Active Authentication: The Panacea of Access Control?

Nathan Clarke & Fudong Li
Centre for Security, Communications & Network Research,
Plymouth University, Plymouth, United Kingdom
Email: nclarke@plymouth.ac.uk; sfurnell@plymouth.ac.uk

Abstract

User authentication is an essential component of securing our electronic devices. It is the gatekeeper that enables subsequent access control and accountability mechanisms to operate successfully. Whilst technology and the way in which people use it has changed enormously, from the days of centralized mainframe computing (available to few), to a highly mobilized, personal and service orientated approach (utilized by (almost) all), the way in which people authenticate has barely changed – with the password still the most popular technique implemented. This paper discusses the role of active authentication – a fundamentally different approach to user authentication that moves away from point-of-entry Boolean decisions and provides a real-time measure of identity assurance that can be associated with each and every access control decision. Whilst active authentication can take many forms, the paper proposes the evolution of the technique into a centralized managed service that offers the opportunity to provide highly secure, robust, multi-device and intelligent handling of every authentication decision. Taking a device-independent approach to authentication removes the need for each and every device and service to make its own authentication decision and enable it to be incorporated in a true identity assurance federation system.

Introduction

Authentication is widely understood to be a founding protection mechanism that enables access to systems and services. Without successful authentication, access control and accountability services are meaningless, providing little support for the core principles of confidentiality, integrity and availability. Unfortunately, authentication approaches: secret knowledge, token and biometric, all fail to provide universally strong user authentication – with various well-documented failings existing (Clarke and Furnell, 2005; Kurkovsky and Syta, 2010; Alaswad et al, 2014). Moreover, existing approaches fail to identify the real information security risk. Authenticating users at point-of-entry, and failing to require re-authentication of the user during the session provides a vast opportunity for attackers to compromise a system. Arguably there is a complete disconnect between the time an authentication decision is made and the subsequent access control decisions that rely upon it. However, forcing users to continuously re-authenticate to systems is cumbersome and fails to take into account the human factors of good security design, in order to ensure good levels of acceptability. Unfortunately, within this context, the need to authenticate is increasing rather than decreasing, with users interacting and engaging with a prolific variety of technologies from PCs to mobiles, social networking to share dealing, and Instant Messenger to Texting. A solution is therefore required to ensure user authentication is relevant, usable, secure and ubiquitous.

The domain of active authentication, often also referred to as transparent or continuous authentication seeks to remove the burden upon the individual and enable authentication non-intrusively. Research into transparent authentication has been ongoing since the turn of the millennium, with some studies into specific biometric modalities going back even further. However, it was the recent DARPA call in 2011 that has brought the topic to the fore (DARPA, 2011).

This paper explores the domain of active authentication, initially providing a justification of the approach through an examination of the current solutions and subsequently through demonstrating how authentication can be reinvented from a binary point-of-entry approach into a continuous confidence-based measure that organizations can integrate within their systems to provide a multi-level risk-based access control solution. The paper then proceeds to illustrate how further developing this approach would enable a true federated authentication system and lead to the development of new managed authentication services.

The Problem with Current Authentication

Fundamentally, authentication can only take one of three forms: secret-knowledge, tokens or biometrics (albeit a combination of these approaches can also be applied (i.e. two-factor authentication)), which have traditionally left system designers with a limited set of options. Secret-knowledge systems have typically manifested themselves as password and PIN-based techniques – easy and cheap to design and well understood by the end-user population. Conversely, both token and biometric-based approaches require additional hardware and software, more complex design and end-user education – leading them to be only incorporated within more specialist devices and services.

Whilst the problems of authentication are well understood, it is only in recent times that more consideration is being placed upon how the user authenticates. Banking services have led the revolution, through the use of token-based approaches within their online service provision (HSBC, n.d.; Barclays, n.d.). Implementations do differ, with some requiring the token to log in, but all require its use when setting up new payments. This is a key step forward for the application of user authentication in that it's the first mainstream example of appreciating the information security risk associated with a particular action and requiring further re-authentication of the user within a service using a stronger authentication approach. They have differentiated the level of authenticity required depending upon whether you are fundamentally reading or writing to a system. All other existing systems utilize a single, point-of-entry, approach that enables the user to complete all actions which the device/service is able to provide.

