EXHIBIT E

Using Geographical Location as an Authentication Factor to Enhance mCommerce Applications on Smartphones

Torben Kuseler *torben.kuseler@buckingham.ac.uk*
Applied Computing Department
The University of Buckingham
Hunter Street, Buckingham, MK18 1EG, UK

Ihsan Alshahib Lami *ihsan.lami@buckingham.ac.uk*
Applied Computing Department
The University of Buckingham
Hunter Street, Buckingham, MK18 1EG, UK

Abstract

Smartphones are increasingly used to perform mCommerce applications whilst on the move. 50% of all Smartphone owners in the U.S. used their Smartphone for banking transactions in the first quarter of 2011. This is an increase of nearly 100% compared to the year before. Current techniques used to remotely authenticate the client to the service provider in an mCommerce application are based on "static" authentication factors like passwords or tokens. The fact that the client is on the move, whilst using these mCommerce applications is not considered or used to enhance the authentication security. This paper is concerned with including client's geographical location as an important authentication factor to enhance security of mCommerce applications, especially those requiring robust client authentication. Techniques to integrate location as an authentication factor as well as techniques to generation location-based cryptographic keys are reviewed and discussed. This paper further outlines restrictions of location as an authentication factor and gives recommendations about correct usage of client's location information for mCommerce application's authentication on Smartphones.

Keywords: Authentication, Location, mCommerce Applications, Security, Smartphone.

1. INTRODUCTION

Smartphones are becoming a major part in everybody's daily life. All kinds of activities, including banking or financial mCommerce transactions (e.g. online shopping), are nowadays performed online via Smartphone applications whilst on the move. 50% of all Smartphone owners in the U.S. used their Smartphone for banking transactions in the first quarter of 2011. This is an increase of nearly 100% compared to the year before [1]. However, most of the techniques used to authenticate the client towards the remote authenticator (i.e. the bank offering a financial service) in these mCommerce applications still base upon classic (and static) authentication factors like passwords, tokens or biometrics. The fact that the client is on the move, whilst using these mCommerce applications is not considered or used to enhance the authentication security.

Reliable client authentication and data protection are still major concerns for mCommerce application providers because the classical authentication factors are open for hackers. As a result, mCommerce application providers restrict access, on average, to 30% of possible services to their clients via Smartphone applications [2].

This paper a) reviews techniques that use location as an authentication factor, and b) makes recommendations how location can be used to enhance the security of mCommerce applications requiring robust client authentication. This shall encourage mCommerce application providers to offer more services via Smartphone application to their clients.

The rest of this paper is organised as follows. Section 2 gives technical background information about methods to determine the location of Smartphones. Section 3 reviews techniques that use location as an authentication factor. In section 4, the use of location to generate cryptographic keys is discussed. Section 5 outlines restrictions of location as an authentication factor and makes recommendation towards a secure and reliable usage of location information in authentication. Finally, section 6 concludes the findings studied in this paper.

2. TECHNICAL BACKGROUND OF METHODS TO LOCATE SMARTPHONES

Three localisation techniques are commonly used to establish the location of Smartphones [3]. These techniques vary in the provided location accuracy (i.e. how exact can the technique determine the Smartphone's location?) as well as the availability (i.e. does the technique cover the complete earth or only urban areas? Is the technique available indoors or does the client have to be outdoors to determine his/her position?).

2.1 Global Positioning System (GPS)

GPS-based positioning [4] has become the positioning technique mostly used on Smartphones. All new developed Smartphones feature a GPS receiver. GPS positioning is based on the reception of signals continuously transmitted from satellites. These signals contain the precise time the message was sent, as well as the location in orbit of the satellite. The GPS receiver uses the received signals of four or more satellites to calculate the current position based on trilateration. When outdoors, current GPS receivers onboard Smartphones are able to reduce the positional error to few meters [5]. However, GPS requires a line of sight to the satellites. Because of that, GPS can not be used (or the use is limited and the position becomes imprecise) indoors or in urban areas with many high glass-front buildings, where a direct line of sight to the satellites is not available. New satellite systems are rolling out such as GLONASS, and Galileo. These systems offer more enhanced signals and will provide better localisation accuracy than GPS.

