BYOD Threats Mitigation Approach using Elliptic Curve Cryptography

Stephen M. Musili[1] Dr. Richard Rimiru[2] Dr. Michael Kimwele[3]
[1,2,3]Department of Computing
[1,2,3]School of Computing and Information Technology Jomo Kenyatta University of Agriculture and Technology Nairobi, Kenya

Abstract— In the last decade, most of organizations have made it their priority to embrace digital technologies in running their services. Cyberspace has hugely dominated how organizations use electronics and the electromagnetic spectrum to store, manipulate, and exchange data via networked 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 citizens' daily activities and also organizations' systems. 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 losses are being incurred. Many people from executives to ICT administrators to partners, have access to sensitive data that if publicly exposed, could have significant ramifications to an organization's business—or even its existence. Even the existence of some personnel can be at stake if the data is leaked. While many organizations focus their security efforts on their network border via excellently configured firewall and systems and Demilitarized Zones, it is with no doubt that it is insider who perhaps poses the most risk to cyber-security. To mitigate the above massive risks from insiders, organizations have as well abundantly embarked on the fence approach other than monitoring of the PDA's that are already in use within the organization premises as a result of BYOD emerging policies. Organizations have also used normal encryption techniques, common sense approach not forgetting normal network monitoring which have proven to be futile. In this paper, we have proposed ECC based encryption and decryption algorithm and framework which are aimed at providing a near real time mitigation (Detection, Prevention and Response) solution. In our case, we target to protect that data on use such that if any insider purports to save data in his foreign device it will automatically be encrypted until he gets back to the authorized gadget. As well, we have a solution for the data that is in storage such that if any malicious insider decides to penetrate the storage locations or due to a configuration error the data will be inaccessible. 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.

Key words: Cyberspace, Mitigation, Cybercrime, Data Security, Elliptic Curve Cryptography, BYOD, PDAs, Public Key, Private Key

I. INTRODUCTION

As organizations work out on the best mechanisms for addressing the world's economic crunch, they find themselves pressed between a rock and a hard surface trying to figure out on how to address the security threats brought about by the indulgence of insider cyber security threats more so from the presence of BYOD approaches. Bring your own device (BYOD) has gained high momentum in enterprises. Instead of preventing employees from using their own devices and purchasing separate ones for company use, enterprises are adopting BYOD management policies that let them capitalize on the employees' available PDA devices. There is no doubt that, due to the increased number of the introduction of these devices in the working environment, employees are happy using devices that they're comfortable with to perform work-related tasks. It is strongly assumed as a win-win for both sides though this is highly seasonal as long as the unexpected data loss doesn't happen.

The initial issue facing the ICT business is that, like it or not, the BYOD phenomenon is happening already. Research conducted by the analysts Ovum indicated that around the world 57 percent of full-time employees use their personal gadgets at work in some capacity. However, the benefits of BYOD can only be hassle-free if companies can effectively manage these multifarious devices and protect their data from being compromised. The concept of take home work related assignments is also proving to be a key factor as to why employees feel more comfortable using their own devices for they can conveniently save various tasks and wind them up at the comfort of their homes.

With data security threats facing all organizations' networked zones; irrespective of size or financial muscles, ICT departments have devised means and ways of mitigating most of the threats and more so those threats that are as a result of outsiders. But just when those departments assumed they had the local networks locked and somewhat secure, BYOD is proving to be a thorn in the flesh for it has mutated a litany of unforeseen untamed challenges. Several new trends in information access are impacting organizations' ability to control and secure sensitive corporate data. The increase in web applications and cloud computing, the BYOD phenomenon among others mean that employees, business partners and stakeholders are increasingly accessing information using a web browser on a device not owned or managed by the organization.

BYOD has led to an increase of mobile devices, cloud storage repositories, different kinds of data types, and, of course, data theft by disgruntled employees. This has resulted in security implications for data leakage, data theft and regulatory compliance.

