2011

A preliminary investigation of distributed and cooperative user authentication

C G. Hocking
Plymouth University, UK

S M. Furnell
Edith Cowan University

N L. Clarke
Edith Cowan University

P L. Reynolds
Plymouth University, UK

DOI: 10.4225/75/57b531b8cd8bd
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

A PRELIMINARY INVESTIGATION OF DISTRIBUTED AND COOPERATIVE USER AUTHENTICATION

C. G. Hocking[1], S. M. Furnell[1,2], N. L. Clarke[1,2] & P. L. Reynolds[1]
[1] Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK
[2] School of Computer and Information Science, Edith Cowan University, Perth, Western Australia
info@cscan.org

Abstract
Smartphones and other highly mobile yet sophisticated technologies are rapidly spreading through society and increasingly finding their way into pockets and handbags. As reliance upon these intensifies and familiarity grows, human nature dictates that more and more personal details and information is now to be found upon such devices. The need to secure and protect this valuable and desirable information is becoming ever more prevalent. Building upon previous work which proposed a novel approach to user authentication, an Authentication Aura, this paper investigates the latent security potential contained in surrounding devices in everyday life. An experiment has been undertaken to ascertain the technological infrastructure, devices and inert objects that surround individuals to establish if these items might be significant. The results suggest that inert possessions may offer a surprisingly large potential with some being in close proximity to experimental subjects for over 45% of the entire period. With other graphical analysis illustrating the consistency of presence, this work suggests that everyday possessions and devices can be leveraged to augment traditional approaches and even in certain circumstances, during device activation remove the need to authenticate.

Keywords
Authentication, identification, mobile, security, identity

INTRODUCTION

As modern communication technology permeates ever further throughout society, the desire to remain in constant contact with colleagues, friends and family is increasingly met. The recent surge in sales of smart phones and other sophisticated mobile devices has driven a correlated explosion in Wi-Fi hotspot usage (In-stat, 2009; In-stat, 2011). Technological boundaries are stretching and the devices people carry are evolving with expanding storage capabilities and processing power, enabling the porting of greater amounts of information and personal details. As this becomes the norm for us all, these personal items become an ever-increasing target for theft (CPP, 2010; Home Office, 2009). 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 (Design Council, 2010; Rohde, 2001).

Authentication of the user's identity by any device provides the first line of defence in the battle to maintain data integrity following theft or loss. Establishing as far as possible that the operator is whom they purport to be, provides a device with the necessary degree of confidence to allow access and service utilisation. However, although steps have been taken to ensure the devices are only accessed by accredited individuals, the ubiquitous point of entry user identity code and password has been rendered susceptible to abuse through the inability or unwillingness of individuals to protect and administer this sensitive information correctly (Albrechtsen, 2007; Clarke and Furnell, 2005). In the event that several devices are carried simultaneously, the repeated intrusive accreditation process becomes laborious and inconvenient. Improving and evolving the employed authentication mechanism will go some way to counteract this burden and potentially provide an opportunity to increase the confidence in user identity. If a user has previously authenticated upon a device, why not use that confidence to provide automated access to other devices within a close proximity? Alternatively, authentication judgements made across several devices could also be used to deliver a collective confidence level – increasing the level of identity confidence that any one device could provide. Authentication Aura proposes to enable this distributed and collaborative environment that seeks to improve the level of authentication security and minimise user inconvenience.

With intelligent gadgets, technical infrastructure, possessions and other factors playing such a pivotal role in the Authentication Aura's operation it is vital to establish the viability of such an approach. Experiments have been carried out to assess the latent potential the presence of the electronic devices and currently dumb objects offer by assessing the amount of time individuals spend within detectable range of these pervasive items.

The following two sections further outline the Authentication Aura concept and then proceed to detail the experiment which has been undertaken. This is then succeeded by an analysis of the experimental findings,

exploring the manner in which identity confidence could be influenced and how it could be utilised to calculate a new and reactive status. A summary of the paper's findings are then outlined in a conclusion.

BACKGROUND

With the accepted fragility of the ubiquitous point of entry user identity and password authentication, research has been widespread in attempting to improve upon this current situation (O' Gorman, 2003; Vu et al., 2007). One tranche of work, the Authentication Aura, suggested a distributed approach in which trusted and known devices that had all performed unilateral authentication, shared information between one another to bolster confidence in their own user's identity (Hocking et al., 2010). This section briefly outlines the concept of the Aura, enabling the reader to gain an understanding of the motivation behind the current research.