2.2 Wi-Fi-based Positioning

Wi-Fi-based positioning uses Wi-Fi access points (Wi-Fi APs) to determine the position of the Smartphone. Wi-Fi APs continuously transmit beacons, including an AP identifier, to their surrounding area to inform potential Wi-Fi clients, such as a Smartphone, about their existence. Over the last years, several databases of APs and their corresponding geographical locations were collected by companies like Skyhook [6]. The Smartphone can use the AP identifier enclosed in the beacons and these databases, via an internet link, to determine the locations of the surrounding APs, by searching the identifier in the database. Depending on the number of APs in range, the achieved location accuracy of Wi-Fi-based positioning can vary between a few to 100 meters. Wi-Fi-based positioning can be used indoors as well as outdoors, as long as the AP transmitted beacon can reach the Smartphone. However, the number of available APs differs greatly between urban and rural areas, making Wi-Fi-based positioning a technique to be mainly used in big cities with lots of existing and known APs [5]. APs are also used to transport needed aiding information to the GPS device onboard the Smartphone. This helps the GPS receiver to fix much quicker.

2.3 Cellular Network Based Positioning

Cellular network based positioning use trilateration techniques to calculate the current Smartphone location [7]. The cellular network is divided into cells, in which each cell has a unique identifier (cell-ID). Depending on the trilateration technique used to determine the current phone location (e.g. U-TDOA [8]) and the cell size, cellular network based positioning accuracy can range between 50 metres to a few kilometres [5].

3. LOCATION AS AN AUTHENTICATION FACTOR IN REMOTE AUTHENTICATION

3.1 Classic Authentication Factors

Classic authentication factors are mostly used to authenticate the client towards the remote authenticator in mCommerce applications. Classic authentication factors can be categorised into three groups [9]:

1) Knowledge-based, or "something you know"
   Knowledge-based authentication factors rely on a memorised piece of information, e.g. PIN or password. Long and random passwords can offer a high level of security in authentication systems. However, in practice, clients have huge difficulties to memorise random and strong passwords. This often results in the use of short passwords that are therefore simple to guess and do not provide high authentication security.

2) Object-based, or "something you have"
   Object-based authentication factors rely on physical possessions, e.g. tokens. A token has the advantage over a knowledge-based authentication factor that clients do not need to memorise anything. This eliminates the risk of attackers guessing passwords easily because simple passwords are used. However, the main security drawback of physical tokens is that, when lost or stolen, an attacker gains unauthorised access.

3) Identity-based, or "something you are"
   Identity-based authentication factors, i.e. Biometrics rely on the uniqueness of physiological (e.g. fingerprint, facial features) or behavioural (e.g. hand-writing, speech) characteristics of a client. Biometric-based authentication offers two advantages over the other classic authentication factors:
   1) A client does not need to remember or carry anything.
   2) Biometrics verify the de facto client and not only knowledge of a password or possession of a token, i.e. the genuine client needs to be present at the biometric sensor.

   Biometric authentication systems are not perfect and their security can also be undermined. For example, the genuine client's biometric can be replaced in the biometric template database or a biometric sample can by replayed by an attacker.

These classic authentication factors can be used to define the "**who**" of an authentication attempt. They define neither the "**where**" nor the "**when**" of the attempt, two similarly important properties of secure remote client authentication, for example to tackle distance or replay attacks. Thus, location (to define the "**where**") and time (to define the "**when**") should be integrated as further authentication factors, to define all these properties in remote client authentication.

3.2 Location as an Authentication Factor

Location was integrated into authentication systems as a factor to "ground" authentication attempts [9]. This "grounding" reduces the risk of distance attacks, because an attacker cannot claim to be at a location, the attacker actually does not is [10]. To achieve "grounding", a unique identifier (digital signature) was derived from a GPS-based location and real-time on a specialised location signature sensor (LSS). The generated digital signature was then combined with further authentication data in such a way that it stamps the data with location and time information in a forgery-proof way. The security and uniqueness of the LSS digital signature bases upon the fact that bit values of GPS signals change every 20 milliseconds and so the resultant signature changes accordingly. However, current GPS receivers available on Smartphones cannot be used to generate such unique and trusted signatures, because these GPS receivers compute longitude and latitude from the received signals straightaway. Also, dedicated LSS are required to verify the client's location signature. This aspect prevents that the LSS-based system can be deployed on a

large scale, e.g. country wide, because this requires installation of thousands of LSS for verification of the client's claimed location. Thus, the LSS-based system is more suitable for limited areas like company premises but not for general mCommerce applications.

