International Journal of Security and Its Applications
Vol. 11, No. 6 (2017), pp.27-34
http://dx.doi.org/10.14257/ijsia.2017.11.6.03

Security Enhancement in Android using Ellipic Curve Cryptography

Muneer Ahmad Dar[1] and Javed Parvez[2]

[1]*National Institute of Electronics and Information Technology Srinagar,*
[2]*University of Kashmir*
[1]*muneer@nielit.gov.in,* [2]*javedparvez1225@gmail.com*

Abstract

Android has become an active area of research owing to its vast range of applications called apps. Traditional security protocols which are complex are not feasible for such systems due to the limitation of resources. However, Elliptic Curve Cryptography has been considered as a viable cryptographic technique due to its low computational overhead. In this paper we study the application of ECC on a popular Android operating system. Practical implementation of the ECC operations has been performed using Android library. Android operating system has been used to develop custom security protocols on a Smartphone. The performance benchmarking of the proposed protocols has also been carried out.

Keywords: *Android; Apps; Cryptography; ECC*

1. Introduction

Android based smart phones have limited resources in terms of processing, power, and Memory. Android play a critical role in the popularity of smart phones applications also called apps. As these applications involve transmission of data over the network, there is a dreadful requirement to provide security primitives like validation, reliability and privacy. However, due to their resource restricted nature, predictable security protocols cannot be openly employed [1-2].

Public key cryptography along with symmetric key cryptography has been practical in giving security primitive for conventional networks. on the other hand, this attitude has not been leveraged in the case of Android due to its resource restriction nature. conventional PKC is not viable as they absorb weighty computational operations. However, ECC based alternative of PKC has emerged as a practical alternative for providing PKC platform.

Researchers verified that the ECC can be efficiently implemented in the resource constraints devices. The benefit of using ECC as an alternative of conventional RSA is in the fact that 160 bit key in ECC provides corresponding security to that of 1024 bits of RSA as shown in Table 1.

Table 1. Key Comparison between RSA and ECC in Terms of Security Equivalence

Key length of RSA	Key length of ECC	Ratio of RSA/ECC
512	106	5:1
768	132	6:1
1024	160	7:1
2048	210	10:1

ISSN: 1738-9976 IJSIA

This paper provides the study and application of ECC on a popular Android smart phone operating system. Rest of the paper is organized as Section 2 provides the context knowledge pertaining to Android platform. Section 3 gives the background about Elliptic Curve Cryptography. Section 4 proposes the implementation of ECC in Android and proof of concept implementation is presented. Section 5 designs a key exchange protocol based ECC on Android finally we present our analysis and conclusion in Section 6

2. Android Platform

Andy Rubin, Google's director of smart phones, said "There should be nothing that desktop users can access on their PCs that they can't access on their smart phones" [2]. With this imagination and vision, the acceptance of smart phones having Google's Android Operating System is continuously on the rise in the 21st century.

Android is an operating environment based on Linux kernel, it is also a superimposed or layered system [3]; the comprehensive architecture of Android system is shown in Figure 1. Application layer is the UI of all Android applications including an Email, SMS, GPS, web browser and others. All applications are developed using the Java programming language and Java APIs. All Android apps are based on the application framework. The Android application framework includes the following components:

- A rich set of Views that can be implemented to build an app with colorful UI, It includes set of lists, grid views, input boxes, buttons, and also an engrafted browser.
- A variety of Content Providers that facilitates the programmers to build the applications which can access data from other apps, or to share their own data with other apps.
- A Resource Manager that facilitates to provide access to resources such as strings, and layouts.
- A Notification Manager that gives provision to all applications to display user defined alarms in the status bar of the app.
- An Activity Manager that facilitates the app to handle the lifecycle of applications and provides a common navigation to the app [4-7].

