Security of Mobile Phones and their Usage in Business

Abdullah Saleh Alqahtani
School of Computer Science, Engineering and Mathematics,
Faculty of Science and Engineering, Flinders University,
Adelaide SA 5001, Australia

***Abstract*—The purpose of this document is to provide an overview on the growth on mobile phone and PDA devices and use in business-oriented modern day life style. The explosion of smartphones in enterprise and personal computing heighten the concerns of security and privacy of users. Now a day's use of mobile is in every walk of life like shopping, trading, paying bill and even using internet banking. But with these facilities some draw backs are also there. Recent studies have shown that applications can host new types of malware. This discussion explores smartphone security through several research works and how user himself can avoid from data hacking and other insecurities.**

Keywords—Smartphone; PDA; security; business-oriented; applications

I. Introduction

The main intention of this manuscript is to give an impression on the growth of mobile phone and PDA devices, which are now indispensable for our business-oriented modern day lifestyle. This document also put emphasis on those technology risks that are associated with using these devices as well as available safeguards to diminish any problems. This information will help organizations to improve their levels of security and to decrease such occurrences concerning the use of these handheld wireless devices. It can be envisioned that the more mobile devices continue to accelerate, the more sophisticated applications can be predicted. [9] Internet connectivity has helped accelerate the tendency of mobile phones from 'voice-centric to data-centric' networking systems. These two worlds are gradually converging to support each other. [7]

Since security concerns have supreme importance in fiscal transactions or a mobile payment, that's why it is important that the attacker present in this application are examined by taking a holistic view of the vulnerabilities. [6] The increasing demand and functionalities of the hi-definition Smartphone category of mobile devices will make an attractive target for malware writers and infiltration of malware on mobile devices can raise serious business and safety concerns. [13] Moreover, Not sufficient security in wireless connection may tempt to numerous unlawful attackers including but not limited to hacking, fraud of system integrity, surveillance and loss or stealing of the device itself [14] In contrast, the security of handheld devices cannot be maintained without users' involvement. Users must be instructed about what measures to follow and what precautions to take while they use organization-issued equipment or a personally owned one. When taking full advantage of all the facilities afforded by cell phones or PDAs, it is important that the user should have a good knowledge of the security safeguards. [9]

On a related note the current economic environment and the advent of new technologies has interested organizations in availing the Cloud storage services provider model. Cloud storage providers can suggest cost-cutting measures by using equal storage capacity to meet organizations' needs to initiate transitional cost-savings measures for their customer base. [21] From 2010 on a majority of the cellular networks started undertaking switch-over from the existing third generation communications systems (3G) to the fourth generation systems (4G). This (4G) system mostly incorporates broadband IP-based heterogeneous multimedia services that let users use diverse networks on an anytime and anywhere basis. [22] The 4G system is a modified version of third generation mobiles and certainly is a 'must have' gadget for the organization. [18]

II. The Commonly Used Mobile Features

In today's high-tech business-oriented lifestyle cell (or mobile) phones and Personal Digital Assistants (PDAs) have turn into indispensable. For the most part these small and economical devices are being used for making calls, sending short text messages and supporting Enhanced Messaging Services (EMS). They can also be used for Personal Information Management (PIM), i.e. phonebook, calendar, and notepad, etc. These tiny devices can perform a whole array of functions that previously could only be done on desktop computers. Computers generally perform many functions such as sending and retrieving e-mails, web browsing, retrieving and modifying documents, delivering and making presentations, and can access available data from remote servers. Currently mobile device are now being equipped with built in devices like camera, GPS receiver, removable media card incision, and also are host to a vast assortment of wireless interfaces, including but not limited to, infrared, Wireless Fidelity (Wi-Fi), Bluetooth connectivity, and more than one type of cellular interfaces, etc. [9]

Research and advances in Information and Communication Technology (ICT) have resulted in today's high-end smart phones and Personal Digital Assistants (PDAs), which now possess fairly equal processing power and memory storage capacity that was previously the hallmark of Personal Computers (PCs). Today's smart phones converge with full-featured mobile phones in that they function much like

computers. Users can now make phone calls and run applications, besides accessing and stockpiling useable data communications from shared networks and the Internet. In the meantime the memory cards of cell phones are now approaching the maximum of 8 GB capacity, which aims to provide adequate space to stockpile business information. Since highly developed mobile phones have the capacity to connect to the Internet and access websites and also have e-mail and multimedia set-ups, mobile devices are increasingly more "data-centric" compared to when they were traditionally "voice-centric" networks. [13]

Mobile manufacturing companies are taking the initiative to install those potential mobile enabling applications on mobile podiums, for instance Symbian™, OS, Microsoft™ and Windows™. Owing to the improved capacity, induction of new applications, available service support on cellular as well as local-area networks along with Bluetooth connectivity, the business community has an ever-increasing demand for mobile devices. These full-featured devices are improving workers' output by giving them ready access to the information they require. Even though these devices can boost competence and productivity, they also possess some inherent threats to organizations. What if the classified corporate and private data goes astray or a device is stolen? The types of threats that appear in the shape of spam, malware infections, and hacking will be discussed in the proceeding chapters. [13]

A. An overview of device transformation

The evolution of mobile telephony can be traced back to the continuous socio-historical development of the landline phone industry. One major reason for the acceptance of telephones at the beginning of the 20th century was "security". However, with the emerging American economy "business concerns" became yet another good reason for acquiring a landline phone. From1910 onwards the social use of the telephone became another factor for acquiring a landline phone. It is pertinent to mention here that the main disparity between the social setting of the early days of both landline and mobile telephones was the fear of breach of confidentiality, resulting from neighbors trying to 'snoop in' on their next door neighbors' conversations or business rivals abusing switch boards, etc.

Gradually, handheld devices began to appear in different shapes and sizes. The first cell or mobile phones appeared in the United State of America in 1978, after AT&T Company carried out its test communications under the auspices of the Federal Communications Commission in Chicago, Newark and New Jersey simultaneously. The device then had the weight and size of a brick and was restricted to voice communications only. From then on phenomenal improvements have been made in the appearance and performance of handsets, and the infrastructural capacity of their networking. By and large the capacities of these devices may vary but at the heart of technology there are certain similarities as well. In 1993 Apple introduced its very first PDA, "the Newton". Battery powered and compact in size PDAs are intrinsically designed for mobility as they stockpile a user's data in the form of solid-state memory rather than putting it on a hard disk. Nevertheless, certain vulnerabilities are accredited to the use of PDAs as preserved data in unpredictable memory may be lost and/or erased if the device is re-organized for some reason. In many ways, PDAs are akin to handheld (PCs) and are not used for telephony. Mobile phones on the other hand, are much like PDAs apart from an important disparity in that they support more than one radio interface to cellular telecommunications networks. Moreover, mobile phones have a different legacy as well in that mobile services have *enabled "follow me anywhere/always on" telephony"*.

What makes cell phones different from the rest of the handheld devices is their ability to communicate through cellular networks. In cellular networks - as their name suggests - cells play a pivotal role in reprocessing radio frequencies in a restricted radio band by allowing more and more calls to happen. Taking an example from the U.S.A. where a diversity of digital cellular networks is thriving which pursues dissimilar and incompatible sets of standards, it is evident that virtually everyone in that country is now covered by a digital network of some kind. [18] Two leading digital cellular network operating in the U.S.A are Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSm). Common cellular network are Time Division Multiple Access (TDMA) and integrated Digital Enhanced Network (iDEN). iDEN use proprietary protocol while other follow standardized open protocols. Last but not least a digital version of the ingenious parallel standards as designed for cellular telephone service also subsists in the field and to date has been referred to as recognized as Digital Advanced Mobile Phone Service (D-AMPS). [9]

B. Some common trends in mobile devices

The omnipresent exploitation of mobile systems, extensive use of the Internet as well as the speedy development in wireless technologies [18] in recent years is the contributing factors that have improved the functions and characteristics of mobile handheld devices. In particular, cell phones have witnessed those features which were once only accessible in high-end smart phones and gradually introduced into more basic phones. For instance, LCD screens have progressed from the colorless display to grayscale and finally to high resolution colored display technologies along with built-in cameras which, some time ago, were considered a scarcity. Today, however, they are just as ordinary feature. In the same way text messages have converted to chat messages and then multimedia messages and more enhanced messages, i.e. EMS and now ending with e-mail. At present mobile devices are expected to develop into more complex, powerful, communicative functions at high-speed and having better processing capabilities and greater bandwidth, apart from having the facility of "always on" connection such as those existing on desktop computers. As a consequence of the said developments, cell phones are becoming more of a depository for a wide range of private and organizational data and the core is changing to packet data as opposed to voice data. [9].

