# A Generic Information Security Framework for Mobile Systems

A.Sharma and N.L.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

## Abstract

Mobile devices have faced tremendous changes in the past few years. Mobile devices are now tending to blend in to the category of PCs. While providing a bundle of services such as email, calendar, managing appointment and contacts, these mobile devices can also connect to a network via wifi. The risk caused by this is tremendous as there is no proper security framework at place. Many organizations being aware of this fact implement few add-on such as user authentication, virus protection, firewall, intrusion detection, etc. but these add on provide solution in a very different way. Many solution provided take action after the problem has occurred. This paper suggests a framework which can be incorporated in to the security mechanisms so as to avoid the above mentioned problems.

## Key words

Mobile security, user authentication**,** security framework, ISO 17799, levels of users, Organizational user, General users

## 1 Introduction

Mobile device are becoming to be one of the most vital devices in not only corporate network but also they are turning out to be one of the most powerful devices for commutation with many networks on the move. It can be recognized that mobile devices are becoming one of the most vital tool for business, but there has not been a standard framework to protect the data. The mobile devices are not connected single network but they are connected to multiple networks at the same time, which means that the risks to the mobile devices and the network they are connected increases with these connectivity.

There has also been consideration on the authentication methods, the efficiency of authentication provided by PIN, and the impact of security on the mobile network as well as the mobile device. A look at the connectivity of the mobile network is also taken which provides the various risks by the various connectivities.

According to a survey by Frost & Sullivan there are more than 50 million workers whose jobs required them to perform work outside the office, in the near future with a growth of 6%, its going to be 72 million, and the number of mobile professionals using mobile devices to store data is going to be more than 37 million in the year

2007. According to this survey, Executives directors and midlevel managers make up to 57% of the enterprise professionals using mobile devices, field services employees conduction installation, service and repair comprise 17%, mobile sales employees 16% and vehicle operators make the remaining 10% (Frost, 2006)

According to another survey 36% of their employees carry laptops and mobile devices containing sensitive customer information. 98% of respondents say their organizations allow remote access to their corporate networks. As a result of recent world events and varying airline travel restrictions, 73% of respondents now believe more laptops and mobile devices may be lost or stolen during air travel. While 37% of respondents indicate they have already experienced some form of data breach due to loss or theft of mobile devices, a staggering 68% of respondents indicate it is likely they too could experience a data breach in the future. In fact, during a recent Entrust webinar, 60% of attendees noted that someone on their immediate team had a mobile device lost, misplaced or stolen. 64% of respondents have implemented specific policies and/or procedures instructing employees on how to avoid a sensitive data breach. Over 90% of organizations indicate they are reliant on their employees to take specific actions to help comply with these policies, with 37% indicating they are "very reliant" on employees. This reliance, coupled with the fact that 84% of respondents indicate a degree of difficulty in trying to influence employees' behavior in adhering to these policies makes policy alone an ineffective means to mitigate the risk of a data breach. (Etrust, 2006)

## 2 PIN Authentication

In the past few years we have noticed the number of mobile phones being used grow exponentially. According to a recent survey the mobile phone subscribers in the world has exceeded more than 2.14 billion (Mobiletracker, 2006). According to CIA fact book there are more number of mobile than the population of people in UK (CIA, 2006). Escalating number of mobile phones are lost or stolen each year, indicating valuable information of the user is at threat. In a second generation mobile phones (GSM) the security from unauthorized usage is achieved by combination of 2 secure radio encryption interfaces, SIM (Subscriber Identity Module) and IMEI (International Mobile Equipment Identifier). This enables the legitimacy of the devices before allowing it to utilize the network. The two identification numbers being used, they are mainly concerned to service provider. However the user vastly depended on the Personal Identification Number (PIN) authentication. This facility is enabled by the user before any level of protection is provided. It can be noticed that the security provided by the PIN is arguable, since the mobile devices contains a considerable amount of information of the user. (gsmworld, 2006)

