Data and Endpoint Security in Mobile Computing

Sait Murat GİRAY

***Abstract*—Nowadays laptops, tablets and smartphones have capabilities and abilities once have only been dreamed. Mobile platforms and mobile computing became an inseparable part of daily and professional life. Their widespread use is motivated by the flexibility and productivity they provide as well as rich options of accessing and processing content with them. This new trend and different form factors also present several security risks for the devices and data stored in and/or accessed via them. Data and endpoint security is particularly challenging in corporate world. Current study discusses data on mobile endpoints and provides a comparison of security mechanisms on the basis of convenience, security efficiency and deployment cost against several threats to provide a baseline for mobile network use and deployments.**

***Index Terms*—Cost, Convenience, Efficiency, Endpoints and data security**

I. INTRODUCTION

MOBILE computing includes all portable computing/communication devices with wired/wireless connectivity. Recent hardware and software advances lead to versatile devices and a productive environment. Communication and computation habits have been transformed and became user location oriented. Mobility is very attractive for both casual users and corporate world because of the flexibility and efficiency in data use along with social and business services. However several issues and constraints [1] based on the characteristics of mobility are introduced in several studies such as are performance, connection variability and short battery life. Major mobility challenges [2,3] are disconnection handling, low bandwidth in wireless connections, network heterogeneity and limited user interaction. When a technology becomes popular it attracts both users and malicious parties. Therefore security of user, device and data became a major concern.

Today mobile devices are able to store and process large amounts of data but they are mostly exposed since it is easy to lose or steal them. As a result, unauthorized access to device, data and private networks is very likely if necessary precautions are not taken. One of the best security practices would be removing unnecessary and sensitive information from mobile devices unless proper and explicit permissions are granted for it within organization. Mobile endpoints can easily become a security liability if they are not properly managed. The value of a mobile device stems from the data stored in it and installed applications that enable dedicated services through it. Thus security outshines other challenges considering the proliferation of mobile devices in individual and business use. Mobile devices and data are essentially prone to security risks based on mobility and usage patterns. Typical security concerns of traditional stationary systems such as authentication, authorization, confidentiality, privacy and integrity are also valid in mobile endpoints with resource constraints, battery and connectivity [4, 5] issues.

Threat models are mainly loss, theft or physical damage, unauthorized use, malware vulnerabilities and data leak through eavesdropping or sniffing. Backup, password protection, encryption, authentication, remote management, trusted computing approaches and physical precautions are major countermeasures for end user devices. A combination of them at different levels is required for overall security. Focus of this study is corporate users considering more attractive data on their mobile devices. Awareness and employee training are also a part of security. Reference [6] describes this aspect as "the stage of prescriptiveness, i.e. that users should be intrinsically committed to the security objectives of the organization". Proper security policy management and continuous training will realize this capability.

This paper provides a comparison and an evaluation of security mechanisms for mobile endpoints and data based on convenience, cost and security efficiency from the perspective of a decision authority who would answer the following questions:

-Is it easy for users to adopt the security system?

-Do the solutions provide sufficient security?

-Do the value of data and device justify the incurred costs?

Section 2 describes mobile computing environment while Section 3 details challenges and issues of mobility. Security management challenges are handled in Section 4 and the reasoning for comparison criteria with evaluation of techniques are presented in Section 5 while Section 6 includes the final remarks and the conclusion.

II. MOBILE COMPUTING ENVIRONMENT

All kinds of mobile communication /computation devices and portable data storage are considered in this context. Mobile computing provides almost uninterrupted processing of data and it is more utilized every day because of novel and productive communication, data/service access, processing and storage means. Reference [7] shows a global

Sait Murat Giray is with Turkish Naval Forces Command and Middle East Technical University Computer Engineering Department, Ankara (email: giray.s1778@dzkk.tsk.tr or giray.murat@metu.edu.tr)

surge in smartphone usage. In particular, companies heavily use mobility to keep up with market pace. This fact also reminds us that mobile devices store very precious user and employee data [8] as shown in Fig.1.

