A Two-Phase Authentication Protocol Using the Cell Phone as a Token

Carl Adams, University of Portsmouth, UK, carl.adams@port.ac.uk
Alexandros Dimitriou, Nimbus Partners, UK, alex_dimitriou@yahoo.gr

ABSTRACT

In a climate where personal information is 'freely available', such as through the internet and via social networking sites, information based authentication systems have inherent weaknesses: Individuals are leaving a rich information 'footprint' which is easily accessible to others, and so reducing the currency of private information for authentication purposes. Biometric approaches are expensive and lack user acceptance. Token based authentication offers practical alternatives to increase levels of security for remote access and online transactions. This paper extends an existing token mechanism for authentication using mobile/cell phones and presents a novel protocol to address some of the existing limitations and provide wider applicability. The paper hopes to contribute to theory by bringing an information richness perspective on authentication and, contribute to security practice by providing a route to increased security based on the ubiquitous mobile/cell phone and software tokens.

KEY WORDS

Two-Phase Authentication, Mobile Token, Remote Access, Software Tokens

INTRODUCTION

As the trend towards more online economic activity increases, so too does the need for secure mechanisms to conduct transactions and authenticate users (Kotadia, 2007; McClure et al., 2005). There are generally three primary methods used for authenticating the identity of remote users:

1) Using something the users knows (e.g. password, personal information)
2) Using something the user has (e.g. private key, electronic token) or
3) Using something that is unique to the user (e.g. finger prints and other biometrics).

This paper identifies limitations with the first and third approaches, namely systemic problems with information based approaches, high costs and user acceptance with biometric approaches. This leaves approaches based on using 'something the user has', such as a token, as the most likely avenue for practical improvements to authentication. This paper focuses on using software tokens as a route to improve authentication via the ubiquitous mobile devices.

Remote access to systems, such as online bank accounts, using authentication tokens typically involves a two-phase authentication process where separate identification tokens are used to supplement the use of passwords (e.g. Steele, 2005; Sery, 2006; Schneier, 2005). A promising two-phase authentication protocol is suggested by Schuba et al. (2004). It offers the potential for wide scale adoption of authentication tokens. This uses a mobile phone, or cell phone, and the mobile telecommunications infrastructure as a separate channel for handling the token distribution and checking. Schuba et al's solution is part of the Internet ID approach, collaboration between Ericsson, Gieseck & Devrient and Vodafone.

The use of a cell phone has many interesting characteristics which make it ideally suited to supporting widespread adoption of authentication tokens. First, given the very high adoption levels of cell phones, it is very likely that users with online bank accounts will also have cell phones. Second, cell phone users are very attached to their cell phone, typically continually carrying it around with them and using them frequently (Adams et al., 2003). Third, the cell phone with its separate telecommunications infrastructure provides an independent channel for distributing tokens as well as a separate registration and checking mechanism (Schuba et al., 2004). Fourth, cell phones offer an ideal medium for securely keeping the electronic token and performing any processing needed for local management and checking of the token (Schuba et al., 2004; Jammalamadaka et al., 2007): the convergence of several technologies has made the mobile phone a sophisticated computing device (Adams & Fitch, 2005). Fifth, given the close attachment and frequent use of cell phones it is likely that if a cell phone is lost or stolen, it would be noticed and reported quickly.

However, the protocol suggested by Schuba et al. (2004) (see figure 1) does have its weaknesses. There is increased complexity with the reliance on the mobile network as well as the Internet network for each transaction: Two servers will be needed, one on the cellular telecommunications infrastructure and the other on the Internet, with both servers needing to communicate, coordinate and share information to authenticate each transaction. Such a system would involve relatively high management and coordination costs for the authentication process. Other alternative options that use SMS messaging to distribute tokens would also rely on the mobile telecommunications infrastructure. In addition, though SMS messages are usually delivered quickly, say within a few seconds, they are not always timely and delays of several minutes or more could be experienced (a fact that has left lifeboat crew and other emergency services relying on pagers instead of SMS). For transaction based systems, extra delays of more than a few seconds would severely impact the usability of an authentication system.