As an individual authenticates with a personal device, the piece of equipment establishes a confidence in the user's identity. In most scenarios this is Boolean, the user is either whom they claim to be (they pass the authentication process) or they are not (they fail); thus the confidence is set at either complete (100%) and access is granted or it is none and the user is barred. The Authentication Aura suggests the use of confidence erosion following validated access which can in turn be utilised to reduce the availability of device functionality. High confidence will permit the use of expensive applications and access to sensitive data, whilst reduced confidence will block the use of these functions. Then when confidence erodes to a suitably low level, re-authentication of the user will be necessary to ensure continuing availability of use.

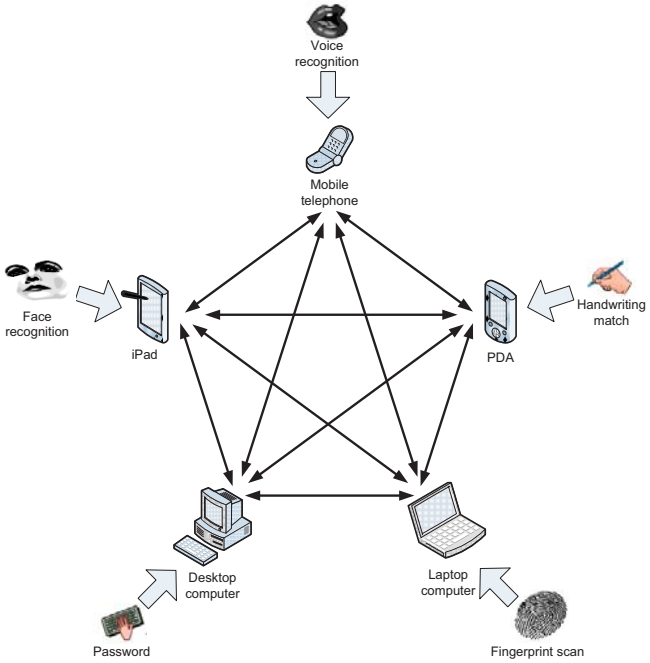

Figure 1.The potential intra-device relationship and authentication techniques (Hocking et al., 2010)

To counteract this one-way-street, information pertaining to location, time since and method of authentication can be communicated between trusted devices; the Authentication Aura utilises each set of these conveyed details and other detected possessions to calculate a positive confidence contribution, slowing the degradation process. Figure 1 shows an example of how the information might be relayed amongst a group of commonly owned devices.

For some intelligent devices it might be possible to undertake continuous authentication (such as voice recognition during telephone calls) to provide frequently reconfirmed identity details and a valuable confidence contribution, whilst others might simply act as tokens, their presence the only information of use. Figure 2 summarises this.

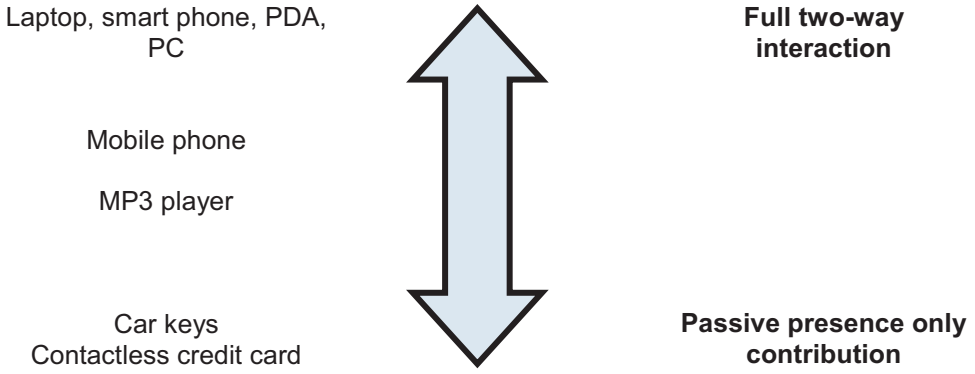

Figure 2. Varying levels of device sophistication and consequent contribution to the authentication process

If the Authentication Aura is successfully implemented, there is even the potential to achieve device activation without the need for authentication. For instance, if a user with a number of present and active devices proceeds to switch on another item of equipment, there might be sufficient relayed confidence available to make the newly activated item content to permit access immediately without additional intervention. With users currently performing many authentications during a day, any savings that can be gleaned must intuitively be of benefit.