Microsoft have incorporated alternative authentication into Windows 8 – still orientated upon secret-knowledge but now focused upon graphical passwords. Notably, Microsoft did introduce token-based authentication into previous versions of the software, but this was solely focused upon organizational use rather than the mainstream market. Graphical passwords seek to overcome the associated cognitive issues with remembering text-based passwords. Studies have confirmed that people generally have a far better ability to recall and recognize pictorial representations (Paivio et al, 1968; Shepard, 1967). Such approaches are favored by some and seek to improve the usability and end-user experience whilst maintaining an appropriate level of security.

Biometrics have also found themselves (finally) becoming incorporated within mainstream devices. The Google Android Operating System (OS) introduced Face Unlock in late 2011, a facial recognition approach that replaced the point-of-entry PIN/password (FaceLock, 2013). Apple has also more recently introduced Touch ID on its latest iPhone 6 Plus mode, a fingerprint-based approach (Apple Inc., 2015). Notably, Apple's implementation of Touch ID does allow for multiple services, currently point-of-entry and for purchases made to its iTunes system; although one could envisage local-based authentication extending to a variety of applications in the future. Moreover, however, Touch ID has been implemented in such a manner as to significantly enhance the user experience. Through integration within the home button, a previously well understood functional aspect of the iPhone design, the user does not have to place or swipe his finger against a separate sensor. Merely placing the finger upon the sensor, as they would typically to switch the device on, is sufficient to provide the fingerprint sample. This is a first for biometrics within the mainstream market.

Unfortunately, however, whilst efforts are clearly being made, there are still fundamental issues that prohibit effective information security being achieved. With both implementations of the biometric techniques, it is highlighted that these approaches are focused upon the usability and convenient of access and do not provide higher levels of security than the secret-knowledge approach. In order to achieve usability and acceptability, system designers have lowered the level of security that can be achieved. With other approaches, implementation is either point-of-entry only or requires a relatively user inconvenient and time-consuming authentication request. Whilst users may tolerate this within banking services, it is unlikely to be so popular amongst mainstream online providers. Indeed, Amazon's One-Click purchase functionality is specifically designed to mitigate any user inconvenience of having to re-type a password. There is also a wider issue of practicality with token-based approaches – whilst perhaps feasible with a single bank; it becomes increasingly less so when you have to have individual tokens for each of the online services. Individuals who bank with several providers are already finding themselves with several tokens to manage.

A shift is required that thinks about user authentication from a different perspective. Firstly, with all techniques, the concept of a blanket-based accept or reject decision does not appropriately map to the associated access control decisions being made. It does not take into account that differing authentication approaches will verify an individual to a differing degree of accuracy. A 4-digit PIN is different to a 14-character randomized password. A fingerprint biometric technique is different to keystroke analysis. Secondly, it does not take into account what the user is wishing to access. It is a different proposition if the user is merely wishing to check his calendar for the next appointment or perhaps enter a reminder, to sending an email or performing a financial transaction.

Transparent and Continuous Authentication

Research has been ongoing within the domain of transparent, non-intrusive or (more recently coined) active authentication for some time. The concept is based upon removing or minimizing user inconvenience by capturing the authentication sample (typically biometric-based but not exclusively) whilst the user is normally interacting with the device or service. For example, a front-facing camera is able to capture a user's face whilst they are reading a text (Clarke et al, 2008), keystroke analysis is able analyze a user's typing characteristics whilst composing an email (Clarke and Furnell, 2006), speaker verification can be applied whilst the user is in a telephone conversation (Woo et al, 2006). Indeed, a wide range of approaches has been proposed (with varying levels of progress and implementation). Through removing the explicit authentication request from the process, the user would not realize such authentication decisions are being made (unless the samples were rejected, in which case, the user would find themselves restricted). Furthermore, through enabling transparent authentication, a second beneficial requirement can also be achieved – continuous re-authentication of the user.

Continuous authentication is a key concept that will enable a closer alignment between the authentication and access control decisions. As illustrated in Figure 1, the Transparent Authentication System (TAS) is able to effectively sit between a traditional access control requests, so that an identity is verified non-intrusively prior to the access control decision being made.