II. WHY THE INCREASE OF BYOD IN ORGANIZATIONS

BYOD policies or even permissions have gained substantial momentum in organizations. Instead of keeping employees from using their own devices and purchasing separate ones for company's use, enterprises are adopting BYOD management policies that let them capitalize on the employees' available PDA resources. As many ICT departments struggle to keep up with progressive technology changes, company employees increasingly want to use their own devices to access corporate data. It's part of a growing

trend dubbed BYOD, which encompasses similar Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP) and Bring Your Own PC (BYOPC) initiatives. All of them have evolved to empower workforces through the so-called 'consumerization of IT'. As part of this consumerisation, this encourages company employees to conveniently choose a gadget of their own to get access to corporate email or general data. This is in a way, if fully utilized with sober and reliable employees on board can increase productivity and reduce on costs. (Evans, 2015)

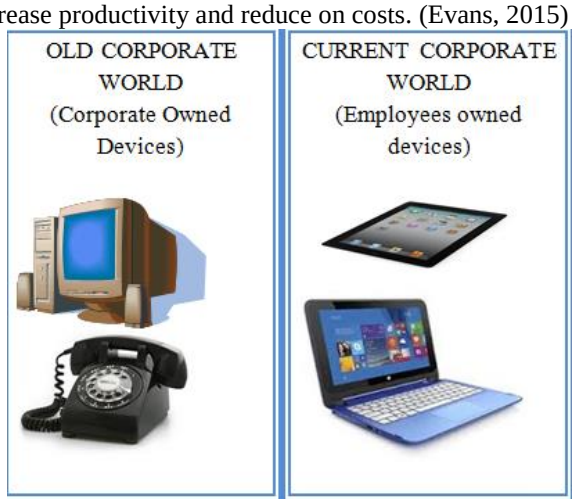


Fig. 1: Screenshot

BYOD promises many benefits including but not limited to:

- High rate of returns on innovation, better work-life balance and increased productivity. Due to the comfort associated with the use of personal gadgets, this makes a good percentage of employees deliver on deadlines hence increase on productivity. Employees also tend to maintain constant upgrade based on emerging technological trends which make the organization benefit from the latest features.
- Employee satisfaction: Most of the organizations will purchase gadgets based on their budgetary allocations whereas many people use the devices they have chosen and invested in—rather than what was selected by the ICT departments. In this relation, allowing employees to use personal devices also helps them avoid carrying multiple devices. Employees in high growth, emerging economies, such as Brazil, South Africa and Malaysia are demonstrating that they have more flexible attitudes to working hours, and are happy to use their own devices to get the job done where necessary. (Adrian Drury, 2013)
- BYOD programs sometimes save budget by shifting costs to the user, with employees paying for mobile devices and data services. However, this often results in little to no savings.

III. Challenges Posed by BYOD in Organizations Today

With the above benefits notwithstanding, BYOD also has a dark side. If not fully understood and regulated, it can threaten Cyber security and put a company's sensitive organizations systems at peril.

The driving force behind BYOD is a new ICT self-sufficiency among company employees who already own and use personal laptops, tablets and smart phones. These mobile devices are often newer and more advanced than the equipment deployed by many ICT departments. The use of these devices has by all means created all the necessary loopholes for them to be declared disastrous to data security. From saving unauthorized data to these devices to recording business meeting conversations are some of the major known threats. (Kaneshige, 2014), a senior writer with CIO believes that secret video and audio recordings has/is already manifested itself into the employers. “With Google Glass and other wearables woven discretely into clothing coming out soon, anyone can become a super spy like James Bond (or maybe someone with less noble intentions” Kaneshige. There's no question secret video and audio recordings will explode in the workplace.