Mobility did not yet reach to Weiser's "Ubiquitous computing" concept of full-fledged integration and interaction of information technology (IT) devices and humans [9]. However, current era has several examples of ubiquity such as Google Glass Project [10]. Nowadays it is common to instruct mobile devices with voice command to perform tasks like web searching, making calls and navigating. Schools are equipped with interactive boards, public and private sectors digitize and mobilize their services. Different transactions take place over dozens of mobile applications. Order management, delivery tracking, mobile payment [11], e-mail exchange, marketing, advertising, banking and customer relationship management (CRM) [12] are some examples of what mobility can achieve The list of what we can with mobile services introduces various restrictions and threats in mobile environment.

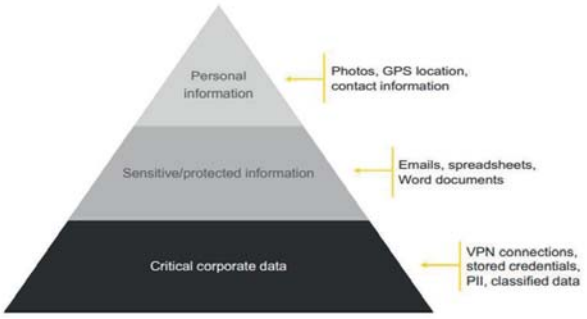

Fig. 1. Mobile devices in corporate environment contain very sensitive data.

III. CONSTRAINTS IN MOBILE COMPUTING

Nowadays smaller, thinner and more powerful devices are at premium. All the efforts in progress serve to eliminate the limitations and obviate inherent challenges of mobile equipment which cause security concerns.

A. Insufficient Resources

Although contemporary mobile devices reached a standard of 2 GHz plus multi-core processor units, tens/hundreds gigabytes of storage along with several gigabytes of memory, they are still considered as resource poor due to size, weight and power consumption limitations [1] which would thwart utilization of a strong security mechanism on the device.

B. Network Heterogeneity

Mobile devices support different communication protocols (Bluetooth, Wireless Fidelity (Wi-Fi), 3G/4G and etc.) and they can rapidly face connection changes. Those shifts may occur within same or different overlapping networks. A marketing agent can talk with a customer on the phone while downloading files simultaneously over a public Wi-Fi with the same device. If it is configured automatically switching to faster/known networks then this endpoint may be exposed to threats in an uncontrolled environment.

C. Connection Fluctuations and Bandwidth Restrictions

Distance to base stations or hotspots and surroundings heavily affect signal quality. Indoors hampers strong signal reception while outdoors puts the device away from the wireless router. Low speeds and connectivity variation may also lead to security threats. An employee may prefer a fast but insecure public Wi-Fi internet rather than intermittent 3G service to send some data. In this scheme, it is apparently easier to interfere with the traffic or impersonate an access point. Therefore employee is more vulnerable to network attacks such as phishing [13] and spoofing [14].

D. Limited User Interaction

User-device interaction is still restrictive on mobile devices mainly because of small sizes and lack of physical input (keyboard, mouse etc.) even though several enhancements such as sliding keypads, touch screens, high resolution displays, voice recognition and customizable user interfaces are introduced. Lack of fast and responsive user interfaces can cause security breaches by making users ignore protections like screen locks.

E. Reliance on External Power

Usability, performance and computation duration of mobile devices depend on battery. Although battery life times are substantially enhanced, they are still in the order of hours and they are heavily affected by usage pattern. For example Wi-Fi is a dominant factor in battery consumption as stressed in CoolSpots study [15] and 3G/4G networks also drain the battery rapidly. Since one cannot always control the environment that he/she plugs in the mobile device, frequent recharges would yield physical threats to device.

IV. SECURITY MANAGEMENT

Since mobile devices became pervasive and affordable, companies hand them out to almost each of their employees. In current market conditions, mobility became a high value asset and a resort to reduce delays and to accelerate service delivery. Neither personnel nor data are any more office bound. Widespread use of mobility is exceeding the organizational boundaries and spanning into ad hoc context which brings a lot of security risks and management problems.