EXPERIMENT

Motivation and approach

The concept of an Authentication Aura relies on the intercommunication of information between intelligent devices supplemented by the detection of inert household or personal items (Hocking et al., 2010). To initially gauge the viability of this concept it is imperative that a data gathering exercise be undertaken to ascertain what devices are present within a short distance of an experimental participant at various points in time. This information can then be analysed to determine if there is a latent potential in surrounding devices that can be leveraged to augment traditional security.

It would have been relatively straightforward to execute such a task on entirely intelligent devices however the premise dictates that both dumb objects and those that might be intelligent in the future (such as household white goods), are also included. An obvious solution would be to provide experimental subjects with pen and paper to record devices and items that surround them at any given moment, over a period of days. Intuitively this is far from practical. Forgetfulness and sheer imposition renders this an inappropriate approach; an alternative means of surveying an individuals surrounding locale needed to be found.

With the requirement to include dumb and currently incapable devices, the selected method by which the appropriate information could be identified and recorded uses radio frequency identity (RFID) tags and associated sensing equipment. Each tag transmits a unique identification marker continuously across a short distance. By positioning a number of these on or near individual devices and objects of interest, it is possible for a small portable lightweight RFID reader to be constantly carried by a subject, allowing all detected tags to be recorded at discrete time intervals. This is of suitable imposition to ensure experimental volunteers were forthcoming.

Details

To facilitate the experiment equipment was purchased to enable the recording of data simultaneously for five subjects. Although in an ideal world as many candidates as possible would undertake the experiment at any one time, the prohibitive cost of equipment restricted the sample groups to five, an affordable number that would yield a meaningful set of results. The PDA RFID readers were Dell Axim x51s, each equipped with CompactFlash RFID nodes, capable of reading both passive and active RFID tags. Passive tags transmit their identity in response to a polled request from the reader inducing their power from the received signal; active tags however contain their own independent power supply in the form of a battery. Although active tags are much more expensive to buy their main advantage is that they can be detected over a far greater range, 10-15m in clear

line-of-sight, opposed to a maximum of 0.5m for the passive tags. Wi-Fi network infrastructure can provide connections over a wide area and so with the need to emulate this, the experiment requires detection of tags across several metres and through walls; it was therefore deemed prudent to spend the extra resource and secure the active variety. As such, seventy-five active tags were purchased enabling each individual volunteer to be supplied with fifteen, permitting them to identify and record a sufficient number of devices both at home and in their workspace.

Table 1. Suggested locations for the RFID tags

Mobile phone	Work PC	Home PC/Laptop	Work Wi-Fi point
Home Wi-Fi Point	TV (s)	Car interior	Car keys
Wallet/purse	mp3 player	Work bag/briefcase	Home telephone
Bedside clock	Fridge	Hi-Fi	Coat pocket

Groups of volunteers that worked together were picked to ensure there was a degree of crossover within their daytime activity allowing each subject's recording equipment to detect other participant's tags. In a functioning Aura environment additional security could be engendered from familiar devices belonging to friends or colleagues even though they are not specifically owned by the same user. Selecting groups in this way would provide a dimension to the results data that could be analysed to assess this premise.

Each group of five subjects was instructed to undertake the experiment for fourteen days continuously, carrying the PDA with them at all times whilst ensuring that it remained charged and active. Software was written and deployed to the PDAs which recorded all detectable tag identities within range, their signal strength and time stamp, at one minute intervals. The individual's tags were placed upon or attached to items of interest representing intelligent and dumb devices, personal possessions and infrastructure. A cross-reference list of tag identities and locations was recorded, enabling the identification of relevant items during later analysis..

Initial observations

Upon removing the data files and commencing analysis some initial observations have been made. With observations occurring each and every minute, twenty four hours a day, seven days a week the data set is intuitively large. For each of the participants the experiment yields 1,440 sets of readings each day which equates to 10,080 in total across a single week.

