

Security Challenges of Location-Aware Mobile Business *

Emin Islam Tatlı, Dirk Stegemann, Stefan Lucks
Department of Computer Science, University of Mannheim
{tatli,stegemann,lucks}@th.informatik.uni-mannheim.de

Abstract

In addition to mobility, the ability of context awareness and especially location awareness has greatly enhanced the opportunities of mobile businesses. Many different kinds of context-aware services ranging from “finding nearby restaurants” to “sending ambulances to people in emergency” have already taken their places in the business. Besides availability and quality of the service, the user acceptance and therefore the economic success of mobile business applications fundamentally depend on a robust and easy-to-use security architecture meeting the users’ needs for privacy, anonymity, confidential communication and secure payment schemes. Based on a generic framework that is able to execute arbitrary context-aware services, we analyse the security challenges in mobile business with special focus on location as a context property and provide directions towards possible solutions.

1. Introduction

With decreasing cost and increasing popularity of high-level mobile devices, mobile applications have already taken their places in today’s electronic business. In addition to mobility, the availability of low-cost auxiliary devices for location determination has introduced a new business area called *location-aware mobile business*. Locating kids [12] and people in emergency [4], locating moving objects (e.g. fleet management) [1], location-based chat and games [5], indoor and outdoor routing [3], locating nearby restaurants, cinemas and gas stations are examples of already implemented location-aware mobile business services.

While mobile business (m-business) and mobile commerce (m-commerce) are commonly used interchangeably

in the current literature, in this paper we define m-business as business transactions over mobile telecommunication networks that are executed via mobile devices like PDAs, mobile telephones, wireless-enabled laptops etc. By m-commerce, we denote the subset of m-business that involves commercial transactions, i.e. the exchange of material goods [31]. Selling books and CD’s over the Internet is a well-known example of m-commerce, whereas a service for locating a person having a heart attack and sending an ambulance to him would be considered as m-business rather than m-commerce.

The functional advantages of mobility and location-awareness lead to various challenges. The mobile environment is very heterogeneous. Different kinds of devices ranging from wireless enabled laptops to mobile phones offer different computational capabilities in terms of memory, CPU speed, battery lifetime, display size and support of input peripherals [31]. An application designed for a new generation PDA can therefore not be expected to run equally smoothly on a low-power mobile phone. Especially with low-end mobile devices, small displays cause usability problems, and very limited memory and CPU speed prevent advanced applications from running at all.

Since security issues directly affect the user-acceptance of m-business applications, they are among the most important challenges for m-business. However, for several reasons, providing security is very problematic and difficult:

- *Security is a difficult challenge in general:* Providing security is an engineering task. A “normal” engineer specifies the challenges and provides solutions. A security engineer, on the other hand, tries to win a game against a dynamically evolving malicious adversary. While the challenges that a normal engineer faces usually do not change unexpectedly, this is a quite normal and common situation for a security engineer.
- *There exists a trade-off between functionality and security:* System designers always face a trade-off between functionality and security. Since security is a

* The work described in this paper has been supported by the “Landesstiftung Baden-Württemberg” and the Ministry of Science, Research and Arts of the state of Baden-Württemberg.

non-functional aspect of a system and end users often intuitively prefer increased functionality over enhanced security, this leads to overlooked security challenges.

- *There are additional security challenges for mobile systems:* Limited capabilities of mobile devices prevent the deployment of common security solutions in the mobile domain. As an example, signing documents with digital signatures in order to ensure integrity in many cases requires much CPU power, and not all mobile devices are capable of completing this task. Similarly, limited I/O functionality prevents long passphrases and other advanced security-related user interaction. Another challenge comes from wireless communication. It is obviously much easier to eavesdrop data that is transmitted over the air than to intercept wired communication channels. Also, it is much more difficult to detect a wireless eavesdropper than to detect that someone has hooked into a wired connection. In addition, the mobile communication neighborhood changes steadily and there is no implicit authentication by “being connected to the cable”.
- *Support for security in standards is marginal and often broken:* Typically, standards for wireless and mobile communication only provide support for basic security features, such as confidential and authentic communication between a mobile device and the next base station or access point. Advanced security features thus have to be implemented at the application level. However, even those basic security features actually supported by standards often are broken by design. A well-known example is “Wired Equivalent Privacy” (WEP) from the IEEE 802.11 standard [33]. (The worst flaws of WEP are fixed now by “WiFi Protected Access” (WPA) and by IEEE 802.11i, finally approved in July, 2004.) Other old and well-known examples are due to the GSM mobile standard: The one-sided authentication protocol (only the mobile device authenticates itself to the base station, but the base station does not authenticate itself to the mobile device), and the insecurity of the GSM A5 stream cipher [35].
- *A new privacy challenge is how to control location information:* This challenge stems from unauthorized disclosure of location information. The owner of a device should be able to explicitly control the transmission of his location. If his location somehow becomes available to malicious adversaries, privacy issues—possibly as severe as danger of life—may arise.