Think about e-mails and financial figures on a smartphone, details of a new state of the art engine in a laptop or a heedless user who saves login credentials of company Virtual Private Network (VPN) client for convenience. In these situations, possession of the device (locally or remotely) directly refers access to private network and/or sensitive data. Necessity of tight security originates from high exposure to different environments. Appropriate management of devices requires clearly specified boundaries between hierarchical levels. A distinctive classification of personnel on an authority and responsibility scale is assumed to exist throughout this study. Otherwise it would be hardly possible to distinguish security exigencies of devices and data at different levels.

A. Threat Model and Countermeasures

Consider an employee who is working at home with a laptop connected to corporate systems. Some data residing only at a company server are required for a report and employee downloads those data to speed up the work. This employee has also a plane to catch so he/she keeps on working at the cab by sharing 3G connection over the smartphone. The report has been completed before getting onboard and it was sent to colleagues over public Wi-Fi as it is faster. Employee used different networks either with some degree of control or none. Considering this scheme, several measures should be utilized for security of the devices and data. Raw data has been processed and became a valuable asset on the go while device was a free pass to the corporate systems. Security of mobile wireless carriers is beyond the scope of this paper.

Major security risks can be classified as physical threats (robbery, loss, damage and unattended use) and cyber threats (unauthorized disclosure or remote access through malware). Since smartphones allow third party applications, malware risk is now valid for them. Countermeasures have a similar categorization too. Physical protection measures consist of being a prudent user, carrying or keeping devices in locked areas and fastening them with cable locks if possible. Mechanisms of cyber domain include encryption, authentication, backup, remote wipe and feature killing, device tracking, anti-malware, system patches and firmware updates.

B. Security Mechanisms

1) Authentication:

It is the process of verifying user identity before granting access to device, data and services. Reference [16] presents a clear classification of authentication by coining the terms "knowledge, possession and property".

a) Single Phase Authentication:

Passwords are the simplest- also cheapest- form of identity confirmation and the most basic component of authentication. Presumably all mobile devices have this function. Password protection may vary among platforms and mobile operating systems but alphanumeric phrases, numerical codes and pattern drawings are commonly used. In addition, visual confirmation with predetermined pictures and prerecorded question-answer pairs are available. Several combinations can be applied to meet the required level of security. A four digit code may suffice to hold some curious friends away from the phone while a banking application deservedly requires a customer ID, a passkey and then combine them with preselected images and location/IP address information.

b) Multi-Phase Authentication:

Passwords can be compromised by guessing, brute force search or over–the–shoulder pries. Multi-phase approach requires possession of a specialized hardware or software as an extra step. USB tokens and credit cards are common examples of physical cards while one time pass code generator applications provide software aided multi-phase authentication. One major disadvantage of them is the very same risks of being forgotten, stolen or lost.

c) Biometrics:

Biometric authentication use unique physical feature such as fingerprint, eye (iris, retina) and voice to verify identity. This concept is explained in four steps as capturing sample, extracting unique data, comparing templates and determining matches and no matches in [17]. It provides top level security and they are generally preferred by high profile organizations like law enforcement, government offices, military services and large industrial enterprises. Biometrics is also used in mobile devices as built-in fingerprint readers or facial recognition software using integrated camera.

2) Encryption:

This procedure converts clear text into unintelligible format which requires a decryption key to reverse the process. It is one of the core pillars of the security. Considering high value data accessed, stored, processed and transmitted on the mobile devices; encryption is crucial for companies and individuals. British government's loss of two password-protected but unencrypted computer disks [18] which include personal records of 25 million individuals is a good example about how correct implementation of a measure is a sharp edge. Encryption can be applied at two levels with respect to location where data rest. First level is full disk encryption (FDE) [19] and the other is file system level encryption (FSLE) [20]. FDE encrypts entire storage of the device and it requires correct user credentials to authorize access [21]. FDE can be implemented in software or hardware. Latter one has a separate encryption processor. In FSLE, files and directories are encrypted instead of the entire disk. Both are the last line of defense if device falls into hands of illegitimate users.