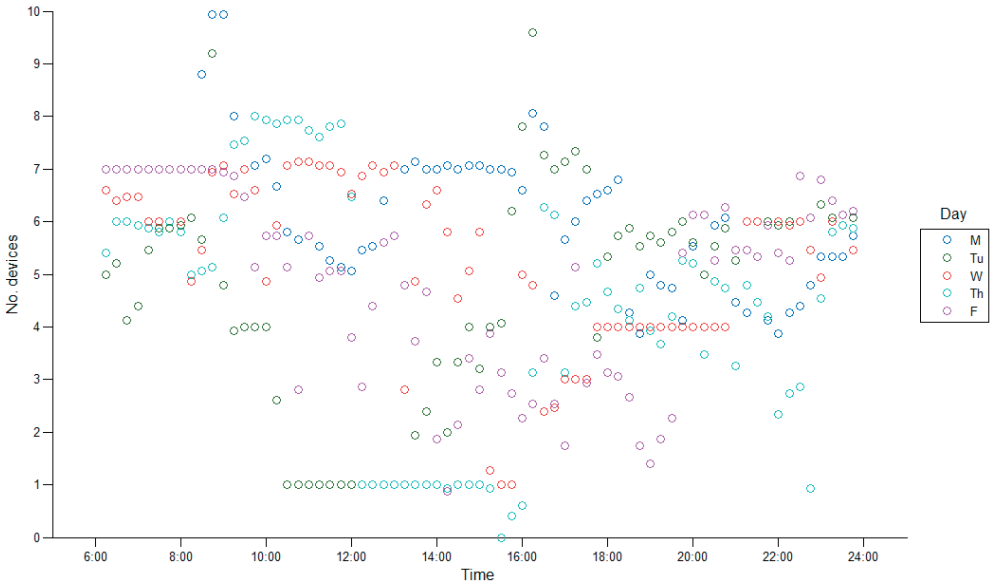

Figure 3. A typical user's weekday observations

Figure 3 illustrates the number of unique devices observed by an individual during a working week (Monday-Friday). Each day is plotted as a separate set of readings with individual data points representing the average number of detected devices within a fifteen minute period plotted against the time of day that the observation was made.

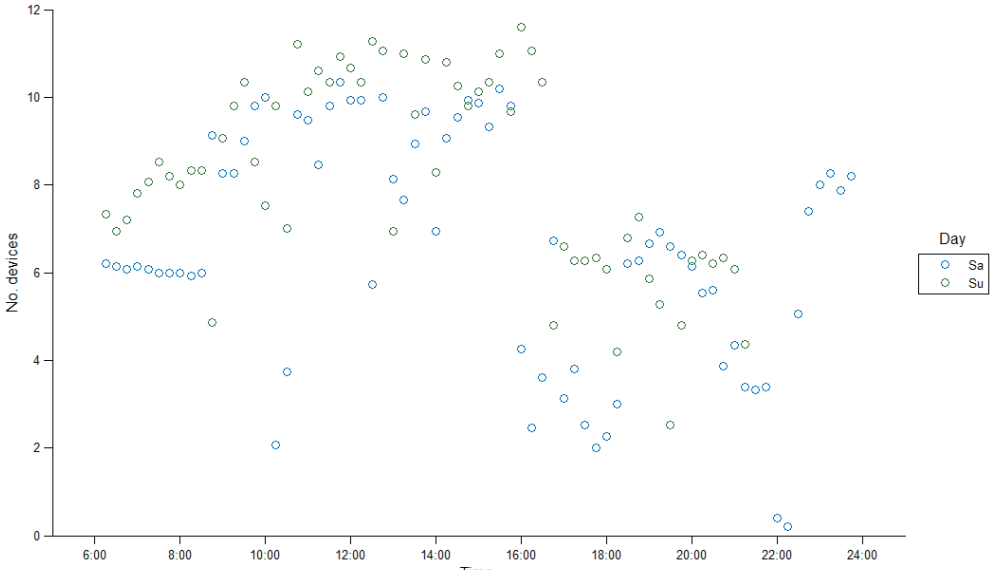

Figure 4. The same typical user's weekend observations

The weekday plot exhibits a maximum average of ten devices being detected in any given fifteen minute slot whilst at the weekend this figure peaks at twelve, suggesting that more static tags were located at home rather than at work. However, with such a high number of observations being recorded at both home and work it is apparent that the majority of tags were placed on portable possessions that the subject carried with them throughout the day. During the workdays there appears a high degree of variation in the number of observed devices implying that this subject is active during their employment and even spends time out of the office. Time away from their usual location can be perceived from the data on Tuesday and Thursday between 10a.m. and 4p.m. where the average falls to a single unit.

With the observed variations, fluctuations and even periods of consistency it is possible to immediately conjecture that scope exists to leverage this information for use in security.