In contrast, the 3rd generation mobile phones are not merely devices for communication. The advancements in the mobile have changed drastically in the past few years with easier ways effective ways of communication, the authentication methods of the mobile phone have not changed a bit for the pas 15 to 20 years. Since the introduction of the mobile phone the only authentication methods that is being used is "PIN" (Personal Identification Number). Mobile phones previously

were only used to make and receive calls and for texts. But the whole idea of mobile phones has changed, they are not just phones they are devices which whole bunch of entertainment and connectivity, they are having more processing speed than normal PC 5 to 6 years before. Loss of Mobile phone is loss of valuable information

In a survey conducted to determine the attitude of the user on security of mobile device 89% of the users knew about PIN authentication, but only 56 percent actually used it. It was also observed that only 76 percent of the users used only single lever PIN security (at power on). Of those 76 percent of users only 36 percent of them used the PIN to protect at the standby mode.The other key finding were that more than 11 percent of the users didn't even know about the PIN facility which can be more than 84 million user in real world, Of those 44 percent of the user who did not use PIN facility, 65 percent of the users gave the reason as it being incontinent. A large number of respondents, 41 percent have little confidence offered by the pin authentication. (Clarke et al. 2002)

# 3 Connectivity of Mobile Devices

These latest handheld devices are connected in more than one way which are

- traditional network, the service provider
- GSM or 3G depending on the connection
- Infrared
- Bluetooth
- IEEE 802.11 (Wifi)

Which make the device 5 times more vulnerable than the traditional PC.

The focus of this paper is mainly on Bluetooth and Wifi as they are more susceptible to attacks.

## 3.1 Impact of Bluetooth on mobile security

According to security advisor Kaspersky Lab, reports that Russia had earned the dubious distinction of becoming the ninth country with a confirmed infection of a virus targeted at Bluetooth devices called "Cabir.a" worm, which had already been stricken handheld devices in many country.(Kaspersky, 2007). The devices can also be attacked by Bluebug, and Bluesnarfing.

## 3.2 Impacts of IEEE 802.11(Wifi)

In Wifi there are mainly 2 different types of attack Denial of Service and Man in the Middle. Denial of service attack mainly prevents user from accessing network resources, it simply denies them from the service, hence the name denial of service. The usual method that triggers DoS is to flood a network with degenerate or faulty packets, crowding out the legitimate traffic causing the system not to respond.

Similar to DoS attacks, man-in-the-middle attacks on a wireless network are significantly easier to mount than against physical networks, typically because such attacks on a wired network require some sort of access to the network. Man-in-the-middle attacks take two common forms: eavesdropping and manipulation

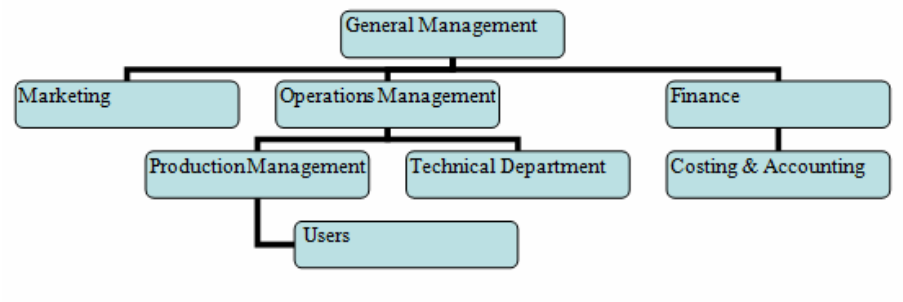
## 4 BS ISO/IEC 17799 Applicability to Mobile devices

In the following section these standards have been analyzed and they are applied mobile devices, most of the controls specified in this standard are universal which can be applied to any kind of devices and networks. The controls have been directly taken from BS ISO/IEC 17799 to check the applicability for mobile devices

Out of 11 categories, 39 control objectives, and 133 controls in ISO 17799 almost 99of the controls can be applicable to mobile devices and 9 being applied in special cases. A mobile device in some senses is similar to a normal PC and in more senses similar to a Laptop either of them can be connected via Wifi in a network. More over a Laptop has more similarities to a mobile device as it is more flexible to take from place to place. Most of these controls were defined to stationary devices like a standard PC. With a bit of similarities between a PC and mobile devices being there these Controls can be applicable. In the below section the applicability of each control has been explained.

