Journal of Information Assurance and Security
ISSN 1554-1010 Volume 6 (2011) pp. 149-156

Authentication Aura - A distributed approach to user authentication

C. G. Hocking[1], S. M. Furnell[1,2], N. L. Clarke[1,2] and P. L. Reynolds[1]

[1] Centre for Security, Communications and Network Research, University of Plymouth, Drake Circus, Plymouth, United Kingdom
info@csan.org

[2] School of Computer and Security Science, Edith Cowan University, Perth, Western Australia

***Abstract*: The ubiquitous password or personal identification number (PIN) has been the accepted form of user authentication on mobile devices since their inception. With increasing numbers of owners failing to implement these simple barriers or taking any greater precaution against misuse, the requirement to secure the information contained within has never been so great. This paper proposes a new approach to identity authentication on mobile devices based upon a framework that can transparently improve user security confidence. Information pertaining to user authentication is shared amongst the owner's devices, collectively enabling a near field adaptive security envelope to be established and maintained around the individual; the user's Authentication Aura.**

***Keywords*:** authentication, identification, mobile, security, biometric, authentication aura**.**

I. Introduction

The aspiration of people to be mobile and yet remain in communication with colleagues, family and friends has driven the use of devices that support and complement this lifestyle. Estimates suggest that worldwide Wi-Fi hotspot usage during 2009 grew to 1.2 billion connections, an increase of 47% from 2008, with this being driven by a 50% growth in the sale of Wi-Fi capable handsets between 2007 and 2008 [1]. Surveys indicate that, mobile devices have become the preferred method of accessing the Internet amongst young users [2]. With technological evolution enabling powerful and sophisticated systems to be accommodated into these handheld electronic gadgets, their extensive storage and processing capabilities has made them an increasing target for thieves. In 2007-8 over 700,000 handsets were stolen in the UK, with 50% of all robberies targeting a mobile phone in the items taken and in 33% of those offences it was the only stolen possession [3]. Between May and June 2009 alone, the UK saw an 11% increase in the reporting of missing/stolen mobile phones, with 84% of theft victims failing to retrieve their lost handsets [4].

However, theft is not the sole reason for concern; a New York survey revealed that during a six month period in 2008, 31,544 phones and 2,752 other types of handheld device (laptops, PDAs, memory sticks etc.) were simply left in the city's Yellow Cabs, an average of more than two per cab [5]. In this climate, the requirement to protect and secure the potentially large volumes of sensitive and personal information contained within these desirable pieces of equipment is imperative and even acknowledged and supported by Government [6], [7].

As time passes and the proportion of technically-aware digital natives (i.e. those who have been born and grown up surrounded by technology) [8] grows, one would expect security usage and awareness to be greatly improved. Surprisingly though, this is not the case. Recent research has indicated that there has been no significant improvement in users' attitudes or habits during 2005 to 2010 [2], [9]. In this period the use of a PIN as a means of security by 18-25 year-olds has in fact dropped by 50% [2]. Device owners are simply failing to take responsibility for protecting themselves.

The problem is magnified because users are finding themselves in possession of an ever growing number of digital devices, each one having its own associated security requirements. With several being carried concurrently, at the moment of initial use it is likely that similar procedures of authentication are undertaken repeatedly across the disparate entities to ensure full activation. This repetitive and time-consuming operation raises the question of whether there is a better way and does the collective identity knowledge possessed by the multiplicity of secured devices utilized by an individual at any given time present an opportunity to improve security. As each device is activated a set of authentication credentials are determined and access is either granted or denied. By enabling the individual and distinct devices to communicate their own authentication status and to share established user identity confidence it may be possible to synthesize an enhanced form of security.

This paper explores this concept and proposes an approach through which authentication credentials can be distributed amongst devices and how this information can be used to create a novel method of security and user control. It addresses the requirements to produce a flexible, adaptive and non-intrusive security mechanism that will meet future demands and provide a foundation for further development. Firstly, the background explores the current methods of

securing mobile devices and the associated weaknesses. Once these foundations have been laid the paper continues to outline the new proposals and considers how they will improve upon the situation at present.

II. Background

Security is founded on three key principles – something an individual knows, they possess or they are [9]. Knowledge and possession based security both rely upon the inherently weak link in the chain – the user. The first utilizes a piece of significant or memorable information which is often forgotten or written down [11]; the second, the presentation of a physical key or token at the required moment. Forgetting, mislaying or losing the crucial item or information will bar further access attempts.