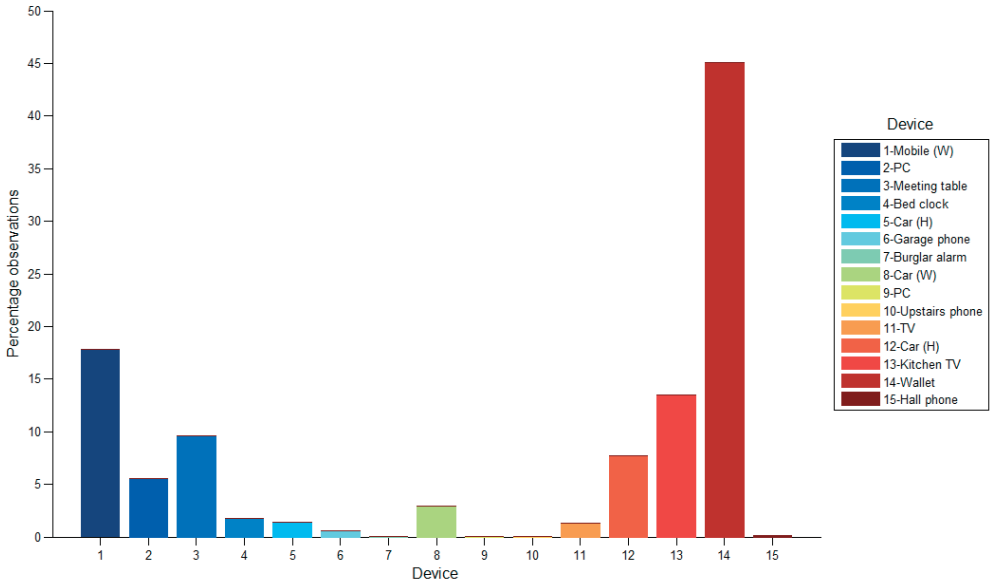

Figure 5. A single user's specific device observations

Figure 5 above illustrates a histogram that has been compiled from observations of specific devices for a user throughout the duration of their fourteen day experimental participation. It shows the percentage of observations that recorded each of their fifteen RFID tags, cross-referenced to identify the specific devices or items of equipment. Clearly from this diagram, there is one personal item that was detected far more often than any other. The subject's wallet was observed during approximately 45% of all recordings executed during the two week

experiment. So do inert devices or personal items provide greater security leverage than intelligent ones? For the same user, by plotting days' observations in isolation (Figures 6 and 7) it is possible to examine more clearly how the user's routine affects the devices that are detected. These diagrams illustrate the continuity of presence for each possession or item of equipment across the day, when contact is established and when it is lost. Additionally, other users' devices are also shown (Other devices) indicating when they are also detected. Intuitively, these foreign device contacts mainly appear on the weekday plot (Figure 6) because the other members of the experimental group were all work colleagues but there is a single set of blips visible at approximately 16:15 at the weekend, suggesting that the subject briefly visited their work premises.

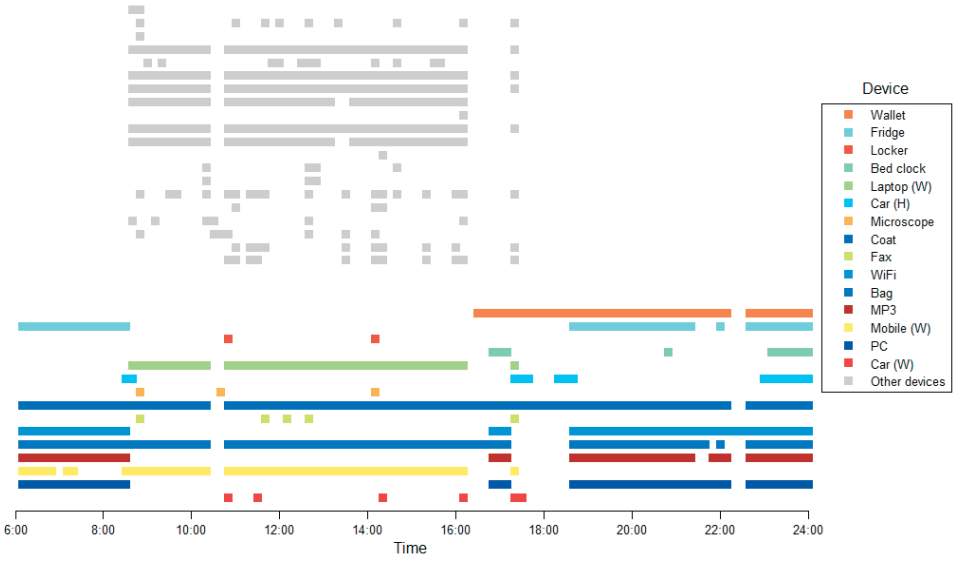

Figure 6. A user's isolated single weekday activity

It is interesting to note that in both examples nearly the entire observation window from 6a.m. to 12p.m. has at least one device within detection range at any given moment. Indeed, closer examination appears to suggest that the inert devices are present most consistently throughout the day, supporting the potential for security leverage.