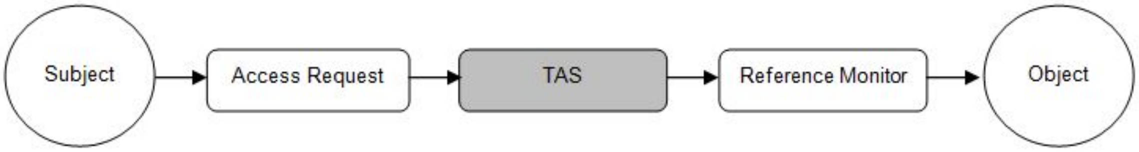

Figure 1: Integration of Authentication and Access Control Decisions

With this closer integration, the system is now able to determine whether the current level of confidence in the user's identity is sufficient to provide access to the specific service/device being requested. The current model, as illustrated in Figure 2, takes no account of the service/device being requested and assumes the initial authentication decision provides a sufficient basis to provide access to all subsequent services, until such time as the device locks. However, this is not a true reflection of levels of security actually required. What is required is a measure of identity confidence that is associated to both the authentication mechanism utilized and to the service being accessed. As illustrated in Figure 3, this subsequently leads to a situation where you have a continuous identity measure that varies over time depending on the transparent authentication decisions. If the confidence is above the level set for a particular service, access is granted, if not reject. Although in practice, a rejection is likely to lead to an intrusive request for the user to re-authenticate.

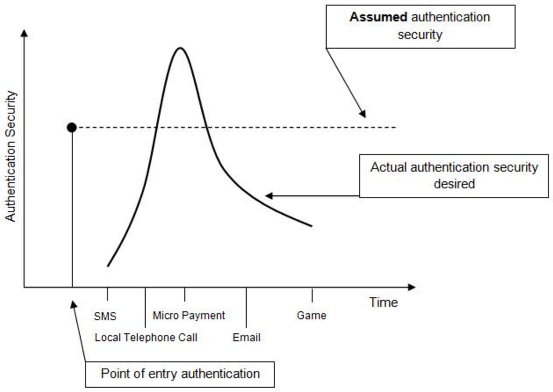
Assumed authentication security
Actual authentication security desired
Authentication Security
Time
SMS
Local Telephone Call
Micro Payment
Email
Game
Point of entry authentication

Figure 2: Current Model of User Authentication Confidence

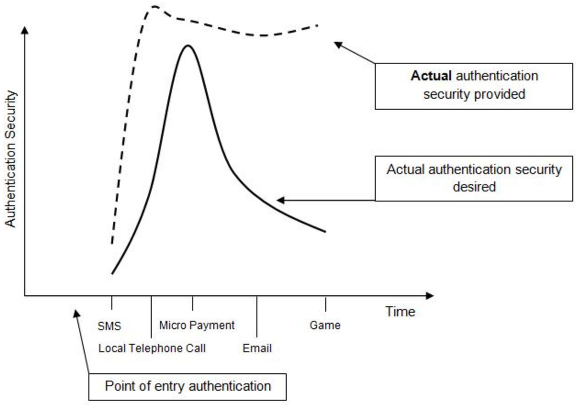
Actual authentication security provided
Actual authentication security desired
Authentication Security
Time
SMS
Local Telephone Call
Micro Payment
Email
Game
Point of entry authentication

Figure 3: Continuous User Authentication Confidence

To enable transparent authentication, it is envisaged that a device will need to support a range of techniques – to ensure sufficient samples are being captured through a variety of user interactions. For example, it would not be effective to merely rely upon speaker verification, as mobile devices are utilized for a variety of purposes and the time between telephone conversations is unlikely to be short enough to provide a continuous confidence level. That said, as illustrated in Figure 4, a typical device has the potential to incorporate a wide range of authentication techniques – notably biometric-based. Whilst tokens in the correct implementation could also enable transparent authentication (e.g. a Radio Frequency IDentification (RFID) enabled watch or ring would be capable of providing such authentication), they are limited in comparison to what biometrics have to offer.

