

# Mobile devices evolution and revolution: A cause for security concern

Abdullah Al-Zakwani  
School of Computing and Technology  
University of East London, UK  
Email:[a.al-zakwani@uel.ac.uk](mailto:a.al-zakwani@uel.ac.uk)

## Abstract

*Today's mobile phones are considered as fashion gadgets, communication devices, personal organisers and are rapidly moving toward becoming personal computers. The devices, networks and operating systems are getting ever sophisticated, while the price of devices and network connection is falling rapidly. This has increased the span of mobile users and ability to explore the limitation of the devices for the hackers and crackers. The current authentication mechanism and lack of security tools (such as the lack of good antivirus) should be considered critically and measures should be put in place for the near future. The paper looks at development in mobile technology and revises mobile industry improvements, with regards to security implications and attempts to provide some solutions.*

*Keyword: Mobile devices, security, GSM, Bluetooth technology, authentication and Agents.*

## 1.0 Introduction

The increasing drop in price of mobile devices and connection charges, have brought a situation where the devices are used not only as tools to facilitate long distance communication but also play role of personal computer, organiser and/or as a multipurpose computer like the desktops and laptops [17]. Nowadays the mobile have extensive power in terms of processing mechanism, random access memory, and hard drives, such as the Nokia N91 with 4 GB. The technology trends and in effects the human development in communication have also introduced security issues that are to be considered critically. Issues such as internet browsing has made younger generation to embrace the technology and learn it well, thus providing learning interest to the new generation. However the lack of security on these devices is currently starting to worry many in the industry. The importance of mobile telephone to the community and its controversial implication are elaborated in [16]. He argues that "mobile phones are important to this population because they can compensate for missing or reduced physical capability. Another approach is that the mobile environment itself can reduce capability. Features that help some people compensate for reduced capability help others amplify average ability." At the moment mobile usage ranges from being a simple communication means to seriously data storage device with computer like capabilities. Many in the business industry are already using mobile phones for internal E-Mail exchange that also facilitates download and upload of data. Due to these issues security needs to be taken seriously in mobile phone devices and architectures needs to be developed to protect sensitive data on the device, over the air, in the cell, and in the server. TrustDigital [23], put it this way "your sensitive information, patient information, client financial information and competitive intelligence are now lost on the subway".

This paper discusses the current structure of security implementation, the suggested structure of security implementation and suggesting new measures to handle security issues. The paper is divided into four sections starting with the Operating Systems (OS) and devices improvement which also emphasises the network capabilities. The service orientation of mobile devices and the security issues (authentication and viruses). Suggestions to the solution to the issues encountered are given thereafter.

## 2.0 Mobile systems evolution and revolution

Mobile devices are normally very small and required too many functions apart of communication (making a call). However, all the mobile devices are classified by certain characteristics. Below are common mobile devices characteristics provided in [2], and [24]:

- Limited memory
- Limited disc space
- Limited screen size
- Low power consumption
- Restricted user input facilities

Most of these characteristics are being overturned and mobile devices are increasingly striving to take over laptops and even desktops. Improvements in devices capability, capacity functionality have proved to quickly be on the rise. Among all of these, the operating systems (OS) play the most important role on this development front.

## **2.1 The evolution of the Operating Systems**

The capability of the mobile devices improvement is highly credited due to the introduction of formal Operating Systems. The current OS functionality is a complete revolution to what was originally running the mobile phone devices. In the early years of mobile devices introduction, the devices did not have formal OS in that each device had its own machine code that ran the device. This code was rigid and offer no control and capability for third party developers [14]. However since the introduction of Palm, Symbian and Microsoft Mobile Windows operating systems, this problem has been solved. However, one could say the trend of computing environment is that every solution introduces its own problem. This has given the capability to third party developers (including hackers) to be able to create software which are sometimes buggy (sometimes the bugs are intentional).

## **2.2 The capability of operating systems**

Operating systems have moved from being each manufacturer has their own machine code running the device to a unified OS developed by third party manufacturers - like Symbian and Microsoft. What we were able to do and what we can do today is not only to be praised on the expansion of memory and processing capabilities as even with all this power third party developers would not be able to rapidly develop software without the uniformity of OS [26].

