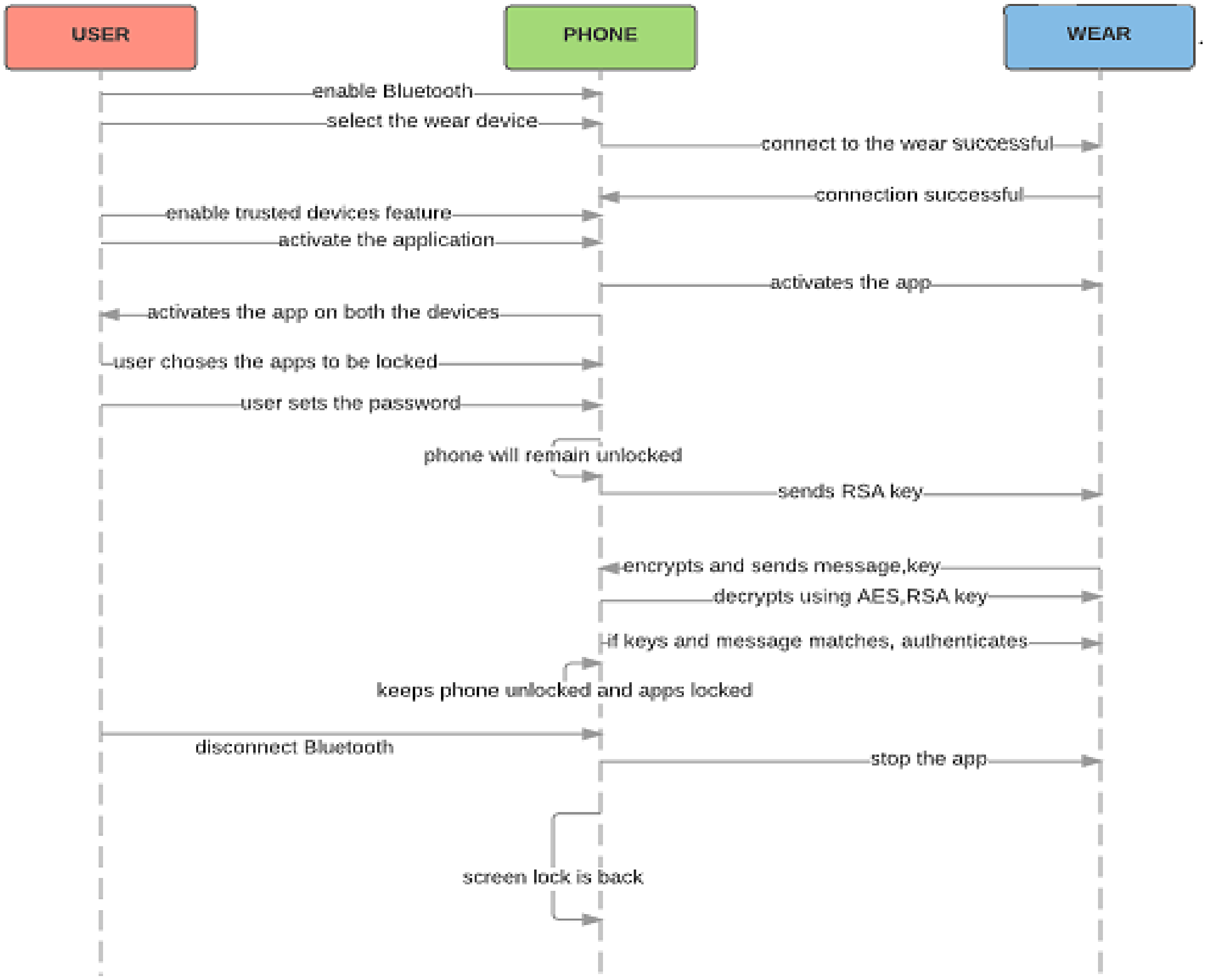
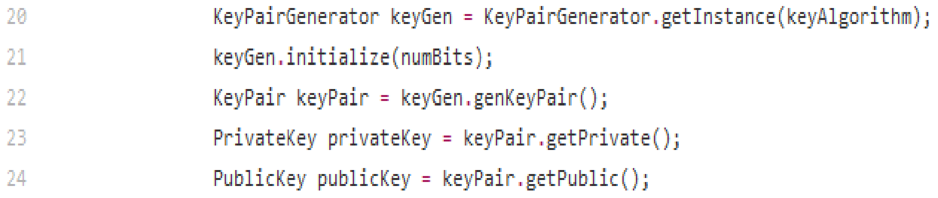

USER
PHONE
WEAR
enable Bluetooth
select the wear device
connect to the wear successful
connection successful
enable trusted devices feature
activate the application
activates the app
activates the app on both the devices
user choses the apps to be locked
user sets the password
phone will remain unlocked
sends RSA key
encrypts and sends message,key
decrypts using AES,RSA key
if keys and message matches, authenticates
keeps phone unlocked and apps locked
disconnect Bluetooth
stop the app
screen lock is back

Figure 17: Sequence diagram of the proposed system

4.2.2 CRYPTOGRAPHIC ROUTINE

Our cryptographic routine uses RSA public key algorithm and AES block cipher. Two devices phone and watch act as two entities.

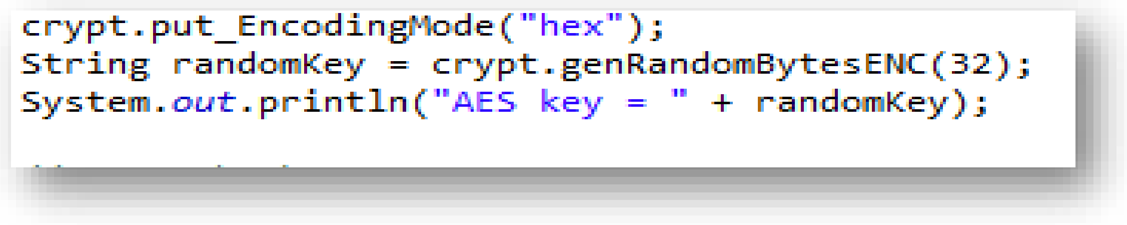
- The application on the phone side generates RSA key pair (public key and private key). Phone can send this public key to as many other entities as it wishes to but here we will restrict it to the device which has paired application. These keys generated are 1024 bits long. Public key uses X.509 and private keys use PKCS#8.



```
KeyPairGenerator keyGen = KeyPairGenerator.getInstance(keyAlgorithm);
keyGen.initialize(numBits);
KeyPair keyPair = keyGen.genKeyPair();
PrivateKey privateKey = keyPair.getPrivate();
PublicKey publicKey = keyPair.getPublic();
```

Figure 18: Code snippet for generating RSA keys

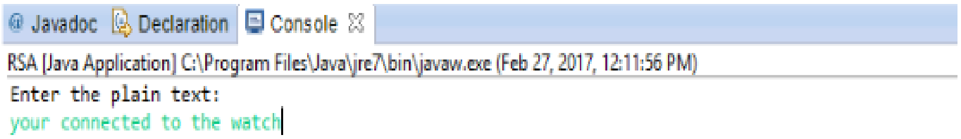
- We save the keys generated. Which we use for checking later.
- Once the public key of the phone reaches the watch, it generates its AES 256-bit key locally. AES is generated randomly. This will generate (2 ^ 255) guesses.
- A known IV code is set so that both sides will be able to use it.



```
crypt.put_EncodingMode("hex");
String randomKey = crypt.genRandomBytesENC(32);
System.out.println("AES key = " + randomKey);
```

