Torben Kuseler; Hisham Al-Assam; Sabah A. Jassim and Ihsan Lami, "Privacy preserving, real-time and location secured biometrics for mCommerce authentication", Proc. SPIE 8063, Mobile Multimedia/Image Processing, Security, and Applications 2011 (May 26, 2011); doi: 10.1117/12.883101

Privacy preserving, real-time and location secured biometrics for mCommerce authentication

Torben Kuseler, Hisham Al-Assam, Sabah Jassim, Ihsan A. Lami
Applied Computing Department
University of Buckingham
Hunter Street, Buckingham, MK18 1EG, UK
(phone: 44-1280-814080; email: first.last@buckingham.ac.uk)

ABSTRACT

Secure wireless connectivity between mobile devices and financial/commercial establishments is mature, and so is the security of remote authentication for mCommerce. However, the current techniques are open for hacking, false misrepresentation, replay and other attacks. This is because of the lack of real-time and current-precise-location in the authentication process. This paper proposes a new technique that includes freshly-generated real-time personal biometric data of the client and present-position of the mobile device used by the client to perform the mCommerce so to form a real-time biometric representation to authenticate any remote transaction. A fresh GPS fix generates the "time and location" to stamp the biometric data freshly captured to produce a single, real-time biometric representation on the mobile device. A trusted Certification Authority (CA) acts as an independent authenticator of such client's claimed real-time location and his/her provided fresh biometric data. Thus eliminates the necessity of user enrolment with many mCommerce services and application providers. This CA can also "independently from the client" and "at that instant of time" collect the client's mobile device "time and location" from the cellular network operator so to compare with the received information, together with the client's stored biometric information. Finally, to preserve the client's location privacy and to eliminate the possibility of cross-application client tracking, this paper proposes shielding the real location of the mobile device used prior to submission to the CA or authenticators.

Keywords: Authentication, Biometrics, Cellular Towers, GPS, Location, mCommerce, Privacy, Time

1. INTRODUCTION

The sales and distribution of advanced Smartphones and Tablet-PCs has significantly increased over the last few years. This makes these mobile devices a valuable and powerful companion in our modern and highly mobile life. On the move access to social websites or company intranets, online checks of bank accounts or even complete mCommerce transactions are widely accepted operations performed by various users on their mobile phones. But secure, reliable authentication which can be subsequently prove the genuine users after mobile transaction scenarios is difficult. This is due to the lack of personal contact between the involved parties, which is one of the main security relevant characteristic in "static" store- or office-based business dealings (i.e. location and time is known and can be proven at the time of the transaction). The number of adult consumers, who were affected by identity theft increased tremendously in the last years, reaching a total number of more than 11 millions in the United States in 2009. This was an increase of more than 10 percent, or over one million victims, compared to the previous year. Forty-two percent of the questioned victims reported that their personal information was misused in an online purchase or transaction [1].

This paper proposes to enhance the security of mCommerce applications by combining the biometric-based authentication process to identify a genuine person with including a proof of the current user's location, which is independently verified through a trusted certification authority (CA) during authentication. The CA will request the current mobile device position from the cellular network operators, who can locate a mobile device during their normal operation by cellular basestation/tower triangulation. To ensure the privacy of the client, this paper proposes an algorithm so that the actual mobile device location is transferred into a "different domain" based on a "dynamic secret" shared between the mobile device and the cellular network operators, which is also unknown to the CA or any other legitimate/fake party involved. This proposed transformation preserves the relative distances necessary to verify the claimed location of the mobile device, but does not reveal the actual real physical location of the client to the CA. In

addition, to further enhance the security and to guarantee the liveliness of the communication process, this paper further proposes that the transaction messages between the mobile device and the CA are protected by a biometric-based challenge / response encryption scheme.

Latest generations of Smartphones and Tablet PCs incorporate a large diversity of sensors, and wireless communications transceivers. 3G, GSM, Wi-Fi, Bluetooth and GPS receivers, cameras, microphones and multi-touch displays are very common features in most mobile devices. Integration of these additional features into mCommerce applications offers new possibilities to enhance the security and to strengthen the authentication process. For example, the mobile device location and the highly-accurate time extracted from received GPS messages can be used to tag the single steps in an authentication or communication process. Similar, various user biometrics (e.g. fingerprint) can be effortlessly gathered by the device sensors and used in tight combination with the location and time to 1) clearly identify the user by his/her biometrics, 2) ensure the freshness of the authentication process by integrating the GPS-based time and 3) determine and verify the position of the mobile device by using GPS and the cellular network.

