2007

Device- versus Network-Centric Authentication Paradigms for Mobile Devices: Operational and Perceptual Trade-Offs

S. Karatzouni
University of Plymouth

N. L. Clarke
University of Plymouth

S. M. Furnell
University of Plymouth

DOI: 10.4225/75/57b54ac1b875c
Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007

Device- versus Network-Centric Authentication Paradigms for Mobile Devices: Operational and Perceptual Trade-Offs

S. Karatzouni, N.L. Clarke and S.M. Furnell
Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

The increasing capability and functionality of mobile devices is leading to a corresponding increase in the need for security to prevent unauthorised access. Indeed, as the data and services accessed via mobile devices become more sensitive, the existing method of user authentication (predominately based upon Personal Identification Numbers) appears increasingly insufficient. An alternative basis for authentication is offered by biometric approaches; which have the potential to be implemented in a non-intrusive manner and also enable authentication to be applied in an ongoing manner, beyond initial point-of-entry. However, the implementation of any authentication mechanism, particularly biometric approaches, introduces considerations of where the main elements of functionality (such as the processing of authentication data, decisions making, and storing user templates/profiles) should reside. At the extremes, there are two alternatives: a device-centric paradigm, in which the aforementioned aspects are handled locally; or a network-centric paradigm, in which the actions occur remotely and under the jurisdiction of the network operator. This paper examines the alternatives and determines that each context introduces considerations in relation to the privacy of user data, the processing and storage of authentication data, network bandwidth demands, and service availability. In view of the various advantages and disadvantages, it is concluded that a hybrid approach represents the most feasible solution; enabling data storage and processing to be split between the two locations depending upon individual circumstances. This represents the most flexible approach, and will enable an authentication architecture to be more adaptable to the needs of different users, devices and security requirements.

Keywords

User Authentication, Biometrics, Mobility.

INTRODUCTION

The mobile networking landscape has changed significantly over the last decade with a transition from large form factor telephony devices to small multi-purpose multimedia communications devices. The recent introduction of Third Generation (3G) technologies has provided the underlying mechanism for a wide variety of innovative data orientated services, with approximately one million users every day adopting these new features (Best, 2006a). At the same time, the level of functionality can be seen to be significantly expanding, with devices today having similar processing and memory capabilities to PCs of a few years ago.

This transition imposes serious security considerations for mobile users, especially as incidents involving mobile devices and the disclosure of personal and corporate information are appearing within the media more frequently (Vance, 2006; Noguchi, 2005). One survey in the UK reported that within six months more than 54,000 mobile handsets were simply left on the back of London cabs, and another survey reported UK mobile phone theft accounted for 45% of all theft (Leyden, 2005; British Transport Police, 2006).

In this context it is relevant to consider the degree to which related security measures are already provided and utilised. It is widely recognised that authentication can be achieved by utilising one or more of three fundamental approaches: something the user *knows* (password); something the user *has* (token) and something the user *is* (biometric) (Nanavati et al. 2002). Currently, the most widely deployed authentication methods are passwords and PINs - secret knowledge approaches that rely heavily upon the user to ensure continued validity. For example, the user should not use the default factory settings, share their details with others, or write the information down. However, the poor use of passwords and PINs has been widely documented (Pointsec, 2005; Clarke et al. 2002), and many mobile users do not even use the security which is available. Similarly to secret knowledge techniques, token based approaches fundamentally rely upon the user to remember something, with the token needing to be physically present in order to access the device. However, it is considered that this does not lend itself particularly well to the mobile device context either. The most likely scenario is that users would simply leave the token within the mobile handset for convenience.

In contrast to the other methods, the third approach to authentication does not rely upon the user to remember anything – it just requires them to be themselves. Such techniques are collectively known as biometrics, and it is here that the most suitable alternatives for going beyond the PIN may be found. Biometrics have been suggested to be able to provide a more secure approach to authentication as the technique relies upon unique personal identifiers of the person. Therefore a user is not required to remember anything, and at the same time they cannot be lost or forgotten.

However, in order to establish an authentication mechanism for mobile devices - especially when biometric approaches are utilised, careful consideration is needed to address the trade-off between a network-centric versus device-centric implementation, with issues such as performance, privacy and mobility being essential to the adoption of a new approach. The purpose of this paper is to discuss the technical and perceptual issues that are involved in the implementation of the either approach and propose a solution that takes the best advantage of both. To this end, the basic characteristics of the two paradigms are presented in section 2, followed by a discussion of the resultant trade-offs in section 3. Section 4 then presents the proposed hybrid paradigm, leading to overall conclusions in section 5.

