Ubiquitous Secure Cash Withdrawal

Abdullahi Arabo, Qi Shi and Madjid Merabti
School of Computing and Mathematical Sciences
Liverpool John Mores University
Byrom Street, Liverpool, L3 3AF, UK
{a.arabo, q.shi, M.Merabti}@ljmu.ac.uk

Abstract

We have seen an increase use of technology in contactless payment card as well as access cards that make the same Mifare technology. However, it has been shown that such a technology is carrying serious security flows that allow card cloning by suing a simple personal laptop. The use of mobile handheld devices is expanding rapidly within both the business and individual contexts. These devices are now essential tools that offer competitive business advantages in today's growing world of ubiquitous computing environments. The technology advancement has made it possible to embed more facilities in mobile phones. While they provide benefits, they also pose new risks on security by either the information they contain or information that they can access remotely. Secure cash transaction is of serious concerns in growing use of cash cards and internet transactions. Cash withdrawal card, chip and pin facilities have increasingly been used for business and social activities. This paper will propose the concept of physical browsing and development of a system that will allow users to use their mobile phones to securely withdraw cash from ATM machines. The paper presents the architecture for the M-Cash withdrawal application, discusses relevant technologies and security issues, and provides an analysis of relevant procedures and steps for fully implementing the application.

1. Introduction

There has been a growing use of Radio Frequency Identification Tags (RFID)[1] in different business environments. A typical example includes supermarkets, airline industry and the majority of supply chains. The main advantages of RFID to businesses include the effectiveness of identifying physical objects such as luggage/products; providing good customer services; and facilitating cost reduction and flexibility. In this paper this technology has been used in a new application called Secure M-Cash Withdrawal, a system whereby a mobile phone is equipped with a RFID tag(s) and NFC[2]. The mobile will interact with an ATM machine which is equipped with a RFID reader and writer as well as a banking system. The process of interaction will be utilized using the physical browsing phenomenon. The main purpose of interacting via mobile phones is to improve the security of transactions as well as eliminating the need to use cash/credit cards.

The application of a physical selection/ browsing method used in mobile phones can be categorized into three forms: mainly pointing, touching and scanning [1]. This paper is

[1] System that transmits the identity (in the form of a unique serial number) of an object wirelessly, using radio waves
[2] A short-range wireless technology mainly aimed at usage with Mobile phones

mainly concerned with pointing and touching. Pointing is seen as a long-distance selection mechanism, where NFC is used within a giving range of an ATM machine. Touching is used as a way of sending the required information between the devices as well as capturing biometrical information needed for authentication.

In the proposed Secure M-Cash Withdrawal scheme, the following components are needed: a mobile phone with an ISO 14443 compliant RFID tag and NFC, a cash machine with a RFID reader and transmitter, and a banking system that deals with other operations. Each of these components will be examined. Known security issues[3] and other critical future security threats are addressed accordingly.

Mobile devices offer potential means of making use of various technologies that will result in a more flexible and efficient way of delivering services to customers. Hence, it can be deduced that there are many other applications that can be realized – time and technology permitting. To achieve various functionality and make good use of mobile devices so that people can utilize their potentials.

In this paper, the main focus is in describing the framework of M-Cash transaction and presenting the background and implication of the concept. The main contribution of the paper is twofold, we first provide an understanding of the use and implications of cash transaction in the ubiquitous context and secondly we proposed a novel framework to rectify the problem of insecure cash transaction called M-cash withdrawal. It also provides a framework that would help in a wider understanding of the security issues, protocols, communication mediums as well as predicting the future needs of using mobile devices in ubiquitous environment. We have also provided some of the likely users concerns and addressed the issue of providing services to users based on contextual information.

The reminder of the paper is structured as follows: in section two, we have presented some of the related work done in this area and our motivation for this research. Section three describes the proposed design and architectural framework of M-cash transaction. Section four deals with the issues of network communication requirements and alternatives and highlight the possibilities and options available for the stakeholders. Section five highlights some of the major security issues that need to be addressed and proposed a mechanism to tackle such problems and providing a secure service for the proposed framework. Finally, section six concludes the paper with future direction of study as the implementation of the framework among others.

2. Related work

The physical browsing phenomenon in mobile phones has been used in many applications such as M-Wallet. Mobile payment [2], SMS picture synchronization and booking items in libraries with the use of the touch-me paradigm. Other applications include: goods purchases at vending machines, topping up phones at ATM machines and M-Banking (iMod) from the Citibank portal.