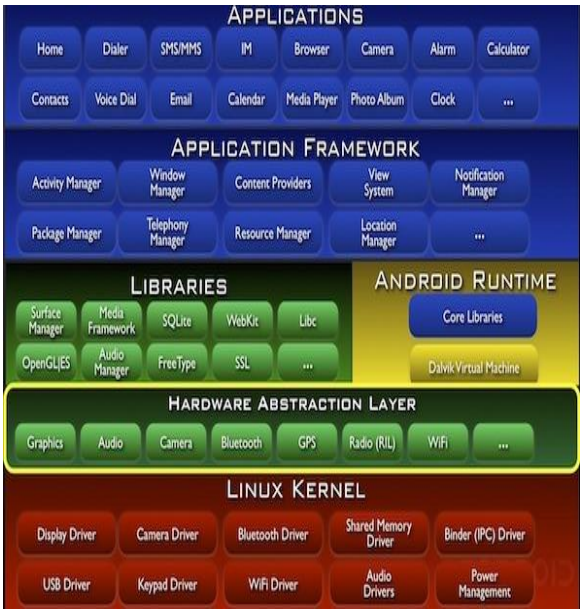


Figure 1. Android System Architecture

Some of the advantages of Android over other Smartphone operating systems are summarized below.

- The android is open source with its ability to run lacs of apps just like the iPhone but with variety of phone models unlike iPhone whose apps can run on iPhone only.
- Android allows developers & programmers to develop apps (applications) in an "application without borders" environment.
- Android is beginner friendly and supremely customizable. Android has the major share of the market because the user friendly experience and improving quickly as per their needs.
- Google's android now navigates user location and calendar to scientifically show you pertinent info *e.g.* traffic to work, cafes, and flight information and lets you explore with voice commands and replies with natural speech.
- Android is an open source service. This means we can freely download it and start building our own apps. Anyone can download to modify and enhance the software quality by making it more effective and user friendly. Apps are freely developed and designed by numerous app programmers worldwide and these developed apps are freely available on the Android market. This attractive feature of being open source has also attracted mobile phone companies to manufacture attractive phones using Android OS.
- Android is not just an operating system designed for individuals but it also fulfills serious business needs at the same time. Android market offers wide range of apps that are particularly designed to manage a business. It enables a closer look at various business processes on the go with the help of these apps.

3. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography all users or the appliances captivating part in the message exchange normally include a couple of keys, a open or public key and a private key, and a set of operations coupled with the keys to carry out the cryptographic operations. merely the particular client knows the private key where as the public key is circulated to all users taking part in the communication [2]. Each public key cryptosystem requires a set of predefined constants to be recognized by each and every one device captivating part in the communication. In the case of elliptic curve cryptography "area parameters" are the constants. Public key cryptography, contrasting private key cryptography, does not need any joint secret between the communicating parties but it is to a great extent slower than the private key cryptography [1-3].

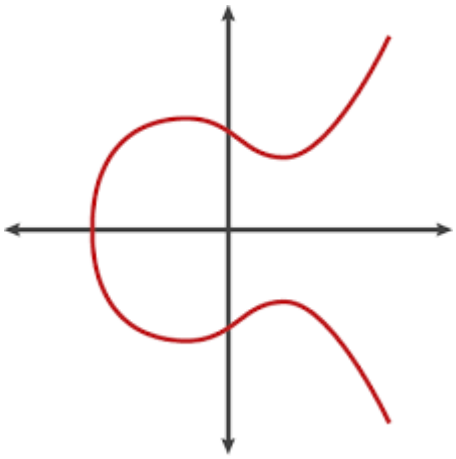


Figure 2. Elliptic Curve

The area parameters of elliptic curve are a sextuple:

$$T = (P, a, b, G, n, h)$$

An elliptic curve above a field K is a curve defined by an equation of the form

$$\mathbf{y^2 = x^3 + ax + b}$$

Where a, b Є K and $4a^3 + 27b^2 \neq 0$.

A. Discrete Logarithm Problem

The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem. Let P and Q be two points on an elliptic curve such that kP = Q, where k is a scalar. Given P and Q, it is computationally infeasible to obtain k, if k is sufficiently large. k is the discrete logarithm of Q to the base P.

B. ECC Public Key Cryptosystem

In the public key elliptic curve cryptosystems, assume that entity A wants to send a message 'm' to entity B securely. Order of a point on the curve can be defined as a value n such that, nP = P+P+..+P…. n times = O (infinity).