With the advent of broadband interactive multimedia applications in wireless devices the plethora of new trends and functionalities has overwhelmed certain device features. A few have been discussed in the preceding paragraphs and this does not include simple icon-menu, touch-pad, and artificial-intelligence-based natural languages. The said devices and

communication systems have also developed especially designed software to curb any instances of encroachment, namely:

- Invasion detective system - detects intruders and takes defensive measures upon the information it has,
- Anti-virus software - restrains malicious codes and offers support for reliable servers and applications.
- Almost every individual device will perform as:
- personal organizer - alarms, clocks, calculators, time zones, flash lights, calendars, dictionaries, compasses, video and music player, pocket PCs with office-type applications (for example, Blackberry).
- Gauge meters - to measure temperature, air pressure, humidity, and heartbeat, etc.
- virtual keys - to secure ID cards, digital cash, tag-readers, remote control devices, pagers, locating sensitive devices, etc. [18]

In such devices there is still room for new applications by new invigorating platforms such as Android. Android is a relatively new and dynamic platform that possesses some of the most sophisticated phone applications and is theoretically in conflict with iPhone. Android is striving hard to launch as many operating systems as possible whilst iPhone intends to get the best users experience by imposing restrictions to its hardware and software standards. [19]

From 2010 a majority of the cellular networks started switching over from the existing third generation communications systems (3G) to the fourth generation systems (4G). This (4G) system mostly incorporates broadband IP-based multimedia services in diverse networks. 4G systems represent a modified version of third generation mobiles and certainly have an edge over them. Their basic objectives entail higher transmission rates, larger storage capacity, higher frequency and greater bandwidth, better coverage and conduit features, cheaper access costs, higher quality of service with lower system costs, and a single yet omnipresent, multi-functional and multi-band intelligent device that can handle a variety of contents. [18]

C. An insight into futuristic devices what technologies may prevail

As mobile devices accelerate in terms of services offered, the more sophisticated applications can be predicted. For instance, like "Google Earth", today the Global Satellite Positioning (GPS) system has enabled wireless devices to run applications for designing software that can provide a full socio-historical account of an image or video of any building besides indicating its geographical location. Software can even detect whether an apartment house on a boulevard is for rent or sale, or whether it is mortgaged and even who owns it. If a picture has some text the enabling technologies of these devices can translate it into English. These devices have supermarket applications and can scan products' barcodes; iPhone has the same applications. [9]

In Europe drink and potato chips vending machine services initially started using mobile applications for immediate purchases. In recent years, Telstra, one of Australia's leading telecommunications provider companies, has taken the initiative by carrying out an exclusive "dial a coke" on trial basis where everyone can purchase a coke by making a phone call from a "Telstra mobile" to a number on a coke vending machine. By utilizing location sensitive mobile applications a person may find the nearest petrol and/or gas station or comparing prices when they go shopping, etc.[17]

The futuristic wireless devices can be envisioned to perform endless business functions such as:

- Electronic wallets - mobile phones may be used to hold credit cards and other monetary information for making electronic transactions. For this purpose mobile handsets are basically used as a security coupon registered with the user's identity. When the transaction is done its verification directly corresponds to the user either by a phone call or SMS. In some parts of the world they can practically be used to buy small-value things such as tickets, public transport, parking fees and/or retailing machinery, etc. [9]
- Speech recognition and converter - while the data available on mobiles continues to accelerate and mostly mobile devices have become "data centric" instead of "voice centric" , voice leads the field and will remain a dominant form of communications. New built-in technologies in the wireless devices can now translate verbal communications into transcript form to shun the use of alpha-numeric key pads, etc. [18]
- Speech fusion - this innovative technology can translate e-mails into understandable verbal communications in order to listen to the received e-mails. This system can be dubbed the "automated interpreter". [18]
- Optical/Visual character recognition - wireless handheld devices can also assist and enhance learning. As its name implies, visual features of these phones may convert any hand-written content to a typed-written format with a high degree of precision and with the help of its built-in learning apparatus. [18]
- Voice activation - the enabling technologies of wireless devices can bring voice-control to steer websites and to replace a long chain of chronological input with an automatic "voice-menu-driven" phone system. [18]
- The expanding functionalities of mobile phones have opened the door to refined applications. In this context Android is exceptional in that Google is aggressively developing its Linux-based mobile phone operating system. Google has formed an alliance of hardware, software, and telecommunication companies to consolidate Android development. As long as fragmentation issues can be avoided, Android phones are well ahead in the development stage since Android devices are tailored for specific hardware and user interface upgrades. [19]

D. Some examples of user-related success stories

Mobile phone-enabling technologies and similar applications have widely been accepted in Australia. Australia is a country where a substantial amount of revenue stems from subscribers using mobile phones. In recent years, the trend of sending text messages has increased considerably and this has implications for M-commerce users. An empirical study indicates that approximately 300 million text messages are sent by 11.5 million mobile phone users on a per month average over Australia's three leading mobile networks. Nevertheless, it is widely believed that the inception of a third generation (3G) mobile networking system is the driving force in expanding M-commerce applications.[17]

Application writers and operators are working on new business models which are able to generate a sufficient amount of revenue that can pay for new high-speed wireless networks. The billing systems, however, have been identified as a significant factor in retarding M-commerce services and applications to an extent. Rapid technological progress is the answer to these issues, and it is envisaged that M-commerce will be much more widely accepted in the future. [17]

Another important issue that needs the attention of mobile network operators is to decide and What the importance of emerging world of M-Commerce if it is restricted for business-to-business or business-to-consumer and/or consumer-to-consumer transactions or will expand their services to act as a reservoir for offering credit for airtime, or for goods and can provide loans or billing services to intermediary companies. To capture the small business market, operators can carry transactions between consumers and business for cash withdrawals, payments through mobile phone for soft drinks, car wash, train tickets as well as for larger dealings through debit card, VISA™ and MasterCard™, etc.[8]

1) Swissair

IBM has developed an application through which they can facilitate the Swissair's preferred passengers by sending updates for their flights. Passengers get all updates on mobile screen and subsequently printed on their boarding passes, i.e. departure time, gate and seat number etc In case of any changes in the flight schedule the passengers receive automatic updates on their phone display.[8]

2) Woolwich

Woolwich was the first British bank who introduces internet banking for customers using WAP. With the help of this they can manage their bank account personally. Customer services make sure to customer that their transaction safely transmitted from WPA phone to Woolwich server. [8]

III. E-Business Trends Through Mobile Devices

Mobile commerce or M-Commerce as its name implies can be defined as "the use of handheld wireless devices to communicate, interact, and/or conduct business transactions using high-speed connection to the Internet." [17] M-commerce is gradually becoming a leading force for doing business and in society generally. For more than two decades there has been a persistent "push" for moving forward technologies and a common "pull" of public demand for low-cost, high-speed and cost-effective communications and for an omnipresent access to information on a "follow me anytime/anywhere" basis that has transformed the telecommunications industry. Consequently, Internet access and high computing capacity of wireless devices has heralded the induction of new broadband interactive multimedia applications. Apart from the fact that the wireless web market is still in its infancy stage, M-commerce is likely to evolve dramatically in the coming years due to the emergence of 4G systems integrating many wireless networks, for example WBAN, WPAN, WLAN, and WMAN. [18]

The developments in M-commerce applications are relatively more complicated than those concerning e-commerce and therefore require specialized knowledge. Regarding the present state of technology all technological requirements such as high-speed access and low power devices plus business requirements cannot be achieved all at once, because there are interests in the value chain that are clearly in conflict with each other. Amongst those M-commerce applications which are considered highly personalized, context aware and location sensitive the most inspiring of them all include digital cash (for micro payments), human-to-machine communications (from still to moving objects for access, safety, asset and logistics using RFID).

A. Mobile banking services

The broad dispersal of personal mobile phones in general and dependability on mobile communication technologies in particular have made mobile solutions suitable for an array of financial services including mobile banking and other micropayment solutions. Mobile banking services have won the confidence of their users because there is an absence of time and place restrictions as well as the need to make a physical effort. [2] In Australia, lawmaking and enforcement regimes are working at both federal and state levels to control and regulate mobile commerce. Different regulatory bodies have also been set up especially for the banking, credit and telecommunications industries. [17]

Banking services make it possible for users to retrieve information on their account balances using SMS. However, the new wireless devices using GPRS applications can now support many banking services, for instance transfer of funds between accounts, stock trading, and can verify direct payments through a phone's micro browser. Characteristically, mobile banking services are the modified edition of Internet banking services offered by each respective bank which are designed and financed by a banking industry syndicate, for instance Mobey forum and ECBS, etc. Now WAP replace GPRS, people can pay their utility bills, to do shopping and connect to solo market where pay can be made using WAP services. For secure business transaction user can change their passwords and WTLS. [2]

Mobile networks are being upgraded with WAP, GPRS and UMTS applications and other enabling technologies to deliver next-generation multimedia services. Consequently, customers are now able to check their account statements, transfer of funds, and they are also notified of larger payments. Generally, they have immediate and full control over their online finances. The next generation of mobile banking services will improve their user-friendly image including motivated instructions, direct access, safety issues and immediate transaction

processing with minimum costs. The banks will receive more customer confidence and increased dependability by providing them with a secure form of instant banking. Customers will have less low administrative costs, facing no branch restrictions, and modernized call centers with lower handling charges. [8]

