Advances in Wireless Communications and Networks
2017; 3(4): 29-38
http://www.sciencepublishinggroup.com/j/awcn
doi: 10.11648/j.awcn.20170304.11

Hybrid Insider Cyber Security Threats Mitigation Scheme Using ECC and Behavoural Analysis Methodology

Stephen M. Musili, Michael Kimwele, Richard Rimiru

Department of Computing, School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Email address:
stevemusilih@gmail.com (S. M. Musili)

To cite this article:
Stephen M. Musili, Michael Kimwele, Richard Rimiru. Hybrid Insider Cyber Security Threats Mitigation Scheme Using ECC and Behavoural Analysis Methodology. *Advances in Wireless Communications and Networks.* Vol. 3, No. 4, 2017, pp. 29-38.
doi: 10.11648/j.awcn.20170304.11

Received: December 3, 2016; **Accepted**: December 23, 2016; **Published**: July 4, 2017

Abstract: The last decade has been characterized by many organizations making it their priority to embrace digital technologies in running their services. Cyberspace has hugely dominated how organizations use electronics and the electromagnetic spectrum to manipulate, and exchange data via interconnected systems. Due to cyber space's great dependence on informatics and telecommunications for almost every activity and service, it's extremely catastrophic to ignore the growing phenomenon of cybercrimes and the increasing number of threats to organizations' systems. The threat to enterprises from insider activities is increasing, getting worse and that significant losses are being incurred. ESG research indicates that more than half (54%) of IT and security professionals believe that insider threats are more difficult to detect or even prevent today than they were in 2011 (Jon Oltsik, 2013). While many organizations focus their security efforts on their network border via excellently configured firewall systems, it is actually the insider who perhaps poses the most risk to cyber-security. Even the existence of some personnel can be at stake if the data is leaked. Cyber Security takes many forms and the range and nature of threat is so varied that there just isn't any getting away from the fact that it will require a multi-faceted solution. This paper suggests a hybrid framework aimed at guiding the management in coming up with a near real time mitigation solution that can be used to mitigate (*Detecting, Preventing and Responding*) the dynamic enigma of insider threats. The framework is based on behavioral variation analysis in conjunction with the use of technical techniques. We tried to change the landscape by adding the technological and behavioral equivalent of security cameras or additional lighting, and see whether the resulting uncertainty will eradicate the risk of attack in the cyber space.

Keywords: Cyberspace, Mitigation, Cybercrime, Elliptic Curve Cryptography, Public Key, Private Key

1. Introduction

Organizations are faced by various modes of attacks but it is widely believed that the threat to enterprises from insider activities is increasing, getting worse and that significant costs are being incurred. The multi-faceted dimensions of insider threats and compromising actions have resulted in a diverse experience and understanding of what insider threats are and how to detect or prevent them. Insiders commit these security breaches in various forms including liaising with outsiders.

Cyber-security is usually thought of as a technical field, with highly-skilled defenders seeking to outwit attackers in a contest of intellect and will. A significant proportion of computer and organizational security professionals believe insider threat is the greatest risk to their enterprise, and more than 40% report that their greatest security concern is employees accidentally/maliciously jeopardizing security through data leaks or similar errors. (Mellon, 2013)

While managing and maintaining organization's cyber space is a very challenging task already, the difficulties for systems administrators grow with each day. Unlike in the past when organization data securely sat on a server in the data center protected by access control and perimeter defenses, now it's everywhere. Organizations are dealing with the "Enemy Within" effects which have proved to be a major threat to cyber security. With technology growth been so dynamic, not only do these administrators have to keep pace, but also be willing to embrace change. Integration of

Mobile computing, Personal Digital Assistants (PDA) devices, Bring Your Own Device (BYOD) policies, Bring Your Own Technology (BYOT), Bring Your Own Application (BYOA), social media applications, cloud computing, Google worn technology among others have recently added a new twist to the work place. The fact that these facilities can have access to data from various locations complicates the whole issue of cyber security. There is no longer a perimeter to defend, and the devices cannot always be protected not forgetting the other issue of the unknown whereby no one knows what exactly the problem is.

2. Understanding the Insider Cyber Security Threats

An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. The term can also apply to an outsider who poses as an employee or officer by obtaining false credentials. (Rouse M. , 2010). A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. (Mellon, 2013)

In this particular paper, we will define an insider as accepted member (current or former employee, contractor, or other business partner) of any given group or organization who possess legitimate unlimited access to confidential information and the right to represent, or decide about one or more assets of the organization's structure.

As we try to understand the concept of Insider cyber security threats, it is equally important to understand that there is a very thin line between insider cyber security threat and a whistle blower and is equally easy for us to mistaken one for the other. Take the case of the leaked Wikileaks cables, Edward Snowden was entrusted with data that could not have gone outside the perimeter fence but by the end of the day, the data leaked to the surprise of many. Wikileaks cables concerning the USA activities in relation to some nations shouldn't have leaked where it not for trusted employees (insiders) abusing the trust accorded to them by their employers and compromising the integrity and confidentiality of data. "Insider threats are an intriguing and complex problem. Some assert that they are the most significant threat faced by organizations today. High profile insider threat cases, such as those conducted by people who stole and passed proprietary and classified information to wikileaks, certainly support that assertion, and demonstrate the danger posed by insiders in both government and private industry". (Dawn Cappelli, 2012).