This novel location verification concept joined with the guarantee of fresh GPS real-time stamped biometric authentication shall bring back the "location, time and participating individual" confidence of office-based businesses to mCommerce applications. The algorithms proposed in this paper extend the previously published eBiometrics mobile authentication scheme [2] with the proof of the mobile device location and the certainty of a real-time and fresh authentication process.

The reminder of the paper is organised as follows: Section 2 describes the background of this paper and outlines related work in biometric-based authentication and privacy preserving mobile device location verification technologies. Section 3 introduces the general idea of the proposed biometric-based challenge / response location verification method. Section 4 extends this algorithm to preserve the location privacy of the mobile device user. Finally, we conclude the paper and outline future work in Section 5.

2. BACKGROUND AND RELATED WORK

Authentication can be defined as a procedure which confirms, that a person is who he/she claims to be, by the use of one or more different methods or factors. Nowadays, the three most accepted authentication factors are: something a user *knows* (e.g. password), something a user *has* (e.g. credit card or token) or something a user *being/is* (e.g. biometrics) [3]. Recently, researchers have proposed additional authentication features, e.g. "*somebody you know*" (vouching) [4] or "*where you are*" which can be used in conjunction with the classical factors to enhance authentication security. Strong passwords can offer a high authentication security if deployed properly. Unfortunately, password-based authentication is often easy to crack/hack in to because users select only very short passwords which can be easily memorised and therefore guessed by a hacker. The security of a token relies completely on the physical ownership. Once lost or stolen, a token can be used by everyone and does not offer any authentication security any more. Biometric authentication is based on human physical properties or behaviours and is accepted as a very reliable and robust authentication method. However, various ways to offend a biometric-based system have been identified, e.g. template replacement or replay attacks [5]. Therefore, the objectives of recent research efforts in biometric-based authentication have widened to involve improving the security of biometric templates. Template protection schemes have been proposed in the literature to produce cancellable/revocable biometrics. Theses schemes can be classified into two main categories [6]: feature transformation and biometric cryptosystem. In this paper, we focus on the first category (i.e. feature transformation), and more precisely on Random Orthonormal Projection (ROP) proposed in [7, 8]. ROP technique relies on user-based orthonormal matrices to transform individual's biometric features (points in high dimensional space) to a secure space where the distances between original points and the secure ones are preserved.

Aloul and El-Hajj proposed in [9] to use a mobile phone as a software token, which generates a one-time password (OTP) based on unique phone identifiers (IMEI, IMSI) and a username/PIN. Time is included in the OTP to ensure the one-time property and to avoid the re-use of previously generated passwords. [10] suggested to cross-check a user location in a business transaction (e.g. an ATM machine cash withdrawal or a purchase in a shop) to identify and defeat identity theft. Their proposed scheme relies on a pre-defined set of locations which are compared against the actual location of the mobile device. A continuous device tracking is required to recognize irregular actions or possible attacks, which is very difficult to maintain, as mobile devices can be switched off or out of monitoring range and can lead to privacy concerns by the continuously tracked client.

Saroiu and Wolman introduced the concept of location proofs [11], which are generated for example by trusted Wi-Fi access points or cellular operator. A location proof is requested and stored by the mobile device user and attached to the communication messages once needed. As the demand of a location proof and the storage is completely managed by the user, privacy concerns are reduced to a minimum. However, as the proof is available to the user, an attacker could try to forge it. In [12], Luo and Hengartner outlined an architecture to prove the mobile device location without affecting the users privacy. They proposed to use a group signature scheme and cryptographic hashes to ensure the validity of a location proof generated by a proof issuer.

Cellular network operators can locate mobile devices through signal triangulation from serving and neighbouring basestations/towers during their normal operation by measuring signals, which are constantly exchanged between mobile devices and basestations. The accuracy of cellular tower based positioning varies, depending on the used technique [13] and the area of operation [14]. However, the overall accuracy of this positioning method increased enormously in the recent past, mainly driven by the United States E911 mandate [15].