C. Generation of Public and Private Key

Both the entities in the cryptosystem agree upon the Domain Parameters (a, b, P, G, n). G is called generator point and n is the order of G. Now A generates a random number nA < n as his private key and calculates his public key set PA = G.nA B generates a random number nB < n as his private key and calculates his public key set PB = G.nB

D. Generation of common key

After exchange of the public key between the two parties Entity A computes his Common Key by Computing K= nA.PB Entity B computes his Common Key by Computing K= nB.PA The two above keys have same value because:

$$nA.PB = nA.\ (nB.G) = nB\ (nA.G) = nB.\ PA.$$

E. Encryption

Consider a message 'Pm' sent from A to B. 'A' chooses a random positive integer 'k', a private key 'nA' and generates the public key PA = nA × G and produces the cipher text 'Cm' consisting of pair of points Cm = {kG, Pm + kPB} where G is the base point selected on the Elliptic Curve, PB= nB.G is the public key of B with private key 'nB'.

F. Decryption

To decrypt the cipher text, B multiplies the 1st point in the pair by B's secret & subtracts the result from the 2nd point

$$Pm + kPB - nB(kG) = Pm + k(nB\ G) - nB(kG) = Pm.$$

4. Proposed Work and Implementation

The projected method uses the above model of elliptic curve cryptography to encrypt the message to communicate and launch it over a regular channel. The dispatcher writes a

message and gives the recipient's number, as soon as he sends the message the algorithm is launched on both the smart phones. The keys are generated and shared between the devices and the encryption takes place at the senders stop. Following encryption, the message is sent to the recipient and he decrypts it by means of his key to interpret it. The Encryption and Decryption methods in ECC are intended to encode and decode a point on the curve and not the whole message. During encryption, each character in the message has to be changed into bytes then the bytes into points of the structure (x, y) and after that the points have to be encoded by mapping every one of them with all points on the elliptic curve and after that the complete encoded points have to be transformed back to bytes and then to strings as SMS can hold only string values.

Once the message reaches the recipient, throughout the route of decryption, the string has to be transformed to bytes; these bytes should be decoded to points once more by means of the mapping method and after that the points to bytes and to finish to characters that form the message and only then the decrypted basic text can be viewed by the recipient. The below figure describes the entire process.

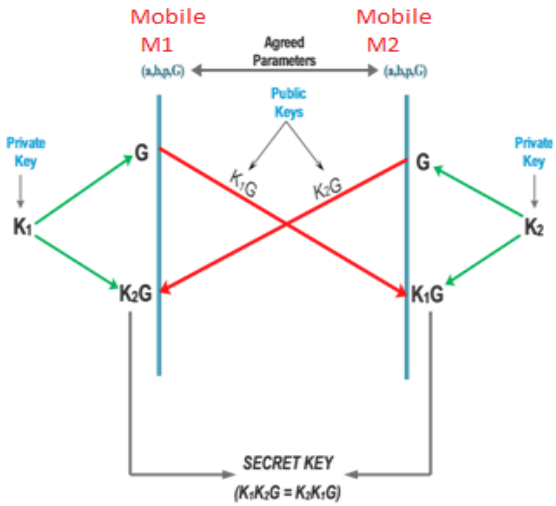


Figure 3. Elliptic Curve Diffie-Hellman Message Exchange

Javax.Crypto is loaded with the classes and interfaces for crypto-graphical operations. The crypto-graphical operations outlined within this package include the cryptographic classes, key generation and key agreement, and Message Authentication Code (MAC) generation. Support for cryptography includes bilaterally symmetric, asymmetric, block, and stream ciphers. This package additionally supports secure streams and sealed objects. several of the classes provided within this package are provider-based. The classes itself defines a programming interface to that applications could write. The implementations themselves could then be written by freelance third-party vendors and obstructed in seamlessly as required. So application developers could benefit of any range of provider-based implementations while not having to modify or rewrite code[10].