This article is organized as follows: In Section 2, we explain the principals and their functions in the m-business framework that we base our analysis on. Section 3 discusses the security challenges and possible solutions from the per-

spectives of each principal in the framework. Section 4 explains our future work and research focus. Some existing location-aware mobile systems and their security aspects are described in Section 5, and finally Section 6 concludes the paper.

2. The M-business Framework

In the near future, more advanced mobile devices will become part of our daily lives, many more location-aware services will be implemented, and many more mobile transactions will be executed.

In order to generalize from particular applications, devices and protocols, we analyze the security challenges in m-business within the generic framework proposed by the m-business research group at the University of Mannheim [6].

This framework consists of three main principals: *mobile users*, *service providers* and a *broker*. Mobile users with mobile devices are interested in receiving m-business services. A service provider offers chargeable and/or free services and registers them with the broker. The broker maintains a repository of available services and provides mobile users with context-aware “yellow pages”, i.e. it takes requests from mobile users and returns the service descriptions from the repository that are most suitable for the user according to her preferences and her context.

A user’s context includes information like health, mood, schedule, level of mobility (e.g. scooter, bike, car) and location [30]. In this paper, we focus on the location as the main contextual property of a user.

For data transmission, the framework utilizes the services of infrastructure providers such as telecommunication providers.

As Figure 1 illustrates, the application logic of the framework works as follows:

1. Service providers apply to the broker in order to register their services within the repository of the broker. In case the broker approves this application, the broker and the service provider sign a contract, and the service becomes available for mobile users.
2. Mobile users choose a service category (e.g. restaurants) through the interface of the applications running on their mobile devices and query the broker for available services in this particular category. If the user is interested in location-based services, he sends his location information to the broker along with his request. The user also sends his profile, which represents his preferences and special interests.
3. Based on the profile, the broker determines the relevant services within its repository and sends back the corresponding service descriptions. A service description

typically includes information about price, provider location and quality description.

4. Upon getting the service descriptions, the user decides on a service and applies to the provider of this particular service.
5. The service provider charges the user (if required), and presents the service.

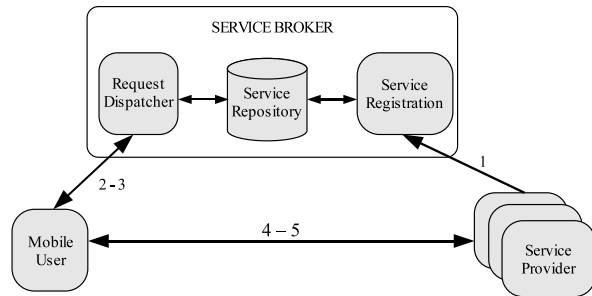


Figure 1. Application Logic of the M-business Framework

2.1. Use Case Examples

The services supported by the described architecture are not limited to classical location-based services like *finding the nearest gas stations*, but also include the following:

1. *Buying products from billboards*: A user wants to buy a product which he sees on a billboard. He chooses the “billboard” service category, and receives, based on his location, a list of the products shown on the nearest billboards along with directions to the nearest retailers providing the products.
2. *Buying theater/cinema tickets*: A user chooses the “theater/cinema” category in order to discover current programs, their prices and available tickets. He can then book a ticket for a particular theater/cinema.
3. *Timetables for bus/tram/train*: Upon request, a list of nearby stations is retrieved and sent to the user. He can then get departure and arrival times of public transportation vehicles stopping at these stations.
4. *Location-based notes*: A user prepares a to-do list for a specific shop. When he walks by this shop, his PDA rings and reminds him of the to-do list.
5. *Indoor navigation in fairs*: A user receives a list of all exhibitors of a fair. He chooses one exhibitor, and a

#	Security Challenge	U	B	SP
1	Anonymity	+	-	-
2	Unlinkability of pseudonyms	+	-	-
3	Privacy of personal data	+	-	-
4	Location-based spamming	+	+	+
5	Integrity and authenticity of service descriptions and results	+	+	+
6	Authentication and authorization	+	+	+
7	Confidentiality of the communication	+	+	+
8	Confidentiality of locally stored data	+	-	-
9	Usability vs. security	+	-	-
10	Secure mobile payment and fair exchange	+	+	+
11	Rogue access points and forged GPS-signals	+	-	-

Table 1. List of Security Challenges (U:User, B:Broker, SP:Service Provider, +:challenge, -:no challenge)

map showing the way to the selected exhibitor navigates the user.