## 5 Organizational Hierarchy

Given below is a simple model of organizational hierarchy, which gives most of the departments and users working.




The chart given above is a typical hierarchy of any organization. The best named companies such as Spryance Inc. and Acusis India. These companies are basically into ITES (Information technology enables services), health care business processing outsourcing. These companies are into outsourcing the healthcare services business to developing countries such as India, Pakistan, and Philippines due to low cost labor.

The general management is at the top of the chart followed by operations management. General management is directly connected to finance and costing &

accounting. Production management, technical department are directly below operations management, and users are directly under production management.

The process of work activity a is done in the following fashion

- The operation management plans the whole activity of the team as per the requirement.
- The operation management provides tasks to production management team
- Technical staff is directly under level operational management as it can take orders directly from them and do the necessary changes in the network
- General management is provided with reports by operation management on the tasks achieved.
- Marketing team gives the status of the market to operations management to provide with future implementations, and operation management does the task with the help of all other staff.
- The general management has a direct control over finance, cost & accounting. Marketing is under operations which give suggestions on strategies to operation management.
- The planning is done by operational management to be implemented by production management.
- These plans are implemented by production management team and users. The technical department is directly under operational management as well as general management

It can be seen from the above hierarchy that the user here can easily be divided in to 4 different levels.

- General management and operational management can be considered under highest level as they have most of the rights in the organizational network.
- Marketing finance, accounting & costing and other departmental management come under this second highest level.
- Technical department and production management team come under this level as they take orders from highest level, operational department and management.
- The rest of the users come under lowest level as they don't have much of rights and they have to work under the production team

From the above discussion it can be understood that there are more than 1 level of users, each block has different priorities and right.

## 6 Introduction to levels of users

In a corporation there are many different job descriptions with different works. In securing the mobile devices there must be different levels of authorization to different users.

For example a manager has the highest level of security as this user might be holding a tremendous amount of information on their mobile devices. A salesperson might be in medium security level as they might be holding most of the sales information and so on.

**Levels of users in corporate network:** When a corporate section is considered, there are many numbers of users. Each with different priorities and different usage. All these different users can be broadly classified in to 4 different levels. The basic definition and properties of these levels are given below

**Level 1:** This is the topmost level. This has the highest security and also the highest right.The user in this level can access to any file of any branch in that corporation.. The user has the rights to Update, modify and also delete certain files according to his\her priorities. As shown in the heirarcy the General management and operational management come under this level. For example the General Managemt of the company can come under this level, as they have many right in the network, they can access update, modify and delete the files according to the managers will. As this is the topmost level, this level must have the highest level of security. They can be considered as the highest percent of users as indicated in survey discussed in the previous section.

**Level 2:** This level user also has access to any files, but their access is limited to their own department. In this level the user can have all the rights specified in the above level, but their access is limited to their branch or department. As shown in the hierarchy departmental manager come under this level such as finance, costing and accounting and marketing users come in this level. The users in this level have access to all the files available in the network. They can update the document with the permission of the manager of the other department. For example HR manager can access only specific set of files which are under them. To access any other files which do not come under them they have to have proper accessing right from the other department they are accessing. This level has a security framework close to that of level 1. They can be considering at the 17% of the users as indicated in the survey.

**Level 3:** This level the user has access to their own profile. They can access modify, update delete information in their profile. They have access to browse files get information from any of the departments but they cannot edit the information. The users in this level can modify files in their own department, if required, this modification can only be done with the permission of the users in level 2 (as per the concerned departments). For example the staff in a sales department can access to the files in his department, if he/she needs to update the information in their department, he needs to get permission from the manager of that department, and only then can he do the necessary update. They do require the security framework, but not as users in level 1 and 2 need. They could come under the 16% of the users that were shown in the surveys discussed above.

**Level 4:** This level of users are similar to that of level 3. But the users in this level do not have any right to modify the files. They can modify their own profile, access files in their department and other department. For example students in the university can only access their files, modify their profile. That's all they can do. They do not require higher security frame work because of their access rights. As they are in a corporate network they will need a proper security frame work. They can be considered as the 10% of the users in the survey discussed above.