The ubiquitous point of entry user identity code/password has been rendered susceptible to abuse through the inability or unwillingness of individuals to protect and administer this sensitive information correctly [9]. To maintain security it is supposedly known or more precisely memorized exclusively by the creator [12] but is too often shared or inadvertently communicated [13]. Although different; identification and authentication both rely upon the recognition of the identity of a user interacting with a device at any given moment. Hand held mobile devices typically assume the identity of the user and utilize personal identification numbers (PINs) to authenticate[1] this at point-of-entry. The authentication is Boolean; the subject is either deemed to be whom they purport to be or they are not, without any middle ground. Frequently passing the one-off process will permit unregulated access to all facilities and utilities installed on the device [14]. Therefore once access has been gained the ability to incur large telephone bills or excessive high-cost data downloads is readily available to impostors who compromise the PIN.

In the search for evermore appropriate and robust authentication, attention has turned to biometrics (something the user is) to establish methods that cannot easily be compromised, are non-intrusive and equally eliminate the potential threat posed by social engineering [15]. A finer granularity of identification can be achieved; ultimately the device will either issue or refuse access to the user, however the starting confidence can precisely reflect how well the supplied identity matches the known template sample. Having this ability will allow a device to tailor its reaction to strong and weak authentication attempts accordingly. Further, without fundamentally changing the habits to which users are accustomed improvements can be implemented. As a supplementary development, layered authentication techniques have been explored and employed to compound protection and expand the sophistication required to circumvent defence mechanisms including; password and facial recognition [16], fingerprint scan and tokenized random number [17], teeth imaging and voice pattern verification [18]. This can then be reinforced by elements such as location information which indicates whether or not a user is operating in a known and unsurprising locale [19].

Currently security that is founded on point of entry authentication that remains static for the duration of interaction is unable to prevent misuse succeeding a hijack, when following a legitimate log-on the piece of equipment is illicitly removed or used by another. If this occurs and the device is kept active and not switched off, free and open use can be maintained for a significant period of time. With 85% of owners admitting their mobile phone is on for over 10 hours per day [9], to counteract this weakness proposals to degrade service availability over time have been made [15], [16] enabling the device to shut down functionality unless re-authentication occurs.

As several gadgets are frequently carried simultaneously any intrinsic security weakness is amplified especially as people will often use the same PIN for more than one device, if not all of them [9]. Once one is compromised by the discovery or disclosure of the PIN then it is possible that all the owned devices become vulnerable.

To circumvent the associated weaknesses of point-of-entry authentication it would be advantageous to augment the process with ongoing reassurances. Establishing user identification during the initial sign-on and then authenticating at intervals to maintain confidence allows opened devices to be secured against potential theft or loss. Although a device may be open and fully usable upon stealing, without successful re-authentication within a limited timeframe it would become inoperable. Ongoing re-authentication can be either intrusive by interrupting the user and requiring a password or PIN to be entered, or non-intrusive in the case of biometrics where for example the user's identity is confirmed by their typing characteristics [20], [21]. If correctly implemented, either will be an improvement upon the current situation but it is important to consider the most flexible and appropriate approach.

Section III discusses and then outlines a potential framework that addresses these weaknesses and provides a means by which mobile device security could be enhanced.

III. Enhancing Security for Mobile Devices

With individuals being likely to carry more than one portable device and simultaneously interact with, or at least be known to, other technology in their local vicinity at any given time, possibilities exist to maximize this security potential. For instance, in the morning on leaving the house a worker might activate their business phone and Personal Digital Assistant (PDA) whilst at the same time picking up their car keys. By leveraging the relationship the user has with these multiple devices and associating the identification knowledge that each independently possesses, enhanced assurance of the owner's identity can be determined. At the time of authentication, each device establishes a confidence in the identity of the user, either true or false. Facilitating a means of communicating the current security status between the unique entities would allow them to bolster their own confidence in the user's identity.

[1] As opposed to devices such as laptop computers that generally rely on a user name and associated password.

Utilizing environmental awareness[2] and enabling the devices to request and trade their current authentication confidence, would provide a more flexible approach to security administration. This self-governing method would allow the party devices to adjust their own status through the consideration of their peers and the surrounding environment. The main drive is to achieve a position where a newly activated piece of equipment would not require an authentication process to be undertaken because the surrounding near vicinity contains sufficient confidence in the user's identity, that it is considered unnecessary to do so. Additionally, as the user relocates between areas of differing threat (public spaces to a home or work environment), the devices could relay the situation to their counterparts allowing each to react accordingly.