Figure 19: Code snippet for generating AES key

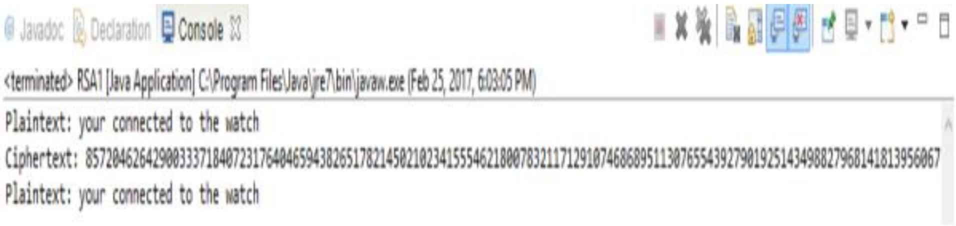
- when watch tries to ping the phone with connection message saying it the device it is connected to, to avoid any kind of third party attack the watch encrypts the message using its AES key and RSA public key of the phone.
- With the message it also sends the AES key encrypted so that it can be used in the decryption process.



```
RSA [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Feb 27, 2017, 12:11:56 PM)
Enter the plain text:
your connected to the watch
```

Figure 20: Plain text to be encrypted

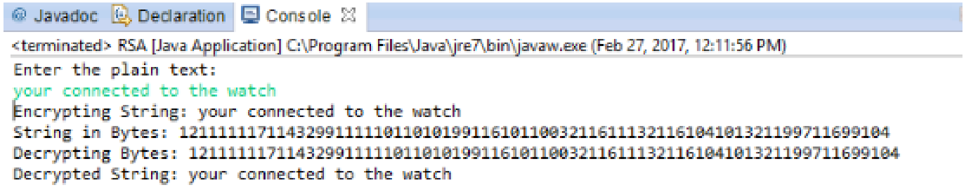
- Phone now decrypts the cipher text of the message and the AES key using its private key that was generated by RSA.



```
<terminated> RSA1 [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Feb 25, 2017, 6:03:05 PM)
Plaintext: your connected to the watch
Ciphertext: 85720462642900333718407231764046594382651782145021023415554621800783211712910746868951130765543927901925143498827968141813956067
Plaintext: your connected to the watch
```

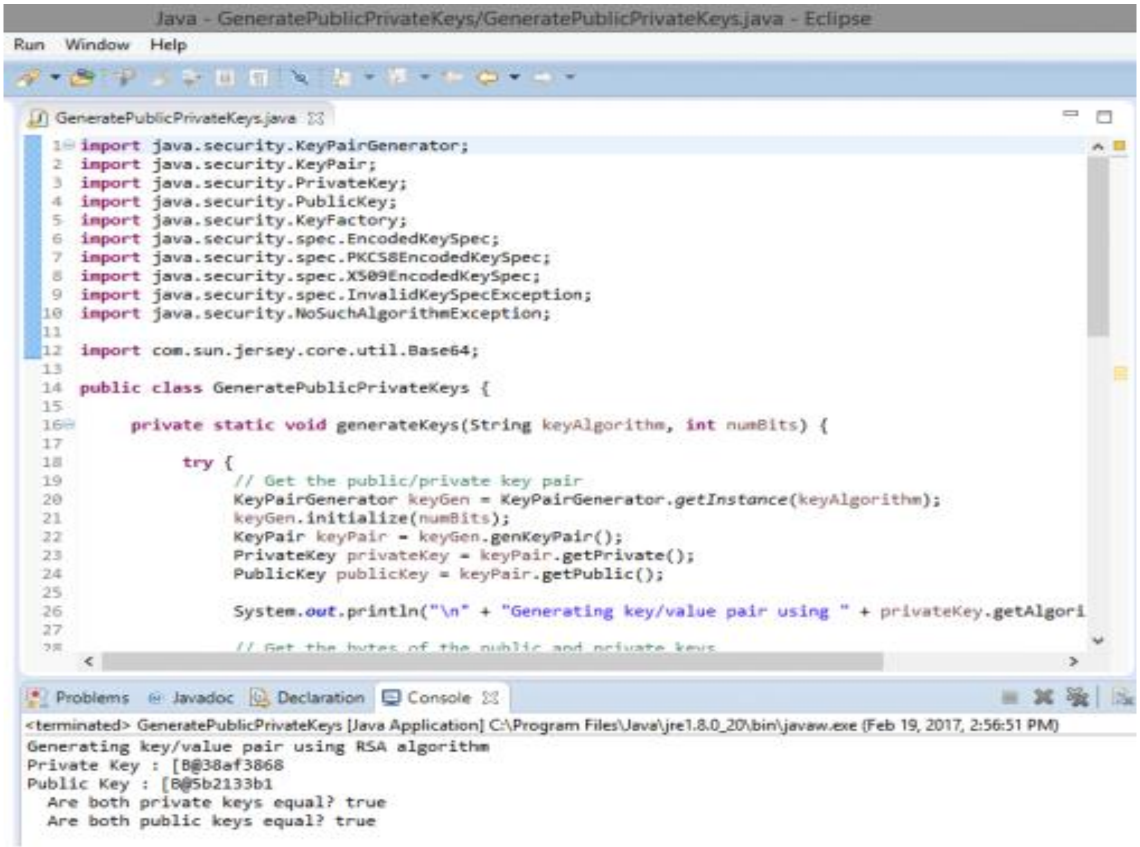
Figure 21: Cipher text example from the output

- Once this message is decrypted, it authenticates the watch. And the communication between them will be secured.
- To be more sure, the keys can be checked, as to if the RSA public key and the private keys are the ones that are generated and that are being sent and used for decryption.



```
<terminated> RSA [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Feb 27, 2017, 12:11:56 PM)
Enter the plain text:
your connected to the watch
Encrypting String: your connected to the watch
String in Bytes: 12111111711432991111101101019911610110032116111321161041013211997116991 04
Decrypting Bytes: 121111117114329911111011010199116101100321161113211610410132119971169910 4
Decrypted String: your connected to the watch
```

Figure 22: Encryption and decryption results


Java - GeneratePublicPrivateKeys/GeneratePublicPrivateKeys.java - Eclipse
Run
Window
Help
GeneratePublicPrivateKeys.java
Problems
Javadoc
Declaration
Console

```
import java.security.KeyPairGenerator;
import java.security.KeyPair;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.KeyFactory;
import java.security.spec.EncodedKeySpec;
import java.security.spec.PKCS8EncodedKeySpec;
import java.security.spec.X509EncodedKeySpec;
import java.security.spec.InvalidKeySpecException;
import java.security.NoSuchAlgorithmException;

import com.sun.jersey.core.util.Base64;

public class GeneratePublicPrivateKeys {

    private static void generateKeys(String keyAlgorithm, int numBits) {

        try {
            // Get the public/private key pair
            KeyPairGenerator keyGen = KeyPairGenerator.getInstance(keyAlgorithm);
            keyGen.initialize(numBits);
            KeyPair keyPair = keyGen.genKeyPair();
            PrivateKey privateKey = keyPair.getPrivate();
            PublicKey publicKey = keyPair.getPublic();

            System.out.println("\n" + "Generating key/value pair using " + privateKey.getAlgori

            // Get the bytes of the public and private keys
```

```
<terminated> GeneratePublicPrivateKeys [Java Application] C:\Program Files\Java\jre1.8.0_20\bin\javaw.exe (Feb 19, 2017, 2:56:51 PM)
Generating key/value pair using RSA algorithm
Private Key : [B@38af3868
Public Key : [B@5b2133b1
  Are both private keys equal? true
  Are both public keys equal? true
```

Figure 23: Key check

4.3 ADVANTAGES OF THIS SYSTEM

The proposed system enables the good use of all three suitable and popular authentication methods. Major advantage of this method is the fact that trusted device can be used but with enough security. As was the case with typical trusted device feature, both the ends of the communication were at risk as phone would remain unlocked as long as the watch was connected which left the device open and data was at risk and at the same time notifications and certain amount of data was at risk due to the lack of screen lock on the watch. This system solves this problem by keeping the user at ease with having phone unlocked and protecting the data by locking apps of user's choosing which user may think of being highly at risk and not frequently accessed.