AUTHENTICATION TOPOLOGIES FOR MOBILE DEVICES:

The topology of an authentication mechanism is an important factor to consider at the outset of the design process. With numerous stakeholders (such as network operators, corporate IT administrators and end-users) the ability to provide identity verification in a manner that maintains both security and privacy, and considers the operational impact upon the mobile device is imperative. Unfortunately, however, it is difficult to maintain all these services for all stakeholders, and a trade-off exists between different security and privacy issues depending upon what the system is trying to optimally achieve. Although to date identity verification has been performed by the device itself this might not be the best approach to take when considering the number of issues that may result from both a security and usability perspective.

A Network-Centric Approach

A network-centric approach will direct all the key computational tasks and storage to the network. The physical placement of the authentication mechanism within the network could be with the network operator, corporate IT administrator, or third-party providing managed authentication services. As illustrated in Figure 1, the mobile device itself will act as the biometric sample capturing device and be able to respond to a decision sent from the server to permit or restrict access to a user.

Depending upon the device, its processing capabilities and security requirements, it could be possible to partially split the biometric process, where the data extraction phase is conducted on the device and classification on the network. This would assist in reducing the amount of traffic sent across the network. Nevertheless however, the focus of this paradigm is on all major computational and memory requirements being resident on the network rather than the device.

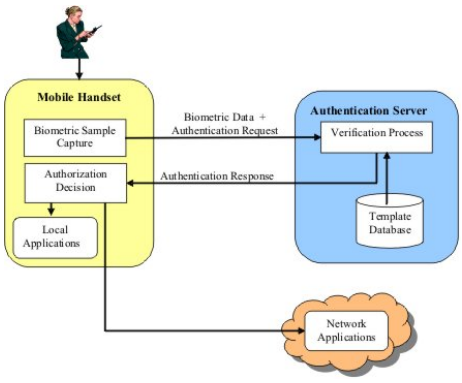


Figure 1 A Network-Centric approach

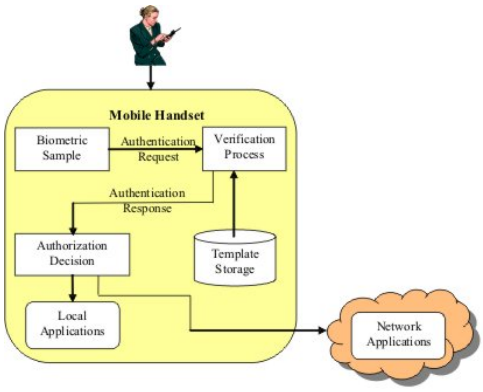


Figure 2 A Device-Centric approach

A Device-Centric Approach

In a device-centric approach the whole biometric process is completed on the device. All the information, algorithms and management controls required for the authentication process are stored upon the device.

Furthermore, all the processing required to perform the verification also takes place on the device. Figure 2 illustrates an example of such an approach.

TRADE-OFFS BETWEEN THE PARADIGMS

The two approaches described above have several advantages and disadvantages from both social and technical perspective. The principal areas to establish the trade-offs that exist are:

- User privacy
- Storage and processing of biometric samples
- Network bandwidth requirements
- Network availability
- Mobility and roaming
-

The following sections address and discuss these issues in turn, examining in detail the trade-offs between the two potential topologies.

User Privacy

When considering which topology to deploy, resolving the issue of user privacy is essential for widespread adoption. This becomes even more important when the topology is looking to utilise biometric techniques as the underlying mechanism. Recent years have seen widespread media attention directed towards biometrics, due largely to their inclusion within passport and national identity card schemes (Gomm, 2005). Unfortunately, and for some legitimate reasons, this attention has been somewhat negative towards the benefits of the technology, focussing instead upon privacy concerns (Porter, 2004; TimesOnLine, 2004). It is therefore important to ensure the authentication mechanism is designed in a fashion that is sensitive to privacy concerns.

The principal issue focuses around the biometric template and sample. In whichever biometric technique that is utilised, these elements represent unique personal information. Unfortunately, unlike other forms of authentication (such as secret knowledge or tokens, which can be simply changed if lost or stolen), it is not possible to change or replace biometric characteristics - they are an inherent part of the person. Therefore, once lost or stolen, they can remain compromised and no longer be reliably used. As such, the creation and storage of a biometric template or profile on either the device or the network leads to significant responsibility for the user or the network provider respectively.