In order for such a system to operate, it is necessary to first give some consideration to the underpinning requirements:

A. Biometrics

Using biometrics fits the requirements of a heightened security methodology for mobile devices, on the basis that they are characteristics that cannot be forgotten, divulged or lost by their owner [22]. Further, biometrics divides into two distinct tranches of study, physiological and behavioural [23]. The use of physiological biometrics is more often preferred for identification purposes because of the greater degree of uniqueness, experienced consistency and resilience to external corruption [24]. However, it is best suited to point-of-entry scenarios where an individual would be happy or certainly less discontent to tolerate the inconvenience necessary to undergo the required process of identification. For instance, having to place a hand upon a particular device, or head at a specific angle, to enable the relevant scan to be taken are both obtrusive procedures. Conversely, behavioural biometrics lend themselves to authentication scenarios where the identity of the individual is already established and confirmation of a user's continuing presence is sought. Behavioural traits can be detected unobtrusively enabling validation to be carried out imperceptibly to the user [9], [16], [20]. Capturing a voice sample during a mobile telephone conversation would allow the device to compare extracted voice patterns and nuances against a known and expected reference vocal template. Executing such a process regularly during use, facilitates a means by which the mobile device could gain appropriate confidence in the user's identity during extended periods of otherwise unchecked access.

Although upon first consideration a single layer of protection maybe deemed sufficient, [25] observed that "Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates". With individual biometrics failing to meet appropriate levels of acceptance, attention has been turned to combining techniques in multimodal authentication systems [16], [26]. There are a plethora of circumstances where multimodal biometrics are advantageous and would be the authentication method of choice but not readily available because of technological limitations.

By combining devices and available techniques it may be possible to achieve the same objective without multi-layering on any individual piece of equipment. Drawing together authentication confidence from a number of disparate devices would enable any one entity to make stronger and more informed judgment calls. With the likelihood that distinct devices will utilize different biometric techniques with differing rigor and strength, combining the otherwise unilateral decisions will further improve the ultimate recognition process. An added advantage of this is that captured identity samples could be communicated from devices without the processing capability to analyze the data, to a local entity sufficiently powerful to complete the operation. However, if no local device was available but network or internet services were, the samples could alternatively be passed to a remote authentication system where the analysis could be executed and decision returned.

B. Security degradation

It can be argued that rather than remain static, the authentication confidence should be eroded over time, reducing service and application availability[3] [15]. Upon reaching a significant point, re-authentication would be necessary to re-determine the user's credentials and once more allocate appropriate confidence. Should this undertaking be unsuccessful (as anticipated in the case of a hijacking), service provision would degrade to such a degree that the entity would be rendered un-usable; protecting the information stored within and further misuse.

Some functions of mobile devices are more sensitive than others and their illicit use could potentially incur greater cost or harm. Rather than regarding every type of feature equally it is sensible to enable a degree of flexibility in how each is treated and protected with the introduction of confidence cut-offs. Operative tasks and applications could be allocated a security tariff allowing some functions to be carried out with a low confidence whilst at an equal level others would be blocked entirely. For instance with low confidence it would be acceptable to operate a calculator application but the ability to instigate a telephone call would be barred. Additionally, the calculator application would not only function at a lower tariff but it could be allowed a slower rate of degradation implying that it would take longer for it to reach the cut-off point of inoperability [22].

Dynamically adjusting the rate of decay to reflect the environment in which a device is being used will enable the model to adapt. In public, high-risk areas, a steeper rate of erosion could be utilized, whilst in a familiar and perceived low risk environment a flatter more sedate timescale employed. Indeed the decay space becomes a complex n-dimensional curve with degrees of freedom including application sensitivity, time, location, method of authentication and user behaviour. Consideration of these

[2] Devices such as mobile phones and laptop computers detect cellular and wireless networks and other such information that provide a means to recognize their current locale at any given time.

[3] For instance, within the first few minutes following device activation the likelihood that the owner has been replaced by an impostor is much less than it would be after an hour.

factors and more will dictate at what percentage point confidence will be at any given moment in time.
Section C builds on this approach and further explores how it could be used to improve security.

C. Device interaction

As proposed at the start of this section, enabling disparate devices owned by the user to communicate will bring advantages in achieving strong methods of authentication. Additional identity confidence could also be obtained by gathering the authentication status of nearby devices. Distinct devices are likely to utilize different methods of authentication and using this array of approaches arguably establishes a more robust security profile. By enabling entities to recognize each other and communicate their current state of user identity confidence, the degradation process could be slowed or even reversed.