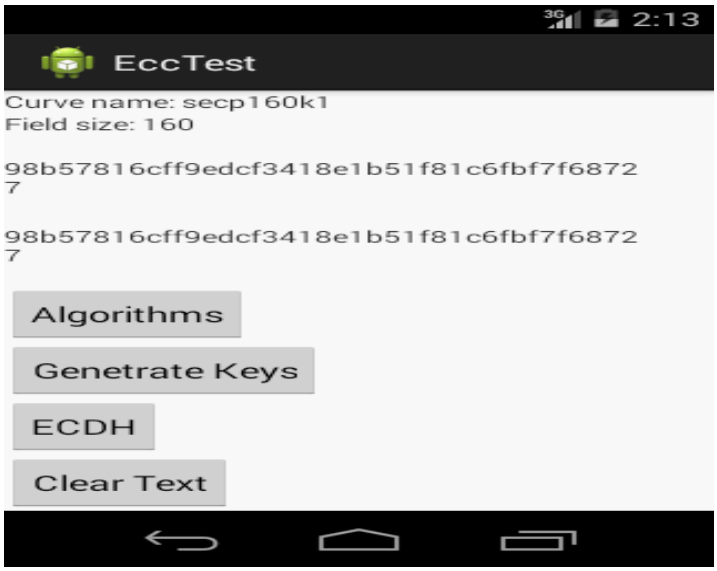


Figure 4. Screen Shot of ECC Implementation

5. Analysis & Conclusion

Think about an ordinary client who visits a banking place on his cell phone to relocate money to his associate. A small processing power-driven mobile appliance would move violently with the 1024 bit computations of RSA. With major monetary institutions, the minimum key size acceptable for RSA is 1024 bits. This action not only takes time to complete but also eats into the battery life of the apparatus. A few months back, the news that German Chancellor Angela Merkel's phone was tapped by the US government has created quite a scene. Amid this debate there was also news that Merkel used 2 phones – one BlackBerry (encrypted) and the other Nokia (not encrypted). In September, new government phones which were manufactured by the Canadian company BlackBerry were delivered to all government officials (including Merkel) after being restructured by the German corporation Secusmart. They include a particular encryption card that scrambles language and information before transmitting it. So this Secusmart card used the Elliptic curve cryptography to encrypt and decrypt the mobile verbal communication. And just because it is encrypted doesn't mean it's protected. It all depends upon how hard it is to break the key. ECC employs a comparatively small encryption key. It is quicker and requires less computing power than other first-generation encryption public key algorithms such as RSA, Diffie-Hellman. For example, a 160-bit ECC encryption key provides the same safety as a 1024-bit RSA encryption key and can be up to 15 times quicker, depending on the stage on which it is implemented. Elliptic curve cryptography has confirmed to be a capable solution for the accomplishment of public-key cryptosystems. As common use of the internet and mobile devices continues to enlarge, transferring data the information with less calculation and in a more protected manner has been the main center. With lesser key sizes and lower processing requirements, elliptic curve cryptography serves the function on mobile devices.

In this paper, a learning and relevance of Elliptical Curve Cryptography for addressing safety requirements of Android users have been discussed. As Elliptical Curve Cryptography consumes a reduced amount of energy and power, it becomes additional appropriate for resource restriction smart phone devices. The ancient security services similar to authentication, confidentiality, and key sharing can be sensibly implemented in Android run devices using ECC.