A similar approach with global availability is Secure Authentication for GPS phone Applications (SAGA) [11]. In contrast to other GPS-based services, SAGA can be used to determine the current location using the Smartphone's onboard GPS receiver as well as used to verify this claimed location. A security analysis of SAGA concluded that SAGA offers reliable and secure location verification, with the advantage that a GPS-based system is available worldwide [12]. However, to perform a verification of the client's claimed location, the SAGA system also requires additional trusted signal receivers at several known locations that are used to receive reference signals from the satellites for comparison. This introduces further costs for installation and maintenance of these receivers for practical authentication in mCommerce applications.

"Location cross-checking" techniques do not require additional receivers to be installed for location verification. Instead, location cross-checking compares the actual location of the Smartphone with a pre-agreed set of known points of businesses related to the registered clients (e.g. an ATM machine) to counter distance attacks [13]. However, location cross-checking requires an ongoing monitoring to track the current location of the Smartphone (to help identify abnormal activities or attacks to the system). This ongoing monitoring is difficult to maintain as Smartphones might be switched off by the client to save energy or might be used outside the traceable area. A further downside of location cross-checking lies in the dependence of the pre-agreed points of businesses, which are difficult to define and maintain in mCommerce applications for Smartphones.

"Location proofs" try to overcome the drawbacks of location cross-checking [14]. A location proof is a piece of data generated by a stationary sender (e.g. Wi-Fi AP) that is then sent to the Smartphone on request. The Smartphone stores the received proof for immediate or later use and attaches it to an authentication message to proof the client's current location. An advantage of location proofs over location cross-checking is that the points of businesses must not be defined in advance. However, location proofs require trusted stationary senders instead (e.g. Wi-Fi AP), which should not be easily susceptible to manipulation.

Location proofs are also critical from a client's privacy point a view [15]. Requesting a location proof discloses the client's identity to the stationary sender, i.e. the proof issuer. This information could then, for example, be used to generate a location profile of the client. To overcome this problem, the VeriPlace architecture [15] extended the location proof concept and included two separated and trusted entities for managing location and identity information of the client. This ensures that location and identity are never available at the same time to one entity.

The Privacy-Preserving Location proof Updating System (APPLAUS) [16] removed the requirement of stationary senders to issue location proofs. Instead other Smartphones in the close neighbourhood serve as location proof issuers and communicate the proof to the requestor via Bluetooth in a peer-to-peer approach. The benefit of APPLAUS is that no specific network infrastructure or specialised trusted senders are required. However, security and reliability of APPLAUS bases completely upon the number and trustworthy of the neighbouring Smartphones that issue the location proofs.Systems like APPLAUS may be adequate for low-value services that require a location proof, e.g. downloading a digital brochure of a museum for free if the client has previously visited the museum. For high-value mCommerce transaction authentication, such peer-to-peer architectures do not offer enough security and reliability, because the neighbouring Smartphones, which issue the location proofs, cannot be fully trusted.

Localisation and certification services [17] are used to tag digital content (e.g. authentication messages) with a location and timestamp DTL-certificate (Data-Location-Time). The DTL-certificate enables the receiver of the stamped content to verify where the content was originally created. To get a DTL-certificate, the client sends the hash value of the message to a localisation

/ certificate authority. This authority then determines the client's location, for example via cellular network based positioning or Wi-Fi-based positioning (cp. section 2). The determined location and current time are then combined with the hash value of the message and send back to the client as the DTL-certificate. To ensure the producer's privacy, the DTL-certificate does not include any information about the producer's identity. Thus, only time and location of the generated content can be verified by the receiver of the DTL-certificate.