## **3.0 The growth of network system**

The ability to perform certain tasks on mobile systems today is due to the introductions of more powerful OSs and network structures. They have caused many changes to the perception and functionality of mobile devices. Here are some of the benefits of improvements:

- More dependency on devices
- More dependency on saving data on mobile[6]
- Bioinformatics aiding the doctors to get patient info on the spot
- Home devices connection and detection structure

### **3.1 Network system capability**

Due to the increasingly network function growth, many services are being deployed into the market, with the capabilities provided by the extensive network of mobile devices [22]. And Third generation (3G) devices provide low broadband type of signals that allow high speed connections [10]. These capabilities produced products like home automation systems. The Home automation system is currently under market focus, because it allows many useful and highly marketable functions to take place. For example, imagine going home from work on a very cold day and be able to switch on your heater an hour before you get home.

The market interest has caused many specifications to be produced which include Consumer Electronic Bus (CEBus) [7], European Home System (EHS) [9] and much more. These specifications and technology behind them is functioning by integration to network technologies such as Integrated Services Digital Network (ISDN), Asymmetric Digital Subscriber Line (ADSL) and even cable TV (CATV). However the basic characteristics offered by these standards are mentioned in [25] as “plug-

and-play compatibility, simple installation, distributed control, multiple applications, and future-orientation”.

The home automation system solution could possibly be achieved by using a specialised server to route the messages that are to be used to perform function to the home devices [19]. In [4], it is envisaged that this structure would “leverage limited resources to provide confidentiality, authentication, authorization, and integrity for remote monitoring and control of home automation devices”. Also creating a connection point into the house and using SMS to a contact point on the system that would activate the home network only when the user is close by. The first sceptic on this structure is this will put an extra burden to the client as he has to send that SMS message. However using a device based software the phone could be configured to detect the home receiving device and when the device is detected, it sends and structure the SMS message.

### 3.2 Possible security threat

With the resource capacity (memory) and processing power on the current mobile devices it is clear that complex algorithm can not be preformed on these systems. Therefore, it is incapacitated to use public-key encryption as is used in the normal computing environment found in the application layer [13]. The major problem on mobile devices is that the processing capacity is very small compare to desktop computing and thus if the information is ciphered with complex algorithm, which could take to long to process the encryption and even crash the system with work load. A better encryption mechanism for small confined devices is AES symmetric ciphering which is the bases on Java phones [15]. In [15] found that typical Java mobile phone device would handle just over 165 Kbits/s for AES encryption and 105 Kbits/s for AES decryption. This is much better mechanism as the devices have extensive capabilities to perform these functions. However, a better suggestion is to use an encryption mechanism that could be applied in stages (of the file download or upload) such that each stage is dealt with and get displayed as it is being encrypted or decrypted.

The MIDlet uses cookies in communication mechanism to allow a device based software to communicate to server based software. This communication structure is similar to that of web browser and the server. However, there is an important difference between MIDlet applications and web applications regarding cookies interchange as in MIDlet application the client software has to explicitly send the session cookie back to the server in every request which in turn verifies the validity and authenticity of the MIDlet.

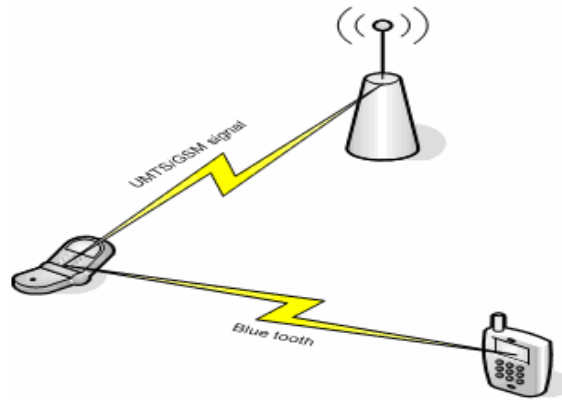
## 4.0 Issues on Wireless technology

Security needs to be considered very serious in terms of mobile devices and radio networks - Bluetooth, WiFi etc. - as radio signals can be easily intercepted. To avoid spoofing and eavesdropping, Bluetooth devices have built-in security. The security provided includes authentication and encryption. In [10], it is confirmed that “Authentication is used to determine if the sender/receiver is authorized, and the encryption is used to prevent eavesdropping on the radio signal”; and suggested three security features:

1. A challenge-response routine for authentication prevents spoofing and unwanted access to critical data and functions.
2. A stream cipher for encryption prevents eavesdropping and maintains link privacy
3. A session keys that can be changed at any time during a connection.