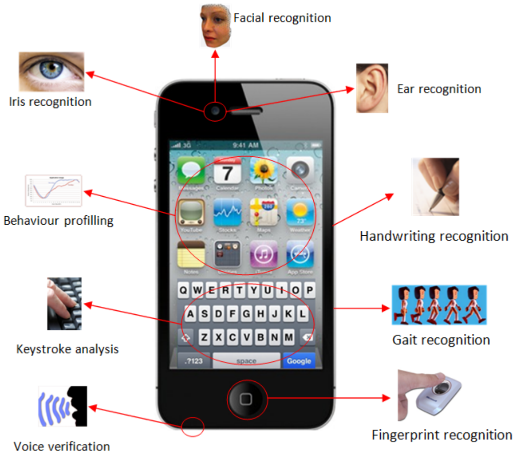

Figure 4: Transparent-Enabling Authentication Techniques

The application of transparent authentication utilizing a range of authentication techniques also serves to solve another key problem with single authentication-based or uni-modal systems: circumvention or forge-ability. Biometrics in particular have been widely reported to have failings when it comes to the forging of biometric samples (Matsumoto et al, 2002; Walker, 2002). Both of the aforementioned biometric implementations on mobile phones have been subject to sample forgery. The FaceLock technique can be compromised through merely showing a photograph of the authorized user. Indeed, attempts by Google to introduce a liveliness test to prevent this attack resulted in the user having to blink – an approach that found itself broken shortly after release, with users merely cutting the eyes out of a photograph and using their own eyes to simulate the blinking action. Whilst moving to a transparent platform does not remove the opportunity of forgery, it does significantly complicate the process. The attacker will have to be able to continuously forge the biometric credential – as they will be unaware when the system will actually capture the sample. They will also be required to provide forged samples across all of the supported techniques that a system is utilizing (which in itself will differ across devices). The ability to continuously provide forged samples across a range of biometric techniques is a significantly more challenging and expensive task than developing an attack against a single point-of-entry approach.

As one might expect, however, the world of transparent authentication is not rosy – otherwise people would probably have been using them. Fundamentally, the introduction of transparent authentication further complicates the underlying authentication system that is required. Rather than having to design and support a single biometric (which few providers are willing to do), they will need to support a number of such techniques. Decisions also need to be made on developing a risk profile for the services being accessed, the effective level of security that each individual authentication technique is able to provide, configuration and optimization of the system – a degree of customization will be required depending upon the techniques and user's ability to use them. The biggest inhibiting factor however is the biometric techniques themselves. In many cases, it is not appropriate to merely apply the current point-of-entry biometric technique into a transparent fashion. For example, whilst facial recognition approaches are well accepted they are designed to operate within very tight environmental conditions (i.e. specific levels of illumination and facial orientation). Such assumptions in a transparent application are unlikely to hold true – implemented on a mobile phone, you would expect to capture a user's face in a variety of orientations and during differing times of the day. Research has been undertaken (including by the authors) exploring many of these issues and developing biometric modalities that operate in a transparent fashion:

- Transparent Facial Recognition (Clarke et al., 2008) – exploring the application of pre-existing facial recognition algorithms for transparent authentication.
- Application of Signature Recognition to Transparent Handwriting Verification for Mobile Devices (Clarke and Mekala, 2007) – developing handwriting recognition for use in transparent authentication. It turns out that dynamic signature algorithms are effective when applied to words rather than just signatures.

- Authenticating Mobile Phone Users using Keystroke Analysis (Clarke and Furnell, 2006) – developing a transparent keystroke analysis modality.
- Active Authentication for Mobile Phones using Behavioural Analysis (Li et al., 2013) – investigating the performance of behavioural analysis as a transparent authentication technique.
- SMS Lingustic Profiling Authentication for Mobile Phones (Saevanee et al., 2011) – capitalising upon communications, this approach seeks to understand the degree to which a user's use of language can be used for authentication.
- Risk Analysis for Mobile Devices (Ledermuller & Clarke, 2011) – proposes a model for use within mobile devices for determining the risk profile of services a user might use.
- Advanced Authentication for Mobile Devices (Clarke & Furnell, 2007) – presents the overarching framework that provides the intelligent analysis of biometric inputs and appropriate response.