This trend spells disaster for companies, especially those that encourage the use of personal mobile devices at work under formal BYOD policies. Imagine the fallout -- legal and otherwise -- of a workforce secretly recording the comings and goings of corporate life. Employees can prove managers treated them unfairly in performance reviews, swipe audio in a confidential conference call, record obnoxious behavior, and become whistle blowers for illegal or immoral activity.” Kanshige Tom

- Due to the ever emerging trends in the ICT sector, employees have got SoA gadgets while ICT departments are playing catch up and could easily refuse to embrace the BYOD idea. Though it is simpler to provide approved hardware and software applications so you can retain full control over them, it is still a challenge because the enterprises are as well benefiting from them.
- ICT personnel are as well overwhelmed in this era where the digital world has multi-faceted Operating systems running on various mobile devices. From Windows to Android each subjecting the teams to various diverse security loopholes. All of which requires attention in equal measure.
- But Richard Absalom, an analyst at Ovum, believes that BYOD will happen whether a company plans for it or not. He says: "Trying to stand in the path of consumerised mobility is likely to be a damaging and futile exercise." The best thing that an enterprise can do is be aware of the benefits and understand the risks. (Fulton, 2013)
- Android enabled devices which by default dominate the digital world pose the biggest threat to data security. According to (Sverdlove, 2012), Bit9 analyzed more than 400,000 Android apps in Google Play and the results are a wakeup call to many ICT professionals. 72 per cent of apps use at least; one permission, which gives the app access to private data or control over the smartphone’s functionality. Most users of these gadgets use this without prior knowledge on what happens.
- Learning institutions are as well not left behind as far as these challenges are concerned. The technological zeal that the teachers and students have for BYOD is ahead of the technology the schools can handle. By having BYOD, common sense dictates that institutions to prevent slowing down networks, they will have to increase their bandwidth due to research and other

related uses, which is extremely expensive. I can also see security being an issue, and new policies would have to be written in place to prevent the mistreatment.

- Bring Your Own App is also becoming very phenomenal in today's working environments where employees will try to employ the use of some of the most convenient ways to have their work done. Employees are not just bringing their own devices to work; they are also finding their own applications to get the job done. Ovum has seen that this BYOA activity is widespread around third-party cloud productivity applications (e.g. file sync & share, VoIP, enterprise social networking) though our multimarket employee BYOD survey. For example, over 22% of employees are self-provisioning file sync and share tools such as DropBox or Google Docs to share corporate documents between their different screens or work groups. And 31% are using a self-provisioned VoIP application to communicate with their colleagues, predominantly Skype. (Absalom, 2014)
- Bandwidth and Productivity Drains as many employees have found that mobile devices often do not have the same strict policy enforcement capabilities as desktop devices. This policy gap enables many employees to use their mobile devices to access video streaming and other applications that are denied by standard corporate policy. With mobile devices offering a way to bypass the limits normally imposed on these applications and behaviors, users are putting a strain on the corporate network bandwidth as well as being less productive. (FORTINET, 2015)
- Data and Device Loss: Millions of cell phones and smartphones are lost or stolen every year. It is thought that approximately 22% of the total number of mobile devices produced will be lost or stolen during their lifetime, and over 50% of these will never be recovered. Most devices are stolen for the value of the hardware on the second-hand market; however, a growing amount of lost and stolen phones have their content accessed by someone other than their owners. With devices operating outside the confines of the traditional brick and mortar enterprise, the potential for data loss increases significantly. The threats to mobile users include the risk of malware infection, inadvertent or malicious sharing of critical business data or even the devices being lost or stolen. Additionally, rogue wireless networks exist in the public with the sole purpose of stealing unprotected data. This highlights the importance of basic security features such as password protection, encryption and robust procedures to wipe the device once lost.
- Lack of user security awareness is the other primary contributor to several of the above risks being realized in the organization. Maintaining awareness and good support procedures for handling device loss is critical to the security of the data on the devices. The risk of the device itself should be assessed as a part of the company's risk assessment framework. In some organizations tiered device architecture may be viable to deal with varying degrees of risks tied to job functions. For instance, devices that are being used to present sensitive financial data to the board through a custom app will invariably be more sensitive to theft or accidental loss than a mobile device with access to calendar and email updates.