B. Other financial services ranging from macro to micro payments

One M-commerce application that is likely to emerge concerns mobile payments and how they can be further classified into macro and micro payments. [2] Macro-payments is of $10 whereas; micro-payments is of $10 or less. One major distinction is that for macro-payments, confirmation is required through a trusted financial organization that has to be performed over unrestricted wireless and/or wired-line backed networks besides invoking all defensive and safety measures. In contrast, micro-payments are utilized through an operator's communications systems or entail a cash card in addition to (user's ID card that stores the classified information such as a user's covert confirmation key) for making instant payments over short distances using Bluetooth, Infra-Red, RFID, and UWB technologies, etc. [18] Mobile macro payments are done for bigger purchases either electronically (including e-commerce, mobile ticketing, gaming, etc) or on manned and unmanned POS (i.e. restaurant bills, retail shopping, etc.). On a related note macro payments are facing staunch opposition from conventional payment instruments. Nonetheless, solutions have been developed for user confirmation while making macro payments which provide opportunities for many different services including but not limited to passage control, digital signatures, etc. [2]

The success stories in Europe and Japan as to the sale of wireless services and related products indicate that consumer becoming acclimatized to making small values purchases of digital content. In this context Apple's decision to offer 99¢ MP3 downloads back in 2003 would have been signaled the beginning of a new epoch for micro payments. It can be envisaged that in the future micro payment providers will be confronted by mobile payment systems that have some intrinsic advantages that can persuade them to keep their transactional costs low. Whether any micro payment provider can achieve this critical mass or whether micro payments system is ready for takeoff is debatable. [2]

C. Security mobile phones in the usage in business

It has been resolved that the mobile handheld devices are productivity enhancing tools and bring many benefits for the enterprise but at the same time they are also devoid of many risks for organization's security as a considerable amount of confidential corporate and personal data can amass on a wireless handheld device having enough potential to seek the interest of an attacker. The more the capabilities and functionalities of these devices increase, the more the associated risks increase. [9] Another security risk that is very common with wireless devices is that it provides a favorable setting for unauthorized users since it is rather difficult to track the users having no fixed geographic position hence, they can go online and offline with a practiced ease. Because of their small sizes one more risk that is very typical with mobile devices is the risk of loss or theft. Though the accumulated data on a lost device is proprietary in nature and can not be recovered however, there is a persistent risk that any malicious finder of the lost device can hack into the proprietary corporate systems such as, email servers and file systems and the like. [1]

Today mobile phones have become indispensible for doing business and to watch consumer activity. They have become the most cherished communication devices in the modern world. An enterprise can directly contact peoples lives when it is equipped with WAP enabled phone applications. Up to now, SMS services have provided an easiest and simplest way to communicate one on one basis over a mobile network. However, the WAP experts predict that mobile handheld devices will soon to become the universal personal interface to information as well as services. It is envisaged that WAP technologies will not only enhance the users interest in adopting the existing internet applications i.e., electronic banking but will also let those innovative mobile technologies to control their additional dimensions. Nevertheless, it is important to be familiar with the initial implementations of mobile Internet access which will not be the same with which most of users are familiar. Mobile screen do not have colours it has just tiny graphics capability, but this is not an issue because mobile screen has coloured graphics built in video cameras. GPRS technology will be crucial for enabling the users to stay online via high speed data transferring Technology, without plunging into the formalities of dialing up. To cote Jeff Bezos, the chief executive and founder of Amazon.com supporting m-commerce, "If you look five to ten years out, almost all of e-commerce will be on wireless devices." [8]

D. Probable and persistent threats, theft and loss of data due to asynchronization.

Being tiny in size and portable "anywhere anytime", mobile handheld devices are regularly lost or misplaced or stolen. Unless the proper measures are taken, gaining access to the missing and/or gone data will be too difficult to do, making it difficult to save and access classified data. Today, software has been developed and installed in almost all modern handheld devices besides the above-mentioned data collection websites, to recover the removed data from flash memory synchronization. Generally, manual resetting of mobile devices is used to clean up data and restore its original settings before selling it. From a rational viewpoint it appears as if the cleaned-up data has completely vanished but it has actually been preserved somewhere in the device and marked as unused space. Alternatively, a way to evaluate the risks associated with handheld devices is to compare them to desktop computers. The risk profile of handheld devices is incomparable to that of desktop computers. Nevertheless, the supplementary threats follow from two main sources: firstly, size and portability; and secondly, accessible wireless interfaces and associated services. [9]

Organizations will have to put a ceiling on the access to information resident on a mobile device. This will mean frustrating unauthorized access to data by erasing or encrypting the same data on the device. Or it may be necessary to issue a command from a long distance. On the other hand encryption and data wipe solutions are the best safeguards against data

being lost or stolen from the mobile. [14] On a related note phone flasher units have been designed to rewrite and restore the memory of different types of cell phones and can easily be purchased online, etc. [9]

One more step in preserving precious data placed on a handheld device is to back up the contents on a regular basis. For instance, data can be synched and/or linked to a desktop computer as a principal means for having backup data. Backing up is only effective if the memory card is kept away from the device. Both device and card can be lost or stolen simultaneously, severely compromising the benefits of such data protection. [9]

E. Unauthorized access to e-mail content by vicious hackers

Access to the device and its contents have not escaped the clutches of malicious hackers through forgery and speculating the verification of a user's identification such as PIN or password and/or by bypassing the whole verification system. It appears that a good number of cell/mobile phones and PDA users seldom utilize appropriate security mechanisms built-in to their devices, and if they do so they usually inadvertently apply those settings that can be easily bypassed and/or invaded. Having some inherent vulnerability, cell phones are prey to malicious hackers if they are not properly secured. [9] In wireless networks before an attacker attempts to track a target, targets can very simply come into an attacker's proximity. Wireless devices pass through many different and practically unreliable networks from which service is derived and data can be swapped over. Consequently the information can be stolen or corrupted without the user knowing how or when it was done. Quite often a service may be interrupted and subsequently disengaged. Similarly, communication can become sporadic and then restored on a regular basis without having regard to re-authenticating principles. However, a simple attempt at "revitalizing" the browser to reinstate connection may accidentally invite some risks. [1]

Malicious hackers can find the middle ground wireless connections. An example refers to airline passengers who randomly check their stock portfolios at departure lounges and do business from their mobile phones and a malicious hacker creeps into their favorite financial online site by using a DNS system that drags information to the malicious hacker's site. [1] On a related note "Blue jacking" as suggested by the name is a method of attacking Bluetooth-enabled mobile devices. "Blue jacking" begins when an attacker hijacks users' Bluetooth-enabled devices by sending spontaneous messages which are subsequently used to persuade the user to act in response in some manner and the new contact is added to the device's address book. These messages cause harm when a user responds to "blue jacking" that is sent with a harmful intent. [13]

"Blue bugging" on the other hand, utilizes a security error in the firmware of some older Bluetooth devices to obtain access to the device and its commands. This attack uses the instruction without informing the user, and permitted the attacker to access data. [13] In 2004, Nicholas Tombros pleaded guilty to obtaining unauthorized access to wireless computer networks in order to send spam emails advertising pornographic websites using his laptop connected to insecure wireless access points. This was the first case that was prosecuted under the US CAN-SPAM Act 2003. In light of the above, mobile and wireless security needs to be addressed by users and technical experts as well as law enforcement agencies in order to control or suppress criminal misuse. law enforcement agencies need to be well aware of the ways in which criminals have begun to take advantage of the vulnerabilities of these new forms of information and communication technologies, for example in the case of "Wikkileaks" and 'Julian Assange's "anti-spam and defamation" charges. [15]

F. The factors that drive mobile hacking

Mobile phone hacking is done for reasons of economic gains and viruses allow a burglar to access passwords and/or corporate data amassed on cell phones. Invaders can maneuver from a victim's phone for making calls or send messages and this offense is commonly dubbed "theft of service". As the users of mobile devices are now making macro and micro payments and conducting other financial transactions over their cell phones, these devices are becoming an easy prey to attackers.

Business and finance experts have predicted that such an activity will boom in the next few years. Presently, mobile phone users store their credit cards and other financial information for making electronic transactions by using electronic wallet software. Mobile devices are becoming likely targets due to their extensive use, given that there are millions of prospective targets. They possess several vulnerabilities such as not being well equipped with antivirus software. Another pitfall is that mobile devices compared to desktop computers are more exposed to the outer world and hence face the perils of hacking. Since mobile devices are primarily built to make communication as easy as possible on an "anywhere anytime" basis therefore, "phone users want to communicate, and viruses want to be communicated." [4]

The entire mobile banking system needs to be evaluated because threats like spoofing, tampering, denial of service, information disclosure, disclaimer and elevation of advantages and the like are occurring on mobile phone banking systems. In order to protect the sensitive data that resides on the phone device it has become vitally important that such sensitive data is encrypted during data communication and when the same is stored on the phone and/or kept in external memory cards. In the United States of America the instances of stealing credit card records by hacking through a wireless connection started appearing in 2003.