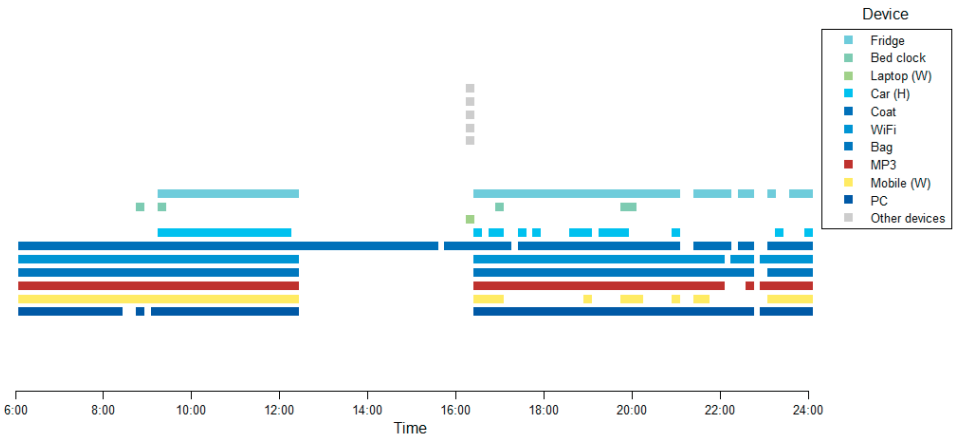

Figure 7. The same user's isolated single weekend day activity

The discussion above has concentrated upon and examined the data from just a single user. It would require a study of many subjects to ascertain if this is unequivocally true or false, a volume of data that is not currently available. However within the current sample set high percentages of experimental detection are attributed to inert personal items when they were selected by an individual; indeed coats, work bags and hand bags all topped the frequency chart for particular participants. Clearly it cannot be stated that they provide a greater security

potential but equally it is important they should be utilised where possible because of their persistence and inconspicuous presence.

CONFIDENCE

Confidence of identity

The concept of an Authentication Aura utilises confidence of the user's identity in two ways. When a device is activated and the initial security check (if there is one) is passed, the confidence of the device in the user's identity at that moment in time is high. The authentication has been passed and usually an implicit trust is made by the device in giving the user unrestricted access to the services and data it holds. This level of trust remains unwavering and unchallenged unless barriers such as a PIN protected screen saver/lock are implemented. Rather than continuing in this way the Aura concept erodes the user identity confidence over time; the longer it has been since an authentication was undertaken the lower the confidence will be. This degrading value will then be assessed and utilised to restrict some of the processes and applications available for use; eventually at a prescribed threshold unobtrusive re-authentication will be executed to reaffirm the user's identity. It is of course rather simplistic to simply erode the confidence and so to counteract this effect the concept incorporates communicated authentication details from other trusted devices to positively boost the device's identity confidence. Thus at a point in time the device has a confidence in the user's identity that is a combination of time since last authentication, the authentication method used and information received from surrounding devices. The Aura concept's calculation of user identity confidence is encapsulated by Equation 1.

$$C_x = \left[F_1(t_x, m_x) + \left(\sum_{i=1}^{n} F_2(t_i, m_i) \right) \right]_{min\ 0}^{max\ 100}$$

Equation 1. Formula for calculating a device's user identity confidence

In the equation:

- x signifies the user device on which the confidence C is being calculated. C is bounded within the range 0.0 to 100.0 inclusively.
- Function F_1 calculates the amount of confidence using t the time since authentication was carried out on the given device (x) and m the authentication method that was used.
- n represents the number of devices (both intelligent and dumb) that constitute the current Authentication Aura.
- Function F_2 yields the contribution to confidence that each Aura member ($i = 1..n$) makes to the receiving device x. Similarly to F_1 this function utilises both time since authentication (t) and the method used (m) in its calculation.

With confidence eroding and a re-authentication threshold in situ the influence of the surrounding Aura members will delay and even potentially postpone the need for the reaffirmation process to be undertaken. If the framework and process model are designed with an appropriate logical path, it may indeed be the case that initial activation authentication be by-passed because a suitably high level of confidence can be drawn from the surrounding trusted devices.

It is appropriate to examine the potential of the confidence contribution to establish if there is sufficient evidence to progress this concept and hone the method by which function F_2 might be invoked.

Contribution from Aura members

It is vital to establish or at least explore how the function (F_2 in Equation 1) might be conceived and operate. Previous work has indicated that inherited confidence should be influenced by and adapt to location, the types of devices active within the Aura and the authentication methods they use (Hocking et al., 2010); these should thus be incorporated into the implemented function. To achieve this it is necessary to quantify scales of numeric values that can be implemented and then assessed to gauge performance.