The independent determination of the client's location by the localisation / certificate authority ensures that the client actually is at the claimed location, i.e. the DTL-certificate does not base upon the location determined by the client. However, the DTL-certificates miss a tight binding between location and client. The generated DTL-certificate can be given away and used by others, which could undermine the authentication system, i.e. an attacker could use a stolen certificate to impersonate a genuine client's location. In addition, DTL-certificates might be subject to malicious modifications, because the DTL-certificates have to be sent back to the client and are stored on the client's phone.

4. LOCATION-BASED KEYS

Section 3 reviewed and discussed approaches that use location information as an authentication factor directly integrated into an authentication message to "ground" the client's authentication attempt. Another possibility to use location information to enhance the security of mCommerce applications is to combine location with established cryptographic algorithms, i.e. message encryption. For example, the authenticator can encrypt his authentication messages to the client with a cryptographic key based on a combination of a) a client specific and pre-agreed password and b) a location-based key. This has the advantage in mCommerce application that an attacker needs to get two pieces of information (i.e. the genuine client's password and the current location) to illegitimately decrypt the authenticator's messages.

The GeoEncryption concept [18] utilises this approach and uses location as a source to generate location-based keys for encryption of digital messages. GeoEncryption extends a classic hybrid cryptographic algorithm with a GeoLock functionality to ensure a secure location binding of the digital message. A geo-encrypted message can be opened successfully (decrypted) by a receiver, if the receiver's actual location is inside the required area. A general GeoLock mapping function, based on the estimated Position, Velocity, and Time (PVT) on the recipient is used to generate the message encryption and decryption key. However, the GeoEncryption concept did not specify a practical and secure PVT mapping function nor does it handle support of mobile and moving recipients, which is an important aspect of mCommerce applications performed on Smartphones.

In the added GeoEncryption mobility model [19], the encrypted message receiver continuously updates the sender about his/her current location. The sender then uses this information to dynamically adjust the decryption area in which the receiver can decrypt the message. A practical mapping function for the GeoEncryption concept uses square areas [20]. This mapping function was then improved to cover any shape [21], which increased the precision of how the decryption area can be specified, i.e. the introduced decryption area error is reduced.

A drawback of these mapping functions is that the generated encryption key merely bases upon the geographical coordinates (longitude and latitude values) of the decryption area and the used hash function as shown in Figure 1 [20]. If the geographical coordinates of the target region (decryption area) can be estimated by an attacker, because the attacker is in close proximity to the recipient, then the complete security of GeoEncryption lies in the secrecy of the hash function. If the used hash function is also known to the attacker, then the attacker is able to decrypt the message. To minimise this risk, the GeoEncryption keys should be combined with further client specific information (e.g. password or a token stored on the client's Smartphone) that is more secret than the "public available" location of the client (cp. section 5).