Public opinion regarding biometrics has been problematic, not least because of the proposed national and boarder control schemes that are in implementation in many countries. These call for a centralised repository of biometric information for all nationals, but the ability to secure such databases from external attack and effectively manage authorisation to protect data from internal misuse is no small undertaking. Despite the safeguards that one can apply, there will always be the potential for vulnerabilities due to both human factors and technical mis-configurations. Such vulnerability, and moreover the lack of confidence that it engenders, was also raised in a focus group that took place in order to acquire users' views and attitude towards security on their devices (Karatzouni et al. 2007), where participants voiced the concern over security and trust:

> *"…would you really want your biometric data then stored on the inside of a company that's possibly got dodgy people, people breaking into it already…"*

> *"And even in the network [I] don't think it's all that secure either, because there is always the rogue employee somewhere, who is in the pay of an attacker"*

These quotes demonstrate a major fear for the security of the information held remotely. Apart from the technicalities that might be overlooked, there are also examples of carelessness taking place that has led to severe incidents. An illustrative example occurred within an Orange call centre, where employees that had been granted access to full customer records (including information such as bank details) were sharing their login credentials with other staff (Mobile Business, 2006). This removed any ability to effectively monitor who and when they had access to information. The increased fear of identity theft and fraud makes people even more cautious about their personal information, and how and where they provide it.

Recent discussions in the UK regarding a national ID card scheme has suggested that people are not very comfortable with providing their biometric information to a centralised system (Lettice, 2006). As such, a device-centric implementation is arguably more favourable from the user's perspective. In such a case, the profile will be stored on their personal device giving no third-party access to the biometric template or samples.

This approach is able to satisfy peoples' desire for privacy preservation by giving them direct responsibility for its protection. However, introducing such responsibility also brings concerns about how reliable and aware the end users will be in safeguarding their devices. As previously mentioned, several surveys have demonstrated that, despite the storage of sensitive information in handsets, and despite the earlier cited evidence of loss and theft, users still disregard the use of the available security measures. This is an important consideration to the choice in topology, as no further protection will be available once the device is stolen. On the other hand, one could suggest that as the fear of misuse becomes greater, the importance that each subscriber will attribute to the device will change respectively. For instance, storing personal identifiers in the device might lead people to consider their device to be comparable to other forms of important information and ID, such as, passports, credit cards, and car keys. Such linkage could potentially change people's perception and attitude toward the security and protection of their devices.

However, there was also a concern raised in the focus group expressing a fear of storage on the device and potential misuse.

> *"…my concern is where would the fingerprint, let's say like signature, where would be stored? Would that be stored on the phone, so if somebody stole my phone they have my signature which is signed on the back of you bank cards and my fingerprint obviously? What then can people do with the information…obviously if someone knows how to hack into a phone could they use the information?"*

It is certain that a biometric database will always constitute an attractive target, making it a more valuable target than a device involving only one person. It would be necessary in such cases to establish regulations and policies for the security of the database and biometric templates, and mandate continuing adherence to them. A central system, though, has an advantage that the system can monitor such activity and try to prevent it, thereby providing a more uniform and controlled protection space, than storage in the device.

People have different views towards the storage of such information as concerns are raised over the security in each storage solution and how potentially easy a breach of confidentiality is. A recent study conducted by the authors' research group attempted to assess public perceptions of biometrics, and performed a survey involving 209 respondents (Furnell and Evangelatos, 2007). One question asked people about their concern regarding the theft of their biometric data and the potential of using them to cheat a system. The responses are illustrated in Figure 3.

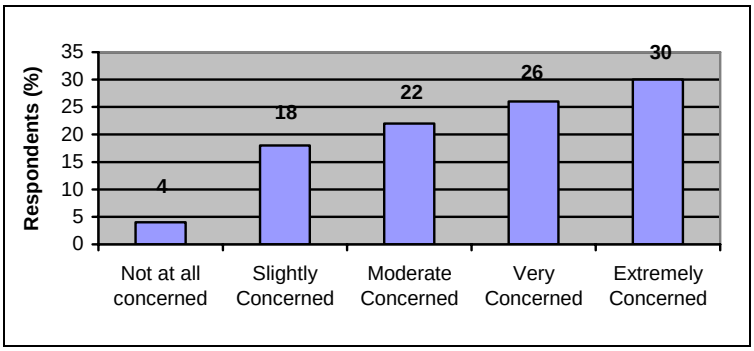


Figure 3 Concern that biometric information could be stolen

As seen from the figure, the majority of the respondents expressed some level of concern about the security of their data, with only 4% not having any fear of misuse. The same survey also asked where respondents would prefer their biometric data to be stored. Forty percent supported the network option whereas only seventeen percent agreed on the device (as illustrated in Figure 4). Interestingly, 18% would prefer their biometric templates to be stored in a smartcard. This is analogous to a device-centric approach, as the smartcard must remain with the user, but represents a significant enhancement in physical and logical security of the information.