**Levels of users in General sector*:*** The non corporate users generally do not require the level of security as the corporate users need, although they have vital information to protect. They can be classified in to three levels which are given below

**Level 1:** This level user has the highest level in non corporate users. They are the people who have home offices, and users who are connected to their house network. They are mainly the people who use the Hotpoint where the service is available. For example users who sell products on eBay or even a stock broker who need constant update of market to do better business. They are not a big corporation. They are people who do their business. They check their update on the market and also do the banking on net. Their service is mainly dependent on their network service provider. Like the users in level 3 of corporate network who are governed by the rules and regulation of that certain corporate network these users have certain policies by the service provider. Level3 users in corporate have to follow rules of the corporation, here they are give certain policies which should be followed for their protection, following not following is their choice. Here the user is independent unlike corporate user.

**Level 2:** This level users are the users who do not get connected to any network. They only access the check their mails and surfing the net. They are also the users who use the Hotpoint to get connected to the network. They mainly use the internet for fun rather than work. For example the user access net where they don't have any computer to access their mails and surfing. They are in some way similar to user level4 in corporate users.

**Level 3:** The users in this level are the users who do not have any access to any of the connectivity. They use their mobile devices only to send and receive calls and also SMS. These are the users who do not need any protection. They are the users who either do not have device which is not advanced enough or either they are ignorant of the functionalities of a device or even both

Applicability of ISO 17799 Standards to each Level:

Corporate user:

- 99+9 controls can be Applicable Level 1 users
- 58+1 controls can be Applicable to Level 2 users
- 33+3 controls can be Applicable to Level 3 users
- 31+2 controls can be Applicable to Level 4 users

General User:

- 15+15 controls can be applicable to Level 1 users
- 9+9 controls can be applicable to Level 2 users
- 5 controls can be applicable to Level 3 users

*Note:* + X are the controls which can be applied to the users depending on the situation.

Similarities between level:

- 21 controls are similar between level 3 and level 1 in both the levels.
- 16 controls are similar between level 4 and level 2 in both the levels.

# 7 Conclusion

Mobile devices as known are changing. With new versions and new features included in to the mobile devices, making it more and more advanced each day. As they are becoming more and more indispensable devices, both in organizational and general level. All though mobile devices provide wide varieties of benefits they are at threat and pose a great danger both to the network as well as the device. The PIN authentication lacks in security. By the observations done in the above sections about the authentication of the mobile devices by PIN is quite questionable. The connectivity of the mobile devices are given an importance as they are the main cause for any kind of attack occurring. The important bits of those concepts were taken in to consideration to provide a framework. A deep analysis of ISO 17799 revealed that most of the standards were applicable which helps to make the base of this framework.

Studies have reveled that there are different levels of users who use a network, both in organizational and general level. The concept of different levels of users which gives a new dimension of security, each level user would need different security standards, by applying this ISO 17799 Standards appropriate policies needs to be applied. The framework suggested may provide a possible solution to many security issues.

# 8 References

Acusis India, 2007 - organizational hierarchy http://www.acusisindia.com/AIP0302/AcusisCompany/Associations.asp

Bitpipe, 2006 – Mobile device Security http://wp.bitpipe.com/resource/org_1108588893_863/Mobile_Device_Security_11579_edp.pdf?site_cd=bp

CIA, 2006 https://www.cia.gov/cia/publications/factbook/index.html

Clarke, Furnell, Rodwell, Reynolds, 2002 – "Acceptance of subscriber authentication methods for mobile telephony devices", Computers & Security

Etrust, 2006- Mobile Workforce Security Survey www.entrust.com/resources/download.cfm/22721/Entrust%202006%20Mobile%20Workforce%20Security%20Survey.pdf

Frost, 2006 – Frost & Sulivan, mobile office report 2004 www.frost.com

GSMworld, 2006 http://www.gsmworld.com/technology/glossary.shtml

Kaspersky, 2007 http://www.technewsworld.com/story/40124.html

OstermanResearch, 2006 www.ostermanresearch.com

Spryance.inc, 2007 – organizational hierarchy, http://www.spryance.com/aboutus/team.html