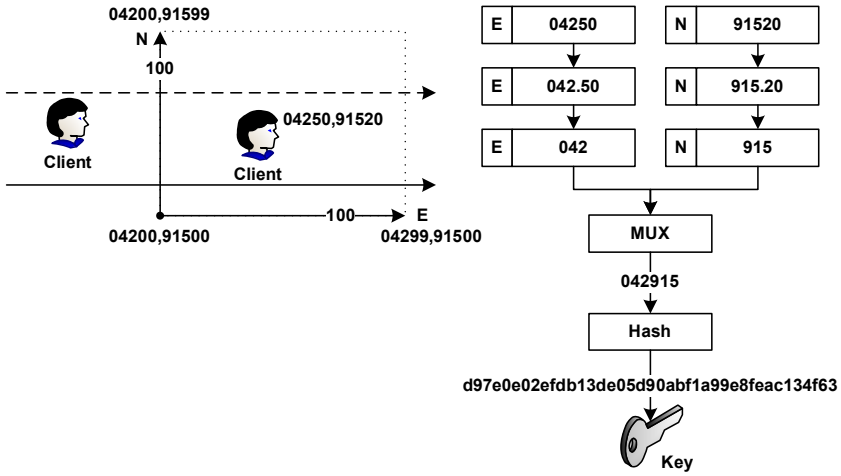

FIGURE 1: GeoEncryption mapping function

Time and Location Based One-Time-Passwords (TLB OTP) [22] utilises the estimated location of the client with the current time to calculate a TLB OTP. This TLB OTP is then used as a key to (de)encrypt all further communication messages between client and authenticator. Adding location to classical OTP schemes, which are merely time-dependent, strengthens the authentication security, because it is more difficult for an attacker to determine the client's current location and precise time simultaneously [22]. To enhance and ensure correctness of the client's location and future position estimation, the client sends periodically update information about the client's current location and movement to the authenticator.

The practical mapping functions for GeoEncryption also require that the recipient's direction of movement is known during encryption of the message to correctly define the decryption area. To achieve this, the receiver also transmits periodically movement updates, which are then used to calculate the correct decryption area [20]. The importance of these updates can be seen in the example of Figure 1. The starting point of the decryption region is chosen to be at: "E04200" and "N91500", and the client is assumed to travel eastwards (E) in a maximum range of 100 meters (i.e. location will be equal to "E04299" after 100 meters). If the client travels more than 100 meters, a different key is produced. For example, travelling 110 meters results in "E04310" and hence the hashed value is completely different. A similar problem occurs if the direction of the client's movement is unknown. In this case, the phone needs to move one meter westwards instead of eastwards (i.e. to location E04199) to produce a different key. Such precise client location estimation is difficult to achieve in mCommerce applications, because clients often change directions when using their Smartphone's whilst on the move.

The Location-Dependent Data Encryption Algorithm (LDEA) introduces a Toleration Distance (TD) during encryption of the messages to overcome the receiver's movement uncertainty [23]. The TD shall guarantee that always the same key is generated on sender and receiver side, if the receiver is within the TD area. However, analyses of the LDEA showed that LDEA is not able to generate always the correct decryption key even if the client is within the specified TD area as shown in Figure 2.