As an initial first step, location can be allocated a simple tri-value range, home, work or other; equated to 3, 2 or 1 respectively. Apportioning values in this way will enable a variation in confidence contribution to be accomplished. It is reasonable to argue that whilst at home devices should operate with less heightened security and be more relaxed about the way in which they are being used. Similarly at work, although assured the operating environment is less safe than within the owner's home. Finally being away from both home and work is the time when a device should be most wary and inherit least confidence from surrounding pieces of equipment. Initially for assessment purposes this three point scale can be used as a simple multiplier resulting in inherited confidence at home being 50% more significant than that received from the same devices at work and three times more whilst in other unrecognised locations.

In addition to location, it is imperative that the significance of the device is somehow incorporated into the contribution formula. As highlighted earlier in this paper some devices are more often detectable and less visible, a combination which arguably makes them of greater significance. With this being a mathematical calculation it seems sensible to allocate a ranking value (in the range 1..10) to each item of equipment owned by a user and use this within the formula, this will be referred to as the device's rank. It is proposed that a rank of 1 should indicate the most significant pieces of equipment whilst 10 the least. This value can then be used as a divisor to reduce the relative contribution of each device.

To establish the latent potential of drawing confidence from surrounding devices it is initially advantageous to keep the function as simple as possible. Therefore, although Equation 1 indicated that the specific confidence of any communicating device would be used currently a rigid maximum value will be set for each. To initiate investigation this will be fixed at 15%. In a fully operational model this would be allocated on a device by device basis and then reduced by the time that has elapsed since authentication and the method used.

Thus the initial formula for F_2 and the contribution made by device i becomes:-

$$c_i = \left(\frac{15}{r_i}\right) \times l$$

Equation 2. Formula for F2 to test the potential of confidence contribution made by each device

Where …

- i signifies the contributing device.
- r is the significance rank of device i (in the range 1..10).
- l is the location multiplier (in the range 1..3).

Thus a device whose presence is regarded as being most significant (i.e. has a rank of 1) that is detected whilst the user is at home (location multiplier equal to 3) contributes 45% to the confidence of the host device. However, in the same location a device of medium significance (rank 5) would only contribute 9% and one of least significance (rank 10) just 4.5%.

To aid in the clarity of this brief investigation a single day's data for one user will be isolated and plotted so a subjective appraisal can be made.

Table 2. Table of selected equipment and allocated rankings

Equipment	Rank	Equipment	Rank	Equipment	Rank
Wallet	2	Car (Home)	3	Bag	4
Fridge	4	Microscope	5	MP3	6
Locker	6	Coat	4	PC	6
Bed clock	4	Fax	9	Car (Work)	5
Laptop (Work)	8	WiFi (Home)	5	Mobile (Work)	5

The user chose to tag the fifteen items of equipment shown in the table above, enabling them to be detected during the experiment. The table also indicates the allocated ranking to each device.

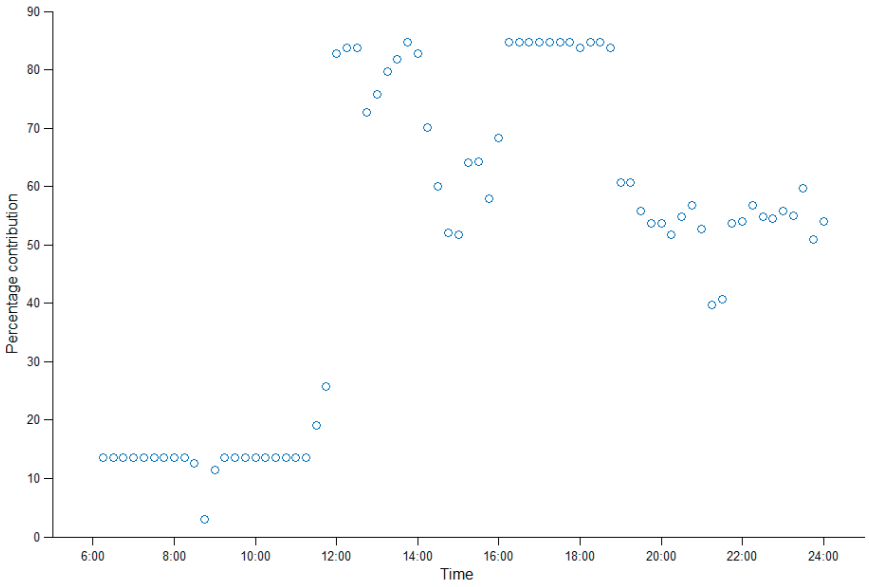

Figure 8. Subjective rankings for a single day's data and the associated percentage contribution