The communication between the devices is encrypted, by which the watch authenticates itself to the phone which reduces the risk of third party device in between. If the screen lock is activated on the watch which usually should have version above 5.1 then both the ends will be secured. AES key will not give way too much of Brute force attacks because it will take (2 ^ 255) guesses. Most of the attacks are avoided by the AES key. The lock applications can be accessed by entering the passcode which will intensify the security

CHAPTER 5

APPLICATION DEVELOPMENT PROCESS

Android apps can be developed by using various different software. There is humongous amount of tools available in the market for development of android applications. Some of the tools use web technologies and some use cross platforms. Android apps can be built using alternative languages and other IDEs. These cannot be restricted but few examples on which apps can be worked are Ruby, C#, HTML, JavaScript, Python, Perl, Java, AppInventor. Official tool for developing android applications is by Google which has most of the above stated technologies support but also easily one of the most used and popular tool. For this tool to work there are certain primitives that are to be downloaded in the system of development, the major software needed is Java Development Kit. Along with Java JDK some of the components from Google are required like SDK, Native Development Kit(NDK), Eclipse for android and its plugins for android app development, Eclipse for ADT plugin. Google has made it easy for the developers to download all the components by combining SDK, Eclipse tools like ADT plugin or otherwise into one component called ADT bundle which was otherwise installed through Android SDK Manager. Some java programs and command line tools are present in SDK tools and uses of these tools are mentioned by Google. Whereas Eclipse ADT plugin helps integrate the above stated tools inside the Eclipse IDE which makes users feel at ease as they don't have to switch between their environments while developing. C/C++ code is integrated after compiling into the application by NDK generally used by game developers. NDK has all the necessary components to cross compile and requires Cygwin on windows. Once all the tools are installed android application can be developed [55].

5.1 ANDROID STUDIO FEATURES

Android studio by Google is the official IDE for developing android apps for all kinds of devices with highest quality. It has all the tools required for editing the code, debugging, testing.

5.1.1 RUN TIME AND EFFICIENCY OF THE CODE

Android studio is loosely based on Intellij IDE, which provides fastest running workflow. Android studio has the instant run feature instead of a long process. When changes are made it understands intelligently and changes resources accordingly without having to manually set up resources or restart the APK. It has a fast and feature rich emulator which starts the application after installing and gives the feel of running on actual device. Android configured devices like phone, tablet, TV, android wear are compatible. This emulator lets developers use sensors, GPS location as on any real device. Android studio also has a better code editor which helps users write better code which runs faster and is more productive. It offers advanced features like code completion, code analysis, drop down options [55].

5.1.2 CONFIGURED BUILDS

For all devices APKs can be generated due to the flexibility provided by the structure of android studio and the way gradles are built. Automation building is available in android studio, also available are dependency management and builds can be customizable. Libraries can be included in the project locally and hosted libraries can also be included. Built variants can be defined which includes various different kinds of codes and resources. Code shrinking can be applied and different app signing configurations can be applied too. Unified environment is present in android studio which implies applications can be built for any kind of android device like smartphones, tablets, android auto, android wear, android TV. Code modules are structured in such a way that they can be configured, tested and debugged individually as projects can be divided into parts and their functionality can be tested.

GitHub, subversion are the examples of version control tools which is supported by android studio so that users can manage their huge teams and make sure every member in the team is in sync with all the built changes and changes that take place in projects. Because of the open source gradle built system, continuous integrated servers and configuring the build environment according to the will of the user are possible.

5.1.3 CODE TEMPLATES AND TESTING TOOLS

There are code templates and project templates available in the android studio to make it easy for the users to use already established patterns. These patterns can include navigation drawers, password templates etc. Project can be started by choosing a code template or sample codes by clicking APIs in the editor section. Apps which function regularly can also be imported from version control tools. Extensive tools are provided by android studio which help developers in testing their projects. Examples of such tools are JUnit 4, UI test frameworks etc. Espresso test recorder is one such tool where developers will be able to generate user interface test codes. These test codes are generated by being able to record the interactions of developers with the app on either the device or the emulator. The emulator, device and the integrated environment can run the test cases. Issues in categories like performance, correctness or the security can be resolved by just one click therefore known to fix issues quickly.

5.1.4 MAKING CONNECTED APPLICATIONS

C/C++ projects can be edited and compiled in android studio and after compilation JNI components can be built in the app. The IDE being used also highlights the syntactical errors and helps users refactor the C/C++ projects also the studio supports debugger based on LLDB which lets users debug java and C/C++ code simultaneously. NDK- build or CMake scripts can also be executed by build tools and the modifications are not required and the object created will be added to the APK. App can be connected to the Firebase with the help of firebase assistant. Services like authentication, procedures, analytics can be added to the services in android studio. Cloud platform by Google have built-in tools which help developers create and maintain back-end support for Apps.

5.1.5 SPECIAL FEATURES

Drag and drop editor is provided in android studio to help users in developing XML layouts which Is easier to create than before. API named Constraint Layout was built partnered with layout editor which makes it easier for the layouts to be build that can be adapted to screens of different sizes. This can be done by adding views in place and constraints can be used on layouts. New image assets can be created easily on android studio with the help of vector asset studio. From material provided by Google design icons can be selected and SVG/PSD files can be imported with the help of this studio. Bitmap files are generated by this studio for each screen that can support older android versions that did not support vector drawable format. Contents of APK can be inspected easily by the APK analyzer. Size of every single component is revealed so that the developers will be in a position to reduce the size of APK overall if required. Packaged assets can also be previewed, DEX files can be inspected to troubleshoot any issues related to multidex, two APKs can also be compared. All the translated resources can be viewed in a single view with the help of translations editor. This makes it easy for developers to decide if any changes like adding any translations or adding missing ones. These changes can be made even without opening any XML file and translation service can be ordered.

5.2 SYSTEM REQUIREMENTS FOR ANDROID STUDIO

5.2.1 VERSION 2.X

	Windows	OS X/mac OS	Linux
OS Version	Windows 10/8/7(32/64- bit)	Mac OS 10.9.5 or higher till 10.11.6	GNOME or KDE desktop
RAM	3 GB RAM minimum; 8GB RAM recommended	3 GB RAM minimum; 8GB RAM recommended	3 GB RAM minimum; 8GB RAM recommended
Disk Space	500 MB disk space for Android Studio, at least 1.5 GB for Android SDK, emulator system images, and caches	500 MB disk space for Android Studio, at least 1.5 GB for Android SDK, emulator system images, and caches	500 MB disk space for Android Studio, at least 1.5 GB for Android SDK, emulator system images, and caches
Java Version	Java Development Kit (JDK) 8	Java Development Kit (JDK) 8	Java Development Kit (JDK) 8
Screen Resolution	1280x800 minimum screen resolution	1280x800 minimum screen resolution	1280x800 minimum screen resolution

Table 5: Version 2 system requirements [53]

5.2.2 VERSION 1.X

	Windows	OS X/mac OS	Linux
OS Version	Microsoft Windows 10/8.1/8/7/Vista/2003/XP (32 or 64 bit)	Mac OS X 10.8.5 or higher, up to 10.10 to up 10.10.2 up 10.10.3 or 10.10.5 (Yosemite)	GNOME or KDE or Unity desktop on Ubuntu or Fedora or GNU/Linux Debian
RAM	3 GB RAM minimum, 4 GB RAM recommended	3 GB RAM minimum, 4 GB RAM recommended	3 GB RAM minimum, 4 GB RAM recommended
Disk Space	500 MB disk space	500 MB disk space	500 MB disk space
Space for Android SDK	At least 1 GB for Android SDK, emulator system images, and caches	At least 1 GB for Android SDK, emulator system images, and caches	At least 1 GB for Android SDK, emulator system images, and caches
JDK Version	Java Development Kit (JDK) 7 or higher	Java Development Kit (JDK) 7 or higher	Java Development Kit (JDK) 7 or higher
Screen Resolution	1280x800 minimum screen resolution	1280x800 minimum screen resolution	1280x800 minimum screen resolution

Table 6: Version 1 system requirements [53]