3) Remote Management:

A remote administration can protect the devices and data in case of a loss or theft is by remote data removal and/or feature lockdown. Those features are Bluetooth, Wi-Fi, infrared, camera, microphone, USB or memory card mount, synchronization, messages and e-mail [22].

4) Trusted Computing:

In trusted computing concept, devices always perform as expected and this is it is enforced both by hardware (Trusted Platform Module-TPM) and encryption software. Use of mobile IT entities such as mobile payment, ticketing, portable gaming, multimedia and cloud computing is increasing [23]. They include sensitive data so needs protection. Customer and fiscal data in mobile payment or digital rights management (DRM) in content streaming to the authorized mobile players are a few examples. Trusted Computing Group (TCG) defined Mobile Trusted Module (MTM) [24] to provide a specification of encryption/decryption, signature generation and sensitive data storage to deliver functions such as secure boot, data integrity, device authentication and remote attestation.

5) Security Awareness:

Human instincts drive individuals disregarding tools unless one believes it is useful and bypass rules even if they

are deduced from unquestionable facts but they do not make any sense at the very moment. Extensive security policy training is not only a solid requirement to create awareness but also it is a lucrative investment on the employees. It should teach or remind what type of data they need to carry or not; how and why they secure their devices properly; appropriate reactions against incidents; possible consequences of security breaches and finally their responsibilities. Reference [25] highlights that "learning is a continuum; it starts with awareness, builds to training, and evolves into education". The cost of these trainings proves its worth in the form of reduced number of security breaches and decreased damage. Technical and social elements of security awareness include putting a label onto device with identifiable information, updating the operating system and installed applications regularly, using only official manufacturer firmware and application markets as software sources, avoiding processes like "rooting" or "jailbreaking" the device and using remote device finder services.

V. SECURITY ASSESSMENTS

A. Assessment Criteria Reasoning

Main assessment criteria are convenience, cost and security efficiency. Convenience outweighs others while choosing and implementing a security system in author's perception which is a decision made upon human nature. An advanced but not user friendly security system is likely to be ignored or improperly used by employees. Most of them will prefer being "insecure" instead of using this intricate system. Cost and security efficiency do not matter if/when users do not adopt this solution. Instructing users about strong passwords is much cheaper and convenient than carrying a code generator. Training employees makes this trade-off more manageable in.

Cost is the most crucial one from a business owner's perspective and it is in the same level with security efficiency within this study. A cheap but efficient system may deliver better solutions than an expensive system but it is not the case in real life as you get what you pay for and real cyber security is not cheap. The challenge is justifying incurred costs and showing expensive one is actually more cost effective in the long run. In the end, cost of a security mechanism must match the desired security efficiency within the budget.

B. Convenience

Convenience observes adoptability and acceptance by users. Key consideration is the extent of an applied mobile security mechanism which influences user preferences since it would inevitably introduce some inconvenience while safeguarding.

Password protection is practical and successful when it is properly used but this assumption does not always hold. Employees generally choose simple combinations to facilitate recollection, note down enforced sophisticated passcodes or renew them with a similar one. Eventually ease of use becomes a short circuit in the security mechanism. Two–phase authentication is also integrated into daily life. However, carrying an extra key card is not that much convenient and the card itself is subject to very similar risks of any other mobile device.

Biometrics has an edge over others because of organic integrity. Users do not need to remember surreptitious codes or plug in extra hardware. Fingerprint recognition particularly has an increasing popularity as reported in [26]. Privacy is an unsolved issue for biometrics as it requires recording unique individual features and employees may resist using it daily. Acceptance and legal matters regarding to privacy in biometric authentication are highlighted in [27].

FDE performs transparently as long as mobile device has sufficient resources to support full storage encryption and handle extra I/O. FSLE depends on either system wide policy stipulations or individual data significance perception. It may also require more complex key management [28]. FDE saves users from such intervention but FSLE provides more flexibility and granular control on the data while encrypting.