Figure 1 below shows a conceptual diagram of the

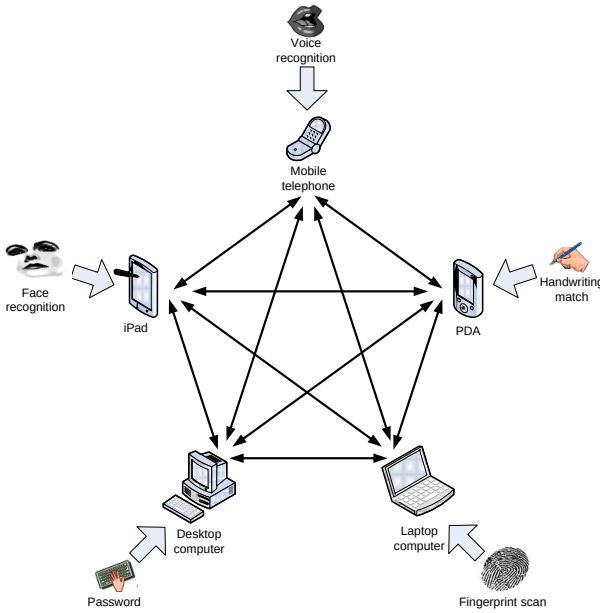

Figure 1. Potential intra-device relationship and authentication techniques

relationship paths that might be established by a user's set of personal devices[4] and the variety of authentication techniques that might be employed.

Information sharing would be carried out between trusted pairs via a near field communication (NFC) channel such as Bluetooth. Utilizing NFC will ensure the security envelope or authentication aura is restricted to the local vicinity and acquired confidence is confined to entities within the physical proximity of the requesting device. Additionally, ensuring the intra device trust would effectively eliminate responses from unknown third party entities. Without doing this, a degrading device might poll the surrounding near vicinity for listening pieces of equipment and one owned by a different user might respond with an assurance of confidence which although true, would not be in the same user's identity. If accepted and permitted to proceed, the alien device would falsely bolster the observed identity confidence.

Furthermore, associating a weighting tariff to the method of authentication would allow equipment to utilize robust techniques that they would otherwise not have the ability to use [15]. The tariff system could then be extended to either slow or accelerate the rate of confidence decay (see section B). For instance, a laptop computer might have an inbuilt fingerprint scanner with a high tariff of robustness. The same person's mobile telephone might only authenticate via a PIN number; a far less rigorous form of authentication. Thus by drawing upon the laptop's high tariff confidence, the mobile phone could gain an enhanced state of assurance and thereby extend a slower degradation than would otherwise have been appropriate. Introducing additional items and allowing every device to trade and negotiate confidence with every other will synthesize a flexible and self maintaining security environment.

This region of localized security can also be augmented by constructing the system in such a way that it can be introduced and subsequently recognize the local environment. This could be achieved by sensing available wireless networks and associating them with locations, allowing degradation tariffs to be correspondingly allocated within an administration function. The tariffs or weightings associated with public spaces can be utilized to degrade confidence more rapidly than those linked with more private arenas. By integrating the ability to detect and consequently recognize known locales, the model will react and adapt independently of human intervention. Hence, as the user crosses environment boundaries security and awareness can be immediately heightened or relaxed respectively increasing or reducing the frequency that re-authentication is requested. It may even be possible to associate the user's behaviour and device interaction with locations or at least perceived security threats. That is, through use and experience each device might be able to recognize that the user only activates certain applications when at home or in equally low threat surroundings. Vice versa particular services or operations might be utilized in public areas or correspondingly high risk locations, allowing immediate yet discrete security adjustments to be made. This is achievable via the adaptation of behaviour based identification techniques [27].

IV. System Anatomy

Having explored the core features and requirements of the proposed approach to mobile device security it is now possible to examine and discuss in greater detail how such a framework could be implemented. This section addresses the core elements, the role each plays and how they might be united to achieve a robust and adaptive security system.

The suggested system would consist of a core control engine with the ability to hook into and utilize five peripheral elements; the local environment, database storage, device operating system, one or more authentication mechanisms and the other member devices. Figure 2 outlines how the elements would combine and the direction of information flow between the disparate parts of the anatomy. It also illustrates the elements that are located within the physical body of the device and those that lie beyond.

[4] The mobile telephone is shown as centric to the scheme because of the likelihood that it is the one device that is ever present upon the legitimate user's person.