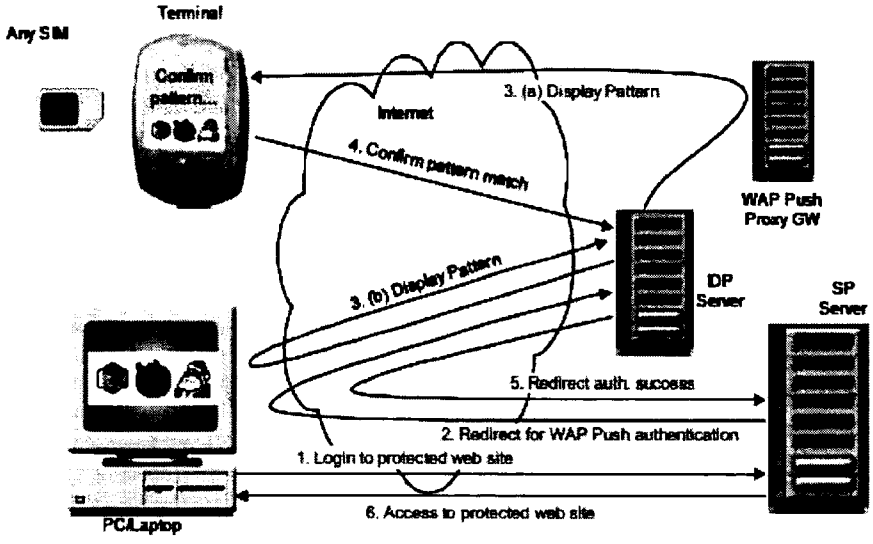

Figure 1. Approach to Two-Phase Authentication (Schuba et al, 2004)

Schuba et al's (2004) solution, and similar approaches, does provide the opportunity to increase security by making use of the ubiquitous cell phone system for processing tokens in a two-factor authentication process. However, it does involve a high level of complexity and inherent timing problems for transaction authentication. The aim of this research project is to explore possible improvements and simplifications to the token based authentication model suggested by Schuba et al. (2004). This paper describes the development of a simplified protocol involving a two-phase authentication process which also uses the ubiquitous cell phone but without the high management and coordination overheads for each transaction. The use of the cell phone, as in Schuba et al's (2004) case, is a good starting point for two-factor authentication for the reasons discussed earlier (e.g. high level of adoption, and likely to be carried by users, and a good channel for electronic tokens). The Scuba et al. approach makes a particularly good starting point since it is based upon open standards and designed for wide scale adoption.

The rest of the paper is structured as follows: First, some background is given on security and the need for better security than that offered by password based systems, and different alternatives to two-factor authentication are discussed. The paper then examines information richness as a base for considering authentication mechanisms. The development of a new two-phase authentication protocol is described along with testing the application on a Nokia platform. The paper concludes with discussion of future two-phase authentication making use of cell phones and software based token usage.

BACKGROUND:

Two Factor Authentication to Increase Security

The mainstay of security in technology has been the password, as Gollman (1999, p25) identifies "Passwords have separated friend from foe for centuries". For most users, it is problematic to try to remember many online account details each with their own user name and password. In reality, users tend to choose similar usernames and passwords for multiple accounts, the more accounts they have, the more they tend to choose memorable, and guessable, user names and passwords. There has been a trend towards Single Sign-On (SSO) identity management systems (Schuba et al., 2004). SSO is a session or user authentication process that permits a user to enter one name and password in order to access multiple applications. SSO based identity management systems aim to reduce the number of different accounts and passwords that users have to manage. One such example with a wide user base is Microsoft's Passport (Kormann & Rubin, 2000). This enables users to sign onto many different merchants web pages by the users authenticating themselves only once to a common server. The argument is that SSO will actually improve security over having many separate accounts since users can focus on remembering one account's details involving a difficult to guess password rather than trying to remember several accounts with memorable and easy to guess passwords. The other argument is that SSO's raise increased security concerns since all the accounts have one access, they are still based on passwords and the passwords are often stored in cleartext (e.g. Gollman, 1999; Kormann & Rubin, 2000).

Information Richness Perspective on Authentication

Though adding to customer convenience, SSO's have security challenges in critical transactions such as online purchases or accessing bank accounts, and personal details are often used in the transaction process to verify and authenticate a user. For instance Visa's 3-D Secure protocol involves verifying the identity of each cardholder in enrolment and authenticating cardholders during online transactions, based predominantly on the remote user providing personal details. Increased levels of confidence are gained from this approach to authentication. However, there are systemic weaknesses that become clear when we examine some of the theoretical constructs surrounding an information based authentication approach.

Authentication is about ensuring that the person is who they say they are. For this authentication, authorities have to solicit enough personal information from the customer to be confident that the customer is who they say they are. Katos and Adams (2006), (Adams & Katos, 2007) build on Daft and Lengel's (1984) work to develop an information richness view of security and privacy. A wider information richness perspective provides a theoretical base to consider authentication systems and

limitations. For instance, from an information richness perspective we see that the *currency* of privacy and security information is reduced with both

a) the increase in the use of such information and,
b) the increase in the availability of information from different and unintended channels.

For instance, if every corporation collects the date of birth of customers along with their mother's maiden name for authentication purposes then this data would cease to be useful (Adams & Katos, 2007) since this information would effectively be common knowledge on all corporate systems. Anyone with access to a corporate system would have access to that data. The usefulness of personal information decreases with the number of entities having access to that information.