Trusted computing is criticized in several ways such as privacy, loss of anonymity, inability of device owner to fully control the device, remote validation abuse and manipulating users' choice of software [29,30]. These restrictions would be acceptable in a company environment since IT departments aim to ensure overall security for the registered devices. MTM and TPM do a good job in servicing these needs at a rational enterprise level but they may cause inconvenience too.

C. Efficiency

In security efficiency, main concern is whether the applied system provides sufficient security or not. This measurement requires a classification of devices and data. A password may prevent others using a smartphone but it is not enough to secure unencrypted e-mail attachments. An efficient mechanism prevents breaches before they occur instead of plugging holes later. Ineffective one inflicts costs with frequent replacements, confidence loss and reputation damage.

Simplicity of password protection brings several shortcomings and supported length or character variety is very important. Security of single phase falls behind because of the tendency of choosing easy to remember (so guess) codes or keeping default passwords [31]. Multi-phase authentication provides considerably more security with extra steps. Two key factors generally use one-time valid code and they carry a time synchronization property [17]. Since smart cards or tokens might be stolen or misplaced, this extra step in security has a potential of turning into total disability of using system as well.

Biometrics eclipses previous techniques in performance since it utilizes absolute metrics which are almost impossible to forge or reproduce. Two main factors should be taken into account on the accuracy and efficiency of biometrics. They are "False Rejection Ratio (FRR)" and "False Acceptance Ratio (FAR)". Former one indicates the number of valid users to whom access is denied while the latter one gives the number of illegitimate users who obtain access [17].

FDE overpowers FSLE in terms of security efficiency because it ensures that no unencrypted data will be written

[21]. Critical data may exist or be copied in multiple locations and FDE eliminates data selection at user's discretion. In FSLE, plaintext data can be discovered in page or temp files with keyword search even after encryption. Vulnerability of FDE against cold boot attacks [32] should be kept in mind and it cannot secure data if a careless employee leaves device unsupervised while a session is open. In terms of efficacy, TPM delivers better protection with hardware and software control while making devices more tamper-resistance but it is not perfect either [33].

D. Cost

Security cost mainly comprises of three elements; initial deployment, training and maintenance (updates/renewals). When selecting a solution, time and fiscal issues must be considered. Value of data/device should justify the incurred costs and it should not outweigh the benefits. It does not make sense to protect a regular smartphone with biometrics while depriving of a hardware security from a laptop which is storing very sensitive government data. Expenses are proportional with desired security.

Passwords are considered free since presumably all mobile operating systems have them. Its cost is covered at the initial procurement. Password management has an IT labor cost since it would erode IT staffs' work hours with frequent password resets. Multi-phase authentication has three components and it is more expensive. First one is the special hardware/software, second item is the hardware reader and the last one is the software which manages identities and keys. There are several factors which cover the cost of biometric security such as hardware, recognition software and employee training as emphasized in [34]. As a result, such deployments should be based on a need basis. Biometrics is also beneficial in saving security management expenses by reducing help desk requests.

Cost evaluation of FDE and FSLE would be performed for worst case scenarios in which the device is lost or stolen. FDE has more overhead and more deployment cost per unit but it delivers better protection for unauthorized data disclosure. TPM and MTM are gaining popularity and major manufacturers are embedding them into their solutions. In most cases, no extra costs are incurred for them unless a specific application of trusted computing is required. In terms of cost, loss of customer trust and reputation upon a breach cause much more than a good initial protection mechanism.

VI. CONCLUSION

Proper implementation and deployment of security methods are vital for avoiding data loss or leaks from a mobile device. Author of this paper evaluated the security measures that provide end–user device and data security by performing comparisons based on convenience, security efficiency and cost. This triplet delivers a strong basis in order to map an extensive organizational ramification of required security at the right level. Challenges about measures are determined upon whether they are easy to adopt or lead to ignorance; whether they provide enough security or result in breaches and whether cost of the applied solution is justified or not. Advantages and disadvantages of mobile operating systems are provided in Appendix. Biometrics and FDE are the strongest but most expensive mechanisms which verifies the notion of "you get what you pay for" in security. It is also concluded that single or multi-phase solutions are sufficient for most of the mobile devices when a meaningful hierarchy is established but biometrics is required if devices store mission critical data. In addition to that, FDE should be preferred over FLSE when mobile devices can run stable without hampering productivity. Use of TPM and MTM provides better protection in overall device security with respect to software modification, authorized use of device and data alterations. Remote administration tools should be considered and their integration with business solutions provides very strong control on mobile devices, data and services. Since humans are the weakest ring in the security chain, their training has great importance in end device and data security.