There are several ways in which an insider can be used to affect the integrity of the organizations data. E.g insiders using organized crime or a terrorist group corrupting a willing insider (a disgruntled employee, for example) or making use of an unsuspecting insider (by getting someone with authorized network access to insert a disk containing hidden code).

The threat of attack from insiders is real and substantial. *Cyber Security Watch Survey (2011)*, conducted by the U. S. Secret Service, the CERT Insider Threat Center, CSO Magazine, and Deloitte, found that in cases where respondents could identify the perpetrator of an electronic crime, 21% were committed by insiders.

Although an insider can have software and hardware acting on his or her behalf, it is the individual's actions that are of primary concern in this project. However, it is also good to note that there is a very thin line between informers and insider security threats camouflaged as trusted personnel.

In addition, extremely trusted insiders who design, maintain, or manage critical information systems are of particular concern because they possess the skills and access necessary to engage in serious abuse or harm. Typical trusted insiders are system administrators, system programmers, and security administrators, although sometimes, ordinary users may have or acquire those privileges (sometimes as a result of design flaws and implementation bugs). Thus, there are different categories of insiders, (DHS Cyber security Research Roadmap, 2010).

These internal attacks can be the most devastating, due to the amount of damage a privileged user can do and the data they can access. Trust from which ever perception is actually a precious commodity–but too much trust can leave you vulnerable.

Insider threats pose significant challenges to any organization irrespective of size of financial power. In the recent past, many solutions have been proposed and others implemented to detect, prevent and even respond to unpredictable and ever changing insider threats. Unfortunately, given the complexity of the problem and the human factors involved, many solutions which have been proposed face strict constraints and limitations when it comes to the working environment. (Zeadally, 2012). This is highly contributed by the constant change in technology and also the untamed employee needs which vary from one organization to the other. "Unfortunately, while organizations are developing new security mechanisms, cybercriminals are cultivating new techniques to circumvent them," says Steve Durbin, Global Vice President of the Information Security Forum (ISF). He argues that businesses of all sizes must prepare for the unknown so that they have the flexibility to withstand unexpected, high impact security events which must be tamed but with the most reliable and economical means possible.

3. Research Results/Findings

Our findings present the study results obtained from the analyzed data. The results are presented in figure and table formats where appropriate. The findings are according to the response obtained from 40 respondents as shown in figure 1 for the response rate. The figure shows that the study obtained a response rate of 77% as out of the 52 targeted respondents, 40 were able to give out reliable feedback whereas 12 respondents did not give response to the study. Case studies are also part of the analysis of our data.

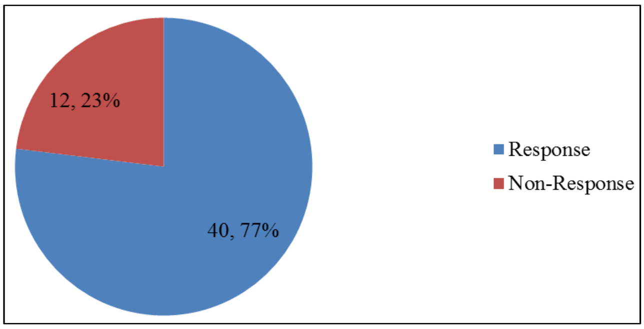


Figure 1. *Response Rate.*

4. Ways and Motives Behind Insiders Becoming Insider Cyber Security Threats

To ascertain exactly what happens in most of the organizations, a study was conducted targeting those employees who were deemed to be dealing with organization's sensitive data. This research was conducted at Machakos county headquarters. Of all the employees interviewed and who dealt with sensitive data had got shocking revelations. It is as well good to note that, the emerging technological concepts are also becoming a complicated issue to deal with. Policies like BYOD, BYOA, BYOT, social media engineering among others were the main contributing factors to information security. The table below gives the analysis of all those details.

Table 1. *Ways of Compromising Security.*

Mechanism used	Percentage
my own device	58.1
Verbal	19.4
Social media	12.9
Printed	9.8
Total (s)	100.0

Results as presented in Table 1 show that majority of the staffs who had shared organizational data had used their own devices such as Ipads, external storage devices, and laptops to share the information. This category had 58.1% of the respondents followed by 19.4% who had shared the information verbally with their friends and other third parties and 12.9% who had shared information through social media mechanisms. The least among the staffs who had shared information had used print media representing 9.8% of the respondents. This therefore reveals that personal devices are the major channels used by insiders in leaking organizations' sensitive data and information. The sharing of printed copies was somehow difficult for some staff members for they did not have a better mechanism to move out of the office with the content. But it is the combination of the other three mechanisms (My own device+verbal+social media) that lives a lot to be desired leading to 90.4%).

Table 2. *Precautions Adhered to in sending emails/using social media.*

	Percent
I always confirm what I am sending	12.5
I rarely check because I trust my recipients	82.5
There is nothing to worry about	5.0
Total	100.0

According to the results as presented in table 2 (12.5%) of the respondents reported that they always confirm what they are about to send before sending emails or using social media. This confirms that some employees are extra careful in observing security policies when dealing with digital communication mechanisms that can expose their information to unintended parties. However, 82.5% of the respondents reported that they rarely check since they trusted their recipients. This was due to the assumption that they commonly used customized internal staff emails, whereas 5% felt there was nothing to worry about whenever sending an email or using social media. Thus, some employees never observe carefulness in dealing with any sort of information regardless of the channel used to send the information.