In addition with ICT there are many channels for flows of personal information, many unknown or unintentionally divulged by individuals. For instance, Brunk (2003) focusing on protection of privacy information, produces a comprehensive coverage of unconscious and unintentional flows of personal data. Brunk describes these unintentional data flows as exoinformation, and also identifies that individuals have little or no control over who collects that information and how it may be used. Adams and Katos (2007) draw upon Brunk's work to identify the kinds of exoinformation through different channels that individuals and corporations give out. As an example, consider one of the significant trends in society, the use of social networking sites (e.g. Randall & Richards 2008). There is a wealth of embedded exoinformation on such sites, information that covers not only individuals active in socializing sites, but their friends and relatives as well. Information such as age, data of birth, own or mother's maiden name, names of family members and pets, home cities, previous addresses, current addresses, hobbies – in fact all the information that is often required as part of an authentication and registration scheme. Outside of social networking sites, there is a wealth of personal exoinformation from employer web sites (e.g. telephone and contact details, news items etc), citizen registers, corporate web sites and personal websites.

Even if new personal data sets are generated, the currency of these will diminish with each instance used. That is, of course, assuming that it is possible to generate a further set of personal information that customers can remember and use in a meaningful way in an online environment. An information richness perspective highlights some systemic weaknesses for using authentication systems based on using personal information.

Two-Factor Authentication

Increased security can be provided by the use of two-factor authentication. Two-factor authentication is a mechanism in which two procedures are required to authenticate a

user. The typical components of two-factor authentication are first, something you know, such as a password, and then "something you have", such as a token. The token is usually distributed by a different channel to the account channel, say by post or email. The token then acts as a further authentication and security measure over and above the username and password. A common implementation of two-factor authentication includes the password and a small token card consisting of an electronic device which provides the user with a PIN number on a small screen.

Another approach is the use of biometrics as "something you have". Biometrics offer the potential of heightened levels of authentication (Prabhakar et al., 2003) since the users will be using their own unique attributes such as fingerprints, hand prints, face or voice. There is also the potential of increased convenience over traditional methods of personal recognition since the user will always have their biometric identification with them. However, there are challenges in setting up biometric systems, including high costs. For instance, if fingerprint biometrics were used, the users would have to have installed relatively expensive finger print reading terminals on their access devices. Also, users would need to go through some independent administration and checking system to register their fingerprints. This would entail high levels of expense (e.g. technology, infrastructure, management and administration processes for the authentication service providers which would ultimately be passed on to users. The largest barrier to wide spread adoption of biometrics could possibly be the concerns over privacy (Prabhakar et al., 2003). As Ratha et al. (2001) identify, "we have touched on the often-neglected problems of privacy and revocation of biometrics. It is somewhat ironic that the greatest strength of biometrics, the fact that the biometrics do not change over time, is at the same time its greatest liability. Once a set of biometric data has been compromised, it is compromised forever". Ratha et al., (2001) highlight eight points of vulnerability in generic biometric systems and possible attacks, but also show how these threats can be alleviated, all which have cost implications. Biometric two-factor authentications have much potential, but are high cost options and attract wide concerns over privacy issues.

Another approach to two factor authentication has been adopted by banks based on the use of a separate card reader for token management. For instance, Barclays Bank (Barclays, n.d.), the Nationwide bank (Nationwide, n.d.) and the National West Minster bank (NatWest, n.d.) use a separate card reader which has been distributed to their customers who use online accounts. The card reader is a calculator sized device with a credit/debit card slot, customers must carry this with them when they want to do transactions or access account information via the Internet. For each transaction, customers are required to put their card into the card-reader which will ask them to type in their card PIN number. The card reader then generates a unique run time authorization code used to authenticate the online transaction. This approach does provide increased security but has limitations, including the cost to distribute the device to each account holder (over 2 million card readers have been distributed to these banks customers) and the increased user inconvenience of carrying an extra device with them to conduct a transaction on the Internet. In addition, there is limited

standardization between the banks on the card reading devices so customers with accounts at more than one bank will need more than one card reader. Blackberry provides a similar two-phase authentication solution for their devices, the BlackBerry smart card reader (Blackberry, n.d.).

A cell phone offers much potential for storing an appropriate token for two-factor authentication (e.g. high adoption levels, users close attachment, provides an independent channel for distributing tokens and, local processing and storage capabilities). A cell phone based token system has potential for widespread adoption given low costs (the infrastructure is already in place), wide availability and easy of use.