6. *Mobile dating*: The user enters relevant personal information (e.g. age, gender, interests) of the partner he/she is looking for. A list of close-by people matching the given profile is displayed to the user. He/she chooses one of the matches and if the partner accepts, they start chatting.

3. Security Challenges and Possible Solutions

In this section, we analyze the security challenges in the mobile business framework described above. The analysis is done from the perspectives of each framework principal, i.e. mobile users, the broker and service providers. As Table 1 shows, some challenges are common for each principal, whereas others are relevant only for a particular principal.

Assuming the infrastructure providers to be untrusted by all main principals, we enforce end-to-end security between the principals in the framework and do not consider infrastructure providers in further detail.

3.1. Anonymity

Anonymity ensures that a user may use a resource or service without disclosing his real-world identity [15]. Similarly to non-electronic business, most users do not like to unnecessarily reveal their identity when requesting an m-business service. For example, a celebrity may not want others to know which film in which cinema he watches, but also

less famous people may not want others to learn what kind of books they buy and read.

On the other hand, service providers can generally perform transactions with different clients in parallel and therefore have to be able to uniquely identify them for technical reasons. A (partial) solution to this dilemma is pseudonymity. Pseudonyms are faked names like nicknames. When communicating with service providers, users introduce themselves with their pseudonyms instead of their real identities. They can use even different pseudonyms for the same providers. Provided that no two clients are using the same pseudonym simultaneously, service providers can thus uniquely identify clients without knowing their real-world identities.

3.2. Unlinkability of Pseudonyms

Even if a client uses pseudonyms for receiving services, each provider is likely to obtain some partial information about the client, e.g. her location at the time she requested the service, her name, or the company she works for. Based on the gathered information, a provider may not be able to determine the user's identity on his own, but collaborating service providers who are able to link the pseudonyms could eventually deduce her identity from the data they collected. We note that linkability does not *necessarily* eliminate anonymity [22], but cooperating service providers may at least be able to perform user-profiling.

If, on the other hand, service providers have no way of determining for any two individually anonymous transactions whether they were caused by the same user (unlinkability [15]), profiling is impossible and anonymity is guaranteed.

It is therefore reasonable to require unlinkability in the m-business framework. However, commonly deployed Mix-net [20] based protocols are impractical for the m-business framework since they require senders to encrypt their messages and extra payload with the public key of each Mix in the Mix-net. Symmetric key encryption can also be enforced for building a Mix-net protocol, but public key encryption is still initially required to distribute the secret keys between mobile clients and each "Mix". In general, mobile devices with limited capabilities can hardly put up with such complicated cryptographic operations.

Analyzing and enhancing existing protocols which focus on mobile unlinkability and anonymity is therefore an important area of future research.

3.3. Privacy of Personal Data

Regardless of whether unlinkability and therefore anonymity can be guaranteed in the framework, users are

generally concerned about revealing personal data [21], even if service providers are practically unable to reconstruct their identities from the information they receive. Besides conventional attributes like name, address, phone and credit card number, special interests etc., this is especially the case for context information such as the user's location at a specific point in time, which, on the other hand, is an essential input for any location-based service; a mobile dating service, for example, is pointless if the clients are not willing to disclose their location and part of their personal data.

In order to enforce privacy, i.e. to let the user retain control over his personal secrets [17], Jendricke et al. present an identity manager to control personal data sent from mobile devices through networks [25]. An identity manager provides an interface with which one creates different virtual identifications (IDs), i.e. pseudonyms, and binds a subset of his personal data to each ID. When communicating with a service provider, the user chooses an ID that is suitable for this particular type of communication. Before any personal data is sent to a service provider, the user is explicitly asked to allow the transmission.

In most cases, identity managers can ensure that each provider gets just as much personal information as needed for executing the service, but how can service providers be prevented from abusing the legally collected information?

Obviously, on the technical level, the framework cannot control the further usage of information, once it has been transmitted to service providers. Abuse of gathered personal information for profiling etc. has to be prohibited on the business level, e.g. by establishing a Privacy Management Code of Practice that is obligatory for all service providers registering with the broker [32]. Providers violating this code will be banned from the service repository and not be able to further advertise their services through the broker. Legally proving a code-violation is supposedly difficult, but the framework could enforce the pressure on malicious service providers by keeping log-files of transaction data, by collecting and managing abuse complaints and by operating complaint-dedicated communication channels between clients and service providers.