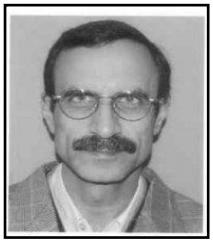
References

[1] L. A. Perlow, "Sleeping with your smartphone: how to break the 24-7 habit", Harvard Business review press, **(2012)**.
[2] A. Kataria, T. Anjali and R. Venkat, "Quantifying the smartphone vulnerabilities", Signal Processing & Integrated Networks (SPIN), International Conference on, 2014doi: 10.1109/SPIN.2014, **(2014)**, pp.645, 649.
[3] B. Dan, "Dalvik VM Internals", http://sites.google.com/site/io/dalvik-vm-internals, **(2008)**.
[4] M. A. Dar and J. Parvez, "Smartphone operating systems: Evaluation & enhancements," IEEE Conference on Control, Instrumentation", Communication and Computational Technologies (ICCICCT), 2014 International Conference on, Kanyakumari, **(2014)**, pp. 734-738.
[5] M. A. Dar and J. Parvez, "Evaluating Smartphone Application Security: A Case Study on Android", Global Journal of Computer Science and Technology Network, Web & Security, vol. 13, no. 12, **(2013)**.
[6] M. A. Dar and J. Parvez, "A Novel Strategy to Enhance the Android Security Framework", International Journal of Computer Applications (IJCA), Foundation of Computer Science (FCS), New York, USA, vol. 91, no. 8, **(2014)**, pp. 37-41.
[7] M. A. Dar and J. Parvez, "Enhancing Security of Android & iOS by implementing Need-Based Security (NBS)", IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT-2014), 10th and 11th, **(2014)**.
[8] M. A. Dar and J. Parvez, "Smartphone Operating Systems: Evaluation & Enhancements",IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT-2014), 10th and 11th, **(2014)**.
[9] M. A. Dar and J. Parvez, "A Live-Tracking Framework for Smartphones", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15, **(2015)**.
[10] https://developer.android.com/reference/javax/crypto/package-summary.html
[11] Cryptography and Network Security by Behrouz A. Forouzan
[12] "Implementation of elliptic curve cryptography on text and image", International Journal of Enterprise Computing and Business Systems, ISSN (Online): 2230-8849, vol. 1, no. 2, **(2011)**.
[13] "Securing MMS with High Performance Elliptic Curve Cryptography", International Journal of Computer Applications (0975 – 8887), vol. 8, no. 7, **(2010)**.
[14] "SMS Encryption using AES Algorithm on Android", International Journal of Computer Applications (0975 – 8887), vol. 50, no. 19, **(2012)**.
[15] "State of Security for SMS on Mobile Devices", IEEE Electronics, Robotics and Automotive Mechanics Conference, **(2008)**.
[16] N. Gura and A. Patel, "Comparing Elliptic Curve Cryptography and RSA on 8 bit CPU", Workshop on cryptographic hardware and embedded systems, **(2004)**.
[17] N. Gura, A. Patel, A. S. Wander, H. Eberle and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs", Cryptographic Hardware and Embedded Systems, vol. 3156, **(2004)**, pp. 119–132.
[18] D. J. Mallan, M. Welish and D. M. Smith, "A Public Key Infrastructure for Key Distribution in TinyOS based on Elliptic Curve Cryptography", First Annual IEEE Communications Society Conference on Sensor and Adhoc Communications and Networks, **(2004)**, pp. 71-80.
[19] A. S. Wander, N. Gura, H. Eberle, V. Gupta and S. C. Shantz, "Energy analysis of Public Key cryptography on Small Wireless Devices", 3rd. IEEE International Conference on Pervasive Computing and Communications, pp. 324-328.
[20] B. Menzes, "Network Security and Cryptography", Cengage Learning.
[21] D. Hankerson, "Guide to Elliptic Curve Cryptography", Springer.

Authors

Muneer Ahmad Dar, has completed his Bachelor's degree in science from university of Kashmir and M.C.A from the same university. He completed his M.Phil from Madurai Kamaraj University and is pursuing P.hD. from University of Kashmir. He has participated in more than 15 national and international conferences and has published various papers in some reputed journals. He is also the member of IETE. His areas of research are information Security, Smart phone Security, Data Mining and Algorithms He has served as Assistant Professor at different Government Colleges in Kashmir and currently is working as Scientist-B at National Institute of Electronics

& Information Technology (NIELIT) J&K which is the department under Deity, Govt. of India. E-Mail: muneer@nielit.gov.in



Javed Parvez, has served as an Assistant Professor with P.G Department of Computer Science, University of Kashmir since 2002. He received B.E. (Electrical & Electronics Engg.) from BITS, Pilani (INDIA) and M.S. (Computer Science) from University of Oklahoma (USA). He also received Ph.D (Computer Science) from the University of Kashmir (INDIA). His areas of research interest include the Security, Reliability and Performance of Computer and Mobile Communication Networks. Before joining our department he served in the R&D divisions of technology companies such as Epson, Synopsys, and Qualcomm & Ericsson. He has taught several subjects at the MCA level including C/C++ programming, Data Structures, Software Engineering, Data Communications, Computer Networks and has introduced and taught elective subjects such as Wireless/Mobile Communications. In addition he has taught and delivered lectures on interdisciplinary subjects such as Computer Viruses & Ecological Modeling. He is actively involved in guiding (M.Phil and Ph.D) research scholars & has published 32 research papers related to his fields of interest. He is a member of the IEEE, ACM and Computer Society of India(CSI).