IV. Current Strategies Used in Mitigating BYOD Threats

Due to the magnitude of the threats posed by the use of these devices in organizations, various ICT departments have invented means and ways of taming this known yet very complex issue of data leakage via BYOD. While some draconian approaches (such as denying all personal devices on the corporate network) might be warranted for extremely secure organizations, most organizations want to adopt a BYOD policy that offers some flexibility for users while enforcing corporate policies and adopting best practices. As this problem varies from one organization to the other, the solutions vary as well. Some of these strategies include but not limited to:

- Implementation of policies aimed at regulating the use of these mobile devices more so in the work place. According to (Evans, 2015), the advent of BYOD is forcing IT departments and IT managers to develop and implement policies that govern the management of unsupported devices. Network security is paramount. Beyond pass code-protecting employee devices, these policies might involve encrypting sensitive data, preventing local storage of corporate documents and/or limiting corporate access to non-sensitive areas.
  - Various organizations have put in place massive technical controls aimed at mitigating the insider cyber security threats been posed as a result of emerging trends in this BYOD digital era. Technical controls can vary from network-based to device-based and no single solution is appropriate for all organizations. Some of the most common technical controls associated with enforcing BYOD policies include but not limited to:
  - Virtual Desktop Infrastructure (VDI): Server-based VDI is the creation of a user's desktop environment, from operating system through applications, in a virtual machine (VM), run on a hypervisor and hosted in a centralized server. The hosting server simultaneously supports multiple virtual desktops, with the number of virtual desktops supported limited by several factors, most notably the configurations of the desktops and the computing capacity of the server. The virtual machine instances that contain the virtual desktops are established and torn down based on business requirements— an on-demand attribute. Also, based on business requirements and rules, virtual machines can move from one physical server to another. Allowing mobile devices to access VDI gives organizations the ability to leverage their existing investment in VDI and provides a secure window into the corporate network. VDI does not allow for cross-pollination of data between the user's personal device and the corporate infrastructure. VDI helps alleviate policy enforcement concerns because the

enforcement still occurs on the corporate network.

- Mobile Device Management (MDM): MDM has become synonymous with mobile security. However, MDM is not a complete solution to BYOD challenges as it does not provide a complete security solution—most MDM and endpoint clients are designed to address many challenges that are not security related such as:
  - Software Distribution
  - Policy Management
  - Inventory Management and
  - Service Management

MDM does provide an expanded level of policy enforcement that is not enabled by default. MDM allows policy enforcement on the mobile device itself and many solutions offer remote location/lock/wiping capabilities to protect against loss or theft. However, MDM solutions enforce different policies based on the mobile device they are supporting resulting in inconsistent security coverage. The other major challenge with MDM solutions is that it requires that employees give up control of their devices in order to access corporate applications. However, there have been cases where personal information has been wiped from devices after employees left the company or simply because an IT professional made a mistake. This will definitely lead to a disgruntled employee who will spend most of the working hours trying to restore his PDA's content. (Absalom, 2014)

According to Jeffrey Hunker and Christian W. Probst, it is unclear how effective various prevention, detection, and response techniques are in reducing the insider threat – and therefore in reducing risk. For instance we lack any clear data to say how effective different security policies are depending on the motivation of the insider. It may be that this does not matter; anecdotally it appears that sometimes it is hard to distinguish the execution and consequences of malicious acts from those due to accidents or na¨ıvet´e. On the other hand it may matter a great deal. Insiders may legitimately use domains in unexpected ways that might trigger false alarms.