In the UK, people have started to benefit from the development of contactless payment techniques embedded into mobile phones. Nokia phones have been equipped with similar technology used in Oyster cards [13] and made use of the NFC technology. This allows customers to make payment by swapping their phones on special terminals as well as against special posters which can present users with useful local information such as maps [12]. The spending power of the phones is limited to a credit of £200 and a maximum payment per transaction of £10. Also recent development in the banking industry has led to the adoption of

[3] IET Presentation Around the World panel of judges and audiences

the contactless communication technology, e.g. a new contactless Barclaycard has been introduced [14]. The card combines a chip-and-pin mechanism with the Oyster travelcard methodology. The card is considered secure as it is hard to clone or counterfeit. It is important to point out that this new methodology has done little to address the rising concerns of card fraud, the current card in use can be cancelled when it is lost or stolen, same applies to the introduced card, for the cards not to be usable for contactless payment but for other methods of payment after being reported lost seems not convincing enough. It is also worth pointing out it has been reported [19] that a way has been found to hack into chip-and-pin readers to steel customer details I.e. the pin number and card details in which the card can then be cloned and used. On the other hand it even makes this worst in the sense that, a stolen card can be easily used without making the criminal find any means of identifying i.e. the pin or any other information. UniPay as proposed by *Lehdonvirta et al* [15]*[1]*, is another application/framework that looks into the issue of everyday payments with minimal user intervention and taking into account some contextual information.

3. Proposed Design

This paper proposes a novel framework (M-cash Withdrawal) to rectify the problem of insecure cash transactions. In the Secure M-Cash Withdrawal application, the methodology involves both software and hardware platforms, as well as a system's strength. In addition, the design considers the possibility of using a commercial environment to evaluate the use of such technology.

Fig. 1 demonstrates interactions among the components of the proposed Secure M-cash Withdrawal. It consists of a two-way handshake between the mobile phone and the ATM machine as well as between the ATM machine and the banking system. The handshake process is aimed at establishing the authorization of using the services by the user. When the mobile device is activated for usage, the mobile phone will broadcast a signal to RFID readers available within the range. That is, the ATM machine(s) which is equipped with a secure RFID reader and transmitter. This in turn will initiate the handshake process. After a successful handshake the ATM machine will dispense the required cash for the customer and accounting information is updated automatically.

The basic functionality of the Tag manager is to provide an interface for tag readers, to allow multiple applications from different vendors, i.e. banks in this case, to make use of the same tag. A detailed description of the requirement and design for a phone middleware component called Tag Manager is analyzed by Keränen [3].

In order to implement tags that will work without the requirement of any network connection where bandwidth and network connectivity become a problem, this feature is of paramount importance. The Tag Manager can be implemented as a Server, as shown in Fig 2, which is loaded into the tag reader when the process is initialized. The interface can be either via the tag reader interface on the phone, using the mobile phone interface with some added functionality or designing a new interface to handle Secure M-Transactions.

Fig 3 describes the components that facilitate the interaction between the mobile phone/device, the cash machine and the Banking system application.

The architecture is designed in a flexible way that will enable the use of any of the two technologies: firstly, to make use of mark-up languages like (X) HTML, or the Synchronized Multimedia Interchange Language (SMIL) [4].

The second approach will require making use of downloadable applications, i.e. .NET or Java applications that are based on Mobile Information Device Profile (MIDP) of the Java 2 Platform Micro Edition (J2ME) [5].