The three suspects of this conspiracy allegedly used a laptop that hacked into the "Michigan Lowes Store's" wireless network in the early morning from a car parked outside the building, gaining access to the company's central data centre in the North Carolina and seven other Lowes Stores across the country. They intended to install a data capturing program used to process credit card transactions, thus enabling them to steal credit card details. In 2004, one of the three suspects was sentenced to nine years imprisonment whilst, his collaborator was awarded 26 months of imprisonment in addition to two years of court administered release. [15]

G. Onslaughts on SMS, MMS and emails

A modified version of pagers' SMS services does the same job as mobile phones GSM- and CDMA-based technologies to send concise text messages to mobile phones having little data storage capacity. They are not considered a useful means for spreading mobile viruses but they do allow an influx of damage-causing viruses when a massive amount of SMS traffic flows between different wireless devices. MMS is a highly developed form of SMS for those cell phones that are properly equipped with GPRS-based technologies and can carry up to 50 Kbits of data which is enough for many viruses. Today, most cell phones can run e-mail applications. However, it would be somewhat difficult for a virus author not to write mobile malware application using e-mail attachments to pass on to wireless devices as happens in case of desktop computers. The damage in that way would not be as widespread in that unlike SMS and MMS, most people do not use their cell phones to read e-mails. [4] By and large, users deem it appropriate to install antivirus software in their computers yet these precautionary measures are still not prevalent in the cellular or mobile phone setting. Since most cell phone users are not aware of the prospective mobile malicious code they are not prepared to protect their phones from any attacks. Some mobile companies have started to install antivirus software in their phone sets such as Japan's NTT DoCoMo via the new Symbian-based FOMA 901i phones with McAfee's VirusScan technology. Nokia has launched two phones having a Symantec Client Security software preloaded onto the memory card and can be subsequently upgraded via its Symantec LiveUpdate system. [4]

Mobile wireless devices have a larger attack facade including but not limited to Bluetooth connectivity, Wi-Fi, and supplementary cellular communications interfaces and furthermore protocols for web transactions, electronic mail (e-mails), instantaneous messaging (chat messaging) and SMS, EMS, and MMS messaging. Conversely, the cellular channel encryption that ends at the radio interface is not sufficient to systematize the back-to-back privacy requirements of an organization which requires application-level encryption to be used over the network in future. [9]

The risks involved in using mobile wireless devices may include:

- Wireless devices are vulnerable to attack from a virus emerging from SMS trafficking, Bluetooth connectivity and\or PCs. For instance, a security vendor company "SimWorks International" recently identified that the first Symbian virus is dispersed through MMS messages.
- Frequent file conversion using Bluetooth connectivity between mobile devices and PCs has made malicious code occurrence more manageable, but made data theft or device damage more likely.
- Spam messages - whether they are done for the purpose of marketing and/or fraud - are considered to be the biggest carriers of a virus.
- There is an inherent risk in eavesdropped or accessed by unscrupulous users. Some users store personal data in their devices. Sometimes people reveal sensitive information on mobile communication. [16]

Some recent empirical studies have indicated that 'Trojans' and not worms or viruses are the main enemy. 'Trojans' technically speaking do not need any transmission vector and purely depend on the user's inquisitiveness to download them onto their wireless devices. 'Trojans' camouflage themselves as utility programs and/or popular games and consequently users install such programs without knowing what they are; a spyware capable of recording their incoming and outgoing SMS messages and also snooping on their dialed numbers and received calls. Another 'Trojan' using malware (like PbStealer) can filch sensitive and classified data like the user's PIN from a user's cell phone. Such an attack has to be taken seriously bearing in mind the fact that there are some J2ME based schemes that can store sensitive data, i.e. a user's private key that is persistently stored or retained, etc. 'Trojans' are a big risk regarding the security of the m-payments system in that these transactions need an authentication through SMS messages. The huge potential for SMS fraud for the purpose of financial gain is obvious. [6]

H. Electronic eavesdropping, voice mail recordings and voice messaging hacking.

Most cells phone users feel comfortable if their phones cannot be eavesdropped some unscrupulous listeners. Likewise, any such endeavors to access and overhear from the air is yet another probable risk that needs to be avoided. The problem of 'electronic eavesdropping' occurs by installing spy software onto a device for collecting discreet information via another phone and/or server. This sort of application exists in some specific phone models and is frequently advertised as a means to check on the activities of a spouse or children. The most important feature is their capacity to distantly switch on the microphone and listen to and/or record conversations. Cell phones having certain vulnerabilities can consent to the spy software being subjected to such active communications interfaces e. organizing a Notebook computer at a legitimate access point in a busy public spot can permit data to be stolen from unsuspecting customers. [9]

Since the communications between a handset device and cell tower are cautiously designed with safety and privacy issues they will be exploited by wily attackers. Scientists and researchers in Israel and the USA have explored effective ways to break the encoding/programming system for GSM-enabled cell phone networks to facilitate eavesdropping. With reference to the networking structure, a more focused yet targeted approach is that while having conversations with their subscribers, cell phones can be secretly personalized to allow eavesdropping by networking companies. **[9]** Some social aspects of eavesdropping also persist and this has led to the advent of 'Flexispy' spyware to assist people probe possibly cheating partners. This application can be used and applied by distantly activating the device's microphone to overhear something. As the capabilities of 'Flexispy' are mostly being employed to monitor the activities of spouses and unruly children yet the same also has the potential to be used in the corporate world to keep a check on the activities of the workforce. Sometimes 'Flexispy' spyware logs information

from the device to a central server without the owner's prior knowledge. Once the software is installed, a hacker can read private messages, examine logs from any computer connected through the Internet and may also overhear confidential conversations and thus compromise intellectual property rights, etc**.** [14]

Specific utility programs exist to record the voice data of the calls made by the user. With little modification a hacker very cunningly convert it into a voice recording spyware. The same can be combined with another Trojan such as PbStealer to send the recorded data via Bluetooth. This malware can obstruct the working of some security schemes that use voice recognition apparatus for verification, as the hacker may replay the message recorded with the help of this spyware. The above-mentioned attacks have to be taken seriously as the recent case involving mobile phone hacking by the *News of the World* newspaper testifies. [6]

I. Unwanted spam and instance of malware

Of all the transmission channels, communications networks are the simplest way to transport viruses and other forms of malware to handheld mobile devices. There are many instances of infiltrating malware into wireless devices. For example they can be received while being synchronized with desktop computers and through infected storage media. Malware can also be spread in a number of ways, including but limited to:

- **Internet Downloads** – A user may be at a risk of downloading any corrupted file. As a camouflage tactic the file can either be a game, security patch, utility program or any other useful application posted from somewhere as a free download. Downloading of legitimate content can also create problems if they possess intrinsic vulnerabilities that malware can exploit.
- **Messaging Services** – Generally, malware tainted attachments may be affixed to electronic mail (e-mails) and MMS messages that are transported to a cell phone device. Instant Messaging (IM) services that engage many phones are yet another means to transfer malware. The users have to make a choice to open the attachment and subsequently install the same to invite malware to corrupt the device.
- **Bluetooth Communications** – Bluetooth connectivity is the most convenient method to hook up devices for sending messages or reshuffling files between them. However, the communications via a Bluetooth device may be positioned in various forms: it becomes discoverable whenever it lets a device be noticed by another Bluetooth-enabled device; and it becomes connectable whenever it permits the device to respond to messages retrieved from connected devices until finally switched off. [9]

Mobile phones are exposed to unwanted SMS text messages, e-mail and/or voice messages from advertisers. No matter what sort of inconvenience their removal may cause, however, charges may apply for any interconnected events.

For example, a per-message tax is levied on each SMS message received and/or a further charge is levied for those messages above the outer monthly limit of a service package. On the other hand, downloading of data may cost extra charges if the attachment has visual images, which means that the charges will remain high. Mobile spam has a tendency to be used fraudulently and the aim is to convince users to make a call or send text messages to taxable service numbers by adopting a *modus operandi* based on the concept of social engineering. Conversely, spam may also be used to convince users to disclose their private and confidential data such as passwords, financial details or other sensitive data via web pages, e-mail, or text messages, or to download malware attached to the message or through a web page. Thus spam and fraud complement each other. As stated above that Instant Messaging (IM) and multimedia messages (MMS) are the most convenient method for spreading malware through spamming. Denial of service is also considered to be yet another leeway using spam techniques. [9]

By utilizing the foregoing delivery methods the user generally has to give approval for the malware to be installed and properly executed. An array of malware behaviors and their following consequences are quite extensive. Thus, malware can possibly overhear user input or otherwise filch sensitive information, tear down stored information and subsequently halt a device from working properly. Some malware can also pull together wireless communications fees against a subscriber, i.e. by sending SMS messages or making calls to chargeable tax numbers. The proliferation onto other handheld devices or even with PCs can also be done by malware and virtually compromise the entire communications network. Below are some distinct yet importantly identified malware categories:

- **Spoofing** – Malware provides spurious information to the user to activate an action in the name of security.
- **Data Interruption** – Malware that resides on the device's applications is susceptible to interruption or access data residing on the phone's memory, respectively.
- **Data stealing** – Occupant malware on the device is able to collect and send data out of the device.
- **Backdoor** – Malware resident on the device is able to put forward deliberations to improve functionality that lets an attacker gain access.
- **Abuse of Service** – Occupant malware can execute those functions which can cause higher than expected service provider costs for the user and thus cause embarrassing financial losses.
- **Accessibility** – Malware resident on the device impacts on the availability or reliability of either the device or the data in it.
- **Network Access** – Malware resident on the device uses the device for more than one unlawful and unauthorized network activity such as port scanning or using the device as a substitute for network communications.