It is notably that the majority of techniques that lend themselves to transparent authentication are referred to as behavioral approaches (in comparison to their physiological counterparts). The problem with this is that behavioral approaches tend to not perform as well as physiological techniques (in terms of the ability to correctly and falsely identify the authorized user and impostors) as they tend to have less unique features. Behavioral approaches also suffer in terms of the longevity of the features, as they are more likely to evolve and change over time – and thus require a mechanism for ensuring the enrollment template remains a true reflection of the authorized users patterns.

That said, commercial providers are popping up – mostly offering aspects of transparent authentication (e.g. BehavioSec and Passban). Furthermore, whilst not utilized specifically for authentication, mobile phone operators and credit card providers have been utilizing biometric-based behavioral analysis for years to detect deviations away from normal habits (Moreau et al, 1997; Lerouge et al, 1999; Samfat and Molva, 1997).

Even when biometric modalities have been developed sufficiently for use within a transparent context, there are a number of issues that would make their widespread use challenging. Each device would need to establish and maintain the biometric profiles and the intelligent management infrastructure. This would result in each device requiring the classification algorithms for each technique – thereby increasing licensing costs if credible and well performing solutions are to be utilized. This also places an increased processing and storage footprint on each and every device that incorporate this technology. With many of us now owning a variety of devices and accessing an increasingly larger array of services, this would arguably place a significant configuration and maintenance burden upon the users.

Federated Authentication

With a need to authenticate to an increasing range of devices (e.g. mobile phone, tablet, laptop, PC) and services (e.g. financial services, e-commerce, email, social networking) a universal approach is required that is capable of providing convenient, usable and secure identity verification but in a manner that minimizes system complexity, costs and management. Transitioning the concepts of transparent and continuous authentication into a centralized federated authentication system provides for an approach to authentication where the responsibility for managing and providing identity confidence is placed on a specialized and dedicated service provider.

The specialization of the Managed Authentication Service Provider (MASP) enables economies of scale with respect to the authentication processing algorithms that would not easy be achieved on an individual user basis. However, the significant benefit of the centralized approach is the ability to secure a host of devices and services that would not in themselves be able to utilize strong biometric-level authentication approaches. In a Federated Authentication approach, a user is able to establish a level of identity confidence through the capture of biometric samples on one device and then subsequently use that confidence to access other devices and services. For example, current password-based web services, such as Google email, would now be able to transparently verify your identity – requiring the user to merely access the web page and the background services will check whether the identity confidence is sufficient to provide immediate access. Indeed, combining the functionality of Federated Authentication with Federated Identity would provide the usability of multi-domain access control but with an increased and continuous level of trust upon the authenticity of the user (as illustrated in Figure 5).

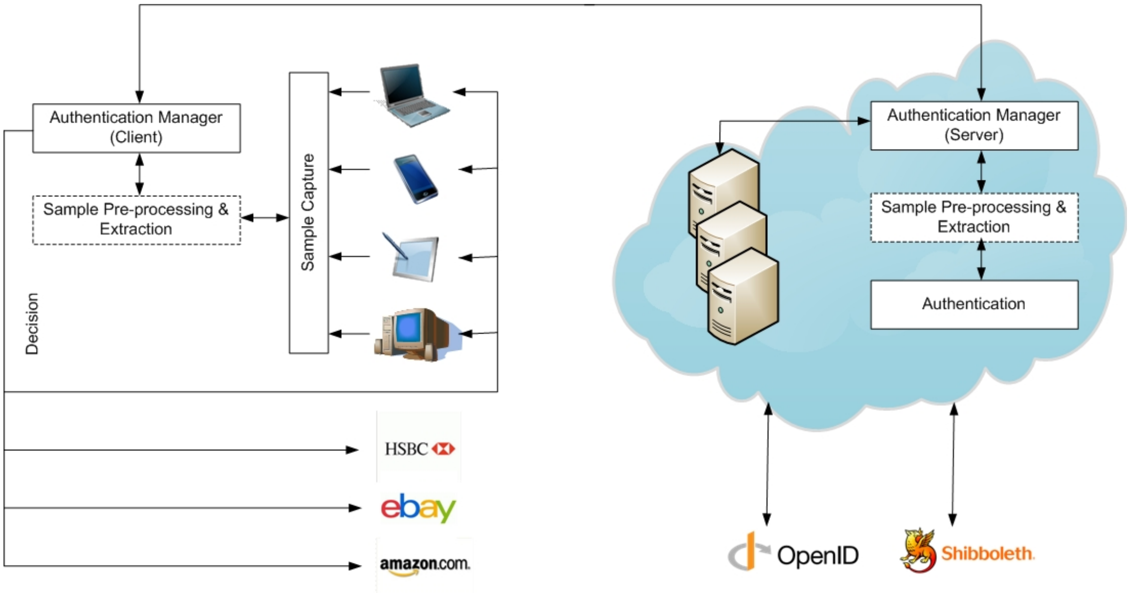
Authentication Manager (Client)
Sample Pre-processing & Extraction
Sample Capture
Decision
HSBC
ebay
amazon.com
Authentication Manager (Server)
Sample Pre-processing & Extraction
Authentication
OpenID
Shibboleth