APPENDIX

Following tables provide insights about the security features of popular mobile operating systems [35].

TABLE I
MOBILE OPERATING SYSTEM COMPARISON-ADVANTAGES

Operating System	Advantages
BlackBerry	Proprietary encryption Enterprise-level features allow setting security policies Secure application installation methods
iOS	Strong device and application security framework Remote GPS location and wipe App Store heavily vetted Data encryption, policies, secure VPN and Wi-Fi
Windows Phone 7	Sandbox with isolated application runtime and storage architecture Central policy management for passwords, remote wipe All apps installed from Windows phone marketplace Mobile IE ensures no malicious code launch from a website
Symbian	SMS remote lock Secure Exchange ActiveSync support
Android	Secure sandbox approach apps Native encryption Remote security management APIs Remote GPS and wipe Openness fosters innovative security products

TABLE II
MOBILE OPERATING SYSTEM COMPARISON-DISADVANTAGES

Operating System	Advantages
BlackBerry	Not many alternative devices supported Business base an attractive target for hackers
iOS	Can't lock mobile device management profiles to prevent end-user opting out Jailbroken devices are a risk Wildly popular platform makes malware more worthwhile
Windows Phone 7	Security policies and management not on par with Windows Mobile Not really new, same concerns as old architecture
Symbian	Dying platform casts shadow over security investment
Android	No way to stop users from opting out of management profiles Too open in terms of application market

TABLE III
MOBILE OPERATING SYSTEM COMPARISON-DECISION

Operating System	Decision for Security
BlackBerry	Very good candidate for corporate world
iOS	Acceptable security for the audience
Windows Phone 7	Promising but requires more work
Symbian	Going to disappear but considered secure
Android	Application policies need discipline but security features are developing fast and rigorously.

REFERENCES

[1] M.Satyanarayanan,"Fundamental Challenges In Mobile Computing.", In Proceedings of the Fifteenth Annual ACM Symposium on Principles of Distributed Computing Philadelphia, Pennsylvania, United States, May 23 - 26, 1996). PODC '96. ACM, New York, NY, 1-7.

[2] G.H.Forman, and J. Zahorjan,"The Challenges of Mobile Computing.", Computer 27, 4 (Apr. 1994), 38-47.

[3] J. Landay,"User interface issues in mobile computing." In Proceedings of the Fourth Workshop on Workstation Operating Systems (WWOS-IV), 40-47. IEEE, October 1993.

[4] S. Ravi, A. Raghunathan, and N. Potlapally, "Securing Wireless Data: System Architecture Challenges",In Proceedings of the 15th International Symposium on System Synthesis (Kyoto, Japan, October 02 - 04, 2002). ISSS '02. ACM, New York, NY, 195-200.

[5] A.Jøsang and G.Sanderud."Security in mobile communications: challenges and opportunities.",In Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21, pp. 43-48. Australian Computer Society, Inc., 2003.

[6] M.T. Siponen,"Five Dimensions of Information Security Awareness." SIGCAS Comput. Soc. 31, 2 (Jun. 2001), 24-29.

[7] Germany, Ipsos MediaCT."Mobile Internet & Smartphone Adoption." Google Mobile Ads Blog, 2012.

[8] J.Y.Chee,"Security Issues In Mobile Computing",IT Governance Conference,2012

[9] M.Wieser," The computer for the 21st century". Scientific American 9,(1991), 933–940.

[10] D.Goldman,"Google unveils 'Project Glass' virtual-reality glasses". Money (CNN). 4 April 2012.