5.3 TERMS TO KNOW

5.3.1 ANDROID SDK

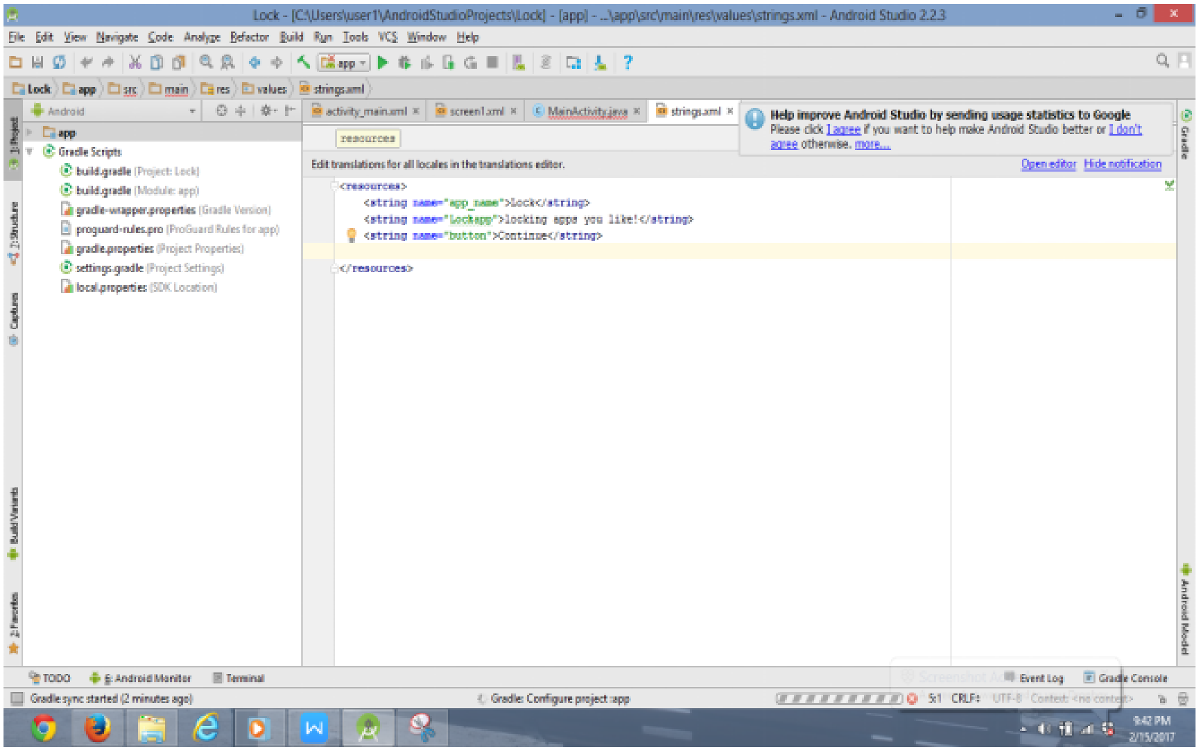
Android Software Development Kit (SDK) comprises of development tools which are used in developing applications for android. It includes libraries, emulator, debugger, sample code templates, Documentation for Application Program Interface(API), tutorials. Google releases new SDK with every new version of android is released. As new android versions have new features, to be able to use them in their applications developers require to keep their SDK tools up-to-date. SDK can be used for writing programs for applications on command prompt but popularly it is used on an IDE. Mostly recommended IDE is eclipse with an android plugin.

5.3.2 ANDROID NDK

Android studio supports editing and also compilation of codes written in C/C++ and can be changed to other languages as well like MIPS, ARM and native code. NDK helps in installing the above created files. Android documentation states that NDK does not benefit a lot of other applications except for C/C++. Android emulator has a root shell given by ADB debugger because of which MIPS, ARM and native code can be uploaded onto it and then executed. Native code uses GCC compiler or any C compiler for compiling and running this code is also considered complicated. NDK projects can be developed by using Android Studio Gradle and also can be developed by third party tools, which can also be integrated into the studio and eclipse.

5.3.3 GRADLE

It is a open source test automation system, it I based on the concepts of Apache Ant and Maven. Instead of XML it proposes domain specific language (DSL) which is used to declare the configuration of the project. Gradle also decides the order in which tasks have to be run by using the concepts of directed acyclic graph. For the projects that are quite big gradle helps them in building even when components of a big project are divided into multiple projects. It is also intelligent in the way it determines which part of the projects need not be re-executed as it beforehand checks the tree for up-to-date tasks and does not execute the dependent tasks again. The plugins that were available initially were majorly focused on java, Scala development and also it's deployment. Now plugins are being designed to work around other languages too.


Lock - [C:\Users\user1\AndroidStudioProjects\Lock] - [app] - ...\app\src\main\res\values\strings.xml - Android Studio 2.2.3
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
Lock app src main res values strings.xml
Android
app
Gradle Scripts
build.gradle (Project: Lock)
build.gradle (Module: app)
gradle-wrapper.properties (Gradle Version)
proguard-rules.pro (ProGuard Rules for app)
gradle.properties (Project Properties)
settings.gradle (Project Settings)
local.properties (SDK Location)
activity_main.xml
screen1.xml
MainActivity.java
strings.xml
resources
TODO
6: Android Monitor
Terminal
Event Log
Gradle Console

Help improve Android Studio by sending usage statistics to Google
Please click I agree if you want to help make Android Studio better or I don't agree otherwise. more...

Edit translations for all locales in the translations editor. Open editor Hide notification

```
<resources>
    <string name="app_name">Lock</string>
    <string name="Lockapp">locking apps you like!</string>
    <string name="button">Continue</string>

</resources>
```

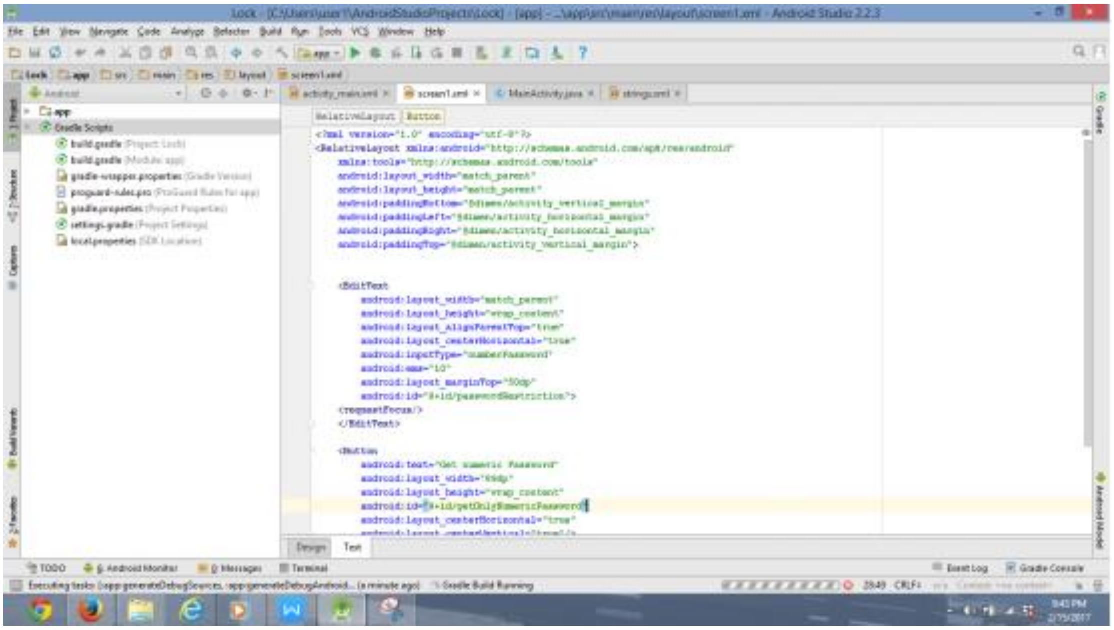
Gradle sync started (2 minutes ago)

Gradle: Configure project :app

Figure 24: String files example

5.4 PROCEDURE TO START EMULATOR

Mainclass.java file will be the main code from which all the XML layouts will be called and functionality is defined.



```
<?xml version="1.0" encoding="utf-8"?>
<RelativeLayout xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:paddingBottom="@dimen/activity_vertical_margin"
    android:paddingLeft="@dimen/activity_horizontal_margin"
    android:paddingRight="@dimen/activity_horizontal_margin"
    android:paddingTop="@dimen/activity_vertical_margin">


    <EditText
        android:layout_width="match_parent"
        android:layout_height="wrap_content"
        android:layout_alignParentTop="true"
        android:layout_centerHorizontal="true"
        android:inputType="numberPassword"
        android:ems="10"
        android:layout_marginTop="50dp"
        android:id="@+id/passwordRestriction">
    <requestFocus/>
    </EditText>

    <Button
        android:text="Get numeric Password"
        android:layout_width="99dp"
        android:layout_height="wrap_content"
        android:id="@+id/getOnlyNumericPassword"
        android:layout_centerHorizontal="true"
        android:layout_centerVertical="true"/>
```

Figure 25: Representation of XML layout code

Once the coding part of the application is done it is time for the application to be tested. From tools android AVD manager is selected to be able to execute the application on a virtual device called emulator.