One approach to using cell phones for two-factor authentication is to use the mobile device to read an electronic token from a card, which would be issued separately by a bank or credit card company. This could consist of an extra slot in the cell phone for a card to be inserted (as in the examples above of a separate card reader, though using the cell phone as the card reader) or have contactless technology, such as RFIDS readers (e.g. Williams, 2006) built into their cards. Contactless technology would remove the need for a slot and allow the phone and card to communicate when they are within a few centimetres of each other. However, this option adds further complications and increased costs. Other cell phone options include using Small Message Service (SMS) to deliver authentication codes. For instance the Commonwealth Bank of Australia operates an SMS based two-factor authentication system for its online banking systems; however apart from the 'timing issue' (i.e. possible delays in SMS messages arriving), Kotadia (2007) argues that the SMS approach also has inherent security limitations.

A different, and more robust, approach also using SMS has been followed by Schuba et al. (2004) which uses security embedded in the SIM cards in cell phones to authenticate users in Liberty Alliance based systems. The Liberty Alliance, formed in 2001, aims to establish open standards, guidelines and best practices for identity management. Later moves in Liberty Alliance explored the interoperability with the Microsoft's competing .NET Passport (Blau, 2002). In the Schuba et al's (2004) approach, the token is not the mobile phone itself, but the SIM card within the phone. Their approach makes use of an Identity Provider (IDP) which manages the authentication aspects of the users. The IDP server has to communicate with the Service Provider (SP) (i.e. an organization such as a bank or retailer) and with the cell phone user via the mobile telecommunications infrastructure (i.e. via a WAP Gateway). The IDP acts as an independent trusted third party. For this approach, there is a separate registration mechanism with the telecommunications operator and the IDP. The protocol followed for each transaction in Schuba et al's (2004) approach is (see Figure 1):

- Step one: the user logs in to a protected website run by organisation/SP (i.e. over a secure connect as usual).Step two: The user's authentication status is checked via the SP server.
- Step three: If authentication is required, the SP server contacts the IDP server which then generates a random pattern of symbols. This pattern is sent to both the SP and the user's cell phone. The user then confirms the pattern to the SP via the PC-SP secure connection.
- Step four: If both patterns of symbols match, the user is authenticated into the website.

The approach builds on the open standards of Liberty Alliance, and, as such, has wide applicability. One disadvantage is the complexity embedded in the protocol. The cell phone has to communicate with the IDP server, via the WAP gateway, and directly with the user's PC via the Internet and, the IDP server has to communicate with the SP server before the authentication is completed. The authentication process relies on both the mobile network and the Internet and coordination between these for the authentication process for each transaction. There are potential problems when there are weak signals or lack of coverage on the cell phone network. The next section describes the development of an alternative two-phase authentication system.

A NOVEL TWO PHASE AUTHENTICATION PROTOCOL

The novelty of this suggested approach is that it makes use of an authentication token stored in an authentication wallet on the cell phone, thereby limiting the need to communicate directly with the authentication server via the cell phone for each transaction. This will provide reduced authentication overhead and increased ease of use for customers. There have been similar examples and prototypes of sending a token via Bluetooth between a mobile device and a PC or laptop (e.g. Schwartz, n.d.; Rania et al., 2005; Mannan & van Oorschot, 2007; Jammalamadaka et al., 2007). However, this protocol is designed to be compatible with existing token based approaches, such as Schuba et al. (2004), and be expandable to include multiple software tokens from different providers. It can also be extended to include different devices other than Bluetooth. The protocol is represented in figure 2.

The process starts with the user registering with an authentication organization and a client 'authentication wallet' being installed on the user's cell phone (stages 1 and 2 in figure 2). This registration is similar to the initial stages of Schuba et al. (2004) approach as well as the registration activity needed for the dual card systems and separate card reader systems operated by Banks. The authentication organization can apply its own criteria for registration and re-registration activity and for distribution options. For instance, one organization, say a retailer could follow its own registration process (e.g. credit rating of new customers, extension of loyalty scheme) and distribute the electronic token via the cell phone network (as in Schuba et al's approach) to be installed directly on the user's cell phone. Another organization, say a

bank, could follow its normal criteria for registration (e.g. extension of existing customer services, credit rating etc) and distribute the electronic token via the user's PC which can then be installed on the user's cell phone via a Bluetooth or other connection. Different tokens can be stored in the authentication wallet from different authentication organizations. This would effectively perform the same function as the card reader devices discussed earlier by generating a unique runtime authentication token for each transaction, however, the token distribution costs are far lower and do not rely on the need for the user to carry an extra device. In addition, tokens could be replaced annually, monthly, weekly or as and when deemed appropriate by the authentication organization or requested by the user.

With the authentication application installed, the user can access the secured web site by entering the username and password as is normal for the first phase of an authentication. The second phase of the authentication then uses the cell phone to provide an independent token which can be checked for a match against the organisation's token for that user. In the application developed use is made of a Bluetooth connection between the cell phone and the PC, with the token exchange between the mobile and the user's computer being encrypted.