3. PRIVACY PRESERVING LOCATION VERIFICATION

The close combination of biometric-based authentication of a user, the independent location verification of the involved mobile device as well as the guaranteed freshness of the transaction process based on the GPS time and the proposed challenge / response encryption scheme offers a strong authentication method for mCommerce applications. During enrolment stage, the genuine client registers his/her biometrics (e.g. fingerprint) with the CA. In the case, that the client wants to use more than one application supported by the CA, the client can enrol different and cancellable versions of his/her biometrics for each application. The multiple versions of the client biometrics will ensure that no linking between applications is possible and in the case that one biometric template is compromised, all others are still secure and the corresponding application protected. The correct biometric template is selected by the CA during authentication, based on the requested application certificate.

3.1 Biometric authentication and key generation

In this paper, fingerprint biometric is adopted for our implementation. Precisely, FingerCode approach proposed by Jain eta al in [16] has been selected due to the fact that Random Orthonormal Projection (ROP) [7, 8] requires fixed length feature vectors. FingerCode approach [16] relies on detecting the Region Of Interest (ROI) and tessellating it around the reference point, then a bank of Gabor filters are applied in eight directions to capture both local and global features of a fingerprint image as illustrated by Figure 1.

In this work, the ROI was divided into 64 sectors so the fixed length of FingerCode features is 64 x 8 (eight discs in eight direction) resulting in 512 features in total for each FingerCode. The 512-feature fingerprint template is then secured by subjecting it to a user-based ROP to produce cancellable version of the fingerprint templates. To evaluate the performance of FingerCode approach, this work trials use the publicly available FVC2002-DB2 fingerprint database [17], which consists of 100 different fingers with 8 impressions per finger. Only the first four impressions from each finger are used here, because extracting FingerCode features requires an accurate detection of the reference points. The first fingerprint image of each user is used as a template and the remaining three images are employed for testing. i.e. 100 images form a gallery set and 300 images form a probe set in total. Experimental results show that the achieved authentication accuracy in terms of the False Acceptance Rate (FAR) and False Rejection Rate (FRR) of the secure version of FingerCode approach (i.e. using ROP based cancellable fingerprint) is FAR=0% and FRR=16%. Note that it is feasible to achieve perfect matching or 100% accuracy or a zero % Equal Error Rate (EER) when the ROP transformation keys are assumed to be secure. However, in this case fingerprint system suffers from a very high FAR when the ROP transformation key is compromised (see [18, 19] for further details on performance evaluation for such systems). To produce a biometric key, there is a need to deal with the fuzziness of biometric samples resulting from the differences between the freshly captured fingerprint sample and the enrolled templates. Therefore, and error correcting codes are used in the same way described in [20] to bridge the gap between the preciseness of cryptographic keys and the fuzziness of biometric samples.

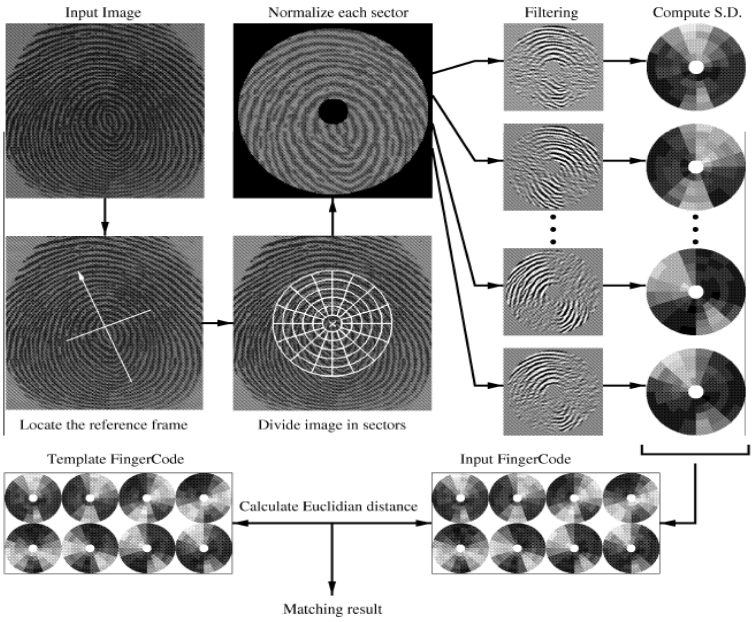

Figure 1: FingerCode-based fingerprint recognition as proposed in [16]