5. Key Motivators for Data Leakage in Organizations

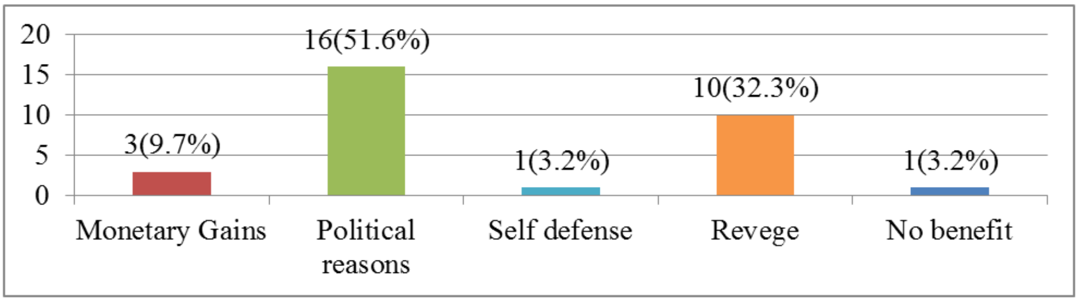


Figure 2. *Some of the major motivators leading data leakage in organizations.*

As illustrated in 2, the major motive for the sharing of the organization's sensitive data is political reasons which were cited by 51.6% of the respondents who had ever shared some information. 32.3% reported that they had to share the information as a form of revenge to some conditions they had undergone in the organization and 9.7% had been motivated by monitory gains who were paid by some other parties to share the information. The least (3.2%) were the respondents who reported that they had no reason for sharing the information and those who had shared the information for their self-defense. This reveals that political influence is the major factor influencing operation of the County Governments in Kenya as opposition leaders are interested in undermining the works of the elected government. This notwithstanding, these motives might as well change from one organizational setup to another for not all organizations setup have got political connotations with them. Financial, Faith Based organizations, learning institutions will have various reasons as to why their employees may leak very sensitive data.

6. Current Techniques and Their Limitations Used in Mitigating Insider Cyber Security Threats

It is believed that insider threats are influenced by a combination of technical, behavioral, and organizational issues and therefore these issues must as well be addressed by policies, procedures, and technologies. Due to this, almost all the organizations have put in place basic mechanisms of controlling insider security threats in various ways. Organizations have always ensured they have mitigation techniques in place according to various studies. These techniques and mechanisms have as well been used to address the threats posed by insiders who are highly trusted but end up betraying the trust accorded to them to leak confidential data.

The motive behind the implementation of various techniques is good but according to Carnegie Mellon University journal, the same commercial tools, techniques, and procedures which combat insider threats have been used for the past decade. One reason for that is that malicious activity by insiders looks like their authorized day-to-day online activity. As a result, many insider threat detection tools produce so many false positives that the tools are unusable. This is according to (Software Engineering Institute - CERT Division, 2014).

Many times, the analysis of security threats has been approached mostly based on terms of data confidentiality and privacy (such as data exfiltration). This alone isn't enough; for data in networks or other locations must be protected based on other important aspects like trustworthiness requirements, such as Privacy, Non-Repudiation, Accountability, Availability, and Integrity (AAI) which can also be breached by disgruntled employees/insiders who may be in the list of the most trusted.

i. Monitoring and filtering technique

The monitoring and filtering approach has got its fair share of challenges. Filtering solutions support monitoring in two ways. It mostly emphasizes on transfer of data mostly via email. However, this does not cater for the issues brought about by the challenges of BYOD and other portable devices among others. In its approach, all data transfers are checked for sensitive information. With some systems, application of business policies prevents or restricts certain types of transfers. In any case, alerting is key when a questionable transfer occurs: including a large file transfer at an odd time or between questionable locations. This is according to *Insider threats: Implementing the right controls;*(Olzak, 2013).

ii. Application-level encryption

Some of the challenges with this encryption method are that insider attackers can use development tools, intended for tasks such as application monitoring or debugging, to gain access to encryption keys or simply to turn off encryption, unlocking information within the application. (Thales E-Security, 2015).

This method can be operationally intrusive and may take considerable time to deploy, especially if multiple applications are in scope; it is not transparent to the application environment and requires a development team that can program, maintain and support the application as business requirements change. This approach is highly costly in terms of time, money, and development staff to integrate encryption into the application and provide ongoing application development support. Without creating additional applications to support them, application-level encryption does not apply to unstructured data such as reports and spreadsheets. Operating system and programming language support are typically limited to what the application-level encryption vendor offers.

iii. File level encryption technique

This is commonly used to safe guard files and folders from malicious insiders. It is in contrast to full disk encryption where the entire partition or disk, in which the file system resides, is encrypted. However, the main challenge with this is that this technique is actually applicable to unstructured data such as reports developed from word processing applications and spreadsheets.