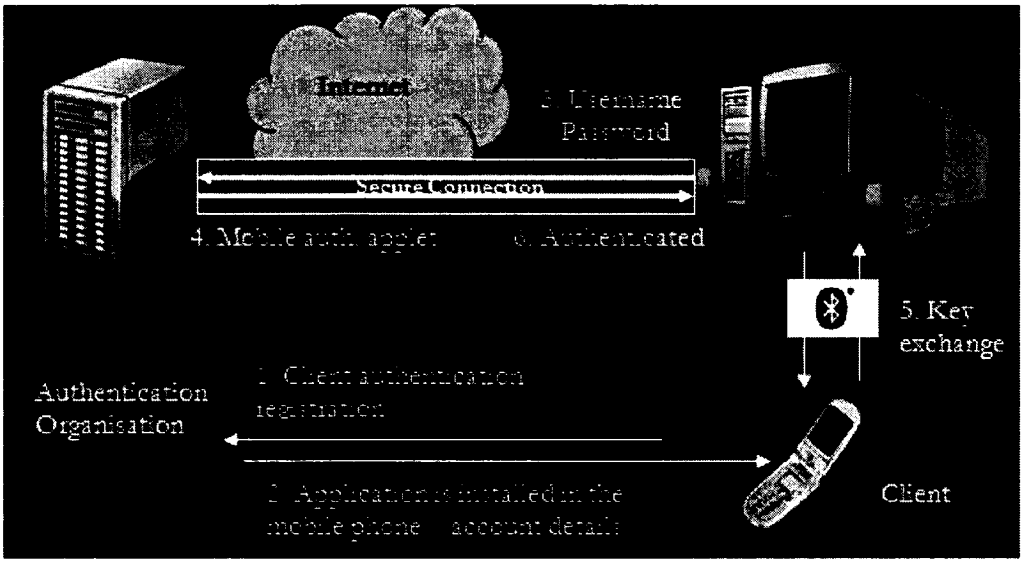

Figure 2. A Novel Two-Phase Authentication Protocol Using Mobile/Cell Phones

The practicality of the enhanced two-phase approach was tested out by developing two applications. One covers the token management on the client side (cell phone) including the secure connection between the cell phone and the PC via a Bluetooth connection. The other application covers the PC activity managing the token distribution from the cell phone to the secure website. These applications are the main new attributes of the suggested protocol. The aim of developing the applications was

to explore the practical aspects of using software tokens on a mobile device (e.g. storage and process requirements, speed) and effects on usability in an authentication process.

For the key exchange between the PC and cell phone, a Diffie-Hellman protocol is used, though alternative encryption protocols could also be used. The application development on the cell phone used Java J2ME (Java Micro Edition) (De Jode, 2004) and Netbeans 5.5.1 IDE. Bluetooth communication on the cell phone is part of the J2ME configuration. The corresponding server side (i.e. PC) made use of the Bluecove Java library to develop the secure Bluetooth communication. The applications were tested by simulating access to an online bank account. Ten participants used the system and gave feedback on the usability.

Server Side (PC) Application

The application is started by activating the Bluetooth on the PC and waiting for connections. A message is displayed on the screen advising the user to activate the Bluetooth and run the application on the mobile phone. When a device is connected, the application runs the first step of the key exchange algorithm, starts sending information and waits for the response. When the connected device sends information, the application runs the second step of the key exchange algorithm and checks if the results of both applications are equal. Finally, a message is displayed on the screen informing user for the results of the authentication procedure. If the results are equal, the authentication is completed, else the user cannot be authenticated and cannot access the account requested.

Client Side (Cell Phone) Application

This performs a complementary application to the server. The Bluetooth on the mobile phone has to be activated in order to find the server. As potentially several devices could have Bluetooth activated, the authentication application looking for devices which run the same services as the cell phone application. When the search of Bluetooth devices is finished the user has to choose the device he wants to connect on from a list of devices. After choosing the correct device, the mobile phone runs the first step of the key exchange algorithm and sends the information to the server. The key exchange algorithm is exactly the same procedure in both applications and uses the same Java class. After sending the information, the application is waiting to read the information sent by the server, calculates the key and sends it to the server. The application then is completed and it goes back to the options menu. The server side compares the results of the two applications and decides if the authentication is successful or not. Extension to the client authentication wallet includes handling multiple tokens to accommodate authentication with multiple organizations.

EVALUATION OF APPLICATION

Both applications were tested in an emulator and on mobile devices. There were some compatibility problems with the older version of mobile phone used but that was due to the Java implementation in those devices. For instance, the software was tested in a Sony Ericsson K750i and was working fine, but had teething problems in a Sony Ericsson K700i. Overall, the final applications ran with no major hitches: the storage and processing requirements were handled comfortably by the devices. Setting up a secure Bluetooth connection between the PC and the mobile device took a few seconds, but also needed user activity to enable Bluetooth on their mobile device. The authentication process was refined to be mostly automatic with the user only needing to select the correct Bluetooth device and press the ok button. Feedback from participants using the system indicated that they found the process straightforward, though they had to do extra processes in activating the Bluetooth on the mobile phone (if not already activated) and initiating the token authentication.