- **Wormable** – Occupant malware uses available technologies to publicize itself in a semi-autonomous manner. [9]

One virus (Commwarrior-B) has appeared on Symbian Series 60 phones and it spreads via MMS message attachments and/or Bluetooth. MMS recipients were asked whether or not they wanted to open the attachment, while Bluetooth recipients were asked if they wanted to accept the file and subsequently run it. The moment the virus is installed it starts finding other Bluetooth-enabled devices to infect. These viruses illustrate that the ways of imitation are many. A classic Trojan (Brador) sends the invaders an email message that contains the IP address of the device as a warning that the backdoor on the tainted device is now activated. The invaders in this way can connect to the device, view and download files or even upload new malicious codes. [9]

J. Electronic tracking

Some cellular carrier companies have acquired the expertise to track a device's location through the development of 'location tracking services' for registered cell phone users. These allow users and their friends and family to be connected with each other 24 hours a day. As for the organizations these services are also made public to keep an eye on their employees' whereabouts and hence improve productivity. Before the tracking service is activated some carrier companies issue a warning for the user that they are about to commence the monitoring, while giving the user an option that he/she may conclude the service if deemed appropriate. Nevertheless other service providers issue no such warnings of monitoring to their customers, if the process of registration is completed. On the technical side radio isolation bags containing metallic fibers create a 'Faraday cage' that frustrates radio frequencies and prevent tracking. However, they make normal use of cell or mobile phones impossible and the battery to deplete quickly. [9]

Of the many security-related technologies being used, Radio Frequency Identification (RFID) can spot objects and users; locations. It is very likely to become an important and core technology in today's global mobile communication systems. This technology has particularly proved useful for organizations that have many functions such as retail, supplies, accounts, design, etc. [11] Tracking services have their own vulnerabilities such as the possibility of clandestinely registering someone else's phone for monitoring purposes. For instance, if the system contemplates completing the registration process in that case a phone will require a sign of authentication. In other words, an SMS must reply with an authenticator code, but uses a code value that is not distinctive. One more approach that can also be utilized includes and is not limited to an online SMS access to engineer the response required to complete registration, etc. [9]

IV. Is Increased Use Of Mobile Phones In Workplaces Raising Productivity Issues?

A statistical survey on the use of mobile phones in the workplace indicated that by the end of 2010 the number of people using such phones was 850 to 1000 million and rising. An estimated speedy growth of smartphones and their bulk consignments on a yearly basis now that they are being used more than ever by employees are the key factors which are forcing businesses to ponder their impact on organizational security. The increasing demand of mobile phones in the workplace is creating productivity concerns because the increased functionalities of these phones are being shadowed by more risk factors. Other empirical surveys have shown that the smartphone market will surpass the laptop market within a couple of years; the global shipments of smartphones will double at the rate of 30% compound annual growth within the next two years. From employees' perspectives the use of smartphones and PDAs will enable major business transactions to be done on a "follow me anytime/anywhere" basis without the need for desktop computers. From the business point of view besides voice telephony, employees can use these wireless handheld devices for the following functions including but not limited to:

- Send and retrieve e-mails where a transaction needs a prompt response,
- Send and receive instant messages (IM) for a quick chat,
- Use vertical applications for administration and business strategies such as Enterprise Resource Planning (ERP), Customer Resource Management (CRM) and Sales Force Automation (SFA),
- Scan barcodes for prices of goods using high definition smartphones like iPhone, etc.,
- Browse web pages,
- Download and share files on the Internet and via Bluetooth connectivity,
- Use Personal Information Management (PIM) for keeping records of phone book contact information to prepare agenda items and convene meetings,
- Store confidential personal and corporate data, etc. [13]

It is important to state here that many companies have started to value access to the above business applications on mobile handheld devices, namely: Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) and/or Sales Force Automation (SFA). These applications invariably contain some classified and sensitive data that will not only be useful for customer dealings but can improve the worth of their future business operations. Consequently, such mobile applications have transformed the purpose and meaning of PDAs and mobile devices which are no longer an optional gadget but a much needed business tool. [13] All of the above mentioned functionalities mobile handheld devices meet the criteria of being the most effective method to raise the workforce's efficiency as well as improve an enterprise's security and privacy risks. [13]

Mobile devices also have certain drawbacks such as any violation of safety setting on the device can be expensive for the organization. The increased number of mobile phone users and global Internet connectivity has diminished the prospects of the conservative "fixed" boundaries for organizations since a

network protected by a central firewall is no longer enough for today's hi-tech lifestyle. [13] Users frequently move beyond these boundaries are they have become more susceptible to data theft and similar threats. Moreover mobile devices are also more vulnerable to carrying viruses, spam and other malware, which can be released through the network when the user is connected behind the network firewall. Portability of these compact tiny devices is yet another drawback attributed to these devices as they can be lost or stolen very easily, compromising the data accessed or stored on them. Major security risks due to mobile devices can hamper productivity and create hazards for a business; this generates the following problem scenarios:

- loss of a company's classified and sensitive data and intellectual property (IP) due to theft or loss of mobile devices,
- loss of employee productivity due to malware and malicious codes,
- loss of intellectual property due to spyware,
- fraud and lost productivity due to hacking, etc. [13]

A. *Theft or loss of mobiles may endanger a company's confidentiality policies*

Statistics show that on a yearly basis hundreds and thousands of cell phones and PDAs are stolen and/or misplaced. [9] However, the worth and price of the hardware and software of a lost device becomes unimportant and irrelevant compared to the worth and price of the data residing on the device. Lost data always remains susceptible to tainted reputations, cut-throat business strategies and possible legal action, etc. People - whether they are general customers, patients, investors, entrepreneurs and business people - put their trust in those companies managing their private and sensitive information. In this context some national governments have developed specific legislation, amendments and/or regulations requiring those companies to protect and administer data from any leaks. [13]

The Australian government has enacted various laws and regulations to cope with different types of content, including personal information. At the federal level the most important statute is the "Privacy Act 1988" which protects personal information and how it is handled by private sector organizations and government agencies. The Act also has relevance to how consumers who use m-commerce services may have their personal information and private details collected and used, particularly by advertisers and service providers including telecommunication operators which already handle a huge amount of private information regarding subscribers to mobile phone services. An individual's privacy rights have also been described in the form of Ten National Privacy Principles (NPPs) which define the parameters of such organizations while collecting, storing, using, disclosing, protecting and transferring customers' personal information, etc. In the case of contravening any of the provisions of the said law(s) for releasing any private and corporate information severe penalties can be imposed. [17]

Organizations should take precautionary measures to protect their valuable data by restricting any unauthorized access to the data stored on a device in case the device is misplaced and/or stolen. In this case encryption and data restoration policies or data wipe-off solutions may provide the best defense. Only data-driven policies cannot completely eradicate all types of risks pertaining to mobile theft or loss of data; it can only persuade employees and managers to remain vigilant in minimizing the risk of data leakage and compliance violations that may hamper a company's reputation. [13] A study conducted by the Readers Digest organization in 2007 suggested that in many of the world's largest cities an estimated 32% of lost phones are never recovered. A cell phone following its reactivation could be used arbitrarily to make international calls that the original subscriber must pay for. If the lost device is able to be restored to its original settings manually or and is reused easily, the contents of the user's data may be expunged. [9]

B. *Threats posed by malware may hamper employee productivity*

It has become abundantly clear that today's viruses and worms are a routine hazard for desktop computers, but the increasing demand and functionalities of hi-definition smartphone mobile devices makes them an attractive target for malware writers. There is every likelihood that the infiltration of malware on mobile devices can increase business and safety concerns. One major attack relating to mobile handheld devices appeared in 2000 and from then on viruses and malware have threatened the most popular mobile operating systems such as Symbian OS, and Windows Mobile3, etc. The built-in email and text messaging faculty of smartphones has made them an easy prey to viruses, as improved functionalities simply increases the risks. Malware can easily be disseminated via built-in Wi-Fi and Bluetooth connectivity through peer-to-peer communication for mobile devices. The viruses can influence a mobile phone's built-in messaging facility and PIM data so that it is sent to other mobile phones. [13]