Although ISF outlines some of the major challenges that are to be witnessed in 2014 due to technological change, (Christian W. Probst, et. al 2014) argue that the "insider threat" or "insider problem" has received considerable attention and is cited as the most serious security problem in many studies. *Sarvesh (2013),* on his Highlights in the History of Cyber Security article, argues that not all organizations are willing and able to change with time because of the financial implications involved in implementing new technologies. He also says that, with many companies unable to keep pace with the technological savvy and creative data manipulation techniques used by cyber criminals, cyber security sometimes seems to be taking a reactive stance instead of a proactive one.

From the Ominous State of Insider Threats research conducted by Jon Oltsik in 2013, he found out that that more than half (54%) of IT and security professionals believe that insider threats are more difficult to detect/prevent today than they were in 2011. Another major challenge to the security is that traditional approach to security protects devices and perimeters–but with the proliferation of Bring Your Own Device (BYOD), cloud, social networks, worn technology and multi-user collaboration, there is no longer a perimeter to defend, and the devices cannot always be protected.

It is believed that, 58% of information security incidents are attributed to insider threats. He also says that Eighty-seven percent of ICT leaders (93% in the finance industry) believe the use of new technology requires constant change and evolution within security policy; but 72% admit to difficulty in keeping up (Jamie, 2013).

Access control however has a number of limitations. As noted earlier, even perfect access control will not prevent insider attacks who are only using privileges deemed necessary to get their job done. Studies reveal a major disconnect between what "real world" practitioners desire and what the research communities offer. Limiting legitimate access can have a negative effect on the productivity of non-threatening staff. What evidence there is suggests that monitoring can suffer from both false negatives and false positives.

Finally, there is the issue of how effective monitoring is. Because there is little insider attack data available, it is impossible to tell whether monitoring helps. Monitoring is, reportedly, useful in confirming an already suspected insider attack. There is a controversy as to whether it serves as a deterrent (Pfleeger, 2007).

7. The Way Forward

The goal remains to develop dynamic mechanisms for integrating, correlating, and fusing the data sources available on a host in a single anomaly detection system to rapidly detect and identify malicious activities in near real-time, and robust against false positives. Work continues on probabilistic anomaly detection with the goal eventually of modeling user intent.

Technology alone; Not the answer.

When it comes to technology solutions for identifying insider threats, Ready said that traditional IT defenses like IPS (intrusion prevention systems), firewalls and anti-virus won't help. An emphasis on people and organizational risk factor is the key. We have to be aware that there is no big button that says "*CLICK HERE TO CATCH A SUSPECT*" and therefore we have to be ready to come up with solutions on how to mitigate the challenge of insider cyber security. This is exactly the reason as to why we have come up with a hybrid approach which involves the combination of Elliptic Curve Cryptography Algorithm And Behavioral Analysis Methodology which has proven to be effective.

Figure 3 indicates that insider cyber security threats may be as a result of deliberate, accidental or even unknown factors that can lead to negative effect of the data Confidentiality, Integrity, Availability (CIA) and probably end up leading to serious damaging of the organizational reputation. With the proposed approach that encompasses the use of ECC technology as well as behavioral analysis, these can lead to improved performance as well as high security levels within the organization. This will as well ensure that the above mentioned properties (CIA and organizational reputation) are not compromised.

i. The Behavoural Approach

Behavioral Indicators for Declaring an Insider a cyber-Security Threat.

57.5% of the respondents reported that it was easier for any given organization to mitigate insider cyber security threats based on behavioral/psychological monitoring.

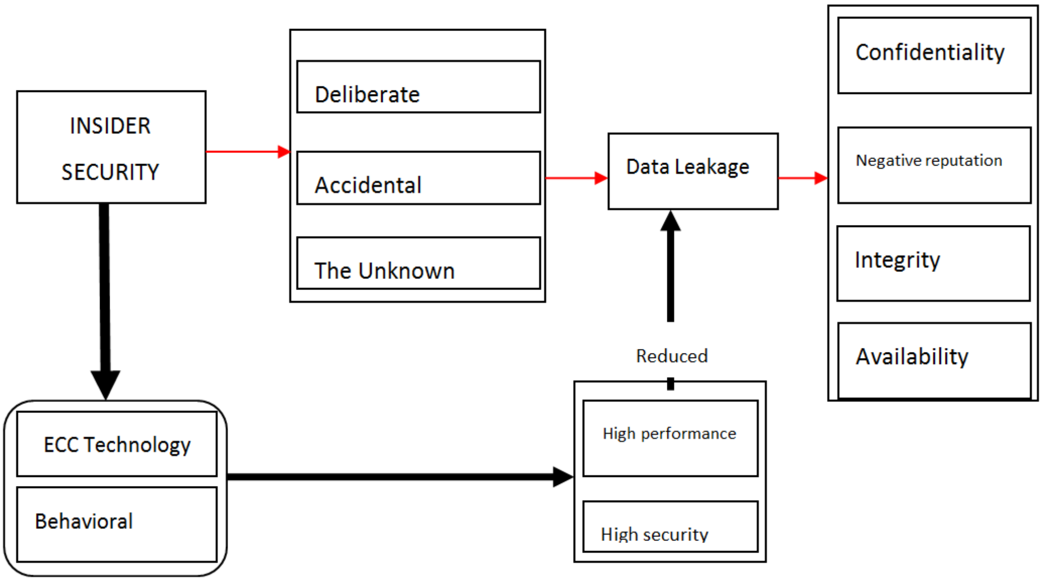


Figure 3. *Conceptual Framework.*

Table 3. *Detection of Security Threat through behavioral monitoring.*

		Organization predict/know when an employee has become a security threat
		Yes
How can it detect	Rebellions and transfer blame	82.8
	Intolerance of criticism	3.4
	Passive aggressiveness	6.9
	views self above set regulations	3.4
	Lateness/absenteeism to work	3.4
Total		100