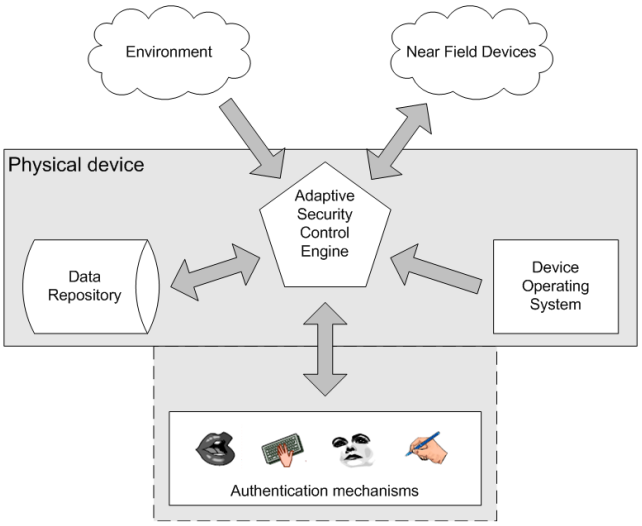

Figure 2. Adaptive security environment

Centric to each device is envisaged to be the Adaptive Security Control Engine (ASCE), which will manage and direct the internal security. It will be required to hook into the device operating system in order to influence and apply relevant security policies based upon the action and authentication success of the user. Post-initial authentication and the establishment of an identity confidence the ASCE will administer the degradation of confidence using the methodology (or similar to) outlined in subsection B. This concept of degradation will potentially be further influenced by the environment in which the device is being operated. To achieve this, ASCE will need to utilize an environment-sensing module that will learn to recognize localities and their associated threat, and use this to affect the rate at which the confidence in the user's identity is being eroded. As discussed earlier in this document, operating a laptop at home is expected to be less of a threat than using one whilst waiting in a public space; by adjusting the rate of decay accordingly, these expectations can be incorporated into the framework.

Authentication, although controlled and requested by the ASCE, will be carried out by authentication mechanisms that communicate via a generic interface. This will allow the ASCE to be a portable concept that can be applied to many different types of device, making it independent of a specific set of hardware. The generic approach aligns itself with the objectives of the BioAPI Consortium [28] which has specified an international standard for interfacing to biometric systems. Utilizing this framework and extending it to both biometric and non-biometric methodologies would enable a single engine to accept and function with a number of identity confirming processes. That is, a mobile phone should be typically capable of utilizing authentication via PIN, voice recognition, facial recognition or even keystroke analysis. One or more of these could be plugged into the engine facilitating the necessary provision of identity recognition. Figure 2 indicates that these authentication mechanisms can potentially be either internal or external to the physical device. Thus it is imperative that the generic interface be capable of meeting this additional requirement and interacting seamlessly with either approach.

Some devices will operate a two-way interaction with their surrounding security counterparts; for instance a laptop computer will both request and provide security details. However, it may be possible to utilize some entities that only contribute by their presence, providing a form of token-based security. Car keys are an example of such an item; incorporating these so that their mere presence, indicated by replying to a polled request, can be used to bolster security confidence in the user's identity (i.e. because the holder can show themselves to be in possession of a larger set of physical artefacts associated with the legitimate user).

Figure 3 below shows a succinct representation of the relative sophistication of devices that might be used by the ASCE. It can be argued that any device that can be placed on

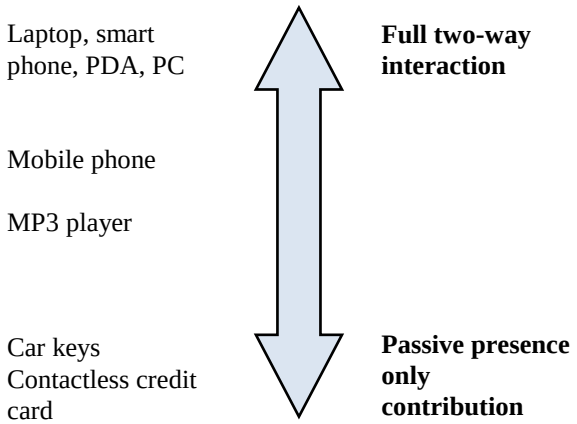

Figure 3. Varying levels of device sophistication and consequential contribution to authentication

the scale from "Full two-way" to "Passive presence only" can in some way contribute to the authentication aura. Indeed it can be argued that the use of passive technology carries a greater significance than active devices. Items that contribute only by their presence are likely to be carried out-of-sight, for instance car keys or contactless travel cards are held in a pocket or handbag and are not readily visible to a potential thief. Thus this inclusive approach is ultimately flexible and scalable to a huge variety of devices with or without built in processing intelligence.

Finally, as illustrated in Figure 2, the ASCE will use a data repository to store relevant information, parameters and details, of its own status and other devices in the security partnership. The repository is made up of a number of data tables that would store both persistent reference information and working details updated in real-time.

V. Discussion

In addition to the base technological concepts there are other matters that will require careful consideration prior to implementation of the framework. Privacy and the associated risk of transmitting biometric template information between devices when one is incapable of unilaterally processing a sample, is such an example. Appropriate encryption and communication channel security will have to be employed to protect against eavesdropping and remove the potential for

man-in-the-middle attacks. Introducing such protection will incur additional processing overheads that will impact upon the operational performance of the framework.

Indeed, computational, memory, battery and network performance issues also demand investigation to ensure that the framework can be adapted to function on as many categories and types of device as possible. Ultimately it is desirable to employ the smallest footprint possible, so it is inevitable that there will be some element of compromise to avoid precluding potential technology. The greater the number of devices that can be usefully employed within the aura, the more robust the system will become.