Some of the limitations in the testing of the applications, has been a low number of participants only part of the full authentication process being covered. Further development will require participation from authentication bodies covering the complete authentication process (e.g. registrations, distribution of tokens), and interaction with multiple 3rd parties (e.g. use of multiple tokens) and more comprehensive testing (e.g. timing, QoS, HCI issues). The use of software tokens for authentication seems a practical option given the development and testing undertaken,

DISCUSSION

A variety of two-phase authentication approaches exist which offer increased levels of security over passwords. As discussed earlier there are challenges and limitations with each of these: Providing an extra physical device to generate tokens is both expensive and is likely to impact convenience and usability; Biometric approaches offer much potential but have high costs and attract wide concerns; approaches based on using cell phones taps into technologies that users are already likely to carry, however, existing approaches have either cost issues (e.g. dual slots cell phones) or have high transaction authentication overhead (e.g. need collaboration between servers on the Internet and telecommunications infrastructure). The suggested two-phase authentication approach in this paper also makes use of the ubiquitous cell phone to store and manage tokens which are used in the second phase of an authentication process; however, it tries to address the weaknesses of costs and transaction overheads found in other approaches.

By developing and testing the application, further attributes and extensions to the suggested two-phase authentication approach emerge, particularly increased flexibility. The initial project focussed on extending and informing the approach by Schuba et al. (2004) which aimed to establish open standards and guidelines for best

practices identity management. The Scuba et al. approach was selected as the base for this study since it was the most promising design for wide scale adoption of authentication tokens. The enhancements investigated focussed on developing alternative authentication channels other than using the telecommunications infrastructure for each transaction (i.e. to address the high transaction authentication overheads and timing limitations). There is a large overlap between the two approaches, not least in the registration processes, the use of the ubiquitous cell phone, and installing of an authentication wallet on the cell phone, and following a similar (but not identical) process to conduct the two-phase authentication. There seems much potential for the suggested approach in this paper to complement the approach taken by Schuba et al. (2004) by providing an alternative authentication mechanism and channel. It may be that certain transactions are more suitable for one authentication approach while other transactions call for an alternative authentication approach (e.g. where there is lack of telecommunications coverage or to meet user or organization preferences). The suggested approach also provides further flexibility in that different organizations can provide their own authentication tokens. The approach could also accommodate different technologies, such as different connections between the cell phone and PC (e.g. infrared, wifi, RFID, USB) or even the use of a different device to the cell phone (e.g. other mobile devices, PDAs, Palmtops, Blackberry, laptops or RFID/smartcard) for storing the token. The encryption used in the application was based on the Diffie-Hellman protocol, however alternative encryption protocols could also be used as well as variations in the token used. A further strength of the suggested approach is that it does not rely upon personal information of the users: As discussed above, from an information richness perspective there are some systemic weaknesses with using personal information for authentication when personal information is 'freely available' through the internet and wider sources.

A cell phone is a very strong candidate for token management within a two-phase authentication process. People are already likely to have and carry a cell phone and be regular and comparatively expert users (as opposed to using a separate card reader). Given the frequency of use and close attachment by users it is likely that people will notice quickly if their cell phone gets lost or stolen (arguably more quickly than say a credit card or separate credit card reader device), and consequently more able to report potential security breaches more quickly than alternative options. However, there are limitations to options based on cell phones, such as trying to incorporate any password protection to control access to an authentication mechanism. For instance, an 8 digit password consisting of a mix of upper and lower case letters and numbers (which would be a basic level 'strong' password on a PC) would take of the order of 40 key strokes on a cell phone. For instance, typing '7sS' on the Nokia device used in the test would take five key stokes for the '7' followed by four key strokes for the 's', followed by a further five key strokes for the 'S', all with a timed delay between each key stroke. The potential for mistakes is fairly high. The same would be true for the majority of other mobile/cell phones that do not have QWERTY key boards. This is likely to result in either using automatic connection between the cell phone and the PC or using a minimal (weak) password. There are further potential problems with relying

on a cell phone such as low battery situations or in the case of 'pay-as-you-go' if the device runs out of credit.