Outsiders acting with illegitimately acquired credentials, insiders acting with malicious intent, insiders acting without malicious intent, and accidental behavior are all insider threats, and yet it remains unclear how effective various security policies are against acts stemming from different motives. (Jeffrey Hunker, 2008)

V. THE WAY FORWARD

Even though the currently ICT personnel cannot report with authority that they can address the challenges brought about by the emerging issues in organizations, there is need to come up with almost long lasting solutions that can be used to fully arrest this situation or basically minimize them. As BYOD introduces risk to the organization, a holistic and methodical approach should be used to define this risk and help to ensure that controls exist to maintain both the security and usability of the devices in the enterprise. (Young, 2013). This is why we have devised an algorithm and near real time framework for mitigating this vice as well as maximizing on the use of these State of the Art gadgets.

At the rate at which innovations and implementation of new and powerful tools is taking place, one sided approach will leave more problems than solutions and there is need to embrace the use of BYOD user policies. There is need as well for creating a secure mobile environment and other technical solutions which should be put in place to enforce policy.

VI. WHY USE ELLIPTIC?

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.

A. 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.

1) RSA

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

Table 2: Equivalent key size recommended by NIST
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.

B. 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

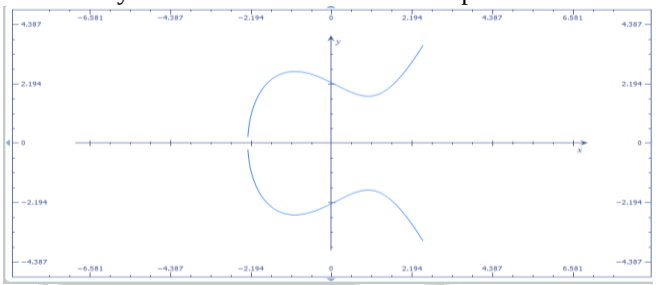
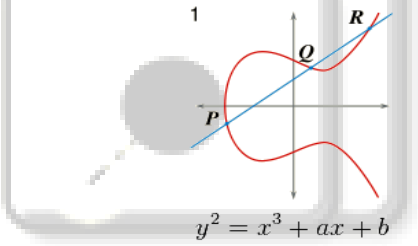


Fig. 2: Parts of the curve



This 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.enP) 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

1) Solution 1

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

2) Solution 2

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

3) Solution 3

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

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.

C. Characteristics of the curve

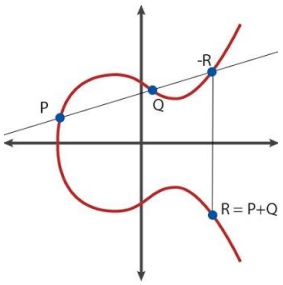


Fig. 3: Diagram 1

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.

D. 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;

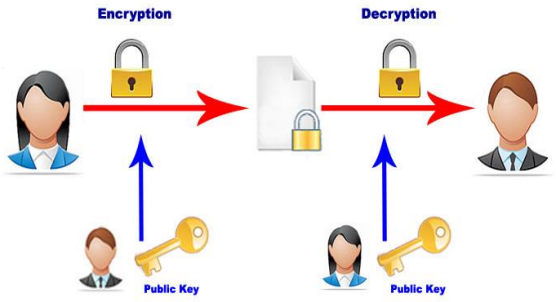


Fig. 4: Diagram 2

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.

1) 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)
2) Jane picks a private key `nA` and computes her public key `Qa = nA.G`
3) Jane encrypts the message `D = M + na.Qb` (D = cipher text) and sends `(Qa, D)` to Charles
4) C1 will be send to Charles.
5) To decrypt the message, Charles computes `M = D + (-nb).Qa` and he recovers `M`

1) Proof

How do we get back the message?

1) M = C2 – d * C1
2) 'M' can be represented as 'C2 – d * C1'
3) C2 – d * C1 = (M + a* Q) – d * (a* P) (C2 = M + a * Q and C1 = a* P)
4) = M + a * d * P – d *a *P (canceling out a * d * P)
5) = M (OriginalMessage)

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.

VII. Conclusion and Future Work Directions

BYOD policies can increase productivity for employees, enabling them to do more business both within/outside the office. The challenge for organizations is to continue to provide the same level of security regardless of the device or location of the employee.