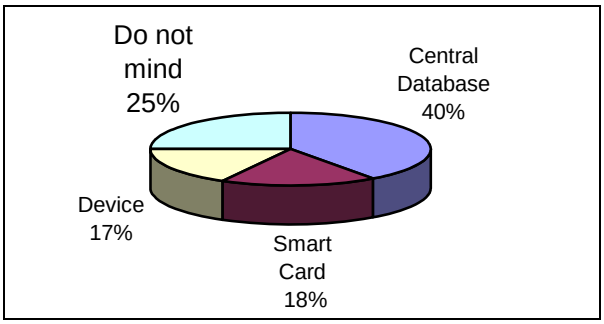


Figure 4 Subscriber preferences on storage of biometric profiles

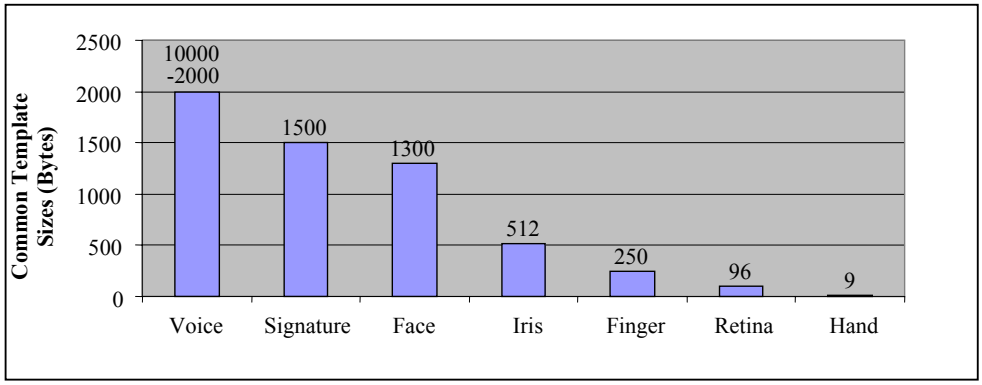
Privacy concerns that exist for the network implementation could be reduced by ensuring only the biometric templates are stored and not any form of raw data. Several studies have taken place to overcome that issue, looking to protect the storage of biometrics using techniques such as distortion of the template. It is also notable that the creation of biometric templates is based upon vendors' own proprietary formats. As such, one biometric template from one vendor will not operate with another vendor's product, as the format and characteristics used to authenticate people differ. This will reduce the potential harm caused by a stolen biometric sample to systems that only utilised that specific vendor's product. The one-way property of creating biometric templates also ensures they cannot be reversed engineered.

Storage and Processing Requirements

While the privacy issue represents a challenge of user trust and perception, there are also technical-level considerations in terms of the storage and processing of biometric data. These will again differ according to the chosen topology.

Consideration needs to be given to the storage of the initial biometric template and also the samples that are subsequently used in the process of verification. For current PIN-based approaches this is not an issue, but the storage demands of biometrics are more significant. Issues of storage might exist in both topologies, with individual devices potentially having limited onboard storage, while the network-centric approach may need to cope with the storage of data for high volumes of users.

Different biometric techniques require differing levels of storage memory. Techniques such as face recognition (where multiple images might be needed from different angles in order to achieve a high consistent outcome), or voice verification (where sound files need to be stored), usually require higher storage capacities. Furthermore, as the proposed authentication mechanism aims to take advantage of a number of different techniques, the device or network will need to store more than one template per user, which could potentially become more demanding. Figure 5 illustrates typical template sizes from a number of more common biometric technologies.