Although this paper has proposed biometrics as a suitable authentication candidate, it is important to note that with distinct methods greatly differing levels of performance can be experienced. This is amplified by the need to adapt some biometric techniques so they can be employed in a non-intrusive manner [15]. Designing the framework to operate with a plug-and-play capability will lessen some of these demands and enable alternatives to be used. Extrapolating this concept further, it will even allow devices to respond to the environment or mode of operation accordingly. Transparent authentication is the most desirable solution and equipping a mobile phone with the ability to undertake voice, facial and typing pattern recognition will provide techniques that cover the majority of occasions. However, such flexibility will concurrently increase the complexity of the necessary interface.

Trust is another major area of focus. Trust between devices will need to be established and at times revoked. It is imperative that this process correctly addresses usability and is implemented in a way that is logical, secure, yet easy to use. Aside from aesthetics, devices will also need the ability to receive and utilize un-trusted environmental information. Parsing this information correctly will enable devices to draw appropriate detail whist remaining secure and removed from threat. Gaining the trust of users is one further aspect that should not be underestimated. For too long, owners have relied upon passwords and PINs to uphold their security. It will not be easy to sufficiently reassure them to accept an approach that could potentially not require them to enter any form of identity confirmation. If enough recognisable devices are present and the aura is strong, a newly activated device may be content to allow usage without any form of polled authentication.

Operational thresholds for applications and device services are one final area that requires further investigation. As yet it is unclear how best to invoke them; a simple ranking and user selected scale may be suitable for some applications but for others a more complex approach dependent upon a number of variables might be more fitting. It is required to empirically establish the latent potential that is believed to exist in the surroundings and the devices that are in regular everyday use. Through this experimentation, ongoing research and as the design of the framework evolves it is hoped that these factors will clarify and allow appropriate decisions to be taken.

VI. Conclusion

It is desirable that security and the way in which most users authenticate themselves with mobile devices should now evolve to a more holistic level. For too long manufacturers have had little choice but to rely upon password or PIN-based mechanisms to secure what are becoming ever more sophisticated devices, with ever increasing replacement and misuse costs. This paper suggests an approach that will allow disparate personal devices to trade security information and glean confidence of identity from their peers. It may potentially offer a way in which user identity can be ascertained and communicated to non-personal devices, supporting the interactions individual's have and augmenting the safeguards that are currently in place.

The ability to create a near-field authentication aura will enable technologists to review device activation procedures. Under certain circumstances they may even be able to demote or possibly remove a user's requirement to repetitively logon to multiple entities during successive activations. Further work will undertake the development of a prototype framework to determine the feasibility and working advantage of such an approach, whilst reviewing the perception and response of the wider user population.

Acknowledgment

It is acknowledged that the research outlined in this paper has been undertaken with the generous backing of Orange-France Telecom.

References

[1] "Hotspot usage is increasingly shifting away from notebooks and laptops and toward handhelds", In-stat website, available: http://www.instat.com/newmk.asp?ID=2695&SourceID=0000035200000000000 [accessed: 18 Jan. 09].

[2] S. Kurkovsky, E. Syta, "Digital natives and mobile phones: A survey of practices and attitudes about privacy and security", In *Prococeedings of IEEE International Symposium on Technology and Society (ISTAS 2010)*, IEEE Press, pp.441-449, 7-9 June 2010 doi: 10.1109/ISTAS.2010.5514610.

[3] "Reducing Crime: Robbery", Home Office website, available: http://www.homeoffice.gov.uk/crime-victims/reducing-crime/robbery/ [accessed: 27 Feb. 10].

[4] " 'IFfraud' Fuels Rise In Scam Phone Claims", CPP Group website, available: http://www.cppgroupplc.com/news/press-release.shtml [accessed: 26 Feb. 10].

[5] "Mountains of Mobiles Left in the Back of New York Cabs", Credant website, available: http://www.credant.com/news-a-events/press-releases/ 229-mountains-of-mobiles-left-in-the-back-of-new-york-cabs.html [accessed: 26 Feb. 10].

[6] L. Rohde, "UK Government Asks Industry to Fight Mobile Phone Theft", *Infoworld*, vol. 23, no. 5, p. 76, Jan. 2001.

[7] "Design Out Crime: Hot Product Crime", Design Council website, available: http://www.designcouncil.

org.uk/Design-Council/Files/ Landing-pages /Design-Out-Crime/Hot-Product-crime
[accessed: 02 Mar 10].

[8] M. Prenksy, "Digital Natives", *Digital Immigrants On the Horizon*, vol. 9, no. 5, pp. 1-6, October 2001
doi: 10.1108/10748120110424816.

[9] N. L. Clarke and S. M. Furnell, "Authentication of Users on Mobile Telephones – A Survey of Attitudes and Opinions", *Computers & Security*, vol. 24, no. 7, pp. 519-527, October 2005
doi:10.1016/j.cose.2005.08.003.