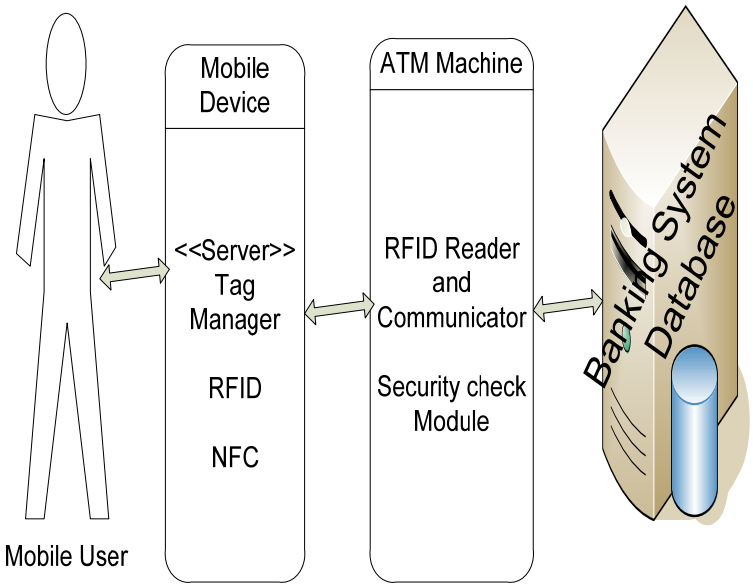

Figure 1. Proposed Design

4. Network Usage

Most mobile phones are equipped with various network interfaces such as WLAN, Bluetooth, GPRS or UMTS. The GPRS signals or co-ordinates will be used for relaying the location of the user in relation to the ATM, so as contextual information of location should be taking into account. The framework is designed to meet the characteristics of MANets and context-awareness in such a way that the user will be able to choose the network that provides high data transfer rates and secure data transaction cost-effectively. This process will be achieved through the use of software wrappers that will enable selection and identification of available communication channels based on the location of the device in an ad-hoc manner.