The BYOD trend is here to stay and businesses will struggle to keep up with the rapid adoption of PDAs. With averagely more than three million portable devices being activated each and every day, it's impossible to argue otherwise. However, the boost in productivity this mobility brings is offset by an outbreak of new security risks.

In this paper, we explain the basics of insider cyber security with its characteristics and various deployment model of BYOD and its major challenges and why it is extremely important for organizations to tame this approach before it blows out of proportion. We reviewed the BYOD approach in organizations and why it should be controlled and encouraged in equal measure. To attain our goal, we have developed an ECC based algorithm for the data security in organizations. This mitigation approach extends access and enforces strong authentication in the use of the PDAs at any given time. Even though we can apply any encryption or authentication method for data security, for better performance with smaller size of data, elliptical curve cryptography method is the most amicable approach compared to other approaches. We have also tried to provide a client side tool using ECC based algorithm form small device because it is more beneficial for smaller device compared to large device as it consumes less power compare to other conventional algorithm.

After examining the security, implementation and performance of ECC applications on various mobile devices, we can conclude that ECC is the most suitable PKC scheme for use in the dynamic BYOD environment. Its efficiency and security makes it an ideal alternative to conventional cryptosystems, like RSA and DSA, not just in constrained devices, but also on powerful computers.

Future work can contribute to the understanding and advancement on data security based on integrity, authentication, and accountability not forgetting an increased performance rate from the insiders in any result oriented organization. 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 policies.

In the future we will try to incorporate mechanisms on how we can mitigate the threat caused by the use both audio and video recording devices due to the challenges they pose to businesses data security. Ravi Gharshi and Suresha believe that ECC makes it an ideal choice for portable, mobile and low power applications and their integration with cloud services but they do not clearly indicate what really happens on data that is locally stored. (Ravi Gharshi, 2013). Other than security on the cloud systems and the locally stored data, it is our sincere dream that we 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.

References

[1] Absalom, R. (2014). The case for supporting. Ovum_Research_Report_Bomgar_Final , 9-10.
[2] Adrian Drury, P. L. (2013). BYOD: an emerging market trend in more ways than one. Ovum , 3.
[3] B.P.I.T., R. (2013). SECURITY ARCHITECTURE OF CLOUD COMPUTING BASED ON. International Journal of Advances in Engineering Sciences , 1.
[4] Evans, D. (2015, October 07). The opportunities and risks of people using their own devices at work. TechRadar, The home of Technology , pp. 1-2.
[5] FORTINET. (2015). Enabling Secure BYOD. FORTINET – Enabling Secure BYOD , 5-8.
[6] Fulton, K. (2013). Ovum survey finds BYOD on the rise. Techradarpro, IT INSIGHTS FOR BUSINESS.
[7] Jeffrey Hunker, C. W. (2008). Insiders and Insider Threats, An Overview of Definitions and Mitigation Techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications , 8.
[8] Kaneshige, T. (2014, 2 6). Secret Video and Audio Recordings a Legal Minefield for Employers. Retrieved 09 05, 2015, from CIO: http://www.cio.com/article/2378933/byod/secret-video-and-audio-recordings-a-legal-minefield-for-employers.html
[9] Mr. Pragnesh G. Patel, S. (2013). Data Security in Cloud Computing using Elliptical. International Research Journal of Computer Science Engineering and Applications , 5.
[10] Ravi Gharshi, S. (2013). Enhancing Security in Cloud Storage using ECC. International Journal of Science

and Research (IJSR), India Online ISSN: 2319-7064 , 59.

[11] Sverdlove, H. (2012, 12 08). Why Every IT Department Should Have a BYOD Policy. Retrieved 06 07, 2015, from ITProPortal: http://www.itproportal.com/2012/12/08/why-every-it-department-should-have-byod-policy

[12] Young, E. &. (2013). Bring your own device, Security and Risk Considerations for your Mobile device Program. Insights on Governance, Risks and Compliance, 5-6.