3.2 Biometric-based challenge / response location verification

By the time a client wants to use one of his registered applications, a message over a secure channel (e.g. by using SSL) to the CA is released as shown in Figure 2, which contains the unique client identification number and the ID of the demanded application (1). The CA generates on reception of the message a random challenge N (2) and sends it back to the client (3). Then, a process on the mobile device is triggered which takes the fresh client biometrics (e.g. fingerprint) and calculates the biometric based key K_B (4). This key is XORed with the received random challenge N (5) to produce a one-time biometric-challenge based encryption key NK_B. Concurrently, the actual device location (longitude and latitude value in decimal fraction notation) and time is gathered from the GGA (Global Positioning System Fix Data) [21] messages received by the GPS receiver on the mobile device every second. The location L_{MD} is then encrypted using NK_B (6) and sent together with the current time T_{MD} to the CA (7). The CA calculates NK'_B with the knowledge of the random challenge N and the stored biometric key of the client and decrypts the received message to extract the claimed mobile device location L_{MD} and time T_{MD} (8). The CA now can verify that the received time is up-to-date and requests the mobile device location at exactly that instant in time from the cellular network operators (9). The current mobile device location L'_{MD} is obtained from the cellular network operator by basestation/cell tower triangulation and send back to the CA. In a final step, the CA verifies that the claimed location of the mobile device and the location received from the network operators are within a certain threshold (10). If this is the case, the client request is authenticated as genuine and a certificate to allow the client to access the third-party application is issued by the CA.

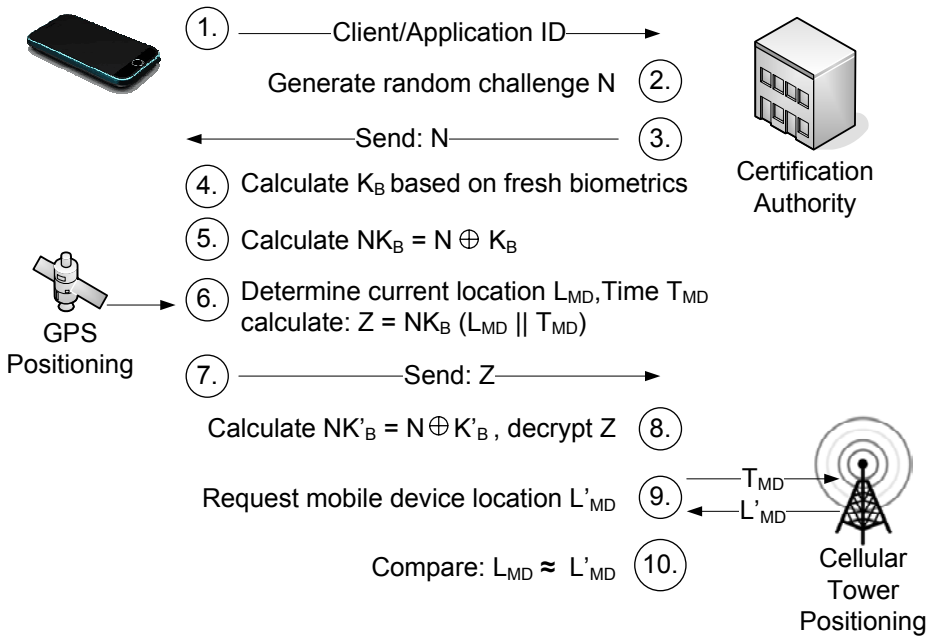

Figure 2. Biometric-based challenge / response process

3.3 Privacy preserving location verification

To reveal the mobile device location and hence the real physical location of the mobile device client to the CA, as described in the biometric-based challenge / response location verification scheme above, is critical from a clients privacy point of view. The CA could use the received location information to track the client's behaviour or to build a precise profile of an individual's movement. The proposed privacy preserving location verification scheme addresses this problem and enables the CA to verify the distance between the claimed location and the location determined by the network operators without actually knowing the real physical location of the mobile device user.

To achieve this, a dynamic secret is defined between the mobile device and the network operator. This secret is only known to these two parties and used to transfer the real physical locations into a different, secure domain. It is important to mention, that the transformation will preserve the distance between the two original locations, but will not reveal any information about their real positions on earth.