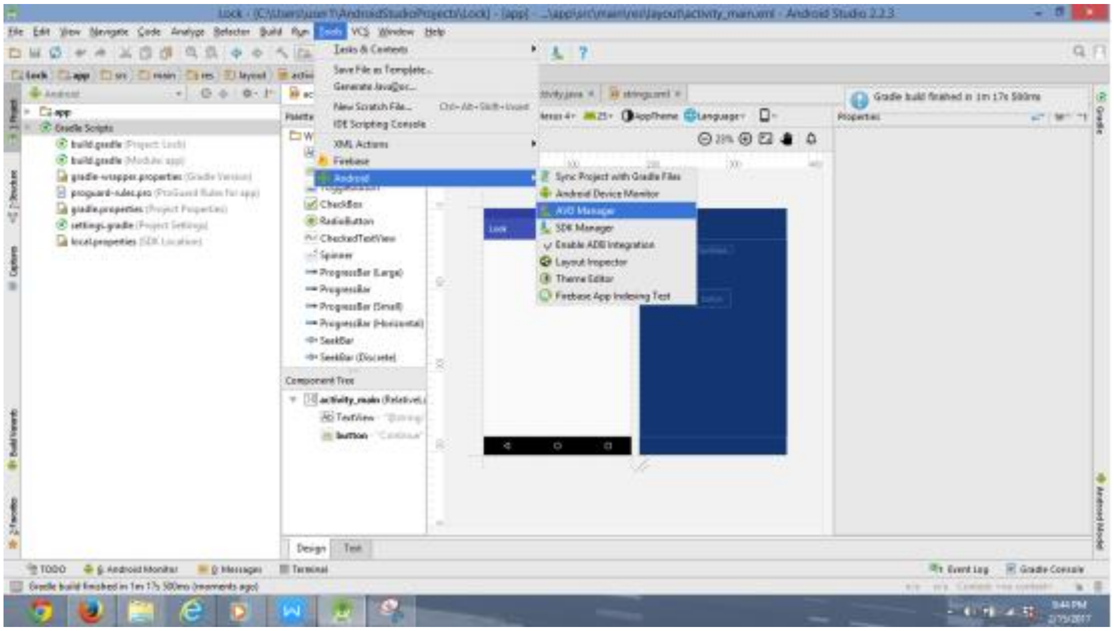
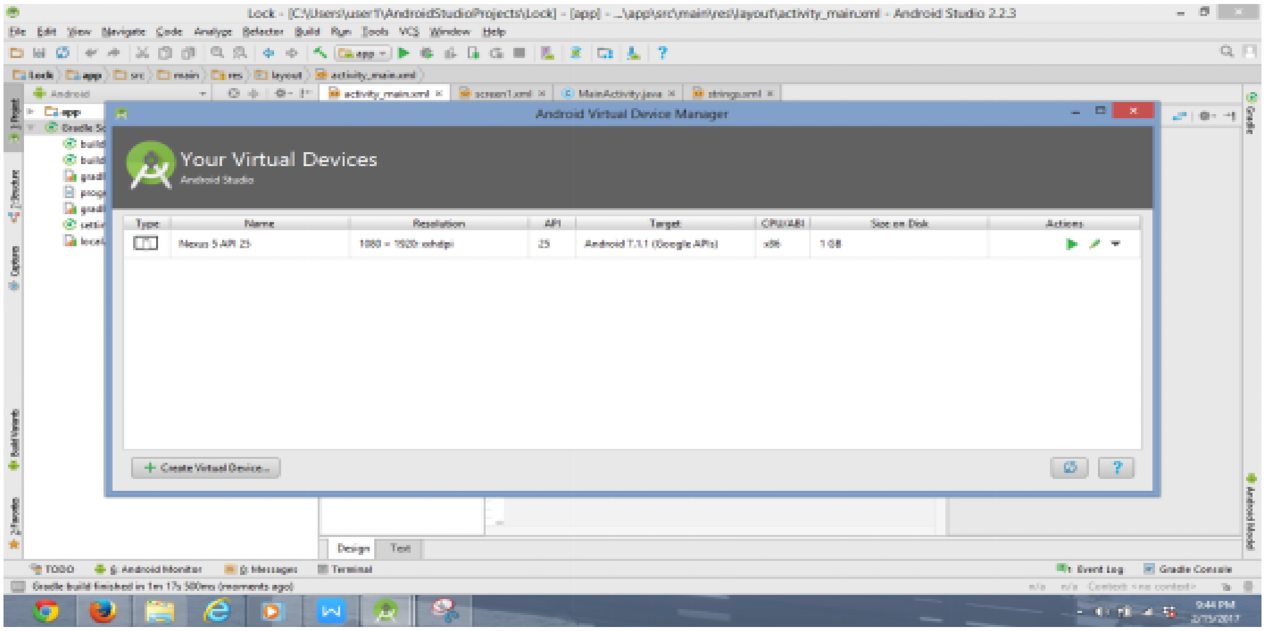


Figure 26: Selection of AVD manager

Once the AVD manager is called it will show up the devices available on the system if already installed else first virtual device has to be installed. For the execution of our app Nexus device is selected.


File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
Lock app src main res layout activity_main.xml
activity_main.xml screen1.xml MainActivity.java strings.xml
Android
app
Android Virtual Device Manager
+ Create Virtual Device...
Design Text
TODO 6: Android Monitor 0: Messages Terminal
Event Log Gradle Console
9:44 PM
2/15/2017

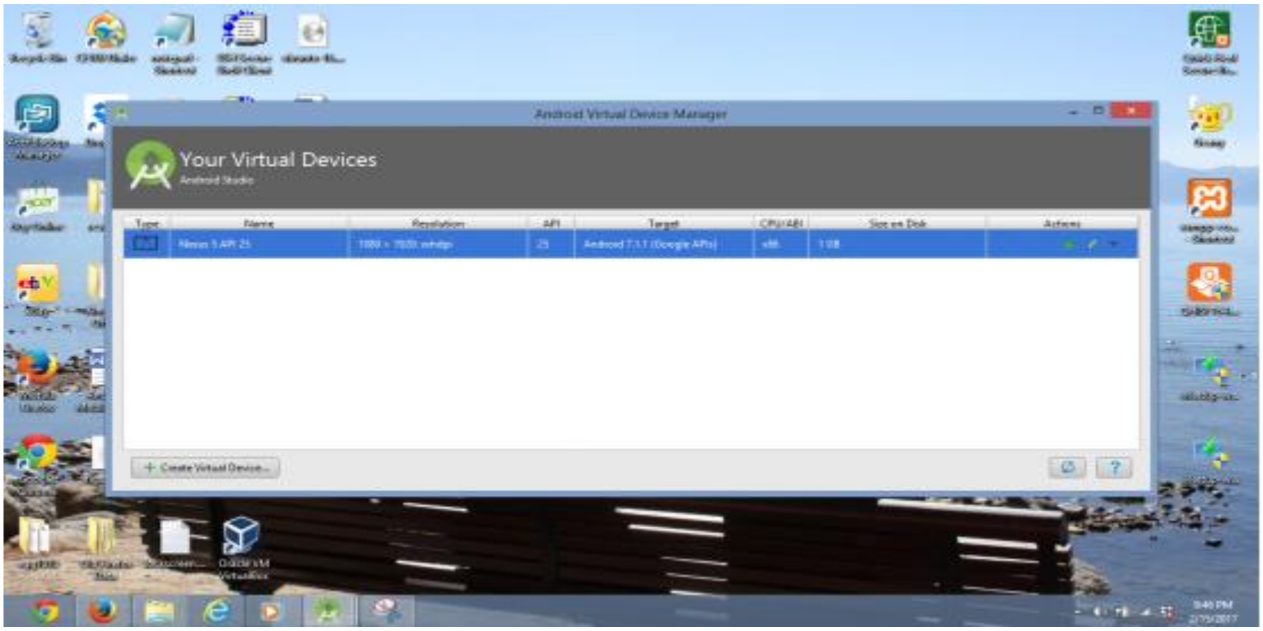
Lock - [C:\Users\user1\AndroidStudioProjects\Lock] - [app] - ...\app\src\main\res\layout\activity_main.xml - Android Studio 2.2.3