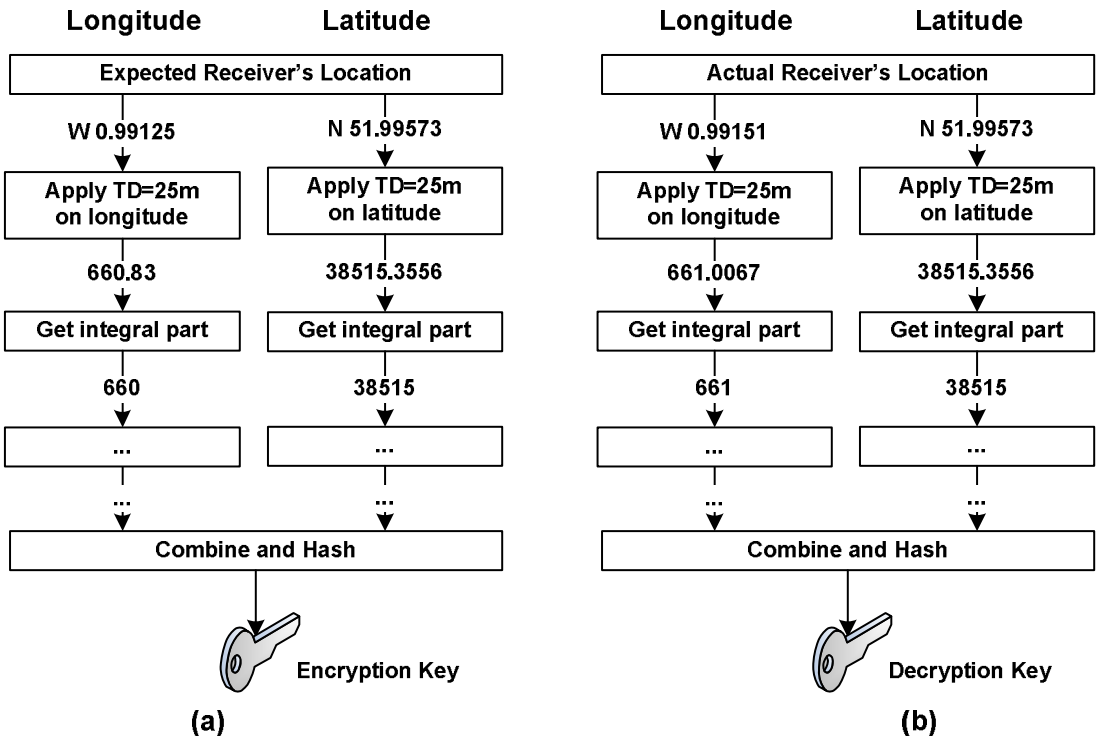

FIGURE 2: GeoEncryption key generation function

Figure 2(a) shows the process to generate the encryption key performed by the sender for the expected receiver's location of: W0.99125 / N51.99573 (cp. [23] for the details of this process). A TD of 25 metres is used in this example. Figure 2(b) shows the same process performed by the receiver on his/her actual location (W0.99151 / N51.99573). These two locations (i.e. expected and actual) are 17 metres away from each other and therefore well within the TD of 25 metres. However, the integral part of the longitude values is different (660 != 661). This means that the decryption key will also differ and that the client is not able to decrypt the message.

5. CONSIDERATIONS FOR USING LOCATION AS AN AUTHENTICATION FACTOR IN mCOMMERCE APPLICATIONS

5.1 Restrictions of Location as an Authentication Factor

Location as an authentication factor has restrictions compared to classical authentication factors (e.g. passwords, tokens or biometrics) and requirements, if location is used to generate cryptographic keys:

1) Location of a Smartphone is "publicly" available knowledge. Location can be easier gathered by an attacker, which is more difficult, for example, for undisclosed password. Attackers could simply follow clients and use the knowledge of the clients' whereabouts to get unauthorised system access, if location is the only factor used in the authentication system.

2) Use of location to generate cryptographic keys needs an appropriate key-generation function to transfer the physical client's location into a key. Utilising an inadequate transfer function can result in simple to guess location-based keys.

   It is important that the generated location-based key does not directly relate to the client's physical location (e.g. latitude and longitude values), i.e. a key for any location should not be predictable from a known location / key pair. If this property is not satisfied, then:

1) Large areas of the earth (e.g. Arctic, Antarctic) must be eliminated from the available key-space area, because it is unlikely that a client is in these areas.
2) The number of keys an attacker needs to try in a brute-force attack reduces tremendously, if the client's location is approximately known.

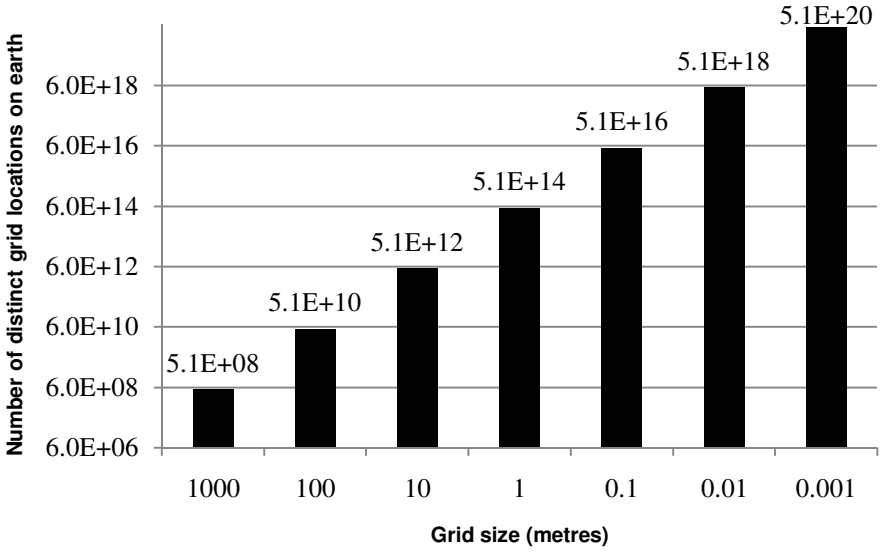

FIGURE 3: Maximum number of possible location-based keys

3) The number of locations on earth is limited. This restricts the number of possible locations to be used as location-based keys, i.e. the location key-space is restricted. Figure 3 shows the maximum number of location-based keys possible on earth, if the earth's surface is divided into a grid of equal-distance squares [24]. For a square size of one metre, $5.1*10^{14}$ different keys can be generated. This number is comparable to the number of eight character (0-9a-zA-Z) long passwords that is $2.2*10^{14}$. However, depending on the technique used to determine the clients location (cp. section 2), the location key-space can be much less, because the location determination technique does not achieve such a high accuracy.