3.4. Location-based Spamming

Spams are unsolicited messages, mostly in the form of commercial advertisements. Meanwhile, the productivity of many companies is more and more affected by an increasing number of spam e-mails since employees need to spend a considerable amount of time separating wanted messages from unwanted advertisements.

Although many Internet users feel annoyed by spam e-mails, graphical user interfaces on modern PCs are able to

give an easy overview of the e-mail inbox, and deleting a single message usually only takes a mouse click.

In a mobile environment, however, small display sizes force the user's attention onto each message, and the restricted user interface requires more user interaction during browsing and deleting. Since mobile phones and handhelds are trusted devices for many people, receiving unwanted messages on these devices is perceived as a massive privacy violation [32, 23].

In order to prevent anonymous spamming from unauthenticated sources, sender authentication can be established. But even authenticated service providers that are legal members of the service repository could betray the user's trust, send unwanted messages along with requested services and abuse personal data in order to perform personalized and location-based spamming. A shoe-store could for example send advertisements to its customers when they pass by the shop.

One way to prevent this type of spamming would be to allow only pull-services, i.e. any communication between clients and service providers has to be initiated by the client. However, there exist many presumably valuable push-services, such as location-based notes or mobile dating services, that would be excluded from the framework by this approach.

In addition to the methods discussed in the previous subsection, the broker should rather support black or white listing of particular service providers. Clients can submit black lists and white lists to the broker, which then executes the lists on the user's behalf by never recommending services providers on the user's black list and assuming those on her white list to be trusted.

3.5. Integrity and Authenticity of Service Descriptions and Results

Integrity protects against unauthorized modification of information [29]. The integrity of the service descriptions stored and transmitted by the broker are obviously very critical for users and service providers because they affect choices of users when they decide on a service to request. Service descriptions from an authentic broker that are modified by adversaries or from a forged broker embarrass users and danger businesses of service providers. Adversaries are especially interested in modifying information about price, location and quality in descriptions.

To forge service descriptions, attackers can follow different methods. They can alter service descriptions of the authentic broker. This modification can be done when service descriptions are either on the communication channel or in the repository of the broker. Another method is that a forged broker pretends to be an authentic broker and sends forged service descriptions to mobile users. Thus, authen-

ticity of messages can also be forged. Modified service descriptions can result in many troubles. Users can be charged more money than the required cost or pushed to get a bad service, for example. Even worse, users can be directed to a faked service provider whose aim is only profiling their personal data and stealing their credit card numbers. Like forged service descriptions, service results which are sent by service providers to mobile clients as replies to service requests can be forged on communication channels.

Digital signatures can be applied as cryptographic methods for both integrity and authenticity which require checking for unauthorized modification of messages and verification of the origins of service descriptions and results, respectively. To enforce a digital signature scheme, the broker and service providers should hold a public and private key pair. The broker should sign its service descriptions with its private key and then distribute them. Service providers should apply the same method for their service results. Users should check the integrity of service descriptions and results with the public key of the broker and service providers, respectively. Digital signature solutions usually require a certificate management system to exist in the framework.

On the other hand, limited memory and CPU powers of mobile devices are big challenges when verifying signatures of messages. The verification algorithm running on mobile devices should therefore be well optimized.

In addition to the protection of unauthorized modification of messages on the channel, data stored in the repository of a broker should obviously be authentic. Service providers as possible adversaries can aim to surpass that of their competitor service providers by modifying the repository in such a way that their service descriptions become more appealing to users.

The solution to repository integrity is enforcing of authentication, authorization and intrusion detection mechanisms. Authentication enables only authenticated principals to access the repository. Authorization provides that authenticated principals can work only with the data that they are allowed to access. Intrusion detection tools like Tripwire [13] can check and audit modifications in the repository and notify administrators of altered data.

3.6. Authentication and Authorization

After the registration process, service providers can apply to the broker to update their service descriptions. To prevent unsanctioned modification of the repository, the broker should authenticate and authorize the service providers. Authenticated service providers are then allowed to modify only entries that they own. Service providers can also require to authenticate brokers against forged brokers and therefore bi-directional authentication is enforced.

Users will want to authenticate service providers in order to protect their personal data from malicious adversaries that pretend to be service providers. Conversely, many service providers need to authenticate their clients, e.g. for accounting purposes.