Some viruses infect other devices that sustain MMS text messaging service if they act in response to the retrieved messages, like the infamous Mabir virus. Offenses like fraud and economic loss are also associated with mobile malware. Mobile malware can disturb the whole Symbian OS system by sending premium-rated messages of which the user has no knowledge. Futuristic mobile spyware may use such unlawful methods that were once considered the domain of desktop computers. For instance, SMS spam disseminates through junk text messages and can reveal users' confidential and private data through SMS-based phishing attacks which at times is known as "smishing." [13]

Wireless handheld devices have a tendency to create a security gap in an organization's security firewall. It has been observed that employees who carry their own devices (employee owned equipment) will definitely try to synchronize them with their office terminal (organization-issued equipment) and/or use their own devices to get connected to the terminal's Internet. [9] Many employees would like to improve their productivity by synchronizing their mobile handheld devices to their laptops. Organizations have to protect their mobile

devices in the same way as they protect desktops and laptops. Since mobile handheld devices operate from networks outside the controlled boundaries of an enterprise they can obtain access to the organization's network which causes the whole IT-based system to become infected. Such devices need to install anti-malware software to curb the risk of infection, which are not limited to Viruses, Trojans, Spyware, etc. The persistent danger remains that once malware gets installed on a device the same can not only steal the private and sensitive data residing on the device but may reduce productivity levels and escalate expenses for organizations. [13]

C. Economic issues: customer receipts, taxation and running costs

For organizations it is important to know what kind and model of devices are being used that can maintain their security policy and improve productivity without putting an unnecessary burden on their economic policies. [13] An omission in checking mobile handheld devices can cause financial losses so care must be taken when managing credit cards, which remain under the holders' control. If an organization's mobile phone is lent to a non-related person it is at risk of misuse and activation of malware and unwanted services such as mobile tracking, etc. Organizations may have to pay huge expenses regarding toll calls and if confidential data is misplaced. Tax laws in a number of countries have provided with a limited number of the services offered by mobile companies free of charge up to which a tax or surcharge is levied on each and every transaction hence, an organizational-issued mobile if becomes a prey of the clutches of an unscrupulous user may incur heavy losses to the organizations' reserves, etc. [9]

It is always best not to keep any confidential information on a mobile handheld device such as financial accounts. Verification mechanism can be thwarted by hackers and therefore any sort of authenticating data such as PINs, passwords, user IDs, and financial details should not be placed on a device's memory. If so such sensitive data should be retained only in an encrypted form. Most of today's smartphone devices like Symbian and iPhon support built-in encryption capabilities by providing a "wallet" that stores personal information when needed. Nevertheless, where the device is an organization-issued device then the aforesaid should comply with the company's policies. [9] Large organizations are also endorsing new productivity enhancing policies which have proven to be commercially viable and cost-effective. For instance, in some countries international food chain companies and sky shoppers have provided their employees with printer applications attached to their handheld mobile phone devices, particularly those associated with supply and delivery departments that issue billing receipts to customers to keep financial records. This is financially beneficial to companies so that they can check any billing irregularities. However, this practice is not suitable for smaller organizations such as Third World enterprises which cannot afford such expensive devices supported by a whole integrated workstation system. [9]

It is abundantly clear how mobile handheld devices are becoming indispensable for today's organizations to improve productivity. However, their global acceptance is only happening gradually because they are not integral to all aspects of organizational infrastructure. One core issue which is being faced by the organizations is how to differentiate between the "employee-owned equipment" versus "organization-issued equipment". At the outset, it seems practically workable to let "employee-owned" cell phones and PDAs to be used for business purposes in a cost-effective way. Nevertheless, it is difficult to develop the capabilities to control and handle these devices. More importantly, security concerns for cell phone handheld devices range from those that are commonly linked to computer equipment because they operate from platforms outside the restricted boundaries of "fixed" devices. Furthermore, a number of safeguards are invariably available for desktop and networked workstations but are not commonly available for a wide range of handheld devices. On the other hand "organization-issued devices" can be administered as the basic functionalities of these devices are known, their configurations can be sporadically managed in accordance with company policy. It is therefore suggested that the said functionalities can let organizational applications particularly those developed for PCs be more easily extended to the mobile platform. [9]

D. Fraud and lost productivity are likely hacking targets

Malware, Spam, Trojan as well as unwanted content are considered harmful for mobile security systems and susceptible to being attacked through hacking and/or denial of service, etc. Viruses take advantage of the limitations and vulnerabilities of mobile phone operating systems before initiating any attacks. For instance, one known malware called "Skulls" attacks all links on a mobile handheld device by neutralizing its applications. Consequently, if a device becomes infected with this kind of malware, the user cannot send any e-mails or instant messages; in fact all symbols on the phone device are replaced with the skull image of the "Skulls" virus. These threats can be alleviated by adopting and implementing industry best practices. IT administrators in large organizations can recommend integrated practices for protecting mobile devices from any sort of security-related risks. Advances in technology have led to improvements in security which is a three-fold system in that it involves people, events and blue-chip technology. All these elements need to be considered to create the best security system possible. Some of the prevailing policies have been discussed very briefly in the above sections but in a different context. [13]

The focal point of these integrated best practice policies should be how to protect handheld device from unscrupulous users and for this purpose Password protection is considered to be the most effective barrier to protect data intrusion. All mobile devices must have a power-on-password enabled facility so that phone users can be identified with their respective device. Nevertheless, a vigorous mobile security plan would empower administrators to execute reliable and integrated policies for all devices from a single location. For instance administrators are required to be proficient in preventing all brute force log-on attempts, i.e. multiple attempts with different login/password combinations and the like. [13] On the other hand, encryption is still considered to be the first line of defense against any invasion of a phone to

prevent loss of data or theft. It is also important to protect data in transit (travelling data e-mails, etc.) during "device to server" transmission. There are some security protocols which help ensure that data is properly and safely transmitted. Of these, the "SSL" protocol protects data in transit because it is very economical and simple to implement and does not need any new client software on a mobile device. In contrast, VPNs also secure data in transit but they are expensive, have a propensity to drain battery life and require a client software. Administrators should be properly skilled to configure all forms of data encryption and how to use algorithms. [13]

Anti-malware and anti-spam solutions should be updated on a regular basis so that new prototypes for notorious malware can be discovered and dealt with. Moreover, mobile phone data has to be scanned immediately including data residing on mobile devices and on external memory cards whenever they are inserted. If the administrator deems it necessary a manually scan the devices then this should be done. [9] By and large, malicious programs can easily be disseminated to cell phones via communication channels, i.e. MMS or Bluetooth connections. Whenever, a message or contact is received on a mobile phone from an unknown number it deserves to be treated cautiously. Regularly received MMS messages or e-mails even from a familiar number and/or address, containing an attachment to be installed can become susceptible to a malicious program. [9] Whenever possible, Bluetooth settings must be constructed with the utmost security by sending phone users prior intimations regarding the incoming link requests and obtain their verifications before they take place. Most of today's smart phones offer this service to manage Bluetooth functionalities by allowing only selective profiles which are required to support activation with another mobile handheld device. It has been suggested that device pairing should not be done at public places, but instead in places that are radio isolated and/or in Radio Frequency Identification (RFID)-free environments. This will deter the chance of being monitored or recorded over the air thereby using them to restore protection keys that may be used while eavesdropping. [9]

V. Safeguards And Preventions

Mobile handheld devices are productivity enhancing tools even though they do have serious security problems. Yet organizations are still reluctant to realize their significance as a vital component of a particular organizational infrastructure. Without delving into the advantages and disadvantages of employee-owned tools as well as organization-issued tools, the "control factor" of these wireless devices is rather difficult to ascertain as they are not controlled by approved platforms vis-à-vis "fixed devices". [9]

Since the security concerns pertaining to cell or mobile phone devices intrinsically vary from those of the desktop computers, many safeguards which are invariably available for desktop and other networked computers in the workplace are not as accessible for all kinds of mobile handheld devices. The reason behind this is that on the whole organization-issued devices are much easier to manage because the traits of these "fixed" devices are already identified; their prototypes can be easily managed and joysticks can be installed when needed to enhance the level of security, in conformity with the company's policies. However, a workable suggestion would be that the said attributes of the organizational applications for desktop computers can be extended to mobile platforms as well. Our discussion will include an appraisal of the range of safeguards available for mobile handheld devices, and how they eradicate the associated risks for the organizations. [9]