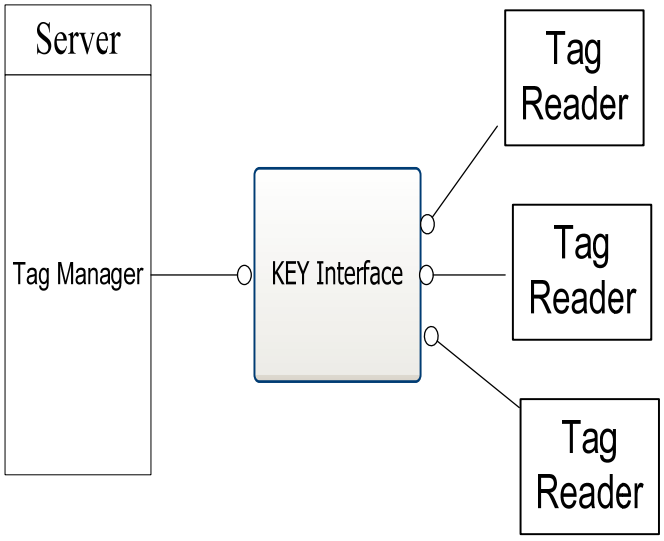

Figure 2. Tag Manager Interface

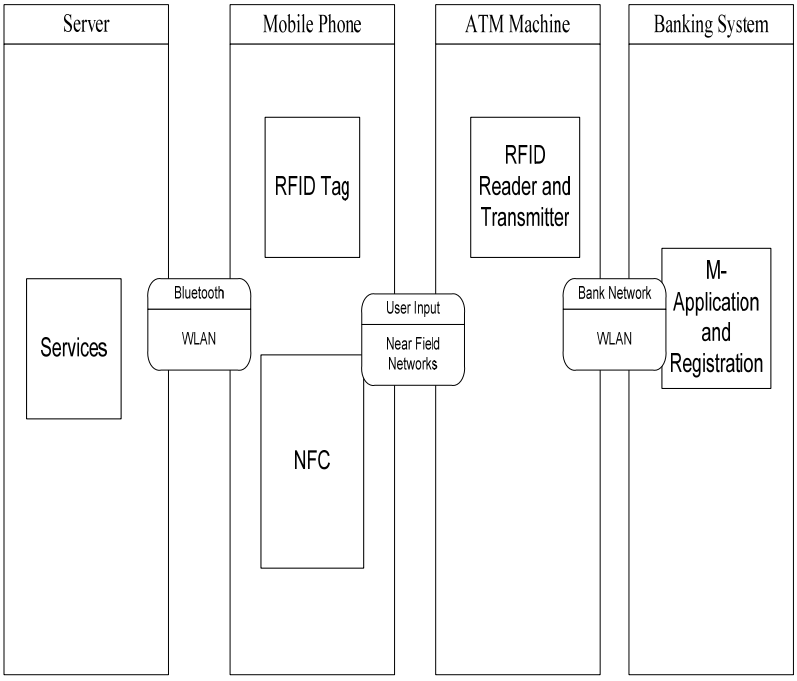

Figure 3. The Architecture

Alternatively, the use of WLAN which is provided by the banking system will be used for the communication, for which an authentication process can be performed before allowing access to the network. In this case security will be better monitored and control. However, one of the main drawbacks of such usage is the risk that a device will try to impersonate identities. Impersonation attacks occurs where and external node *E* or a malicious node *M* try to impersonate the actual node *A*, by making the application believe that either *E* or *M* is the actual node *A*. To prevent this problem the architecture must authenticate the target node during protocol execution. Another mechanism is the use of multi-factor authentication as described in Fig 5 is used to reduce the impact or possibility of this problem, as the entity is linked to the physical devices by way of identifying themselves using biometric information. *Glynos et al,* as provided a discussion on the issue of preventing impersonation attacks and augured that a single factor authentication scheme cannot effectively deal with this problem. However, a combination of well known cryptographic mechanism with a different source of identification is the only way of minimizing such attacks– hence in this architecture we proposed the use of biometric as the second identification factor.

As highlighted in Fig. 4, the application will use all possible available networks in this context. However, it is more preferable if the user will not pay for any network usage or traffic. In this case, Fig. 5 illustrates how to make use of Bluetooth or a WLAN access point that might be provided by the Bank. If not, then the possibility of making use of existing mobile networks like GPRS or UMTS is provided, whereby the bank will pay for the traffic or the cost will be shared between the bank and the customer at a reduced rate – however, this is a very costly method and should be avoided where possible. This enables some elements of user-centricity, making use of contextual information [16] – here the availability of relevant communication channels for the user to choose and allows privacy control and settings.

Another option will be for the Bank(s) to have a dedicated private network for this service. The required information regarding network availability will be provided by the near field network or by the preconfigured Banking network within the application itself. If a near field network is used, there is a need to have some mechanisms that will handle configuration between available networks around a given geographical area as near filed networks will be out of range; this process will be achieved via the use of wrappers.

5. Security consideration

The Secure M-Application deals with information transfer and financial transactions. Hence, the security elements considered during the design and implementation stages consist of making sure that the RFID and NFC used are in compliance with the ISO 14443 standards. One of the major security issues when dealing with proximity cards on ISO 14443 is the Relay Attack. Relay attack effectively allows an attacker to borrow the victim's card without the victim having knowledge of it. The borrowing can only last for a short period of time and there is no need to having any physical access to the victim's card. Relay attacker is well know and *Hancke* [17] has demonstrated with a hardware designed purposely for investigating such attacks, an attacker can successfully execute a relay attack against ISO 14443A contactless smart card, up to a distance of 50m. Replay attack is another problem when dealing with RFID values and identifiers.

As a result of relay attacks, a new crime of digital pick pocketing arises where an attacker can pick pocket while standing next to or merely waking pass his victim, relay attacker are normally executed in order to impersonate and therefore gain benefits from another user. One way of minimizing or eliminating such attack is to disable the automatic activation of contactless cards when close to a reader. In our proposed architecture, communication only begins when the user activates his/her mobile devices by pressing a key to activate the system. After that the RFID tags within the system will be activated and ready for communication. This eliminates the problem of randomly executing relay attacks the victim pas through or near an attacker unless if the victim activates their device for a long time while not suing it. The architecture also have a mechanism of automatically deactivating the mobile devices after few seconds without receiving any commands or message from the user or been used.

WLAN technologies are equipped with the latest encryption protocol standard.

WPA addresses these issues by providing password protection for access control and encryption for privacy.

The wireless security protocol 802.11w which is to be introduced in April 2008 has promised to provide facilities that will prevent denial of service attacks and make use of the AES encryption standards. WPA only deals with access control and privacy issues. That is determining who is allowed to enter your network and hiding information from hackers who may try to intercept information during transmission.

However because the Secure M-application is more susceptible to security threats, the design incorporates other security measures such as making use of Biometric data, as a further identification. It can utilize any of the fourteen different types of biometrics that fall within two categories, namely, those that measure behavior and those that measure physical traits [9]. Any of the Biometric information within these types can be used in identifying users, by making use of individual anatomy or physiology, that is either deeply ingrained into the skin, or other behavioral characteristics, or it can be a combination of the two. Hence, the data will be used as a unique personal attribute for security and authentication purposes. Since the focus of this paper is not on analyzing biometrics as a means of authentication, details on

the use of biometric can be found in [10, 9] and using biometric data to generated encryption and decryption keys [11]. Fig. 5 describes the process of authentication using both password/pin and biometric data. Both authentication factors are needed to match the stored once before allowing access to transactions.