Figure 5: A Model for Federated Authentication

Through providing a device and service independent authentication approach, the centralised authority is able to provide and apply the most appropriate authentication technologies and remove duplication – as the user would not need to enroll, configure and authenticate to each device. Instead, the user has a single authentication profile within the MASP, where they are able to manage and monitor their profile. Any MASP-enabled device or service will merely send a request to the MASP and be informed of its current real-time identity confidence. In this manner, individual devices themselves are relieved of a significant amount of data processing and storage, including a large volume of duplicated activities that would be occurring with TAS enabled systems.

An advantage of a centralized solution is the ability to unify all authentication information, providing an in-depth understanding of what the user is doing (in terms of devices and services) and thereby providing additional identity intelligence of the user. For example, it will be possible to determine if two authentication requests are simultaneously made from different locations from devices that belong to the owner or otherwise – thus highlighting potential misuse. The centralized approach also enables the use of multibiometrics and multi-factor authentication – providing a robust framework of authentication models that are stronger than any uni-modal or single factor authentication approach. For example, depending upon the available authentication approaches (which themselves will be dependent upon the devices and technology a user utilizes), a variety of multi-instance, multi-algorithmic, multi-modal approaches exist that seek to optimize the authentication decision. As illustrated in Figure 6, a multibiometric approach would enable a MASP to utilize a range of biometric extraction and classification algorithms (each crafted to focus of differing aspects of the problem) and combine the result through fusion. Typically, cost, processing and vendor-specific solutions have prevented this for happening to date and continue to do so. As a centralized authentication service, the MASP, through ISO standards (i.e. ISO 19794, 19784, 19785) will be in a position to incorporate any and all approaches – something individual devices would not be able to achieve due to prohibitive costs and processing requirements (ISO,2011; ISO, 2006a; ISO, 2006b).