A. User-oriented measures for maintaining security

The security of handheld devices cannot be maintained without users' involvement. Users must be instructed about what measures to follow and what precautions to take while they use organization-issued equipment. For instance, numerous built-in configuration settings and security prototypes of handheld devices are seldom used. Taking full advantage of all the facilities afforded by cell phones or PDAs, it is vitally important that the user know all the security safeguards. [9] By and large, user authentication methods are available on a majority of devices such as PINs and passwords though they are considered to be the first barrier to any unscrupulous access, yet have certain pitfalls. For users it is rather difficult to understand and analyze the plethora of documents involving all the features and options available on a handheld device for authentication, as it entails accurate and secure choices. [9] Users should prevent keeping any sort of confidential data on a handheld device since the authentication mechanism is not devoid of certain weaknesses and can easily be bypassed or wrecked and/or recycled from the deleted data. Even if confidential data is kept on detachable memory cards, it should be kept away from the device unless required. When it becomes imperative to keep the sensitive data on devices, it should be kept in encrypted form since most of today's smart phones do support built-in encryption capabilities to meet this requirement. [9]

Yet another simple protective measure against various forms of malware that users can employ is just to simply turn off Bluetooth, Wi-Fi, infrared, and other wireless interfaces, unless absolutely needed. This is because Bluetooth devices are prone to escalating risk factors due to mobile malware, particularly in crowded surroundings such as airports, sports events and/or music concerts that proffer a target-enriched environment. Immobilizing a wireless interface also has the advantage of extending the battery life of the device. In addition to the above, automatic connections to cellular data services, that is, GPRS or EDGE systems, are also better to be turned off while not being used. Staying offline brings many fringe benefits as well since it averts the risks posed by malware infection and it can also thwart an infected device from sending contaminated data to other parties. If a phone device automatically connects to data services it can also be a direct warning that the phone has been infected by malware and is now attempting to spread itself through various applications. [9]

In case the device is misplaced or stolen the user can take precautionary measures even from a distance, such as disabling service, locking the device and/or completely wiping out its contents by immediately reporting the incident to the cellular carrier company. In this regard GSM carriers in many countries have taken a quantum leap as they can now register the identifier of the phone, for instance International Mobile

Equipment Identity or (IMEI) in a global database that prevents it being used elsewhere. It is, however, important to understand regarding the whole reporting system prior to the incident what kind of information is essential. Stolen devices may accrue substantial charges that the subscriber of the phone must pay until the device is reported as stolen. A copy of the filed police report may be required for phone charges to be dropped. [9]

B. User authentication and physical control on the mobile device

Of all the available safeguards concerning the security of mobile handheld devices, users' authentication techniques are commonly available in many devices, for example PINs and passwords. Although these knowledge-based authentication techniques are not infallible and have certain vulnerabilities, they are considered to be the first line of defense against unauthorized users' access. There are three main categories of users' authentication techniques commonly being used for authentication:

- proof by knowledge (passwords),
- proof by possession (tokens, i.e. smart cards),
- proof by property (fingerprints).

The aforementioned techniques can be used either alone or in tandem with others. However, using more than one type of authentication technique is also feasible and affords better protection. Passwords on one hand are believed to be the oldest and most popular form of proof-by-knowledge technique for handheld devices. Likewise, smart card authentication is best known for its proof-by-possession technique. Having entrenched the computer chip operating system, programs and data storage systems, these credit card-sized security tokens have become an integral part of the internal security infrastructure of some organizations, which are extending the already installed smart cards to handheld devices. Smart cards are able to transmit users' security identification and policy rules to a device that administers users' authorization and permissible behavior. Passwords fingerprints are also considered to be the oldest proof-by-property technique that involves the biometric system. This technology is relatively complex compared to the rest of the above two and therefore, a small number of mobile handheld devices have built-in fingerprint-based technology authentication. [9]

The proof by knowledge technique (passwords) can be divided into two categories, where the former enables users to choose a series of displayed images and the latter refers to sketch a series of lines over a network or follows the icon pattern. The former, however, is being applied in various commercial security products for handheld devices. The most notable development in proof by possession (smart cards) technique is that now wireless smart cards insert a radio frequency chip or in a more compatible mode; some manufacturers have introduced removable media as well. **[9]** Organizations must adopt concrete and meticulous policies regarding passwords and PINs for cell phones and PDAs in a back-to-back and composite manner. Nevertheless, there should be restraints on using the same password for a handheld device which is to be used for network access or access to other devices and applications. In case the password is erased from memory, different techniques can be utilized to recover the same from various handheld devices. This infers collaboration access to the network or other devices in turn. Various authentication techniques incorporate a time-out feature that can automatically lock the device the moment it reaches the verge of a stipulated condition, such as a screen saver, etc. At times these techniques can be rather irritating, but they are meant to help protect a misplaced or stolen device or until the owner recovers it. [9]

Keeping physical control of a mobile handheld device is also vitally important. Like all precious possessions these devices should not be left unattended. The contents and confidential data that resides on a device's memory also be jeopardized if an unauthorized and dishonest user gains access to it. It is dangerous to let else to use the device as it inadvertently invites malware and/or activation of unwanted services, such as mishandling while retrieving messages and/or taking unwanted calls. Sometimes, even a slight change in the security settings of the device can expose it to other types of threats that remain unnoticed because the user does not know what kind of changes have been made in the security settings. [9]

C. Minimized functionality of devices and decrease data exposure

The more the augmented functionalities and innovative technologies are taking place the more the proportion of risk is mounting. To cope with this problem the most viable solution could be to decrease the number of functionalities offered by them except those which are particularly needed. Consequently, one good paradigm for getting the desired results is to minimize the wireless interfaces unless urgently required and by rendering all those superfluous features inoperative through configuration settings. However, in certain circumstances some features may also be removed permanently to avoid their involuntary reactivation. Likewise, reducing the use of attached applications and/or plug-ins may also provide desired benefits. As these applications do have certain vulnerabilities, if they are installed they can get into the user's content and compromise the programming interfaces of the device. It is therefore vitally important that prior to the installation of any such applications their advantages and disadvantages have been evaluated. [9]

Cellular service agreements and subsequent service settings are yet another method to manage or simplify the functionality issue. If data service is eradicated for the activation of voice service only the same may avert full access to the Internet, which is be considered to be an appropriate solution. On the other hand, it can be possible to have the carrier restrict access to international destinations which are not being used or blocking other services. An example concerns various cellular carriers who offer to block subscribers' text messages initiated directly from the Internet because this is a major cause of disseminating wireless spam. It has been suggested that it is better not to keep sensitive and private data on mobile devices. This is because the whole authentication system can be easily avoided and deleted information may be restored from a phone's memory. Regardless of how convenient it is for

subscribers to verify their online financial records and/or to other devices via PINs, passwords, user IDs, and account numbers on wireless handheld devices, it should be avoided. Classified and sensitive data can also be stored on detachable memory cards but the same should be kept separate from the device. Moreover, matters pertaining to labeling and tracking of sensitive data residing on these devices can also divert attention. [9]

D. Restoration of back-up data and installation of preventive and detection software

It would be a catastrophe if someone starts using handheld devices as the sole depository for keeping important information. The device may be misplaced or stolen or damaged accidentally. For protecting the precious data residing on a device it is safer to restore back-up of data on a regular basis. For this reason, data can either be synchronized with a desktop computer for keeping a back-up or for any possible dual purpose. Alternatively, this back-up data can also be kept on the memory card but the card can only be supportive if it is kept detached from the handheld device. The chances of restoration of back-up data will be further narrowed down if both the device and the card are lost or stolen simultaneously. [9]

The operating systems and built-in technologies of mobile handheld devices are far more complex than desktop computers, and hence warrant extra security controls for the prevention and detection of attacks against them. In this regard the installation of "Prevention and Detection" software for defending and protecting against any kind of malware onslaught has become indispensable. Consequently, a large range of such equipment is now available for a number of today's handheld devices, especially, for smart phones and PDAs that may be used to supplement the already existing built-in security mechanisms in them. It should be mentioned here that these "add-on" security software systems do have certain vulnerabilities and they should be evaluated very carefully. These types of equipment generally contain one or more of the below mentioned capabilities:

- User authentication alternatives, including biometrics (proof by property) and token-based (proof by possession) techniques,
- Content and memory card encryption,
- Firewall and Intrusion detection system,
- Antivirus and antispam (anti-malware),
- Content and memory card erasure (wipe off technology), and
- Virtual private networking. [9]

Organizations must consider how to protect mobile handheld devices. Although these wireless handheld devices are controlled on the networks which are outside the ambit of organizations' "fixed" boundaries, when they connect back to the network they may pollute organizations' whole IT systems. Extending equal protection to mobile handheld devices with those of the desktops and laptops, these devices must have anti-malware software installed on them to reduce or eradicate infection. Once malware gets into a mobile device it may not only drain off all private and classified data, but may also severely compromise productivity levels and augmented support expenses. Anti-malware software works by finding solutions to scan all the upcoming mobile threats by not having them installed on the device. Commercially available software such as Flexispy has the same application. To be more precise, the most effective anti-malware and anti-spam solutions should obtain updates periodically, about all new prototypes for already identified malware with the lowest amount of users' and/or administrative intervention. It is suggested that data residing on a device's memory has to be scanned instantaneously, including the data residing on external memory cards whenever they are inserted. [13]