CONCLUSION AND CONTRIBUTIONS

There is a clear trend toward more economic activity online which calls for a need to have robust and secure mechanisms to conduct transactions and authenticate users (Kotadia, 2007; McClure et al., 2005): Password protection alone will not provide sufficient levels of security for most organizations and most users, and private information is often used to increase levels of confidence for authenticating that a person is who they say they are. However, the information richness perspective developed in this paper shows that in a climate where personal information is 'freely available' (e.g. through the internet and via social networking sites) an approach based on using private information is not suitable for developing long term authentication systems. A rich set of exoinformation on individuals is relatively easily accessible by other people, and so reducing the currency of any private information that would normally be used for authentication.

As a practical alternative two-phase authentication approaches to improve authentication have been suggested by other researchers and adopted by different organizations. These do provide practical increased levels of security; however, each of the options examined has limitations in costs, usability, convenience, acceptability or complexity. The suggested approach in this paper addresses some of these limitations and would provide a complementary alternative to existing two-phase authentication approaches.

However, the real practical contribution for the authentication approach developed in this paper is in identifying the potential of distributing software based tokens for authentication purposes. A software approach provides clear benefits in terms of costs, flexibility and speed over physical authentication mechanisms (e.g. separate physical tokens, separate card reading devices, biometric reading devices etc). In addition, using software tokens opens the possibility of developing a flexible standard for authentication token distribution and use, while at the same time allowing companies to offer their own tokens. For instance, the existing practices of Banks distributing their own incompatible card readers to their customers is expensive, takes considerable time to coordinate and distribute and is not user friendly (i.e. customers will need to carry card readers for each bank account they have). A software based authentication token system opens up a route to standardization between banks and other corporations to improve authentication practices. In addition, the mobile/cell phone seems an ideal medium and channel for such authentication mechanisms given the ubiquity, close attachment and capabilities of the devices. Other works suggest a similar approach to providing authentication tokens via Bluetooth through cell phones or other mobile devices (e.g. Schwart, n.d.; Rania et al., 2005; Mannan & van Oorschot, 2007; Jammalamadaka et al., 2007): there is clearly a need for standardization in similar token based authentication techniques, the alternative would

be incompatibility between authentication systems and worsening the user experience. This paper also contributes to theory by bringing an information richness perspective on authentication and highlights systemic weaknesses of authentication based on using private information.

There are limitations with the approach suggested and the system developed. The paper identifies some of the limitations of relying on mobile devices for authentication (e.g. potential for mistakes in typing on a mobile device, low battery situations or running out of credit with 'pay-as-you-go' services). The application developed showed the practicality of using software tokens on a cell/mobile phone device but only covered a part of the whole authentication process. This is an area calling for further research and development.

REFERENCES

Adams, C., & Fitch, C. (2005). Conflicts of Convergence: The Mobile as a Schizophrenic Device. *Wireless World Research Forum (WWRF 15)*, Paris, 8-9th December 2005.

Adams, C., Millard, P. & Avison, D. E. (2003). Personal Trust Space in Mobile Commerce. *The Sixth International Conference on Electronic Commerce Research (ICECR-6)*, INFORMAT, Dallas, October 23-26.

Adams, C. & Katos, V. (2007). Exoinformation space audits: an information richness view of privacy and security obligations. *Journal of Information Privacy and Security*, 3(3), 29-44.

Barclays (n.d.). Barclays Bank Online Banking PIN Sentry System. Retrieved from http://www.barclays.co.uk/pinsentry/, April 5, 2008.

Blackberry (n.d.). The BlackBerry Smart Card Reader. Retrieved from http://blackberrylinks.com/blackberry-smart-card-reader-security-white-paper.html, accessed 4/6/08, on April 5, 2008.

Blau, J. (2002). Liberty Alliance Plans Interoperability with Passport. *Infoworld*, September 24, 2002. Retrieved from http://www.infoworld.com/articles/hn/xml/02/09/24/020924hnliberty.html, on November 22, 2007.

Brunk, B. D. (2002). Understanding the Privacy Space. *First Monday*, 7(10). Retrieved from http://firstmonday.org/issues/issue710/brunk/index.html, on December 3, 2007.

Brunk, B. D. (2003). A Framework for Understanding the Privacy Space. *PhD Thesis*, University of North Carolina.

De Jode, M. (2004). Programming Java 2 Micro Edition on Symbian OS a Developer's Guide to MIDP 2.0 [Electronic Version]. *Chichester: John Wiley & Sons.*

Daft, R. L., & Lengel, R. H. (1984). Information Richness: A New Approach to Managerial Behavior and Organization Design, *Research in Organizational Behavior,* 6, 191-233.

Gollman D. (1999). *Computer Security.* John Wiley & Sons.

Jammalamadaka, R. C., McIntosh, M., & Austel, P. (2007). SIdeCAR: Secure Identity Consent and Authentication Responder. *IBM Research Report RC24359* by Ravi Chandra. Retrieved from http://domino.research.ibm.com/library/cyberdig.nsf/papers/150C6B752A26CB7C852573700056DBC5/$File/rc24359.pdf, on November 22, 2008.