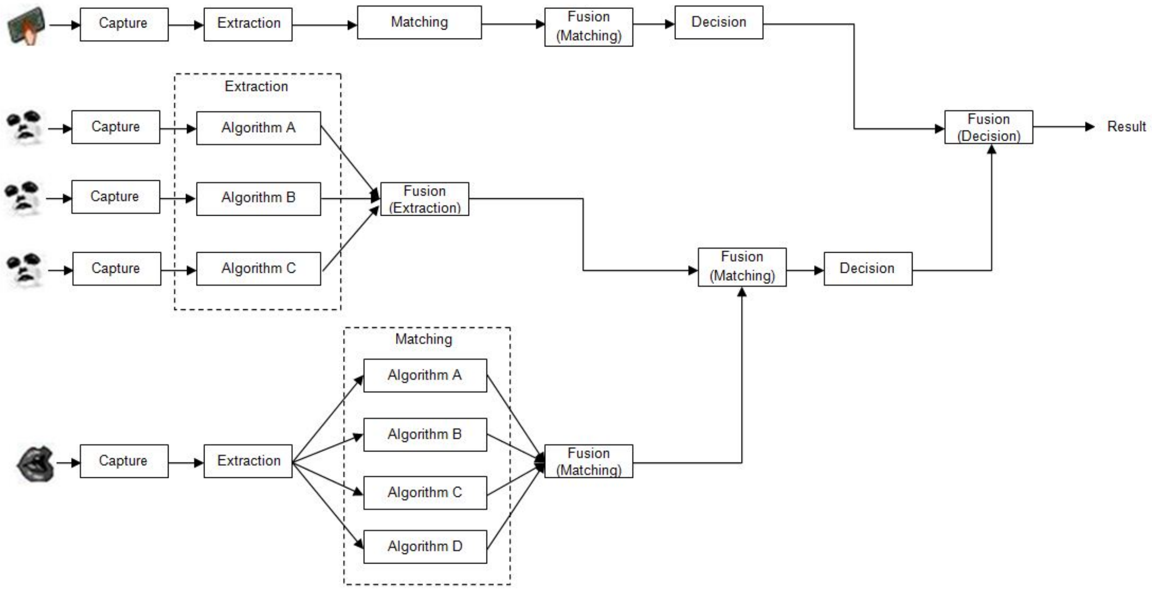

Figure 6: A Model for Multibiometrics within Federated Authentication

Federated Authentication is conceptually a far cry from how authentication typically takes places today. It is an approach that is hugely complex over the existing provision. It is a model that will introduce costs – the MASP will need to charge for its services in some manner (although many differing business models could exist – from a per request, per user, monthly, per business, or dependent on the authentication techniques utilized – higher security approaches costing a premium over open-source algorithms). It is an approach where individuals and organizations need to trust a third-party in storing authentication credentials and reliably monitoring their use.

Whilst challenging, none of these issues appear insurmountable. Federated Identity systems already hold the access control permissions to variety of systems – based upon a single set of (typically weak) credentials. Many companies are releasing the true cost of their authentication solutions – for example, the financial sector investing in token-based approaches. The cost of deploying a Federated Authentication system may yet prove to be a cost effective solution. It will certainly offer many organizations the opportunity to contract out the provision – reducing the in-house cost and through service level agreements providing an effect threat mitigation strategy.

Conclusions

Approaches to user authentication have traditionally failed to achieve their desired objective. Whilst a quiet revolution is underway, with technologies that finally go beyond the password, becoming mainstream, it is clear these approaches are still predicated upon assumptions that no longer hold true. Indeed, they haven't for a long time. Transparent and continuous authentication offers the opportunity to reduce the burden upon the user but in a manner that provides a more secure risk-aware environment.

Whilst such transparent and continuous authentication systems introduce significant complexities, provisioning through a centralized provider results in it becoming their singular issue to resolve – individual service developers and organizations will merely include a pre-defined script or application that will provide the necessary capture, processing and responses. Making the approach, from a system/service developers perspective as simple as placing a password control on the system. This ease of implementation should encourage the wider adoption of such an approach.

Research in transparent approaches is becoming more mature and it is expected that managed authentication services (in various guises) will become prevalent as individuals and organizations seek solutions to their authentication requirements. It will not be acceptable to remain with the status quo.

References

Alaswad, A.O., Montaser, A.H and Mohamad, F.E. (2014) Vulnerabilities of Biometric Authentication "Threats and Countermeasures". International Journal of Information & Computation Technology. (Vol. 4, pp. 947-958). Retrieved from http://www.ripublication.com/irph/ijict_spl/ijictv4n10spl_01.pdf

Apple Inc. (2015) Use Touch ID on iPhone and iPad. Retrieved 02 February 2015 from http://support.apple.com/en-us/HT5883

Barclays (n.d.) Upgrade to PINsentry. Retrieved 28 January 2015 from http://www.barclays.co.uk/Helpsupport/UpgradetoPINsentry/P1242559314766

Clarke, N.L. and Furnell, S.M. (2005) Authentication of users on mobile telephones—a survey of attitudes and practices. Computers and Security (Vol.24, pp.519–527). Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404805001446

Clarke, N.L. and Furnell, S.M. (2006) Authenticating Mobile Phone Users Using Key-stroke Analysis. International Journal of Information Security (Vol. 6, pp.1-14). Retrieved from http://link.springer.com/article/10.1007%2Fs10207-006-0006-6

Clarke NL, Furnell SM (2007) Advanced user authentication for mobile devices. Computers & Security (vol. 26, no. 2, pp.109-119). Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404806001428

Clarke, N.L., Karatzouni, S., and Furnell, S.M. (2008) Transparent Facial Recognition for Mobile Devices. Refereed paper from the 7th Security Conference, Las Vegas, USA

Clarke, N.L and Mekala, A.R. (2007) The application of signature recognition to trans-parent handwriting verification for mobile devices, Information Management & Computer Security (Vol. 15, pp. 214-225).