These features can be simplified using table 1 below.

Security Type	Size of token	Responsible party	Function
The Bluetooth device address	48	User	Challenge response
A private user key	128	network	Stream cipher
A random number	128	device	Session key



Threats in this system include tapping into other's mobile via Bluetooth and can be used to make a call, or log into the net at the user's expense. Even more complication and threats are poised due to the ability of piconet. Piconet is a small network formed by Bluetooth devices. When piconet is formed Bluetooth communication changes from its normal peer-to-peer network structure to master-slave structure, the slave devices are synchronized to the master device's clock and hopping sequence [10].

Bluetooth radios are symmetric structured so that any device could be the master or the slave. However in the piconet this decision is done during the first connecting (of the first two devices) and normally the connecting device acts as the master. However it is possible to reverse the role in the piconet mechanism [10]. One can see the threats poised due to this structure of communication. A hacker can sneak into the piconet and swap its role to master by using simple tricks and sending a message saying, 'I am the administrator, and there was a fault in the system! Please press OK to get rectification'. Most of the users would respond by pressing OK in this situation. However gaining access into a Bluetooth network without authentication is difficult as its frequency hops (1600 hops/s) makes it difficult to tap into.

#### 4.1 Push to Talk (PoC) system

This provides an easy platform for hackers to gain access into user's mobile devices and remotely manipulate them. PoC is activated by a GPRS request using XML based code [18]. The code that is required for establishing communication is provided freely by Nokia [18] and looks like the example below:

```
<characteristic type="APPLICATION">
  <parm name="APPID" value="w-nokia-poc-group"/>
  <characteristic type="RESOURCE">
    <parm name="URI" value="MyFriends@poc.nokia.com"/>
    <parm name="NAME" value="MyFriends"/>
    <parm name="FROM" value="my.friend@poc.nokia.com"/>
    <parm name="FROMNAME" value="Friend"/>
  </characteristic>
```

This message would be addressing;

APPID: "w-nokia-poc-group" — Push to Talk Group Invitation

⌚ Parm: APPID: Must be "w-nokia-poc-group"

⌚ Characteristic: RESOURCE:

- Parm: URI: Group Uri (PocGroupUri)
- Parm: NAME: (PoCGroupNickname) Group name, *optional*
- Parm: FROM: (PoCInviterUri) Inviter Uri, *optional if FROMNAME exists*
- Parm: FROMNAME: (PoCInviterNickname) Inviter's name, *optional if FROM exists*

Here an experienced programmer or hacker could simply embed a few hidden extra lines that would allow this message to change into something else as the receiver expects the message. The ability to code calling algorithms using J2ME and LOG4J will give easy access for hackers to make remote calls.

## 5.0 Mobile Security Structure and its problems

Currently the firewalls and antivirus companies have started to move into the mobile phone (and other mobile devices) world. It is important to deal with the malicious programmes, though presently, the focus is not in making the code not being executed but making sure it does not cause the damage intended [3]. This secures data while on the device but even more important during transfer through the radio networks. Radio network consists of scattered waves which by knowing the right wave length one can easily intercept a signal and read it [14]. Other issues regarding data transfer are similar to those of desktop computers where one can hack into people's e-mail account. User authentication is another area where serious issues may arise from (e.g. one using other's connection to make expensive calls, meanwhile data is naturally exposed when the device falls into wrong hands). Authentication is normally done by asking the user for a Personal Identification Number (PIN). However in terms of data, this is normally useless as most of the data will be on the device and not the Subscriber Identity Module (SIM). PIN only protects the SIM let alone the fact that the PIN could also be easily cracked [3], [12]. Mostly there is a password on the device to protect the data from being accessed. As the data is not encrypted in the device it is even easier to simply break the device and remove the internal memory block and read it using other device. Thus data encryption is an important field to be explored in mobile industry.

### 5.1 GSM Authentication structure

The authentication structure in GSM relies on a key prescribed to the user through the SIM card and its pair being residing in the Authentication centre (AuC). The algorithm used to provide these keys is known as the A3 algorithm. It is explained in [12] that "A3's task is to generate the 32-bit Signed Response (SRES) utilizing the 128-bit random challenge (RAND) generated by the Home Location Register (HLR) and the 128-bit Individual Subscriber Authentication Key (Ki) from the Mobile Station's Subscriber Identity Module (SIM) or the Home Location Register (HLR)". A3 is based on COMP128 algorithm which it generates 128 bits of output to be used for security authentication where the first 32 bits form the Signed Response [12].