5.2 Recommendations for Location as an Authentication Factor

To use location as an authentication factor in mCommerce applications or to generate secure and reliable location-based keys, the following recommendations should be applied:

1) The location-based keys should be determined completely independent from each other, without the need of any further sending of location information or movement direction to establish the same key on the client and authenticator side. This condition is required to guarantee that the authenticator can completely independently verify and consequently trust the claimed location of the client [25].

2) The location-based key needs to be generated with a specific location tolerance. This tolerance is necessary because methods to determine and verify the claimed client location differ in the accuracy (cp. section 2). A tolerance area should be used to handle this difference.

3) All location-based keys outside the tolerance area need to be different to the key representing the tolerance area. This condition ensures that the client is actually inside the tolerance area and not at a different place, which may produce the same key.

4) It must be ensured that the key-space of the generated location-based keys is large enough to minimise the risk of a brute-force attack (cp. section 4). This can be achieved, for example,

be combining client's location with further authentications factors (e.g. passwords) in the key generation process.

5) The location-based key should incorporate location information as well as further, more secret data (e.g. a token stored on the client's Smartphone). This eliminates the risk that an attacker is able to calculate the location-based key, if the attacker knows the client's current whereabouts.

6) Introduction of client's physical location into the authentication process may raise "privacy concern", i.e. tracking clients' location without their consent. To overcome this concern, methods which preserve the client's location privacy [26] and, at the same time, enable the authenticator to verify the client's claimed location independently should be used.

6. CONCLUSION

Integration of geographical location of the client's mobile device as an authentication factor into remote authentication systems for mCommerce application shall enhance the security of such systems:

1) Remote attacks are reduced, because integration of location information into the authentication data "grounds" the authentication attempt to a specific place. If the client's location claim is then independently verified, then an attacker cannot pretend to be at a different place. Independent location verification is important, because the location determined on the phone can be manipulated. For example, the GPS receiver of the phone can be manipulated or an IP-address-based location determination can be fooled by using a proxy server. I.e., for example, a cellular network operator based localisation is used to verify the client's claimed or the GPS predicted location.

2) If the client's location is combined with real-time, then remote replay attacks can also be reduced. Client's authentication data can be uniquely stamped with the current time. I.e. an attacker cannot re-use previously gathered genuine client authentication data, because of the time-stamp expiry.

However, the use of location also introduces requirements (e.g. client's location privacy or limited location-based key-space), which need to be carefully addressed by the authentication system. Privacy preserving algorithms can be deployed to solve such issues. For example, the client's actual location is randomly projected based on the Cell-ID serving the client's mobile device.
Research on secure and reliable integration of location information into authentication as well as generation of location-based key is still ongoing and needs further investigations and improvements to widely deploy location as an authentication factor in mCommerce application for Smartphones.

7. REFERENCES

[1] Frank Diekmann, "Survey: Mobile Bankers Double Over Last Year." Credit Union Journal, vol. 15, no. 18, pp. 19-19, May 2011.

[2] Security's Role in Deploying Transaction-Enabled Mobile Applications, Aug 2010.

[3] G. Sun, J. Chen, W. Guo, and K.J.R. Liu, "Signal processing techniques in network-aided positioning: a survey of state-of-the-art positioning designs." IEEE Signal Processing Magazine, vol. 22, no. 4, pp. 12-23, 2005.

[4] U.S. Government,"Official U.S. Government information about the Global Positioning System (GPS) and related topics."Internet: www.gps.gov, Apr. 20, 2012 [May 15, 2012].