Your Virtual Devices
Android Studio

Type	Name	Resolution	API	Target	CPU/ABI	Size on Disk	Actions
	Nexus 5 API 25	1080 × 1920: xxhdpi	25	Android 7.1.1 (Google APIs)	x86	1 GB	

Gradle build finished in 1m 17s 500ms (moments ago)

Figure 27: Selection of a virtual device



Your Virtual Devices
Android Studio

Type	Name	Resolution	API	Target	CPU/ABI	Size on Disk	Actions
	Nexus 5 API 25	1080 × 1920: xxhdpi	25	Android 7.1.1 (Google APIs)	x86	1 GB	

Figure 28: Nexus virtual device is selected

Android emulator takes time to open up depending on the system.

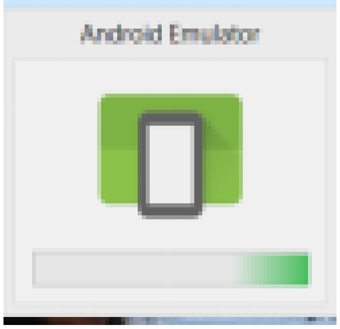


Figure 29: Start of android emulator

Android emulator starts and behaves like a proper functioning device. Once the run is clicked on the tool bar the app starts on the emulator.

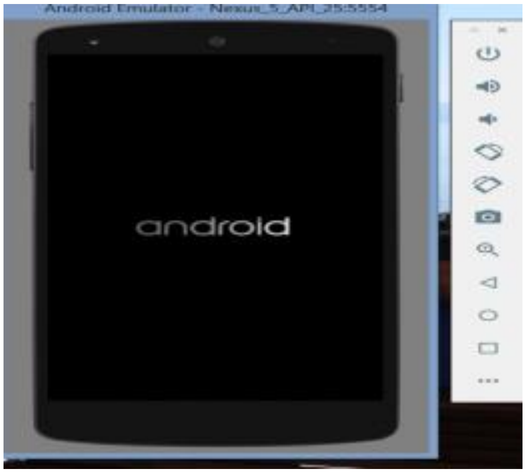
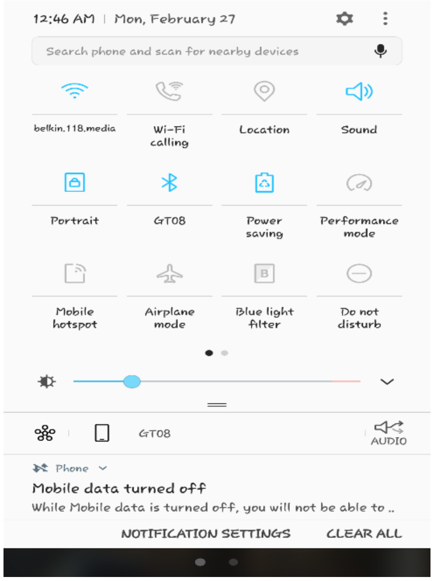


Figure 30: Android emulator

5.5 PAIRING PROCESS BETWEEN THE SMART PHONE AND THE ANDROID WEAR

In our experiment we are using real time commercial devices like Samsung galaxy S7 and MSRM MS08 smart watch. For these two devices to be connected it is important for the Bluetooth to be turned on in both the devices. Once both the devices are connected via Bluetooth, for notifications to be passed over to the watch, watch QR code needs to be scanned and its synchronous software needs to be downloaded on the phone. Here in this scenario, BT notifications application is downloaded on the phone to enable notifications on the watch [26]. Apart from showcasing notifications it is important for watch to access contacts and memory for storing snaps clicked on the watch. For this a SD memory card is inserted in the watch. This watch lets user call from the watch, see notifications even of the apps which are not installed on the watch. Either it can be connected over Wi-Fi or cellular data as it has a port for sim card as well.



Mobile data turned off

While Mobile data is turned off, you will not be able to ..

Figure 31: Connection via Bluetooth

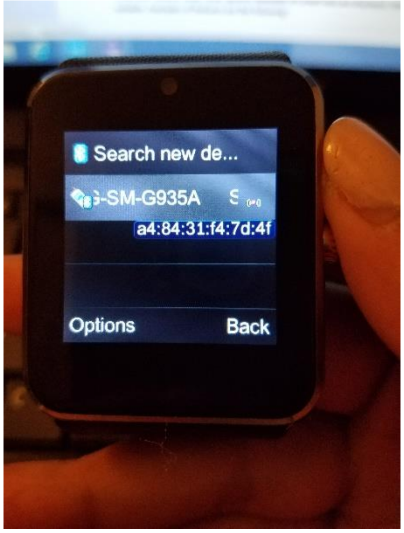
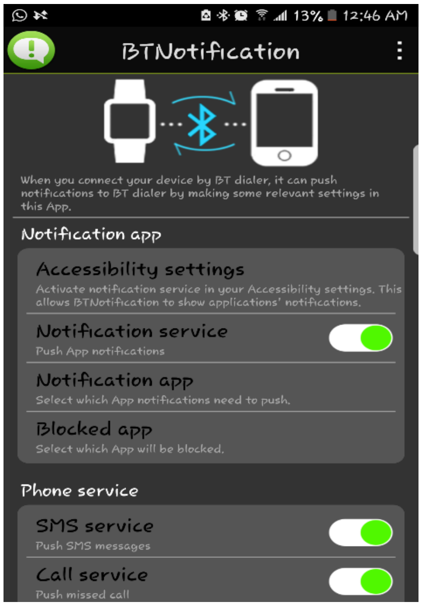


Figure 32: Watch showcasing the connect

Figure 33: QR code required to be scanned by the phone to download appropriate software



13% 12:46 AM

BTNotification

When you connect your device by BT dialer, it can push notifications to BT dialer by making some relevant settings in this App.

Notification app

Accessibility settings
Activate notification service in your Accessibility settings. This allows BTNotification to show applications' notifications.

Notification service
Push App notifications

Notification app
Select which App notifications need to push.

Blocked app
Select which App will be blocked.

Phone service

SMS service
Push SMS messages

Call service
Push missed call

Figure 34: BT notifications app to push the notifications on to the watch

5.6 INSTALLING SOFTWARE OR APPLICATIONS ON SMARTPHONE AND ANDROID WEAR

After developing the application, developer needs to test the application. Usually it can be done by running it on the emulator first and then running it on the real device. Once the application is compiled it gets easy to install and test it on the device as tools required for this action are already present in the SDK tools. Installation process can be done in two ways: either directly from the studio or from command line.

To enable installation on the device it is required that developer options feature is turned on. There are other developer options such as debugging over USB, showcasing percentage of CPU being used, capturing and sending bug reports available.

To set up the device for installing the application, following steps are required:

- Manifestation has to be checked if the application is debuggable [38].
- From phone settings, USB debugging should be enabled.
- User's computer system should be able to detect and connect to the device. In iOS this step is not required, in Linux additional steps are to be taken for connecting the device.
- Once the device is connected over the USB, its authenticity can be checked.
- While using it on android studio and the application is run, instead of the virtual emulator the connected device can be chosen.
- Once the testing part of it is done, the application's apk can be downloaded onto the device.