Considering that mobile devices that are supposed to be integrated into a network, it is important that security is not only considered in the mobile devices but also the desktops that these devices are connecting to in the network. One scenario that could be viewed in this account is that a program might not be malicious for the mobile device which could simply appear corrupted in the device. However this could be fully functional virus (e.g. trap door) that could upload itself into the desktop and cause harm to the network and not the mobile devices. This type of problem could be handled by managing security policies as [3] explained "software is an issue that needs special attention in the PDA environment".

Other ways of tackling this issue is to use a special data transferring software that builds a bridge between the mobile device and desktop or mobile device to mobile device. It could be programmed that data is transferred and received by a specific port and software translates the data. Using ontology based technology would minimise or even remove many threats in mobile environment. Each device should be equipped with an intelligent agent software that has goals and perform function on behalf of the owner) that performs authenticating question during communication [1]. Agent industry is already establishing itself for ubiquitous computing and security is being revised rigorously to tackle authentication issues and even virus attacks. This is important as mentioned by [2] that “mobile terminals become increasingly sophisticated, the need for robust security also increases”.

## 6.0 Virus attacks and implication for mobile devices

In [8] was reported that “PDAs can become just as vulnerable as desktop systems to viruses, mobile code exploits and spam” could be a frightening sentence to those already starting to rely on mobile devices to do many important task like saving critical data (for portability). But, [11] *also* reported that “communication security expert’s do not all agree that cell phone and mobile device viruses pose imminent threats to consumers. Whether virus attacks become a problem in six months or five years might depend on how cell phone carriers react now to the threat potential”. In light of the current security problems antivirus experts have already started delving into antivirus solutions. Symantec (the Norton Antivirus producers) has introduced the Mobile Security 4.0 which aims to protect smartphone using Symbian Series 60 or 80 Operating Systems which is used by many leading manufacturer like Nokia [20]. However most users do not know it exists and even those who know about it mostly cannot update their systems. This is due to its cumbersome nature and lack of good HCI.

A short list of current discovered virus targeted to Mobile Devices exists. And these virus ranges from being very serious to playful ones. As explained in [11] that “most of the viruses targeting mobile devices to date have been proof of concept rather than fully developed attack code”. These viruses caused small damages like application disabling and the worst case complete mobile shutdown that could be fixed simply by resetting the phone to factory settings [11]. Here are some of the viruses that caused extensive damage to the device:

- Skulls - which was discovered in November 2004 is a Trojan horse that pretends to be a visual theme for Nokia 7610. It attacks the phone and disables all applications except voice calling. Its signature is that it turns all application icons into a skull thus confusing the user to what icon is for what function. This virus attacks Symbian Series 60 and spreads via Symbian shareware sites.
- Win CE BRADOR - was discovered in August 2004, opens the TCP/IP port and accepts commands remotely, also capable to uploading and downloading files to and from the device and trickily asks to be installed. It opens the port by sending an email to its creator which is normally the same way it came into the system. It is only able to infect Windows CE.
- Qdial - was discovered in August 2004, it is created to make money for the creator. It sends an SMS message to a premium rate number. The user than get charged for the message. It infects Symbian Series 60 via the Mosquitoes game downloaded from the Internet.
- Dampig - was discovered in March 2005 disables Bluetooth UI, system file manager, messaging applications and the phone book. The major problem is that corrupts the uninstall file so that it can only be uninstalled by being disinfected. Infects Symbian Series 60 by pretending to be a crack for version 3.2 of the FSCaller application.
- Locknut.B - which was developed in Feb 2005 crashes an important system component, preventing any program from being launched. It infects Symbian Series 60 by pretending to be a patch for the OS.

## 7.0 Conclusion

Mobile phone and other mobile devices are arguably becoming the preference to the desktops. With ability to remotely linking into home devices on the go and primarily be able to use multiple devices with no hassle of wiring or geographical distance is an appealing notion to businesses and individuals. However this structure is good to the users but it also introduces its own problems. Due to device memory and processing constraints it is currently not possible to use the authentications, data protection and antivirus software that exist on the market [5] as they require too much power to operate. Measures need to be taken to tackle security features like intelligent agent and more robust client server authentications could enhance security and compromise the device memory. For functions like home networks using external authentication server rather than the service provider server could also enhance security. The external server authentication is a good security structure and should work for all contents prodders.