[5] Paul A. Zandbergen, "Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning." Transactions in GIS, vol. 13, no. s1, pp. 5-25, 2009.

[6] Skyhook, “Skyhook.”Internet: www.skyhookwireless.com, [May 15, 2012].

[7] Axel Kuepper. Location-Based Services: Fundamentals and Operation. Wiley Online Library, Oct. 2005.

[8] TruePosition, U-TDOA: Enabling New Location-Based Safety and Security Solutions, Oct. 2008.

[9] S.Z. Li and A.K. Jain.Encyclopedia of Biometrics. US, Springer US, 2009.

[10] D. Denning and P. MacDoran, "Location-Based Authentication: GroundingCyperspace for Better Security." Computer Fraud and Security Bulletin, Feb. 1996.

[11] A.I.G.T. Ferreres, B.R. Alvarez, and A.R. Garnacho, "Guaranteeing the authenticity of location information." IEEE Pervasive Computing, pp. 72-80, 2008.

[12] S. Lo, D.S. De Lorenzo, P.K. Enge, D. Akos, and P. Bradley, "Signal authentication-a secure civil gnss for today." inside GNSS, vol. 4, no. 5, pp. 30-39, 2009.

[13] G. Becker, S. Lo, D. De Lorenzo, P. Enge, and C. Paar, "Secure Location Verification." Data and Applications Security and Privacy XXIV, 2010, pp. 366-373.

[14] A. Haeberlen et al., "Practical robust localization over large-scale 802.11 wireless networks." in Proceedings of the 10th annual international conference on Mobile computing and networking, ACM, 2004, pp. 70-84.

[15] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs." Proceedings of the 10th workshop on Mobile Computing Systems and Applications, New York, USA, 2009, pp. 3:1--3:6.

[16] W. Luo and U. Hengartner, "VeriPlace: a privacy-aware location proof architecture." Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems, ACM, 2010, pp. 23-32.

[17] Z. Zhu and G. Cao, "Applaus: A privacy-preserving location proof updating system for location-based services." INFOCOM, 2011 Proceedings IEEE, 2011, pp. 1889-1897.

[18] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: applications, challenges and implementations." Proceedings of the 9th workshop on Mobile computing systems and applications, ACM, 2008, pp. 60-64.

[19] L. Scott and D.E. Denning, "A location based encryption technique and some of its applications." in ION National Technical Meeting, vol. 2003, 2003, pp. 730-740.

[20] A. Al-Fuqaha and O. Al-Ibrahim, "Geo-encryption protocol for mobile networks," Computer Communications, vol. 30, no. 11-12, pp. 2510-2517, 2007.

[21] G. Yan and S. Olariu, "An efficient geographic location-based security mechanism for vehicular adhoc networks." IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, MASS'09, 2009, pp. 804-809.

[22] G. Yan, J. Lin, D.B. Rawat, and W. Yang, "A Geographic Location-Based Security Mechanism for Intelligent Vehicular Networks." Intelligent Computing and Information Science, pp. 693-698, 2011.

[23] W.B. Hsieh and J.S. Leu, "Design of a time and location based One-Time Password authentication scheme." Wireless Communications and Mobile Computing Conference (IWCMC), 7th International, IEEE, 2011, pp. 201-206.

[24] H.C. Liao and Y.H. Chao, "A new data encryption algorithm based on the location of mobile users." Information Technology Journal, vol. 7, no. 1, pp. 63-69, 2008.

[25] L. Scott and D.E. Denning, "Location Based Encryption & Its Role In Digital Cinema Distribution." Tech. rep. 2003.

[26] Ihsan A. Lami, Torben Kuseler, Hisham Al-Assam, and Sabah Jassim, "LocBiometrics: Mobile phone based multifactor biometric authentication with time and location assurance," Proc. 18th Telecommunications Forum, IEEE Telfor, Nov. 2010.

[27] Torben Kuseler, Hisham Al-Assam, Sabah Jassim, and Ihsan A. Lami, "Privacy preserving, real-time and location secured biometrics for mCommerce authentication," SPIE Mobile Multimedia/Image Processing, Security, and Applications 2011, vol. 8063, Apr. 2011.