Most of the insiders believe that, with better policies, it was easy the organizations to predict and take actions right before an attack. Of all these respondents, 82.8% reported that the organization could detect security threats through rebellions and transfer blame. Other ways of threat detection included intolerance of criticism (3.4%), passive aggressiveness (6.9%), and employees viewing themselves above the set regulations (3.4%) as well as lateness/absenteeism to work (3.4%). However, 27.5% reported that their organizations could not predict/know whenever an employee has become a security threat since these organizations had no strong surveillance mechanisms for the work being undertaken by their employees.

Findings under this section support the findings of Rouse (2010) which illustrated that employees are the major insider sources of cyber security threats in any organization and these poses a high risk since they have access to all the organization’s data and vital information. However, the study illustrated that there is no need to despair since with proper planning and the use of state of the art digital capabilities, the risks can be kept posed to the organization acceptably low and protect their most valuable information.

ii. Technological Mechanisms

It is important to note that even though the use of behavioral analysis is important, it is as well equally important to apply and invest in technology as a powerful measure of counteracting Insider cyber security threats. Threats posed by BYOD, BYOA, carelessness among others can not only be eradicated with behavioral monitoring alone. Due to this, in this paper, we suggest a workable ECC algorithm that is aimed at protecting data that is in storage; data on transit (E-Mails) and to some extend that data that is in use.

a. Why use ECC?

Over the past 30 years, public key cryptography has become a mainstay for secure communications over the Internet and throughout many other forms of communications. *Rohini,* in relation to cloud computing services says that Elliptic Curve Cryptography Algorithm provides secure message integrity and message authentication, along with non-repudiation of message and data confidentiality. (B.P.I.T., 2013).

ECC is emerging as an attractive public-key cryptosystem for mobile/wireless environments. Compared to traditional cryptosystems like RSA, ECC offers major advances on older systems like equivalent security with smaller key sizes, which results in faster computations; lower power consumption, as well as memory and bandwidth savings thus making it ideal for PDA devices. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity.

i. Elliptic Curve Security and Efficiency:

The majority of public key systems in use today use 1024-bit parameters for RSA and Diffie-Hellman.

The following table gives the key sizes recommended by the National Institute of Standards and Technology to protect keys used in conventional encryption algorithms like the (DES) and (AES) together with the key sizes for RSA, Diffie-Hellman and elliptic curves that are needed to provide equivalent security.

Table 4. *Equivalent key size recommended by NIST.*

ECC key Key	Size RSA	Size Ratio
112	512	1:5
163	1024	1:6
192	1536	1:8
224	2048	1:9
256	3072	1:12
384	7680	1:20

Source: (Mr. Pragnesh G. Patel, 2013), Data Security in Cloud Computing using Elliptical Curve Cryptography

Security is not the only attractive feature of elliptic curve cryptography. Elliptic curve cryptosystems also are more computationally efficient than the first generation public key systems, RSA and Diffie-Hellman.

ii. How it works

Mostly, public key encryption system has two major components, a public key and a private key. In our algorithm, encryption works by taking a message and applying an elliptic curve crypto operation to it to get a random-looking number. Decryption takes the random- looking number and applies a reverse operation to get back to the original number. Encryption with the public key can only be undone by decrypting with the private key.

PDA devices don't do well with arbitrarily large numbers. We can make sure that the numbers we are dealing with do not get too large by choosing a maximum number and only dealing with numbers less than the maximum. We can treat the numbers like the numbers on an analog clock. Any calculation that results in a number larger than the maximum gets wrapped around to a number in the valid range.

ECC needs a different key for encrypting and decrypting. That's why it's called asymmetric encryption.

An elliptic curve is the set of points that satisfy a specific mathematical equation. The equation for an elliptic curve looks something like this:

$y^2=x^3+ax+b$

Components of ECC

E=Elliptic curve

P=Point on the curve

N=Maximum limit

The curve $y^2=x^3+ax+b$ assumes the shape below

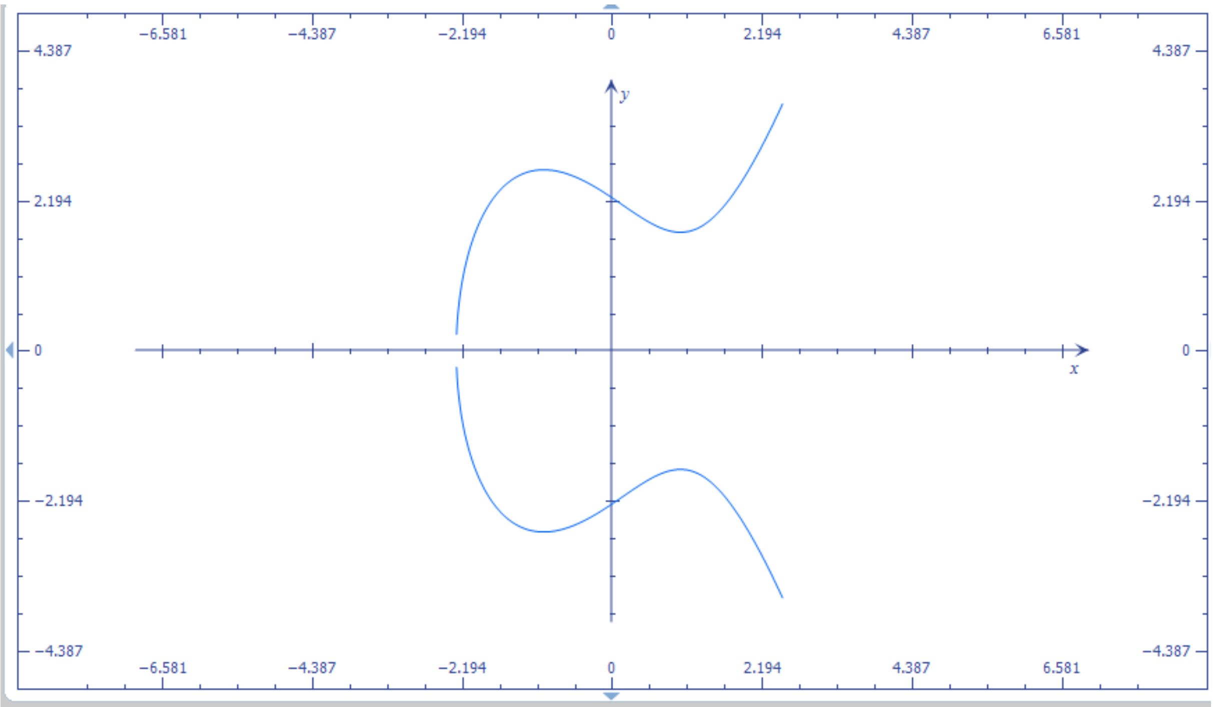
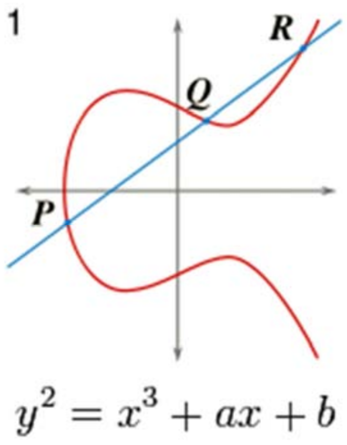


Figure 4. *$y^2=x^3+ax+b$ curve.*

Parts of the curve



This figure shows the addition of two points on an Elliptic curve.

Elliptic curves have interesting properties that having two points on the Elliptic curve yields a third point on the curve. Small changes in P or Q can cause a large change in the position of R.

So let's go back to the original problem statement from above. The point Q is calculated as a multiple of the point P, i.e Q=nP.

An attacker might know P and Q but finding the integer n is a difficult problem to solve.

Q (i.e nP) is the public key and n is the Private Key.

With this representation, you can take messages and represent them as points on the curve. Imagine a message and setting it as the x coordinates and solving for y you get a point on the curve. It is slightly more complicated than in practice, but this is the general idea.

For example, in the equation $y^2=x^3+3x+5$, solving for x will be

Solution 1

$$x=\sqrt[3]{\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}+\sqrt[3]{-\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}$$

$$x=\frac{\sqrt{3}\,i\left(\sqrt[3]{\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}-\sqrt[3]{-\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}\right)-\sqrt[3]{\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}-\sqrt[3]{-\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}}{2}$$

Solution 2

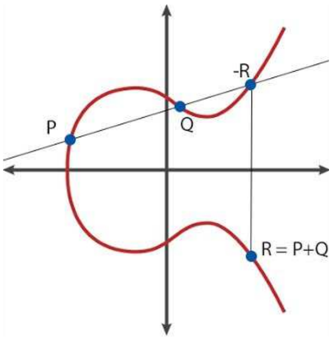
$$x=\frac{-\sqrt{3}\,i\left(\sqrt[3]{\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}-\sqrt[3]{-\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}\right)-\sqrt[3]{\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}-\sqrt[3]{-\sqrt{\left(\frac{y^2-5}{2}\right)^2-1}+\frac{y^2}{2}-\frac{5}{2}}}{2}$$

Solution 3

Note: An Elliptic curve crypto system can be defined by picking a prime number as the maximum, a curve equation a public point on the curve.

Technically, an Elliptic curve is a set point satisfying an equation in two variables in our case (x and y) with degree two in one of the variables and three in the other.

iii. Diagram 1: Characteristics of the curve



Taking a closer look at the elliptic curve plotted above. It has several interesting properties.