[11] Q.Li, X. Zhang, J.P.Seifert and H.Zhong,"Secure Mobile Payment via Trusted Computing", In Proceedings of the 2008 Third Asia-Pacific Trusted Infrastructure Technologies Conference(APTC '08),IEEE Computer Society, Washington, DC, USA, 98-112,2008.

[12] B.Holtz,"CRM for the Mobile Workforce – The Past, the Present, The Future", Customer Interaction Solution, Vol.22, No.5, pp.44-47, 2003.

[13] A.P.Felt, and D.Wagner. "Phishing on mobile devices." University of California, Berkeley (2011).

[14] J.Yang,Y.Chen and W.Trappe. "Detecting spoofing attacks in mobile wireless environments.",In Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on, pp. 1-9. IEEE, 2009.

[15] T. Pering, Y. Agarwal, R. Gupta, and R. Want, "CoolSpots: Reducing the Power Consumption of Wireless Mobile Devices with Multiple Radio Interfaces." In Proceedings of the 4th international Conference on Mobile Systems, Applications and Services (Uppsala, Sweden, June 19 - 22, 2006). MobiSys '06. ACM, New York, NY, 220-232.

[16] W.Jansen,"Authenticating Users on Handheld Devices", Proceedings of the Canadian Information Technology Security Symposium, May 2003.

[17] N.Boertien, E.Middelkoop,''Authentication in Mobile Applications'', CMG, Telematica Instituut, Netherlands, January 2002.

[18] Wikinews,"UK government loses personal information of 25 million people.",November 20, 2007. Available:http://en.wikinews.org/wiki/UK_government_loses_personal_information_of_25_million_people

[19] C. Fruhwirth."New Methods in Hard Disk Encryption". Technical report, Vienna University of Technology, June 2005.

[20] S.Ludwig and W.Kalfa."File system encryption with integrated user management". SIGOPS Oper. Syst. Rev. 35, 4 (October 2001), 88-93.

[21] PGP Corp. White Paper,"How Whole Disk Encryption Works", 2008.

[22] Microsoft White Paper, "A Technical Comparison of Mobile Management Solution Features and Functions", 2008.

[23] Trusted Computing Group, Mobile Phone Work Group. "Selected Use Case Analyses – v 1.0",2009

[24] TCG, "TCG MPWG Mobile Trusted Module Specification", version 1.0, Revision 7.02 29 April 2010.

[25] M.Wilson and J.Hash,"Building Information Technology Security Awareness and Training Program", National Institute of Standards and Technology, NIST Special Publication 800-50, Oct. 2003.

[26] Farpoint Group Technical Note, Document FPG 2008-435.1, "The Broad Reach of Biometrics:Fingerprint Recognition and Mobile Security", November 2008.

[27] T.Greene,"Biometric Security:Practical and Affordable", Global Information Assurance Certification Paper,17 January 2001.

[28] C.J.Kolodgy and G.Pintal, "Securing Laptops with Full Disk Encryption",IDC White Paper, February 2008.

[29] R.Anderson, "Cryptography and competition policy: issues with trusted computing". In Proceedings of the twenty-second annual symposium on Principles of distributed computing (PODC '03). ACM, New York, NY, USA, 3-10.

[30] S.Schoen,"Trusted computing: Promise and Risk.",Electronic Frontier Foundation Article (October 2003).

[31] W.Jansen, K. Scarfone,"Guidelines on Cell Phone and PDA Security", NIST Special Publication 800-124, 2008, page 3-3.

[32] J.Halderman, J. Alex, et al., "Lest we remember: cold-boot attacks on encryption keys." Communications of the ACM 52.5 (2009): 91-98.

[33] E.R.Sparks,et al.,"TPM reset attack.", Available: http://www.cs.dartmouth.edu/~pkilab/sparks/.

[34] D.Polemi,"Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication", Institute of Communication and Computer Systems, National Technical University of Athens, April 1997.

[35] D.Turney,"The Best Mobile OS:Security Showdown",ZDNET,23 May 2011.