Mobile handheld devices also require a complete firewall protection to curb unauthorized access. Firewalls are best known for their cautious scrutinizing capabilities and once set in motion, they can restrict mobile traffic. Moreover, private firewalls are also indispensable for obstructing port scans that the attackers usually use to discover vulnerabilities when a device is linked to a public network. Firewalls also supposed to be the first barrier against any abuse of un-punched security holes in a device operating system and/or client applications. Thus, businesses must install a comprehensive firewall and intrusion detection systems with pre-defined security standards which can further be modified by the administrators in a particular workplace environment. An intrusion detection system (IDS) while implemented on a mobile handheld device can negate service attacks by identifying the prototypes of network traffic. On a related note, a better solution is where administrators are authorized to establish an exemption list to supersede security level settings or by blocking certain types of network traffic. For instance, administrators should be empowered to prohibit certain types of protocols, ports, and IP addresses from inspection because in a particular organizational setting users may have different levels of requirements and usage. The following measures will enhance the level of mobile security:

- Inspection and access perimeters for devices,
- Firewalls to curtail the type and origin of network traffic,
- Easy-to-deploy firewall solutions with pre-defined security levels to be modified by the administrator, and
- Intrusion detection systems to obstruct denial of service attacks, etc. [13]

E. Solution Methods (I-clouds)

A major global IT problem refers to disk storage and particularly its operating costs, which have been estimated as representing nearly 30-50% of gross capital expenditures per annum in many enterprises. Against this background, enterprises must manage effectively the costs of storing data, especially unformed data. Therefore, to address this need, Cloud storage services have emerged and become fashionable. [21] Nevertheless, the current economic state of affairs as well as the advent of new technologies has ignited the interest of organizations in Cloud storage services and/or provider models. Cloud storage providers can suggest cost-cutting measures by

using equal storage capacity to meet organizations' needs, such as transitional cost-savings measures for their customer base. [21]

Cloud storage services/providers are commonly known as "Cloud Backup" which makes back-ups of enterprise archives online automatic, while data is safely stored externally in data centers and is easily recovered. For example, if an unfortunate fire incident happens at any workplace or home both computers and disks (i.e. CD-ROM or tape, etc.) can be damaged. With Cloud Backup this threat is eradicated. A number of platforms are being supported by Cloud Backup such as:

- Windows___ Windows Vista, Windows XP, 2000 Professional, Server 2000/2003,
- Linux_____ and its most popular versions RedHat, SuSE, Debian, and its supportive system like Ubuntu, all with Java 1.5 or higher,
- Mac OS X, etc. [19]

Security has been the core issue in the developing phase of Cloud Backup. Data is first encrypted and condensed and then it is sent to and stored on a Backup Server in a fully secured data center. This involves a fully secured (SSL) network connection that makes the Cloud Backup service as safe as online banking. Nobody can enter the data stored at data centers except the subscriber. In other cases, the moment the data enters into an insecure setting like the Internet, it is vulnerable to hackers. An answer to this is Cloud Backup which encodes data (in encrypted form) before it leaves the terminal and subsequently decodes it while it is restored on a workstation. [19] This is why security and accessibility issues come first when companies choose to transfer their sensitive data to the Cloud Backup system, via the Internet. [21] The market for Cloud Backup services is rapidly growing owing to the huge amount of private and corporate data now being stored on desktop computers and laptops and more recently on smartphones. Smartphones have the equivalent storage capacity of their larger counterparts. [20]

VI. Conclusions

The omnipresent exploitation of mobile systems, extensive use of the Internet as well as the speedy growth in wireless technologies and the broadband interactive multimedia applications in recent years have helped improve the functions and characteristics of mobile handheld devices. [9] The said devices and communication systems have also developed especially built-in software to curb any instances of encroachment. [18] Though mobile devices can provide many productivity benefits for organizations and businesses, these devices are subject to security risks such as malicious codes and communication attacks, theft of data, spam, etc. [15] Security concerns become vitally important vis-à-vis financial transactions so that the assault vectors in this application need to be examined with due diligence. [6] Therefore, mobile security must be tackled by both the users and law enforcement agencies to reduce the risk of criminal misuse. [14] In this economic environment new technologies have made organizations very interested in "Cloud Backup" because it creates automatic back-ups of enterprise archives online, while data remains safely stored in data centers and can easily be recovered. [19] Enhanced wireless security and the broad exploitation of 4G systems in the coming years will enable mobile commerce to become the best way of doing business. [18]

References

[1] Ghosh, A.K. & Tara M. Swaminatha (2001). Examining the risks in wireless computing that will likely influence the emerging m-commerce market: Software Security and Privacy Risks in Mobile E-Commerce. *Communications of the ACM*, vol. 44, no. 2, pp. 51-57.

[2] Mallat, Niina, Matti Rossi & Virpi Kristiina Tuunainen (2004). Adopting new and innovative mobile financial applications and service provisioning methods. *Mobile Banking Service*, vol. 47, no. 5, pp. 42-46.

[3] Wu, Min, Simson Garfinkel & Rob Miller (2004).Secure Web Authentication with Mobile Phones. MIT Computer Science and Artificial Intelligence Laboratory. DIMACS Workshop on Usable Privacy and Security Software.

[4] Leavitt, Neal (2005). Mobile Phones: The Next Frontier for Hackers? *Computers*, vol. 38, no. 4, pp. 20-23.

[5] Milanovic, Nikola, Miroslaw Malek, Anthony Davidson & Veljko Milutinovic (2004). Routing and Security in Mobile Ad Hoc Networks. *Computer*, vol. 37, no. 2, pp. 61-65.

[6] Agarwal, Shivani, Mitesh Khapra, Bernard Menezes & Nirav Uchat (2008). Security Issues in Mobile Payment Systems. Department of Computer Science and Engineering, IIT Bombay, India.

[7] Lehr, William & Lee W. McKnight (2002). A research and education initiative at the MIT Sloan School of Management. Wireless Internet Access: 3G vs. WiFi? Center for Business@MIT, 21p.

[8] Interforum (2001). M-Commerce: E-Business without boundaries. *Interforum: Helping Britain to Trade Electronically*, no. 8.

[9] Jensen, Wayne & Karen Scarfone (2008). PDA Security: Guidelines on Cell Phone and PDA Security: Recommendations of the National Institute of Standards and Technology Special Publication 800-124, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

[10] Varshney, Upkar, Ronald J. Vetter & Ravi Kalakota (2000). *Computer*, vol. 33, no. 10, pp. 32-38.

[11] Lee, Hyanjiin & Jeeyeon Kim (2006). Privacy threats and issues in mobile RFID. *Proceedings of the First International Conference on Availability, Reliability and Security*, 20-22 April, 2006. Korea Information Security Agency, 5p.

[12] Scarfone, Karen & John Padgette (2008). *Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-121. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

[13] Enterprise Mobile Security: Protecting Mobile Data and Increasing Productivity A Trend Micro White Paper, November 2007, Trend Micro, Incorporated

[14] Urbas, Gregor & Tony Krone (2006). Mobile and wireless technologies: security and risk factors Trends & Issues in Crime and Criminal Justice, no. 329, Australian Institute of Criminology.

[15] Ying, Liu, Huang Dinglong, Zhu Haiyi, & Patrick Rau (2007). Users' Perception of Mobile Information Security. *Hacker Journals White Papers*. Computer Security Knowledge Base Portal.

[16] Palen, Leysia, Marilyn Salzman & Ed Youngs (2000). Going Wireless: Behavior & Practice of New Mobile Phone Users. In *Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work*. ACM, pp. 201-210.

[17] Consumer Affairs Victoria (2002). M-Commerce - What is it, What Will it Mean for Consumers? [work in progress]. Department of Justice.

[18] Grami, Ali & Bernadette H. Schell (2004). Future Trends in Mobile Commerce: Service Offerings, Technological Advances and Security Challenges. In *Proceedings Second Annual Conference on Privacy, Security and Trust*, October 13-15, 2004, Wu Centre, University of New Brunswick, Fredericton, New Brunswick, Canada, 14p.

[19] Cloud Backup: Cloud Backup - FAQs, April 2010, Version 1.6, https://backup.eu.businessitondemand.com

[20] Fu, Yinjin, Hong Jiang, Nong Xiao, Lei Tian, Fang Liu, Hong Jiang, Nong Xiao, Lei Tian, & Fang Liu (2011). AA-Dedupe, AA:Application-Aware Source Deduplication Approach for Cloud Backup Services in the Personal Computing Environment: IEEE Cluster 2011 Technical Paper TP-2b. National University of Defense Technology, China.

[21] Ju, Jiehui, Jiyi Wu, Jianqing Fu, & Zhijie Lin (2011), A Survey on Cloud Storage. *Journal of Computers*, vol. 6, no. 8.

[22] Hui, Suk Yu & Kai Hau Yeung (2003). Topics in Wireless Communications: Challenges in the Migration to 4G Mobile Systems. *IEEE Communications Magazine*, December, pp. 54-59