During authentication, the mobile device determines his current location L_{MD} and time T_{MD} using the GPS receiver as stated in Section 3.2. But in contrast to the previous scheme, the location is not directly encrypted by NK_B. Instead, the longitude and latitude geographic coordinates are transferred into a different, secure domain, in which the two values will be represented as binary strings, by the following steps (see Figure 3).

First, the distance between L_{MD} and the point on the equator with the same latitude value as well as between L_{MD} and the point on the prime meridian with the same longitude value is calculated (2) by the use of the Haversine formula [22] (see Formula 1). Both resultant distances are then divided by a pre-defined location binarisation resolution of 100 meters to calculate the number of bits ($Dist_{Bits}$) to represent the distance in binary format (3). The value of 100 meter is based on the F-C-C 911 regulation [15], which requires an accuracy of network-based solutions of 100 meter in 67 percent of the time and 300 meter in 95 percent of the time. Now, a binary location string L_{Bin} is generated, containing $Dist_{Bits}$ "1"s and ($Max_{Bits} - Dist_{Bits}$) "0"s to represent longitude and latitude value of the original location respectively and shuffled by T_{MD} to distribute the zeros and ones (4). The time T_{MD} is later send as part of the mobile device location request to the network operator, who will perform the same shuffling on the tower triangulation based location. Finally, the calculated binary representation L_{Bin} is XORed with a hashed value of the current serving cell-ID (5). The hash function is used to cipher the Cell-ID and to adjust the number of bits according to the binary location string. The cell-ID operates in the process as the dynamic changing secret shared only between the mobile device and the network operator and is

independently available on both sides. This independent retrieval characteristic of the cell-ID makes an exchange mechanism unnecessary which simplifies and strengthens the proposed scheme. The resultant binary string L_{MDBin} is encrypted by NK_B (6) as described in Section 3.2 and send to the CA. During authentication, the network operator will process the triangulation-based mobile device location in the same way and send the result to the CA, which will compare it with the binary strings to calculate the distance. If the distance is within the acceptable threshold, the certificate is issued to the client otherwise the request is denied.

$$
\begin{aligned}
&R = 6371 \\
&\Delta lat = lat_2 - lat_1 \\
&\Delta long = long_2 - long_1 \\
&a = \sin^2\left(\frac{\Delta lat}{2}\right) + \cos(lat_1) * \cos(lat_2) * \sin^2\left(\frac{\Delta long}{2}\right) \\
&c = 2 * a \tan 2\left(\sqrt{a}, \sqrt{(1-a)}\right) \\
&d = R * c
\end{aligned}
$$

Formula 1. Haversine

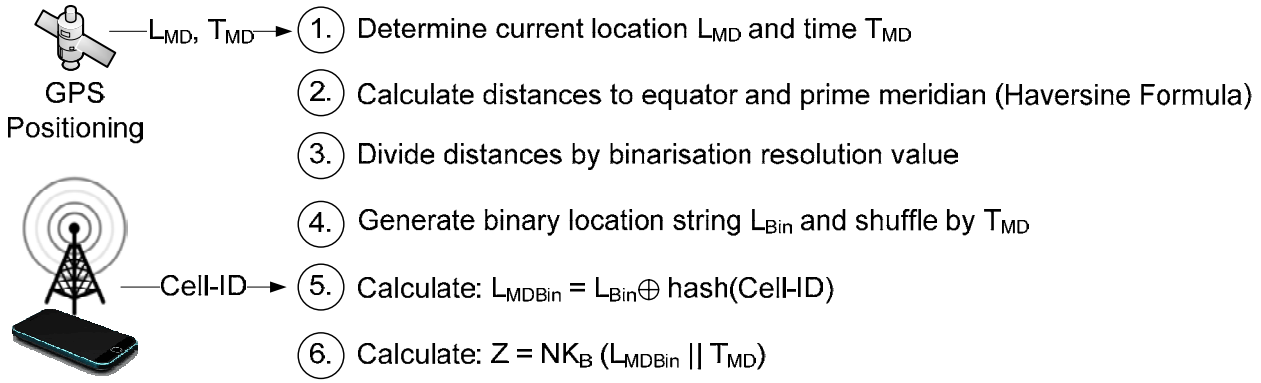

Figure 3. Privacy preserving verification process

4. CONCLUSION AND FUTURE WORK

This paper proposes to use two independent localisation sources to verify the claimed location of a mobile device, e.g. GPS receiver on the mobile device and tower positioning performed by cellular network operators. This two-way location verification tightly coupled with biometric authentication and a biometric-key based challenge / response encryption scheme shall guarantee the freshness and real-time of the authentication process and shall enhance the security of mCommerce applications. A certification authority will control the authentication process, hold securely the biometric data of the client and perform the required communication with the network operators.