[10] H. M. Wood, "The Use of Passwords for Controlling Access to Remote Computer Systems and Services", In *Proceedings of American Federation of Information Processing Societies: 1977 National Computer Conference (AFIPS 77)*, AFIPS Press, pp. 27-33, June 1977
doi: 10.1145/1499402.1499410.

[11] E. Albrechtsen, "A Qualitative Study of Users' Views on Information Security", *Computers & Security*, vol. 26, no. 4, pp. 276-289, June 2007
doi:10.1016/j.cose.2006.11.004.

[12] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", In *Proceedings of the IEEE*, IEEE Press, vol. 91, no. 12, pp. 2019-2040, December 2003
doi: 10.1109/JPROC.2003.819611.

[13] K-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B-L. Tai, J. Cook and E. E. Schultz, "Improving Password Security and Memorability to Protect Personal and Organizational Information", In *International Journal of Human-Computer Studies*, vol. 65, no. 8, pp. 744–757, August 2007
doi: 10.1016/j.ijhcs.2007.03.007.

[14] T. Sim, S. Zhang, R. Janakiraman and S. Kumar, "Continuous Verification Using Multimodal Biometrics", In *IEEE Transactions on Pattern Analysis and Machine Intelligence*, IEEE Press, vol. 29, no. 4, pp. 687-700, April 2007
doi:10.1109/TPAMI.2007.1010.

[15] N. L. Clarke and S. M. Furnell, "Advanced User Authentication for Mobile Devices", *Computers & Security*, vol. 26, no. 2, pp. 109-119, March 2007
doi:10.1016/j.cose.2006.08.008.

[16] A. Azzini, E. Damiani and S. Marrara, "Ensuring the Identity of a User in Time: A Multi-Modal Fuzzy Approach", In *Proceedings of IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA 2007)*, IEEE Press, pp. 94-99, 27-29 June 2007
doi:10.1109/CIMSA.2007.4362546.

[17] A. T. B. Jin, D. N. C. Ling and A. Goh, "Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number", *Pattern Recognition*, vol. 37, no. 11, pp. 2245-2255, November 2004
doi:10.1016/j.patcog.2004.04.011.

[18] D-J. Kim and K-S. Hong, "Multimodal Biometric Authentication using Teeth Image and Voice in Mobile Environment", In *IEEE Transactions on Consumer Electronics*, IEEE Press, vol. 54, no. 4, pp. 1790-1797, November 2008
doi: 10.1109/TCE.2008.4711236.

[19] R. J. Hulsebosch and P. W. G. Ebben, "Enhancing Face Recognition with Location Information", In *Proceedings of 2008 Third International Conference on Availability, Reliability and Security (ARES 08)*, IEEE Press, pp. 397-403, 4-7 March 2008
doi: 10.1109/ARES.2008.45.

[20] N. L. Clarke and S. M. Furnell, "Authenticating Mobile Phone Users Using Keystroke Analysis", In *International Journal of Information Security*, vol. 6, no. 1, pp. 1-14, January 2007
doi:10.1007/s10207-006-0006-6.

[21] F. Monrose and A. D. Rubin, "Keystroke Dynamics as a Biometric for Authentication", *Future Generation Computer Systems*, vol. 16, no. 4, pp. 351–359, February 2000
doi: 10.1016/S0167-739X(99)00059-X.

[22] S. M. Furnell, N. L. Clarke and S. Karatzouni, "Beyond the PIN: Enhancing user authentication for mobile devices", *Computer Fraud & Security*, vol. 2008, no. 8, pp. 12-17, August 2008
doi:10.1016/S1361-3723(08)70127-1.

[23] A. C. Weaver, "Biometric Authentication", *Computer*, vol. 39, no. 2, pp. 96-97, February 2006
doi: 10.1109/MC.2006.47.

[24] S. Prabhakar, S. Pankanti and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33-42, March 2003
doi: 10.1109/MSECP.2003.1193209.

[25] A. Ross and A. K. Jain, "Multimodal Biometrics: An Overview", In *Proceedings of 12th European Signal Processing Conference (EUSIPCO)*, EURASIP Press, pp. 1221-1224, September 2004

[26] O. Arandjelovic, R. Hammoud and R. Cipolla, "Multi-sensory Face Biometric Fusion (for Personal Identification)", In *Proeedings of. IEEE 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 06)*, IEEE Press, p. 52, 17-22 June 2006
doi: 10.1109/CVPRW.2006.136.

[27] A. Boukerche and M. S. M. Annoni Notare, "Behavior-based Intrusion Detection in Mobile Phone Systems", *Parallel and Distributed Computing*, vol. 62, no. 9, pp. 1476-1490, September 2002
doi: 10.1006/jpdc.2002.1857.