Source: International Biometric Group, 2002

Figure 5 Typical sizes of biometric templates

Given the memory available on current mobile device, it can be seen that the storage requirements would not prevent a device-centric implementation. The most demanding approach is voice scanning which can reach the requirements of close to 10KB. Therefore in general terms, storage of biometric templates in a device-centric paradigm does not present any difficulty. However, given the variability in devices and functionality, some care must be taken to ensure that this proposed authentication mechanism is able to operate with all hardware devices, including legacy devices which might have smaller storage footprints.

In terms of processing capabilities, the network-centric approach has an advantage in the sense that devices themselves may have relatively limited capabilities. Indeed, this may actually represent a fundamental obstacle to establishing a device-centric solution. Whereas laptop-level devices may have the capabilities required to process biometric data, the processing power in handheld devices is still limited. Algorithms that are utilised in biometric verification tend to be intensive, as they are based upon complex data extraction and pattern classification techniques (and indeed the impact of this additional processing on the battery of the mobile device would also have to be carefully considered). The process of enrolment and verification will place a serious demand upon resources on many mobile devices. In order to achieve transparent authentication, verification of the user needs to be completed without affecting the user's ability to use the device (e.g. no impairment to other running applications). It would not be satisfactory for the device to pause or hang for a few seconds every time verification was being performed. However, as with the storage footprint, different biometric techniques require varying levels of processing capacity. It is therefore not necessarily infeasible to consider at least some biometrics operating in a device-centric paradigm. Indeed, signature recognition, fingerprint recognition, keystroke analysis and facial recognition have all been developed for mobile devices (PDALok, 2006; NTT DoCoMo, 2003; Clarke and Furnell, 2006; Omron, 2005).

Over time, the processing constraints are likely to be overcome as the capabilities of handhelds continue to advance. However, from an implementation perspective, a network-centric paradigm would still potentially be easier to deploy and offer a wider range of possible biometric techniques. Again, however, consideration needs to be given upon the scalability of such an approach - multiplying individual authentication requests by high volumes of users does place a significant demand upon processing.

Bandwidth Requirements

A particular consideration in the context of the network-centric approach is the network bandwidth that will be required for the transmission of user authentication data. A device-centric approach has no such implications, as at most it will only be required to perform its normal authentication of the device to the network. By contrast, the network-centric approach will require network bandwidth to send biometric samples to the network, and receive authentication decisions back. Communication across the network will also result in a latency occurring between the initial authentication request and the resulting decision.

Typical bandwidth rates in practical 3G network scenarios are 220-320 kbps for UMTS and 550-1100kbps with HSDPA, although the theoretical rates are a lot higher (3G, 2004). An average 3G portal page, for example, has a size of 40 Kbytes and should theoretically take less than a second to load. However, in reality the actual throughput results in an 8-20 second delay. A usability study has shown that users are willing to wait for at least 3 seconds for a page to appear (Gissin, 2005). This willingness to wait is an important consideration in designing the authentication protocols and mechanisms. Forcing users to wait too long before being given access would result in a negative perception, particularly when the approach is meant to be transparent.

As discussed in the previous section, biometric templates can range from as little as a few hundred bytes up to 10Kbytes. These templates contain the unique data that is derived after pre-processing (thereby extracting the required features). The option of the device performing this procedure would be one way to decrease the bandwidth requirements, as the data sent would be far smaller than the raw sample. However, the ability to perform pre-processing on the device will depend upon the individual biometric technique and the processing capabilities of the device. If pre-processing can be implemented on the device it can be assumed that the size of the data being communicated is similar to those presented in Figure 5. A simple computation will show that the largest template of 10Kbytes will require time of 0.36 sec for the lowest given throughput on UTMS (220 kbps). It must be considered though that this might well become larger depending upon the network condition at the time and also takes no consideration of the time taken for the network to actually perform the authentication. Beyond latency for individual users, the issue of scalability needs to be addressed. Large volumes of users sending biometric sample data across the network might have significant impacts upon network resources and increase the level of delay experienced. For example, last year one of the largest operators in the UK accounted over 15 million subscribers (Richardson, 2005). If just 10% of them used such a service, we would be talking about 1.5 million users requesting authentication from the network. Of course the burden of the network will depend upon the authentication frequency and this will vary across users as the different use of their device will result in more or less authentication requests.

At first glance one might suggest that current 3G networks (and certainly future networks) would be able to cope with the requirements. Although this might not be wrong in principle, an investigation of the network consumption does reveal somewhat surprisingly high volumes. Based upon the figures of 1.5 million users Figure 6 illustrates the bandwidth required per day for three different types of biometric approach.