One of these is horizontal symmetry. Any point on the curve can be reflected over the x axis and remain the same curve. A more interesting property is that any non-vertical line will intersect the curve in at most three places.

iv. Sample Application of ECC

Assuming two colleagues Charles and Jane would like to send and receive mails from each other, the operations would be as follows;

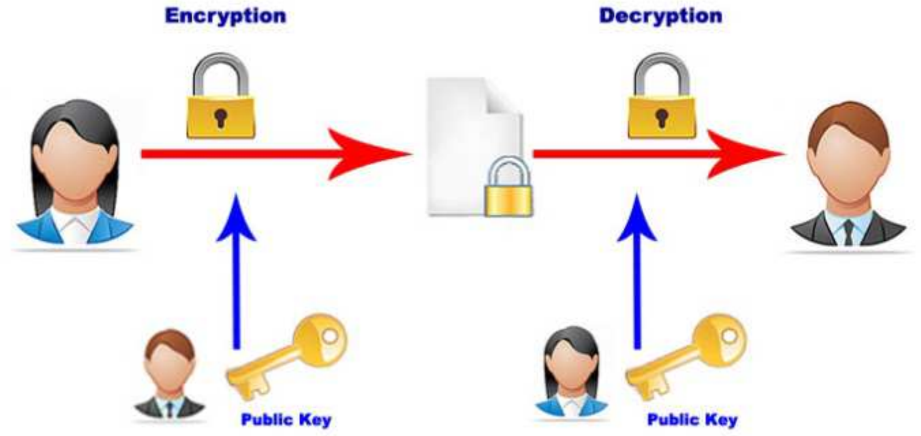


Figure 5. *Conversation between Judy and Steve via E-mails.*

As indicated in Figure 5 (Above), Suppose Jane wants to send a mail M (x, y) to Charles.

From one side i.e the sender's (Jane), both public and private and private keys are generated then the message is generated after which it is encrypted with the private key. The sender as well sends the public key to the receiver (Charles) who then decrypts the message using the sender's public key and vice versa.

During the encryption of the message the ECC algorithm will execute the following operations assuming our message is an e-mail.

Let 'm' be the message that we are sending. We have to represent this message on the curve.

i. The curve function is y^2=x^3+ax+b mod p with a point on the curve G (x, y)

Two cipher texts will be generated let it be C1 and C2.

C1=a*Q (C1 been the public key)

C2=b*Q (C2 been the private key)

ii. Jane picks a private key nA and computes her public key Qa=nA. G

iii. Jane encrypts the message D=M+na. Qb (D=cipher text) and sends (Qa, D) to Charles

iv. C1 will be send to Charles.

v. To decrypt the message, Charles computes M=D+(-nb). Qa and he recovers M

Proof

How do we get back the message?

i. M=C2–d * C1

ii. 'M' can be represented as 'C2–d * C1'

iii. C2–d * C1=(M+a* Q)–d * (a* P) (C2=M+a * Q and C1=a* P)

iv.=M+a * d * P–d *a *P (canceling out a * d * P)

v.=M (Original Message)

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Speed reports for elliptic-curve cryptography and RSA analysis.

The following tables summarize various processor speed reports for elliptic-curve scalar multiplication in respect to various key sizes. This analysis was conducted based on the agreement time between the public key and the private keys, the sign time and the verification time of the transactions for both ECC, and RSA. This was as well conducted based on the analysis of various types of processors for PDA's that are already in use in the ICT industry today.

Table 5. *ECC Comparison and Analysis.*

Processor Type	Processor speed (Ghz)	Key size	Key Generation Speed (Ms)	Key agreement	Sign Time	Verification Time
Intel Core i7	2.20	256	0.685	0.665	0.717	0.952
AMD E2-1800	1.70	256	1.811	1.765	1.896	2.544
Intel (R) Celeron (R)	1.80	256	1.095	1.040	1.153	1.529

Table 6. *RSA Comparison and Analysis.*

Processor Type	Processor speed (Ghz)	Key size	Key Generation Speed (Ms)	Key agreement	Sign Time	Verification Time
Intel Core i7	2.20	2048	0.728	0.724	0.099	1.841
AMD E2-1800	1.70	2048	2.213	2.246	1.334	5.22
Intel (R) Celeron (R)	1.80	2048	1106	1.114	0.148	2.860

8. Conclusion and Future Work

ICT professionals know that cyber security threats become more plentiful and sophisticated every year, and there is no reason for that trend to change. Even the most cautious analyst will admit that the threat is serious and that it needs serious attention. So we all get sold on the need for Cyber Security defense measures and there is plenty of fear, uncertainty and doubt (FUD) used to amplify the urgency and acuteness of the need. The difficulty when determining the right Cyber Security strategy for any given organization and in turn, which technologies and products to use is not too dissimilar to assessing the market choices for keeping our bodies fit and healthy.

The digitization and interconnection of society, and, in particular, critical infrastructures, increase the risk of accidental or deliberate cyber disruptions. International cyber criminals go unpunished and an escalating cyber arms-race threatens global and regional stability.

But there is no need to despair; with proper planning and the use of state of the art digital capabilities, we can keep the risks posed to our organization acceptably low and protect our most valuable information.

From our insider cyber security understanding, organizations should do anything within their reach to safeguard the integrity and confidentiality of their highly valued data. For the organizations to ensure security of their information, it is important for employers to appraise each new employee of the company’s expectations regarding protection of confidential information and critical infrastructure in a one-on-one conversation with a member of management. This should also include in-depth explanations of any policies governing the employee’s access to such information, and any monitoring or other policies that could implicate an employee’s privacy.