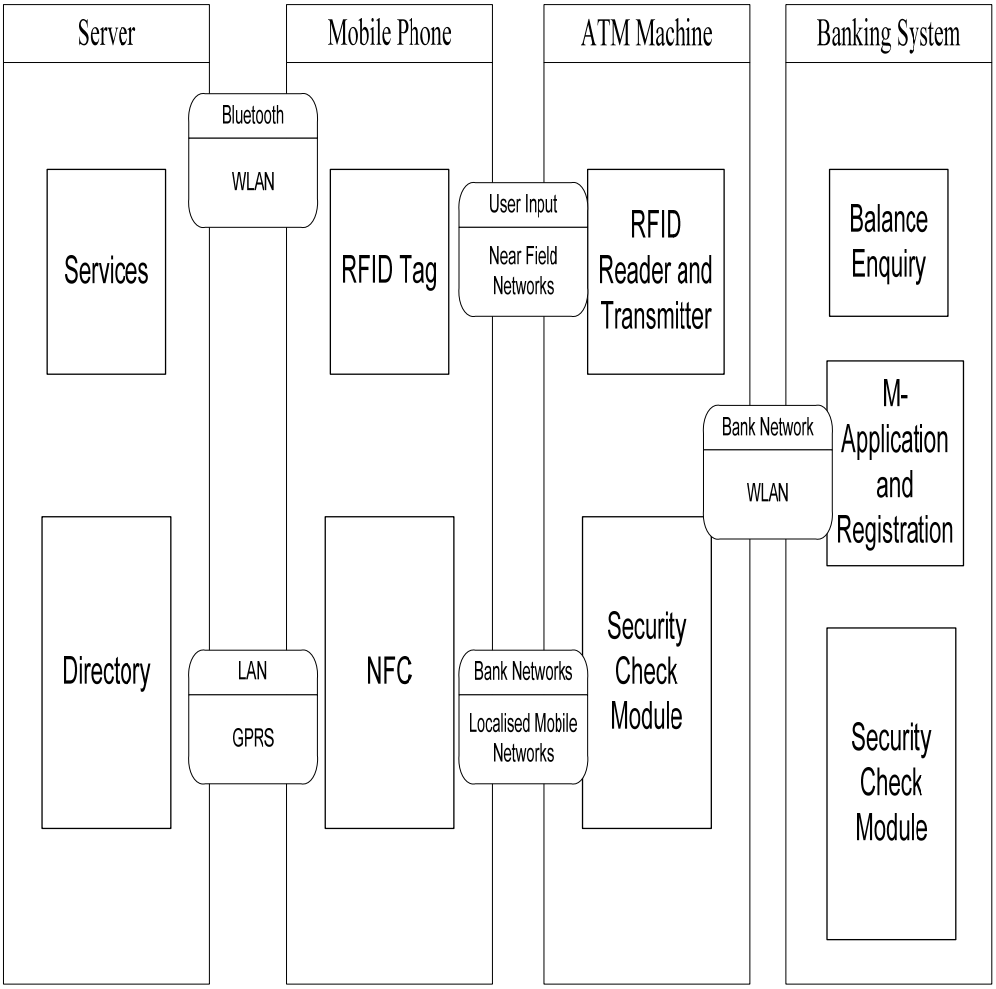

Figure 4. Architectural components

Otherwise the access will be automatically denied. This process will be able to reduce the effects of a brute force attack, as millions of combinations need to be tried before gaining access and as only 3 tries are allowed this should prevent such attacks from occurring. Also it is important to point out that a single sign-on process will improve the reliability of identity management and access control. Having this application as the security measure, the Secure M-Cash Withdrawal will be able to provide an excellent wireless identity management that will remove the current risk of identity theft which accounts to approximately 7.5% of payment card fraud [18] and meet the required security standard of implementing the secure M-cash withdrawal and other M-applications.