Introducing the subjective rankings (as shown in Table 2) to the data has the effect of yielding the cumulative percentage contribution plot shown in Figure 8. The most significant devices and those set with the lowest rank were the subject's home appliances, bag, personal car and mobile phone, whilst the remaining gadgets and possessions were set with mid to high range values. Although this allocation is subjective it is based on the premise that the higher ranking objects should be those that are personal or large and immoveable, providing less obvious security enforcement. For instance, the user's wallet is the highest ranking device (2), closely followed by their personal car, bag, fridge and coat. Applying these ranking values to the devices and employing the user's location, the cumulative percentage contribution for the observed items, at each given point in time, was calculated and then plotted against the associated time of day. This allocation of rankings appears to deliver a good spread of contribution percentages, reflecting the environment and highlighting the potential of this approach to deliver security enhancement. Without any degradation of confidence occurring on the communicating devices the percentage contribution tops out at nearly 90%, a far greater figure than would normally be observed. Although abnormally high this value further supports the argument that it may indeed be possible in certain circumstances for newly activated devices to avoid having to perform a sequence of authentication at all; the communicated confidence in the user's identity being sufficient.

CONCLUSION

An investigation into inherited confidence has demonstrated that there is indeed scope for such a methodology to positively contribute toward this alternative approach to device security. Although the assessment of confidence contribution was founded on simplistic algorithms the findings confirmed the latent potential of this method. Extroverted awareness of surroundings and other objects can be positively leveraged both unilaterally and within a cooperative set of devices. Surprisingly perhaps some of the greatest security reassurance can be drawn from inert possessions that we might not readily expect, especially those that are not immediately visible but are carried on a daily basis.

Utilising these findings as ground work for the next stage of investigation it is now possible to develop a working prototype based upon the concepts outlined in this paper. Functioning agent software can now be written and tested to further establish the practicality of this method and if there are restrictions that are currently unforeseen.

ACKNOWLEDGEMENTS

The research presented in this paper has been undertaken with funding and support from Orange-France Telecom.

REFERENCES

Albrechtsen, E. (2007). 'A Qualitative Study of Users' View on Information Security'. *Computers and Security*. 26(4), pp. 276-289.

Clarke, N. L. and Furnell, S. M. (2005). 'Authentication of users on mobile telephones – a survey of attitudes and opinions'. *Computers & Security*. 24(7), pp. 519-527.

CPP (2010). '"IFfraud" Fuels Rise In Scam Phone Claims'. *CPP Group*. Retrieved February 26, 2010 from http://www.cppgroupplc.com /news/press-release.shtml

Design Council (2010). 'Design Out Crime: Hot Product Crime'. *Design Council*. Retrieved March 2, 2010 from http://www.designcouncil.org.uk/Design-Council/Files/Landing-pages/Design-Out-Crime/Hot-Product-crime/

Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2010). 'A distributed and cooperative user authentication framework': 6th International Conference on Information Assurance and Security (IAS 2010). Atlanta, USA, 23rd-25th August 2010, pp. 304-310.

Home Office (2009). 'Reducing Crime: Robbery', *Home Office website*. Retrieved February 27, 2010 from http://www.homeoffice.gov.uk/crime-victims/reducing-crime/robbery/

In-stat (2009). 'Hotspot Usage is Increasingly Shifting Away From Notebooks and Laptops and Toward Handhelds'. *In-stat*. Retrieved January 18, 2009 from http://www.instat.com/newmk.asp?ID=2695&SourceID=00000352000000000000

In-stat (2011). 'Hotspot Usage to Reach 120 Billion Connects by 2015'. *In-stat*. Retrieved September 15, 2011 from http://www.in-stat.com/press.asp?ID=3246&sku=IN1105002WS

O'Gorman, L. (2003). 'Comparing Passwords, Tokens, and Biometrics for User Authentication'. *Proceedings of the IEEE.* 91(12), pp. 2019-2040.

Rohde, L. (2001). 'UK Government Asks Industry to Fight Mobile Phone Theft'. *Infoworld*. 23(5), p. 76.

Vu, K-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B-L., Cook, J. and Schultz, E. E. (2007). 'Improving password security and memorability to protect personal and organizational information'. *International Journal of Human-Computer Studies.* 65(8), pp. 744–757.