## Acknowledgement

Many thanks to Johnnes Arreymbi, for his guidance and help in finding the required materials for this research and editing the content.

## References

- [1] Al-Zakwani, A., Williams, G. (2005) Agent Security Vulnerability on Network Databases. Proceedings of the Annual international Conference on Advances in Information and Communication Engineering
- [2] Arreymbi, J and Dastbaz, M., (2002) Issues in Delivering Multimedia Content to Mobile Devices. Proceedings of the 6<sup>th</sup> International Conference on Information Visualisation, IEEE Computer Society, London, UK. July 2002
- [3] Aufrieter, R. (2002) Mobile Security — New Needs on New Devices
- [4] Bergstrom, P., Driscoll, K., Kimball, J. (2001) Making home automation communications secure, IEEE Computer 34: 50–56.
- [5] Bresson, E., Chevassut, O., Essiari, A., Pointcheval, D. (2004) Mutual authentication and group key agreement for low-power mobile devices. Computer Communications 27: 1730–1737
- [6] Clarke, N., Furnell, S., Rodwell, P., Reynolds, P. (2002) Acceptance of Subscriber Authentication Methods. Elsevier Science Ltd
- [7] Desbonnet, J., Corcoran, P. (1997) System architecture and implementation of a CEBus/Internet gateway, IEEE Transactions on Consumer Electronics 43: 1057– 1062.
- [8] Dwan, B. (2006) Body Mnemonics in PDA Security
- [9] EHS (1997) EHS European Home System Specification, release 1.2.
- [10] Erasala, N., Yen, D. (2002) Bluetooth technology: a strategic analysis of its role in global 3G wireless communication era. Computer Standards & Interfaces 24: 193–206
- [11] Germain, J. (2005) Threat from Mobile Device Viruses a Sleeping Giant. TechNewsWorld
- [12] GSMSecurity (2006) What algorithm is utilized for authentication in GSM networks? GSM Security <http://www.gsm-security.net/faq/gsm-authentication-algorithm-a3-comp128.shtml> accessed on 01/02/06

- [13] Harbitter, A., Menasce, D. (2001) The performance of public key-enabled Kerberos authentication in mobile computing applications. Proceedings of the 8th ACM conference on Computer and Communications Security.
- [14] Informa (2005) Handset Technology. London: TelecomsAcademy.com
- [15] Itani, W., Kayssi, A. (2004) J2ME application-layer end-to-end security for m-commerce Journal of Network and Computer Applications 27: 13–32
- [16] James, C. (2000) Designing the next generation of mobile communication. Seattle: AOL Mobile / Tegic Communications
- [17] Mupparapu, M., Binder, R., Cummins, J. (2005) Use of a wireless local area network in an orthodontic clinic. New Jersey: The American Association of Orthodontists.
- [18] Nokia (2005) Push To Talk: Invitation Message Structure. Nokia
- [19] Sriskanthan, N., Tan, F., Karande, A. (2002) Bluetooth based home automation system Microprocessors and Microsystems 26: 281–289
- [20] Symantec (2005) Compatibility between WAP connections and Symantec Mobile Security 4.0 for Symbian <http://service1.symantec.com/SUPPORT/> accessed 20/11/05
- [21] T. (2004) Mobile Terminal Security and Tracking. Information Security Technical Report. Vol. 9 No. 4
- [22] Topalis, E., Orphanos, G., Koubias, S., Papadopoulos, G. (2000) A generic network management architecture targeted to support home automation networks and home internet connectivity, IEEE Transactions on Consumer Electronics 46: 44–51.
- [23] TrustDigital (2005) Mobile Edition <http://www.trustedigital.com/solutions/2005mobileedition.asp>
- [24] Vu, P. (2004) Application Development Environment, Warsaw: Forum Nokia- Technical Services and Consultancy.
- [25] Wu, C., Jan, R.(2003) System integration of WAP and SMS for home network system. Computer Networks 42, 493–502 501
- [26] Yi, W., Reddy, C., Ang, G. (2002) J2ME devices: Real-world performance. Performance benchmarks can help device developers build better applications