And it is precisely for this reason that organizations will continue to get breached unless a Cyber Security mind-set becomes second nature for all employees. Because there is no button written “*click here to catch a thief*”, it is as well equally important for organizations to get use technological mechanisms and more so the use of ECC which is highly recommended especially for low power PDAs. With use of well-developed ECC algorithms or security systems, there will be enhanced performance more so on the PDAs use which has attributed to the BYOD, BYOA, BYOT policies. Even though this approach proved to be effective, we realized that it is not possible to cure stupidity for there are those malicious users who will try all they can within their jurisdiction to compromise on security and this is why there is *No such thing as 100% security*. Indeed we do not claim that our approahc is a replacement for all other existing mechanisms, but that it occupies a certain niche and complements other existing approaches.

It is clear that, most of the scientist and researchers have started shifting gears to higher levels of protecting data from the cloud level with a key assumption that all is well for the data stored locally on PDAs. Future work can contribute to the understanding and advancement in the aspects of security on the cloud based systems, Internet of Things (IOT), security for forensic evidence as well as real time solution for Big Data solutions.

However, other than security on the cloud system and other state of the art systems among others, it is our sincere dream that future work will provide a real time solution more so on voice and video data/records that have become a thorn in the flesh for most organizations. The security challenges that are as a result of worn technology must as well be addressed sooner than later if at all the reputation of all organizations needs to be upheld.

References

[1] (DHS), T. D. (2 May 2014). Combating the Insider Threat. *National Cyber Security and Communications Integraton Center*, 1.

[2] (SEI), C. D. (n.d.). *Insider Threat*. Retrieved July 13, 2014, from CERT: http://www.cert.org/insider-threat.

[3] *Software Engineering Institute - CERT Division*. (2014, July 01). Retrieved September 23, 2014, from CERT: http://www.cert.org/insider-threat/research/controls-and-indicators.cfm?

[4] Christian W. Probst, J. H. (2010). *Insider threats in Cyber security.* New York: Springer Science.

[5] David Leigh, L. H. (2011). *Wikileaks, Inside Assange's war on secrecy.* Newyork, NY 10107: United States PublicAffairs.

[6] Dawn Cappelli, A. M. (2012). *The CERT Guide to Insider Threats; How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Pittsburgh,: Addison-Wesley Professional | ISBN: 9780321812575.

[7] E-Security, T. (2015, January). *Thales E-Security*. Retrieved January 02, 2015, from Thales e-Security: https://www.thales-esecurity.com/solutions/by-technology-focus/application-level-encryption.

[8] Foremski, T. (2013, November 14). *Security startups are booming so why is enterprise security getting worse?* Retrieved December 18, 2014, from ZDNet: http://www.zdnet.com/article/security-startups-are-booming-so-why-is-enterprise-security-getting-worse/.

[9] Hunker, J. (2010). Insiders and Insider Threats. *An Overview of Definitions and Mitigation Techniques*, 10.

[10] Jamie, M. (2013, May 03). 58% Information Security Incidents Attributed to Insider Threat. *Info Security Magazine*, 3.

[11] Jon Oltsik, S. P. (2013). The Ominous State of Insider Threats. *2013 Vormetric/ESG Insider Threats Survey*, 3.

[12] Kothari, C. (2011). *Research Methodology.* New Age International.

[13] Mellon, U. C. (2013). Unintentional Insider Threats:. *Software Engineering Insitute*, ix.

[14] Olzak, T. (2013, February 21). *Insider threats: Implementing the right controls*. Retrieved October 20, 2014, from Tech Republic: http://www.techrepublic.com/blog/it-security/insider-threats-implementing-the-right-controls/.

[15] Pfleeger, C. P. (2007). *Reflections on the Insider Threat.* New York City: Springer.

[16] Rouse, M. (2010). *insider threat*. Retrieved November 10, 2014, from insider threat: http://www.techtarget.com/contributor/Margaret-Rouse.

[17] Rouse, M. (2010). *Insider threat*. Retrieved November 10, 2014, from Whatis.com: http://searchsecurity.techtarget.com/definition/insider-threat.

[18] Silowash, G., Dawn, C., P. Moore, A., F. Trzeciak, R., J. Shimeall,. T., & Flynn, L. (2012). *Common Sense Guide to Mitigating Insider Threats, 4th Edition December.* Carnegie Mellon: Software Engineering Institute.

[19] Thibodeaux, T. (2014, Dec 16). *Talkin Cloud.* Retrieved December 18, 2014, from http://www.talkincloud.com: http://talkincloud.com/cloud-computing/12162014/changing-cso-role-what-expect-2015.

[20] Vometric. (2012). Securing Sensitive Data. *Technical White Paper*, 04-06.

[21] Westervelt, R. (2013, January 02). *Dynamic Computer Corporation*. Retrieved 07 18, 2014, from dcc-online: http://dcc-online.com/wordpress/?p=604.

[22] Westervelt, R. (2013, December 20). *Top 5 Technologies That Detect Insider Threats*. Retrieved September 20, 2014, from The Channel Company: http://www.crn.com/slide-shows/security/240164945/top-5-technologies-that-detect-insider-threats.htm/pgno/0/4.

[23] *Wikipedia*. (n.d.). Retrieved from http://en.wikipedia.org/wiki/Insider_threat.

[24] Zeadally, S. (2012). Detecting Insider Threats: Solutions and Trends. *Information Security Journal: A Global Perspective*, 1-2.