To protect the privacy of the client towards the certification authority, the transmitted real location is transferred into a different, secure domain based on a dynamic shared secret between the mobile device and the cellular network operator.

To verify the practicality and to test the proposed algorithms, numerous trials and measurements of GPS-based locations on the mobile device and simultaneously obtained location information from the cellular network have been recorded. Evaluation of the collected data shows a difference of 100 to 300 meters between the two independently obtained positions, which complies with previous measurements in the U.K. [14] and the U.S. FCC 9-1-1 requirements.

Research work on this project is ongoing and future schemes will integrate additional factors (e.g. multi-biometrics and user password) to further strengthen the authentication process.

REFERENCES

[1] J. S. . Research, "Research, "2010 Identity Fraud Survey Report: Consumer Version",," February 2010.

[2] T. Kuseler, I. Lami, S. Jassim, and H. Sellahewa, "ebiometrics: an enhanced multi-biometrics authentication technique for real-time remote applications on mobile devices," in *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, ser. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, S. S. Agaian and S. A. Jassim, Eds., vol. 7708. SPIE, apr 2010, pp. 77080E.1–77080E.9.

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

[4] J. Brainard, A. Juels, R. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: somebody you know," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 168–178.

[5] K. Nandakumar, "Multibiometric systems: fusion strategies and template security," Ph.D. dissertation, East Lansing, MI, USA, 2008, adviser-Jain, Anil K.

[6] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing. Special Issue on Biometrics*, vol. 2008, pp. 1–17, 2008.

[7] H. Al-Assam, H. Sellahewa, and S. Jassim, "A lightweight approach for biometric template protection," in *Proceedings of SPIE*, vol. 7351, March 2009, pp. 73510P.1–73510P.12.

[8] S. A. Jassim, H. Al-Assam, and H. Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques," in *Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis (ISPA)*, 2009, pp. 556 – 561.

[9] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*. IEEE, 2009, pp. 641–644.

[10] P. C. van Oorschot and S. G. Stubblebine, "Countering identity theft through digital uniqueness, location cross-checking, and funneling," in *Financial Cryptography*, ser. Lecture Notes in Computer Science, A. S. Patrick and M. Yung, Eds., vol. 3570. Springer, 2005, pp. 31–43.

[11] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*. ACM, 2009, p. 3.

[12] W. Luo and U. Hengartner, "Proving your location without giving up your privacy," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*. ACM, 2010, pp. 7–12.

[13] J. Caffery and G. Stuber, "Overview of radiolocation in CDMA cellular systems," *Communications Magazine, IEEE*, vol. 36, no. 4, pp. 38–45, 1998.

[14] M. Mohr, C. Edwards, and B. McCarthy, "A study of lbs accuracy in the uk and a novel approach to inferring the positioning technology employed," *Comput. Commun.*, vol. 31, no. 6, pp. 1148–1159, 2008.

[15] U.S. Federal Communications Commission, 9-1-1 Service. [Online]. Available: http://www.fcc.gov/pshs/-services/911-services/

[16] A. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *Image Processing, IEEE Transactions on*, vol. 9, no. 5, pp. 846–859, 2000.

[17] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer-Verlag New York Inc, 2009.

[18] H. Al-Assam, H. Sellahewa, and S. A. Jassim, "Multi-factor biometrics for authentication: A false sense of security," in *Proceedings of the 12th ACM Workshop on Multimedia and Security*, 2010, pp. 81–88.

[19] H. Al-Assam, H. Sellahewa, and S. Jassim, "On security of multi-factor biometric authentication," in *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*. IEEE, 2010, pp. 1–6.

[20] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, pp. 1081–1088, 2006.

[21] *NMEA 0183 - Standard for interfacing marine electronic devices, Version 4.00*, National Marine Electronics Association Std., 2008.

[22] R. Sinnott, "Virtues of the Haversine," *Sky and telescope*, vol. 68, p. 158, 1984.