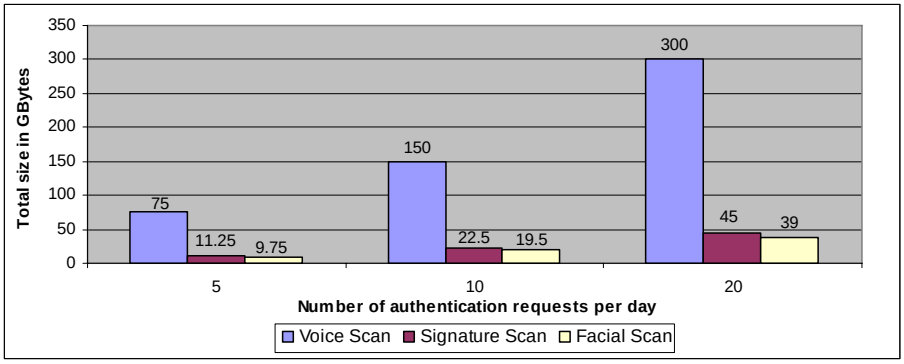


Figure 6 Average biometric data transfer requirements (Based upon 1.5 million Users)

As illustrated in the chart, for voice scan, even a minimum request for authentication of five times results a required data capacity of 75Gbytes for the network provider, whereas with up to twenty requests per day this raises to 300Gbytes. In comparison however, a video stream application, (one of the standard 3G applications), has bandwidth consumption close to 200Kbps for each user (Bruce, 2006). In a population of 1.5 million subscribers that represents 37Gbytes to be transferred every second. That said, there is a real cost associated with sending data across a network and there will be at least an indirect cost, given that the operator may otherwise be able to use the bandwidth to support revenue-generating services.

Availability Requirements

A factor that plays a significant role in a network-centric topology is the establishment of availability. In a fully device-centric approach all aspects required to perform the authentication are self-contained locally within the device. However, having the authentication process relying upon the network makes a key assumption that the network is available at all times to facilitate the process. In practice, there are various reasons why network connectivity might not be available, such as loss of coverage, network overload, or server malfunction. The inability to perform an authentication request as and when required will have a significant impact upon the authentication mechanism and its perceived usability.

Of course, if the authentication request is associated with a network-based application or service then one could reasonably argue that there is no inconvenience, as the service would not be able available anyway. What would be less acceptable, however, would be reliance upon network availability in order to access applications or features that would otherwise be entirely local. For example, opening a document, accessing contacts, or using Bluetooth to connect to another device, might all require authentication, and this would have a real and unacceptable impact if the process were to rely upon the (unavailable) network.

Participants in the focus group were asked to consider this issue and overall there was a negative opinion on always requiring access from the network. The following viewpoint was typical:

> *"I find it difficult that it might be possible just even to interact with the network operator, because I'd like to use that information even when I don't interact with the network operator."*

It can be suggested that apart from the technical issues that can occur, it seems rather inconvenient to require authentication from the provider. The inconvenience does not only relate to the access of local functionality and applications, but also the general concept - that in order to access any service the user will be obliged to explicitly go through the network provider. This places a burden of inconvenience upon the user, network provider and the authentication mechanism. One of the focus group members specifically summed up the issues surrounding the availability of network resources:

> *"There is quite a lot stored in the network. Potentially everything can be stored in the network. There is a trade-off between responsiveness and security….Especially if you are not in coverage*

> *all period of time and you want to look up someone's name, address or whatever in your address book you haven't got it. So that's completely rejected by the operators. There's got to be some balance between security that happens on the network and immediacy you have on the person... there isn't a simple answer to this sort of question"*

Mobility and Roaming

A network-centric approach would enable personal mobility (Thai et al. 2003) - the ability, in principle, to get authenticated on any mobile device and have all subsequent use of the device billed to their account. Having the verification coming from the network, the subscriber will be able to use the system from various devices, without any swapping of SIM cards. The device-centric approach lacks such convenience as the storage and authentication of the user is linked to the specific device.

Conversely, however, when considering the issue of roaming, the device-centric topology is more appropriate as authentication of the user can be performed on the device wherever they might be in the world. A network-centric topology would experience significant increases in latency and have to transverse a far larger open network. Unless the local network provider supported the authentication mechanism and had a local version of the biometric template (which would not be likely due to privacy) this increase in delay would again have an impact upon the authentication mechanism which would need to be considered.