[28] "Objectives", BioAPI Consortium website, available: http://www.bioapi.org/objectives.asp
[accessed: 03 Dec. 09].

Author Biographies

Chris Hocking achieved a BSc (Hons) in mathematics and statistics from the University of London, Goldsmiths' College in 1986. After an eighteen year career in industry he returned to education attaining an MSc in web technologies and security from the University of Plymouth in 2007. Since this time Chris has focussed his research on the security of mobile devices and anticipates completing his PhD during 2011.

Steven Furnell gained a BSc (Hons) in computing and informatics from the University of Plymouth, UK in 1992, followed by a PhD in information security from the same institution in 1995. His research interests continue to focus upon security issues, including user authentication, intrusion detection, usability, and security culture. Prof. Furnell is active within three working groups of the International Federation for Information Processing (IFIP) – namely Information Security Management, Information Security Education, and Human Aspects of Information Security & Assurance. He is the author of over 210 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society (2001) and Computer Insecurity: Risking the System (2005). Further details can be found at www.plymouth.ac.uk/cscan.

Nathan Clarke graduated with a BEng (Hons) degree in electronic engineering in 2001 and a PhD in 2004 from the University of Plymouth. He has remained at the institution and is now an Associate Professor in Information Security and Digital Forensics within the Centre for Security, Communications and Network Research. Dr Clarke is also an adjunct scholar at Edith Cowan University, Western Australia. His research interests include user identity, mobility and intrusion detection; having published 55 papers in international journals and conferences. Dr Clarke is a chartered engineer, a fellow of the British Computing Society (BCS), and a UK representative in the International Federation of Information Processing (IFIP) working groups relating to the Human Aspects of Information Security & Assurance (co-vice chair), Identity Management and Information Security Education. Dr Clarke is the author of Computer Forensics: A Pocket Guide published by IT Governance and a forthcoming book on Transparent Authentication to be published by Springer in 2011.

Paul Reynolds is a technical specialist in Internet based mobile telecommunications. He has a doctorate in Advance Telecommunications and is a Fellow of the Institution of Electrical Engineers. Until recently he was Head of Research for France Telecom/Orange and currently is the CTO of a software start-up company "Conetivita". Among other things he has: directed the European Union's funded research into distributed computing for mobile telecommunications; designed mobile telecommunication networks for eight countries; chaired sessions at two European Union Mobile Communication Summits; been the technical leader of the Mobile Wireless Internet Forum and of two major European Union research projects; and, been the chairman of EU's Group responsible for leadership of Europe wide next generation mobile telecommunications. Since 1993 he has authored 11 patents, and over 40 published technical papers, in the area of telecommunications.

research interests continue to focus upon security issues, including user authentication, intrusion detection, usability, and security culture. Prof. Furnell is active within three working groups of the International Federation for Information Processing (IFIP) – namely Information Security Management, Information Security Education, and Human Aspects of Information Security & Assurance. He is the author of over 210 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society (2001) and Computer Insecurity: Risking the System (2005). Further details can be found at www.plymouth.ac.uk/cscan.

Dr Nathan Clarke graduated with a BEng (Hons) degree in electronic engineering in 2001 and a PhD in 2004 from the University of Plymouth. He has remained at the institution and is now an Associate Professor in Information Security and Digital Forensics within the Centre for Security, Communications and Network Research. Dr Clarke is also an adjunct scholar at Edith Cowan University, Western Australia. His research interests include user identity, mobility and intrusion detection; having published 55 papers in international journals and conferences. Dr Clarke is a chartered engineer, a fellow of the British Computing Society (BCS), and a UK representative in the International Federation of Information Processing (IFIP) working groups relating to the Human Aspects of Information Security & Assurance (co-vice chair), Identity Management and Information Security Education. Dr Clarke is the author of Computer Forensics: A Pocket Guide published by IT Governance and a forthcoming book on Transparent Authentication to be published by Springer in 2011.

Professor Paul Reynolds is a technical specialist in Internet based mobile telecommunications. He has a doctorate in Advance Telecommunications and is a Fellow of the Institution of Electrical Engineers. Until recently he was Head of Research for France Telecom/Orange and currently is the CTO of a software start-up company "Conetivita". Among other things he has: directed the European Union's funded research into distributed computing for mobile telecommunications; designed mobile telecommunication networks for eight countries; chaired sessions at two European Union Mobile Communication Summits; been the technical leader of the Mobile Wireless Internet Forum and of two major European Union research projects; and, been the chairman of EU's Group responsible for leadership of Europe wide next generation mobile telecommunications. Since 1993 he has authored 11 patents, and over 40 published technical papers, in the area of telecommunications.