Katos V. & Adams C. (2005). Modelling Corporate Wireless Security and Privacy. *Journal of Strategic Information Systems*, 14(3), 307-321.

Kormann, K. P., & Rubin A. D. (2000). Risks of the Passport Single Sign on Protocol. *Computer Networks*, 33(1-6), 51-58.

Kotadia, M. (2007). Security Firm U-turns on Banking Breach. *ZDNet Australia*, 04. Retrieved from http://news.zdnet.co.uk/security/0,1000000189, 39286967,00.htm, on November 22, 2007.

Mannan, M., & van Oorschot, P. C. (2007). Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer. In Dietrich, Sven; Dhamija, Rachna (Eds.) *Financial Cryptography and Data Security, 11th International Conference proceedings, FC 2007.* Lecture Notes in Computer Science, Springer Berlin/Heidelberg.

McClure, S., Scambray, J., Kurtz, G. (2005). *Hacking Exposed: Network Security Secret & Solutions* (5th ed.). California: McGraw-Hill.

Nationwide (n.d.). Nation Card Reader Security for FlexAccount Visa Debit Card Customers. Retrieved from http://www.nationwide.co.uk/rca/Introduction/why.htm, on June 10, 2008.

NatWest (n.d.). NatWest Car Reader Guide. Retrieved from http://www.natwest.com/microsites/general/card-reader-user-guide/index.asp, on June 10, 2008.

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric Recognition: Security and Privacy Concerns. IEEE Security & Privacy Magazine, 1(2), 33-42.

Randall, D., & Richards, V., (2008). Facebook Can Ruin Your Life. And So Can MySpace, Bebo: People Will Post Just About Anything on Social Networking Sites. And the Information Can Be Used Against Them. *The Independent*, Sunday, 10 February 2008. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life-and-so-can-myspace-bebo-780521.html, on November 22, 2008.

Rania, A., Khatun, S., Borhanuddin, M. A., & Rahman, R. A. (2005). Application of Cell-Phone in Laptop Security, *Journal of Applied Science*, 5(2), 215-219.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing Security and Privacy in Biometrics-Based Authentication Systems. *IBM Systems Journal*. 40(3).

Schuba, M., Gerstenberger, V., & Lahaije, P. (2004). Internet ID - Flexible Re-Use of Mobile Phone Authentication Security for Service Access. *IEEE Communications Magazine*, 42(9), 7.

Schneier, B. (2005). Two-Factor Authentication: Too Little, Too Late. *CACM*, Vol. 48(4), 136.

Schwartz, M. (n.d.). Using a Bluetooth*Device as a Secure, Wireless Authentication Token. *Presentation covering student project, from New Mexico Tech*, Retrieved from http://216.239.59.132/u/NMTech?q=cache:V7WI331cs4QJ:infohost.nmt.edu/~moses/BTAuthPresentation.ppt+Moses+Schwartz&hl=en&ct=clnk&cd=4&ie=UTF-8, on November 22, 2008.

Sery, P. (2006). Tighter SSH Security with Two-Factor Authentication Linux Journal, 2006(152), 3.

Steele, C. (2005). Paranoid penguin: two-factor authentication. Linux Journal, 2005(139), 10.

Verkaik, R. & Taylor, J. (2007). Facebook Backlash over Sale of Personal Data. *The Independent*, Saturday, 24 November 2007. Retrieved from http://www. independent. co.uk/life-style/gadgets-and-tech/news/facebook-backlash-over-sale-of-personal-data-760221.html, on November 22, 2008.

Williams, L. (2006). Mobiles Set for Key Role in Card Authentication: Two Factor Authentication Devices May Include the Mobile Phone. *Computing*, 13 Jul 2006. Retrieved from http://www.computing.co.uk/computing/news/2160284/mobiles-set-key-role-card, on November 22, 2007.

Carl Adams is a Principal Lecturer and Researcher in the School of Computing, University of Portsmouth, UK. He has over a decade of professional experience in the computer industry as a Software Engineer and consultant before going into academia. He is an active researcher with interests in mobile information systems develop, mobile and electronic commerce, including security and electronic payment systems, and the wider impact of technology. He has an MSc in Management Science and a PhD in the field of Information Systems, both from Southampton University, UK.

Alexandros Nikolaos Dimitriou was born in Athens/Greece and joined the University of Portsmouth in order to obtain a BSc in Computing. His interest lies in computer security, cryptography and digital forensics, so he decided to specialise in this area by obtaining his MSc in Forensic Information Technology from the University of Portsmouth in 2007. Since then he is working for Nimbus Partners, a company producing a Process Management application called Control. In the R&D department he is part of the team responsible to test the application in order to make sure that it is delivered to the clients without defects.