Also, what happens when roaming is not available? In such a situation, the user will have no way to be authenticated as no access to the provider's network will be available, restricting if not completely preventing any use of the device. There is also the consideration of cost. A home network operator implementing the authentication mechanism might be prepared to bear the cost of network consumption. However, this may not be the case for a roaming network, raising questions of who covers the cost. Currently the charges for roaming are very high, although this is expected to reduce in time (Best, 2006b). A device-centric approach would overcome this issue as no reliance upon external resources is required.

DISCUSSION

The prior analysis has shown that comparing the device- and network-centric topologies introduces a varied and complex range of considerations, with each approach offering advantages and disadvantages in different contexts. Attempting to base a solution entirely around the device can introduce processing limitations, whereas bandwidth and the requirement for connectivity may represent practical constraints for a network-based paradigm. In addition, both approaches may introduce their own privacy-related concerns.

Based on the issues arising from both potential architectures, it can be argued that no single approach can cover all aspects that are required for the practical implementation of the proposed authentication framework. In order to try to overcome the troublesome aspects of each implementation, it is suggested that a hybrid approach would be more appropriate. Although complicating the underlying authentication system, it would provide a basis for overcoming the disadvantages of both topologies, while retaining their key advantages, so that the aims and objectives of the authentication mechanism can be met.

In such an approach both storage and processing would be potentially split over the device and the network, compromising between the issues of device processing capabilities, network availability, and privacy. The nature of the split in the authentication mechanism will depend upon the individual requirements of the user in relation to privacy and access, and the device in terms of which biometric techniques it can support locally. There will be therefore a number of hybrid approaches that could exist, each covering different issues on different scenarios for different users. For example, in order to deal with the issue of device processing and privacy, there could be the option to store all of the templates in the device, but place the processing functionality on the network. This would satisfy privacy concerns but at the same time discharge the device of any excessive processing tasks. Cryptographic measures could be used to protect the data in transit and during processing. Depending upon the device capabilities, pre-processing can be performed locally when possible, so that the biometric samples that are being sent over the network are kept as small as possible.

The specific nature of the hybrid system will closely depend upon a wide variety of factors that have been discussed in this paper. In order to remove the concerns surrounding network availability it is suggested that at least one authentication technique will always remain on the local device. Although this technique might not provide the level of security strong network-based biometrics might, it will be able to provide an effective means of authenticating short term usage of local applications and functions.

In devices with more possessing capacity, the hybrid approach would also be able to provide the ability to split the biometric templates, having the most intensive and demanding biometric techniques on the network and the

others with fewer requirements on the device. Another basis for determining this split could also be the uniqueness attributed to them for privacy issues.

This hybrid authentication paradigm must incorporate a level of intelligence so it is able to understand when and how the security requirements can be attributed, and how the framework needs to adapt between different authentication techniques to handle those requirements. For example, if a user sends a text message or makes a local voice call then the operation need not be considered that critical, whereas accessing an mCommerce service or making an international call would demand more protection. The authentication mechanism should recognise this and select techniques that are appropriate to the context.

CONCLUSION

With the growing popularity and functionality of mobile devices, the personal and financial cost of the device being misused or abused is increasing. As such, the ability to ensure and maintain identity verification of the user is imperative. Unfortunately, when considering the different types of authentication mechanism currently available, none satisfy the requirements for all users across all mobile devices. This situation is only complicated when you consider the dynamic and varied environment within which mobile devices operate, with varying functionality, processing and memory capabilities, differing network access technologies and a number of possible stakeholders all interested in the device.

Having discussed in some detail the advantages and disadvantages of network- versus device-centric paradigms, it was concluded that no single approach could achieve the desired aims. Therefore this paper has proposed the principle of a hybrid version that is able to encompass the advantages of both systems and assist in mitigating the key disadvantages. Future research will assess the viability of such an approach via the design and practical implementation of an associated architectural framework.