To install application on the wear, it is very much similar to the installation of an application on the phone. Application is deployed on the device then it works.

- To set up the emulator for phone and watch, following steps are required:
- In the AVD manager, virtual device has to be created.
- In it, wear is selected as the hardware.
- Select and download the required API and version.
- Emulator can be launched how usually it is by clicking the run button.
- Set up a Google account to store data.

Following steps give insight into how to set up a phone companion to a watch application:

- From the devices available, select the watch and connect to it through codes.

- sync the data from Google account, to the watch.
- Apply screen lock. Complete the pairing process.

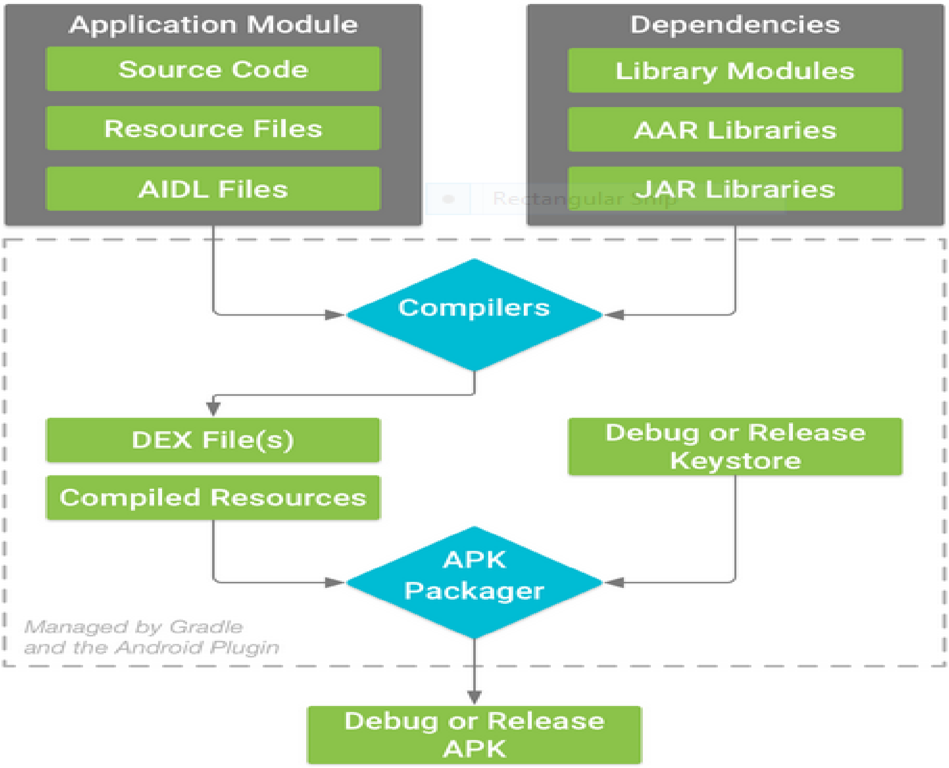


Figure 35: Flow chart showcasing the release of APK

5.7 CHALLENGES OF WORKING IN THE SUDIO ENVIRONMENT

- Software fragmentation
- Hardware fragmentation
- Security
- Android market search engine
- Key generation
- Pairing the devices and establishing a connection

CHAPTER 6

PERFORMANCE AND SECURITY ANALYSIS

6.1 PERFORMANCE ANALYSIS

The proposed system's performance can be analyzed in this chapter. This analysis can be done based on the following criteria:

- Bluetooth connectivity
- Distance limitations
- Speed of encryption and decryption
- Time taken for app locking

6.1.1 BLUETOOTH CONNECTIVITY

Bluetooth connects quickly to the other devices, here talking about the connectivity between the phone Samsung Galaxy S7 and watch MSRM MS08. Bluetooth connectivity is a tad bit slow compared to the time taken by other Google watches and Galaxy phones. Connection takes about 7-8 seconds when compared to 5-6 seconds taken by other devices. This particular watch takes time for connecting due to its lower android version. Bluetooth connection for smart lock feature is active till four hours of in activity which is android specified.

6.1.2 DISTANCE LIMITATIONS

System uses the Bluetooth range specified by the android. Once the range is crossed, phone and watch get disconnected. As distance starts to increase, the communication becomes slower and starts to lag. In general, without getting disconnected the distance can range up to 100 meters. Data rate ranges from 1 to 3 Mbit/second and the frequency would be 2.402 - 2.481 GHz. The speed with which the data is received depends on receiver and the transmitter.

6.1.3 SPEED OF ENCRYPTION AND DECRYPTION

The whole process of encryption and decryption takes place in 10 seconds. The whole cryptographic process encompasses encryption and decryption, where pair of keys are generated over and sent to the other entity. The whole process timing isn't bad but could surely be improved. Time increases proportionally to the length of the text.

RSA encryption and decryption timings:

RSA Encryption ~ 1024 bit/8 * 1000/0.18 = 711 KB/sec

RSA Decryption ~ 1024 bit/8 * 1000/4.77 = 27 KB/sec

6.2 SHORTCOMINGS OF THE SYSTEM

The proposed system has better security features and overcomes the problems faced by using smart lock trusted devices feature. But still it falls short on few areas.

- Dependent on android specified Bluetooth range.
- Dependent on android specified Bluetooth speed.
- Side channel attack is still possible on AES key.
- Time increases with the increase in key length.
- RSA keys do not have a proper public organization certificate.
- Reactivating the smart lock feature every four hours if no activity is detected. Still dependent on android put smart lock specification.
- AES key not flexible.

6.3 SECURITY ANALYSIS

6.3.1 SECURITY ANALYSIS ON PHYSICAL LEVEL

As a security measure Bluetooth has a range in which only the phone will be connected to other devices. In some cases, it acts as a security measure as it can restrict the connections with devices when not near by and can stop attacks like spoofing. So for now this system uses the android specified distance range.

But if the watch is lost, entire device and its data is at risk. Not only the user suffers financial loss but can suffer a major loss if data is sensitive enough. So this system uses the Bluetooth range as the parameter and once two devices are out of range from each other, it will result in phone being back to its usual having a security lock as authentication measure. Smart lock gets disconnected, because of which the lock gets activated by default on the system. Moreover, data transmission stops as well, which does not let the watch have any data or notifications.

6.3.2 EAVESDROPPING ATTACK

Due to the fact that the communication between the two devices over Bluetooth is secured by encryption in general so this kind of attack will not be possible.

6.3.3 REPLAY ATTACK

Data on network won't be delayed or played back due to its secure connection of the network by third party who is not authenticated. Stream of messages can not be delayed as the system only transfers ping message and key which is encrypted.

6.3.4 MAN-IN-THE-MIDDLE-ATTACK

Two party communication is not possible to be altered by the third party when encrypted and majorly because RSA is a secure algorithm which does not let this kind of attack to happen so does AES encryption.

Keys cannot be spoofed as the public key of the phone is not shared with any other device except the connected device which has the pairing software.

6.3.5 CERTIFICATION VULNERABILITY

This vulnerability is prevailed as the public organization is not included in the system to sign the public keys of the entities which may become a liability. Here we will be using a key generation algorithm in java called KeyAlgorithm. AES key is randomly generated.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

The system reaches the aim with which the system was designed, that is of securing the device and its data when connected over the smart lock feature. This system integrates encryption and app locking technique over Bluetooth well thus securing the devices at both ends and reducing the attacks possible on the devices and their communication. It reduces the disadvantages of trusted devices feature fulfills the security requirement by keeping the data secure on the phone and checking the watch connected to the phone.

7.2 FUTURE WORK

This system can be extended with more features adding up. The entire communication through Bluetooth over this app can be encrypted instead of just authenticating the watch, which will make it harder for the third party to access the communication between the devices. Application can be extended to access all the resources on phone and can encrypt the push notifications as well. Passcode used for unlocking the locked apps can be replaced with much stronger security feature like fingerprints which even though can be broken but is still harder. Range of the connectivity can be customized rather than using the default Bluetooth range. This system can be extended to more devices and on different platforms and can also be extended to iWatch. Cryptosystem can be made more strong by using a stronger AES key and RSA public key.