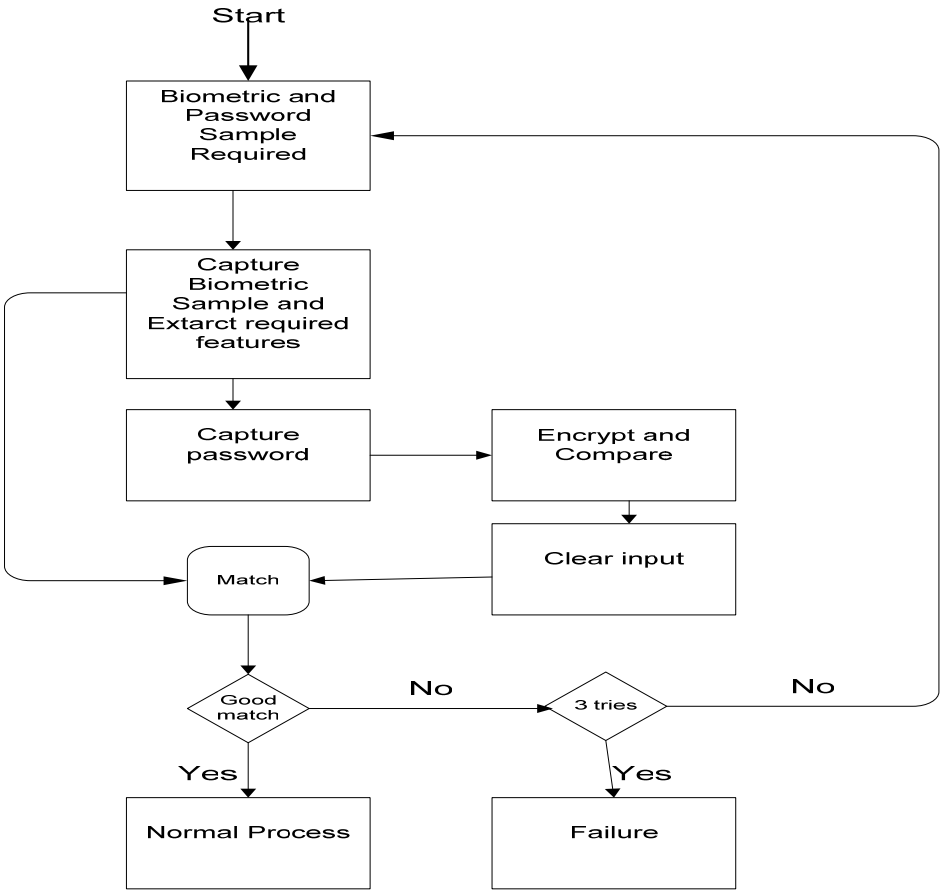

Figure 5. Authentication Process

6. Conclusions

This paper presents a novel architecture – M-cash withdrawal- that can be used as a means of interaction between mobile phone/devices, an ATM machine and a Banking application for the purpose of withdrawing cash. The design of the proposed secure M-cash withdrawal allows the use of mobile phones as a tool of interaction and provides flexibility through robust identity management architecture. The first part of the architecture is in the process of being implemented and all the process involved has been analyzed and justified where possible. As part of our future work, we will be providing in-depth analyses of the design and protocols to be used for the purpose of withdrawing cash. The Secure M-cash has examined the possibility of making use of similar approaches/techniques (RFID and NFC) for other applications and already there are some applications that have adapted this strategy. The Secure M-Cash Withdrawal architecture has been defined, it will form as a foundation for future work within this area, which includes, protocols design, and implementing a PC based simulation of the architecture and implementing the system.