REFERENCES

Best, J. (2006a), "3G reaches 50 million users worldwide", CNET.com, 10 February 2006, URL http://news.cnet.co.uk/mobiles/0,39029678,49251672,00.htm

Best, J. (2006b), "Mobile roaming price-cuts in sight", Silicon.com, 12 December 2006, http://networks.silicon.com/mobile/0,39024665,39164649,00.htm

British Transport Police (2006), "Mobile phone theft", URL

http://www.btp.police.uk/issues/mobile.htm

Bruce, J. (2006), "Trends in high-speed mobile video", Portable Design, March 2006, URL http://pd.pennnet.com/display_article/249575/21/ARTCL/none/Appli/Trends_in_high-speed_mobile_video/

Clarke, N.L., Furnell, S.M, Rodwell, P.M, Reynolds, P.L (2002), "Acceptance of Subscriber Authentication Method for Mobile Telephony Devices", Computers & Security, 21, 3, pp220-228

Clarke, N.L., Furnell, S.M. (2006), "Authenticating Mobile Phone Users Using Keystroke Analysis", International Journal of Information Security, pp1-14, 2006

Denning, D. (1999), "Information Warfare and Security", Addison – Wesley, US

Furnell, S. and Evangelatos, K. (2007), "Public awareness and perceptions of biometrics", *Computer Fraud & Security*, January 2007, pp8-13.

Gissin, I. (2005), "Reality check: A 3G-user experience", TotalTelecom, 19 Octomber 2005, URL http://www.totaltele.com/View.aspx?ID=75921&t=4

Gomm, K. (2005), "Full biometric ID scheme to reach the UK 'by 2009", ZDnet.co.uk, 20 Octomber 2005, URL http://news.zdnet.co.uk/hardware/0,1000000091,39232692,00.htm

IBG (2002), "How large are biometric templates?", International Biometric Group, URL http://www.biometricgroup.com/reports/public/reports/template_size.html

Karatzouni, S., Furnell S.M., Clarke N.L., Botha R.A. (2007), "Perceptions of User Authentication on Mobile Devices", Proceedings of the ISOneWorld Conference, Las Vegas, USA, April 11-13, CD Proceedings (0-9772107-6-6) 200

Lettice, J. (2006), "Compulsory and centralised - UK picks hardest sell for ID cards", The Register, 13 March 2006, http://www.theregister.co.uk/2006/03/13/ou_idcard_study/

Leyden, J. (2005), "Londoners Top World in Leaving Laptops in Taxis", The Register, 25 January 2005, URL http://www.theregister.co.uk/2005/01/25/taxi_survey/

Leyden, J. (2006), "Where's My 3.5G Handset?", The Register, 18 July 2006, URL http://www.theregister.co.uk/2006/07/18/informa_mobile_report/

Mobile Business (2006), "Orange Data Not Secure", Mobile Business Magazine, 22 November 2006, URL

http://www.mbmagazine.co.uk/index.php?option=com_content&task=view&id=1441&Itemid=2&PHPSESSID=d6fc7ad0c429dae5956c3ffd9466a84d

Nanavati, S., Thieme, M., Nanavati, R. (2002), "Biometrics: Identity Verification in a Networked World", John Wiley & Sons, New York, US,2002

Noguchi, Y. (2005), "Lost a BlackBerry? Data Could Open A Security Breach", Washington Post, 25 July 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/07/24/AR2005072401135.html

NTT DoCoMo (2003), "DoCoMo's Newest 505i Handset Features Fingerprint Authentication", http://www.nttdocomo.com/pr/2003/000985.html

Omron. (2005), "Omron Announces "OKAO Vision Face Recognition Sensor", World's First Face Recognition Technology for Mobile Phones", http://www.omron.com/news/n_280205.html

PDALok (2006), "Signature Recognition", PDALok, http://www.pdalok.com

Pointsec (2005), "IT professionals turn blind eye to mobile security as mobile survey reveals sloppy handheld habits", URL http://www.pointsec.com/news/newsreleases/release.cfm?PressId=108

Porter, H. (2004), "If you value your freedom, reject this sinister ID card", The Guardian, 17 December 2004, URL http://www.guardian.co.uk/idcards/story/0,15642,1375858,00.html

Richardson, T. (2005), "O2 posts upbeat trading update", The Register, 27 September 2005, URL http://www.theregister.co.uk/2005/09/27/o2_update/

Thai, B., Wan, R., Seneviratne, A., Rakotoarivelo, T. (2003), "Integrated Personal Mobility Architecture: A Complete Personal Mobility Solution", Mobile Networks and Applications, Vol. 8, No. 1, 27-36

TimesOnLine (2004), "ID and Ego: It is right to experiment with identity cards", Times Online, 27 April 2004, URL http://www.timesonline.co.uk/article/0,,542-1089392,00.html

Vance, A. (2006), "Lost Ernst & Young laptop exposes IBM staff", The Register, 15 March 2006, URL http://www.theregister.co.uk/2006/03/15/ernstyoung_ibm_laptop/

COPYRIGHT