DARPA (2011) Active Authentication. Retrieved 17 January 2015 from http://www.darpa.mil/OurWork/I2O/Programs/ActiveAuthentication.aspx

FaceLock (2013) FaceLock. Retrieved 28 January 2015 from http://www.facelock.mobi/

HSBC (n.d.) Secure Key. Retrieved 20 January 2015 from http://www.hsbc.co.uk/1/2/customer-support/online-banking-security/secure-key

ISO (2006a) ISO/IEC 19784-1: 2006 Information technology – Biometric application programming interface – Part 1: BioAPI specification. Retrieved 12 February 2015 from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=33922

ISO (2006b) ISO/IEC 19785-1: 2006 Information technology – Common Biometric Exchange Formats Framework – Part1: Data element. Retrieved 11 February 2015 from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41047

ISO (2011) ISO/IEC 19794-1:2011 Information technology – Biometric data interchange formats – Part 1: Framework. Retrieved 8 February 2015 from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50862

Kurkovsky, S. and Syta, E. (2010) Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. Refereed paper from the IEEE International Symposium on Technology andSociety (ISTAS) (pp. 441–449). Wollongong, Australia

Lerouge, E., Moreau, Y., Verrelst, H., Vandewalle, J., Stoermann, C., Gosset, P. and Burge, P. (1999) Detection and management of fraud in UMTS networks. Refereed paper from the Third International Conference on The Practical Application of Knowledge Discovery and Data Mining (PADD99) (pp. 127-148). London, UK

Li F., Clarke, N.L., Papadaki, M. and Dowland, P.S. (2013) Active authentication for mo-bile devices utilising behaviour profiling, International Journal of Information Security. Retrieved from 10.1007/s10207-013-0209-6

Ledermuller, T. and Clarke, N.L. (2011) Risk Assessment for Mobile Devices. Refereed paper from Privacy and Security in Digital Business – 8th International Conference (pp. 210-221). Toulouse, France,

Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S. (2002) Impact of Artificial "Gummy" Fingers on Fingerprint Systems. Proceedings of SPIE in Optical Security and Counterfeit Deterrence Techniques IV(pp. 275–289)

Moreau, Y., Verrelst, H., and Vandewalle, J. (1997) Detection of mobile phone fraud using supervised neural networks: A first prototype. Refereed paper from International Conference on Artificial Neural Networks Proceedings (ICANN'97) (pp.1065—1070). Lausanne, Switzerland

Paivio, A., Yuille, J. C. and Madigan, S. A.(1968). Concreteness, imagery, and meaningfulness values for 925 nouns. Journal of Experimental Psychology Monograph Supplement, 76 (1, pt.2).

Saevanee H, Clarke NL and Furnell SM (2011) SMS Linguistic Profiling Authentication on Mobile Devices. Refereed paper from the 5th International Conference on Network and System Security (NSS 2011) (pp.224-229). Milan, Italy.

Samfat, D. and Molva, R. (1997). IDAMN: an Intrusion Detection Architecture for Mobile Networks. IEEE Journal on Selected Areas in Communications (Vol. 15, pp.1373–1380). Retrieved from: doi:10.1109/49.622919

Shepard R N, (1967) Recognition memory for words, sentences and pictures. Journal of Verbal Learning and Verbal Behaviour (Vol6, pp.156-163). Retrieved from http://www.sciencedirect.com/science/article/pii/S0022537167800677

Walker, S. (2002) Biometric Selection: Body Parts Online. Retrieved 10 February 2015 from http://www.sans.org/reading-room/whitepapers/authentication/biometric-selection-body-parts-online-139

Woo, R., Park, A. and Hazen, T. (2006) The MIT Mobile Device Speaker Verification Corpus: Data collection and preliminary experiments. Proceeding of Odyssey, The Speaker & Language Recognition Workshop, San Juan, Puerto Rico.