BIBLIOGRPAHY

[1] David Jaros and Radek Kuchta, New Location-based Authentication Techniques in the Access Management, 2010 Sixth International Conference on Wireless and Mobile Communications.

[2] Yusuf Albayram, Mohammad Maifi Hasan Khan,Athanasios Bamis,Sotirios Kentros,Nhan Nguyen and Ruhua Jiang, A Location-Based Authentication System Leveraging Smartphones, 2014 IEEE 15th International Conference on Mobile Data Management.

[3] Amit Kumar Tyagi,N.Sreenath, Future Challenging Issues in location-based services, International Journal of Computer Applications Volume 114-No 5. March 2015.

[4] Wen-Bin Hsieh and Jenq-Shiou Leu, Design of a Time and Location Based One-Time Password Authentication Scheme.

[5] Shradha D. Ghogare, Swati P. Jhadav, Ankitha R, Hima C. Patil, Location Based Authentication:A New Approach towards Providing Security, International Journal of Scientific and Research Publication,Vol 2, Issue 4, April 2012

[6] L.Scott and D.Dennings, Geo-encryption Using GPS to Enhance Data Security, GPS world,pp.40-49,2003.

[7] Hsien Chou Liao, Yun-Hsiang Chou, A New Data Encryption Algorithm Based on the Location of Mobile Users, Information Technology journal,vol 7, issue 1,pp 63-69,2008.

[8] D.Son, A.Helmy, B.Krishnamachari, The Effect of Mobility-induced Location Errors on Geographic Routing in Ad Hoc and Sensor Networks:Analysis and Improvement using Mobility Prediction, IEEE Transactions on Mobile Computing,Vol 3, Issue 3, pp.233-245,July 2004.

[9] http://us.zyxel.com/

[10] http://ukey.com.tw/site/ukey.html

[11] Mohhamed Hussain , An Authentication Scheme to Protect the Location Privacy of Femtocell Users, IEEE 978-1-4-799--7100-8/14 2014.

[12] Liang Hua , J iazhu Dai, A Location Authentication Scheme Based on Adjacent Users, IEEE 2014.

[13] Min-Hsao Chen, Ching- Han Chen, Secondary User Authentication based on Mobile Device Location, 2010 Fifth IEEE International Conference on Networking, Architecture, and Storage.

[14] Jaoquin Torres, Jose M. Sierra, Antonio Izquierdo, A Realistic Approach on Password-Based Mutual Remote Authentication Schemes with Smart-cards, Digital Ecosystems and Technology Conference, pp. 334-338,2007.

[15] Huixia Jia, Li Tu, Gelan Yang, Yatao Yang, An Improved Mutual Authentication Schemein Multi-Hop WiMax Network, International Conference on Computer and Electrical Engineering, pp. 296-299, 2008.

[16] William Su, Sung-Ju Lee, Mario Geria, Mobility prediction in wireless networks, 21st Century Military Communications Conference Proceeding, vol. 1, pp. 491-495, 2000.

[17] Lei Mu, Geng-Sheng Kuo, Ningning Tao, A Novel Location Algorithm Based on Dynamic Compensation Using Linear Location Prediction in NLOS Situations, Vehicular Technology Conference Proceeding, Vol. 2, pp. 594-598, 2006.

[18] Philip Hoyer, OTP and Challenge/Response algorithms for financial and e-government identity assurance: current landscape and trends, ISSE, 2008

[19] Whitefield Diffie, Martin Hellman, New directions in cryptography, IEEE Transactions on Information Theory, Vol. 22, Issue 6, pp- 644-654, Nov. 1976.

[20] https://www.slideshare.net/jollen/android-hal-introduction-libhardware-and-its-legacy

[21] Feng Zhang, Aron Kondoro, Saed Muftic, Location based Authentication and Authorization using smartphones, 2012 IEEE Conference on Trust,Security and Privacy in Computing and Communication

[22] https://launchkey.com/how-it-works

[23] https://developer.android.com/training/articles/security-tips.html

[24] https://developer.android.com/training/wearables/apps/creating.html

[25]http://www.androidcentral.com/smart-lock-screen-security-options-android-50-lollipop

[26] https://www.youtube.com/watch?v=YBZpNB5cSdI

[27] http://www.androidcentral.com/how-use-smart-lock-galaxy-s7

[28] https://www.wareable.com/android-wear/android-wear-hidden-secrets-tips-and-tricks

[29]https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

[30] https://www.statista.com/topics/876/android/

[31] https://en.wikipedia.org/wiki/Android_version_history

[32] https://www.android.com/security/overview/

[33] https://en.wikipedia.org/wiki/Android_(operating_system)

[34] http://www.developer.com/ws/android/encrypting-with-android-cryptography-api.html

[35] http://security.stackexchange.com/questions/25104/encrypting-data-for-android-mobile-app

[36]http://tutorials2make.blogspot.com/2015/10/set-only-Numeric-password-restriction-in-android.html

[37] http://www.theverge.com/2014/9/5/6111221/from-sketch-to-wrist-the-evolution-of-android-wear

[38] http://bitbar.com/app-development-and-testing-on-wearables/

[39] http://stackoverflow.com/questions/20233775/how-to-generate-secret-key-in-java-once-and-use-that-key-in-2-different-programs

[40] https://www.youtube.com/watch?v=Fa9I2YKq5Gw

[41] http://security.stackexchange.com/questions/93884/is-this-rsa-aes-combination-good

[42]http://stackoverflow.com/questions/11493254/can-aes-encryption-and-rsa-digital-signature-scheme-work-together-for-file-encry

[43] https://www.slideshare.net/ThaleseSecurity/2016-top-trends-in-encryption-and-data-protection

[44] http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html

[45] https://www.cnet.com/news/iphone-android-encryption-fbi/

[46]http://www.securityweek.com/communications-between-smartwatches-and-phones-exposed-hack-attacks-researchers

[47] https://www.mwrinfosecurity.com/our-thinking/is-security-a-concern-for-wearables/

[48]http://www.greenbot.com/article/2361100/encrypt-your-android-communications-to-prevent-spying-and-stop-thieves.html

[49] Stefan Illic ,Slavica Dukic**,** Protection of Android applications from decompilation using class encryption and native code, 2016 Zooming Innovation in Consumer Electronics International Conference (ZINC)

[50] Suriyani Ariffi, Ramlan Mahmod, Ratini Rahmat,Nuzul Annisa Idris, SMS Encryption Using 3D-AES Block Cipher on Android Message Application, Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on Advanced Computer Science Applications and Technologies

[51] Sarah Sohana, Rahma Bintey Mufiz Mukta, Agent command manipulation system using two keys encryption model, Informatics, Electronics and Vision (ICIEV), 2016 5th International Conference on Informatics

[52] Sudhanshu Suhas Gonge , Ashok A. Ghatol, A hybrid intelligent security technique used for digital still imageAdvances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on Advances in Computing

[53] https://en.wikipedia.org/wiki/Android_Studio

[54] https://simple.wikipedia.org/wiki/RSA_(algorithm)

[55] https://developer.android.com/studio/intro/index.html

CURRICULUM VITAE

GRADUATE COLLEGE

UNIVERSITY OF NEVADA, LAS VEGAS

Akshitha Reddy Chintalaphani

Degrees:

Bachelors in Information Technology, 2015

Stanley College of Engineering & Technology for Women, Osmania University

Masters in Computer Science, 2017

University of Nevada, Las Vegas

Thesis Title: Survey and Analysis of Android Authentication Using App Locker

Thesis examination committee:

Chair Person, Dr. Yoohwan Kim, Ph.D.

Committee Member, Dr. Ajoy K. Datta, Ph.D.

Committee Member, Dr. Juyeon Jo, Ph.D

Graduate College Representative, Dr. Venkatesan Muthukumar, Ph.D.