References

[1] Välkkynen, P. Korhonen, I., Plomp, J., Tuomisto, T., Cluitmans, L., Ailisto, H. and Seppä, H. "A user interaction paradigm for physical browsing and near-object control based on tags": in *Proc. Physical Interaction Workshop on Real World User Interfaces*, (2003), 31-34.
[2] *Lauri Pohjanheimo, Heikki Keränen and Heikki Ailisto, "*Implementing TouchMe Paradigm with a Mobile Phone", ACM International Conference Proceeding Series; Vol. 121, 2005.
[3] Keränen, H., Pohjanheimo, L., Ailisto, H. (2005) *Tag Manager: a Mobile Phone Platform for Physical Selection Services* in *International conference on Pervasive Services (*ICPS 2005). Santorini, Greece. pp 405-412.
[4] Synchronized Multimedia Integration Language (SMIL 2.0), W3C Recommendation 07 August 2001 http://www.w3.org/TR/smil20/ .
[5] Java 2 Platform, Micro Edition (J2ME). http://java.sun.com/j2me/ .
[6] M. Johns and G. Marsden *"Mobile Interaction Design"*, Wiley and Sons Ltd 2006, pg 178-182.
[7] *"Openwave Phone Simulator"* http://developer.openwave.com/dvl/tools_and_sdk/ phone_ simulator/ .
[8] European ATM Security Team, *"European ATM Security Team"*, Diebold, Incorporated 2006, http://www.diebold.com/rd/whitepapers/atmfraud&security.pdf .
[9] A. Jain, R. Bolle, and S. Pankati, "*Biometrics: personal identification in networked society*", Kluwer Academic Publishers, 1998.
[10] J. Chirillo and S. Blaul, "*Implementing Biometric Security*", Wiley & Sons, 2003.
[11] S. Hoque, M.C. Fairhurst, F. Deravi, W.G.J. Howells, "*On the Feasibility of Generating Biometric Encryption Keys"* IEE Electronics Letters, 41(6), 309-311, 2005.
[12] Cellan-Jones, R., *London starts digital cash trial* in Technology correspondent, BBC News Online, http://news.bbc.co.uk/1/hi/technology/7117213.stm. 2007: UK.
[13] Blythe, P.T. *Improving public transport ticketing through smart cards*. in Proceedings of the Institution of Civil Engineers: Municipal Engineer. 2004.
[14]New Barclaycard is touch-and-pay in BBC News ,*http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6945991.stm*. 2007.
[15] Vili, L., Hiroaki, Kirmura, Hayuru, Soma, Tatsuo, Nakajima, Hitoshi, Ito; *UniPay: Conducting Everyday Payments with Minimum user Involvement; In* CHI 2008 proceedings 2008. Florence-Italy.
[16]Dimitris, Glynos, Panayiotis, Kotzanikolaou, Christos, Douligeris; *Preventing Impersonation Attacks in MANET with Multi-factor Authentication; In* Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2005. WIOPT 2005. 59- 64
[17] Gerhard Hancke, A Practical Relay Attack on ISO 14443 Proximity Cards, in http://www.cl.cam.ac.uk/~gh275/relay.pdf accessed 11/08/08
[18] APACS, "Card fraud losses continue to fall," Press Release, APACS, March 2007, http://www.apacs.org.uk/media_centre/press/07_14_03.html
[19] Story from BBC NEWS: **Device 'steals chip-and-pin data',** http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/7557956.stm, Published: 2008/08/13 10:06:40 GMT

Authors

Abdullahi Arabo graduated from University of Wales Swansea in 2007, where he obtained his MEng Computing qualification. He is current working as a Researcher in Network Security for the School of Computing and Mathematical Sciences in Liverpool John Moores University UK. He is also a PhD student under the supervision of Dr Qi Shi and Prof Madjid Merabti within the filed of Ubiquitous computing and MANets. Mr Arabo is currently a member of the British Computer Society (MBCS). He is presently working on a project funded by EPSRC looking at the security implications of interactions between devices in real world scenarios, in collaboration with Thales Research and Technology UK. In which the project will form part of his PhD studies. He has been involved in various conference committees TPC (i.e. CCNC Short Papers), paper reviewing of many other conferences and journals (i.e. IMIS 2009, SecTech 2008, IJNS). His research interest includes: Ubiquitous Computing Security, Context-aware and User-centred applications, Identity Management, Mobile ad hoc Networks, Sensor Networks, Network Security and Secure Systems of Systems Component Composition. He is involved in various projects within these areas.

Qi Shi received his PhD in Computing from the Dalian University of Technology, P.R. China. He worked as a research associate for the Department of Computer Science at the University of York in the UK. Dr Shi then joined the School of Computing & Mathematical Sciences at Liverpool John Moores University in the UK, and he is currently a Reader in Computer Security. His research interests include network security, security protocol design, formal security models, intrusion detection, ubiquitous computing security and computer forensics. He is supervising a number of research projects in these research areas.

Madjid Merabti is a graduate from Lancaster University where he gained a PhD in Computing. He is now Professor of Networked Systems. His current research interests include architectures, services and protocols for distributed multimedia systems, including multimedia content and extraction, mobile networks, security, and e-commerce technology support. He is involved in a number of projects in these areas where he leads the Distributed Multimedia Systems Group.