Authentication can be enforced by three different methods: something you know (e.g. passwords), something you have (e.g. smart cards) or something you are (e.g. fingerprints). Since all three methods by themselves would provide only weak authentication, a combination of two methods (*two-factor authentication*) is commonly used. As an example, token-based authentication requires a combination of the methods *what you have* and *what you know*. In token-based systems, the user holds a tamper-proof card that periodically generates a new random token. The same token stream is also generated on the remote server. The server authenticates the user if and only if he is able to present the currently valid token and a PIN [10].

Two-factor authentication is desirable from a security point of view, but requires additional infrastructure and in many cases limits usability and scalability of the system as the authenticated entity has to provide at least two pieces of information in each authentication process. A quite natural solution is therefore to combine two-factor authentication and single sign-on mechanisms in order to ensure the usability of the system. With single sign-on, the identity is initially proved to the single sign-on service, and subsequent authentications are performed against the sign-on service instead of the authenticated entity itself. Both for authenticating users and service providers, a single sign-on service could be integrated into the broker.

Another important aspect regarding authentication is that anonymity should not be eliminated by authentication if users wish to stay anonymous while being authenticated. That means it should be possible for the user to show her authenticity by proving a certain fact about herself, e.g. being a legal subscriber of a service, without revealing her identity to the service provider. Conventional techniques such as transmitting passwords or biometric information or identifying the user's smart card do not protect her anonymity. But cryptographic techniques based on cryptographic credentials and zero-knowledge proofs of knowledge [24] allow to solve this problem: The authenticator *can verify* that the user actually is a legal subscriber, but he *cannot learn anything else* about the user's identity.

For authorization, existing solutions like access control lists, certificate-based authorization (e.g. SPKI [11]) which binds access rights to public keys, role-based authorization etc. are within our concern. In order to keep the security architecture open, the architecture should not be restricted to only a specific set of solutions, rather all solutions required by different services should be provided.

3.7. Confidentiality of the Communication

Communication messages transmitted among the framework principals contain sensitive information like personal data, credit card numbers, location, queries of mobile users, registration data of providers, results from broker and service providers etc. As mentioned in the previous sections, an identity manager enables users to control the personal data transmitted. But the disclosure of these sensitive information would not be difficult in mobile networks where data is transmitted over air and easily received by any mobile device. To prevent the unauthorized disclosure of data in messages (confidentiality), encrypted message transmission in which only authorized parties are able to decrypt and read messages is required.

Many telecommunication technologies provide encryption mechanisms between sender and network bearer. But since we do not trust the infrastructure providers, we need to enforce end-to-end security which enables confidential message transmission between the principals (users-broker, users-providers, broker-providers). For end-to-end security, an SSL-based protocol can be implemented. Authentication of broker and service providers, on-the-fly generation of session keys and its wide deployment in the public domain are the main advantages of SSL. In the protocol, messages are encrypted with a symmetric key, but public key encryption is used for the session key exchange. Hence, SSL requires also a certificate management system.

The process of creating session keys is called *handshake* in the SSL protocol. Especially in the mobile domain, the handshake process causes actually a very long time delay. We therefore need to implement an SSL-like protocol that decreases the time delays in the handshake phase to a reasonable delay.

Communication protocols often require additional data to be associated with encrypted payload messages, e.g. for routing purposes. This data needs to be publicly readable and therefore must not be encrypted, but its authenticity should be established in the same way as for the payload message. In this context, authenticated-encryption with associated-data (AEAD) schemes [28] could significantly speed up the communication compared to conventional methods, especially on low-capability mobile devices.

3.8. Confidentiality of Locally Stored Data

In the mobile domain, where thefts of devices are very common [16], confidentiality is especially required for protecting data stored locally on mobile devices. Local data is sensitive, because it contains private information like name, address, special interests and possibly even credit card numbers. To prevent thieves and other unauthorized users from

reading the data, the mobile device needs to authenticate the user trying to access it. This can be done by two-factor authentication (see Section 3.6), e.g. by fingerprint authentication in combination with a PIN. Even if thieves figure out the PIN by brute-forcing, they will not be able to circumvent the fingerprint authentication, and the device will not allow access to the data.

However, in many cases, it is possible to get around the access control of the operating system by simply removing memory cards from the device and plugging them into another system. Therefore, sensitive data should always be stored encrypted, preferably by password-based symmetric encryption, in which passwords are used to generate keys for the encryption and decryption operations.

Alternatively, public key encryption can be used. The mobile user encrypts his local data with his public key. The corresponding private key is stored by a remote system and can only be retrieved after authentication by a password.

3.9. Usability vs. Security

It is a widely known fact that users when faced with trading-off usability and security mostly prefer usability. As an example, consider password-based authentication of service subscribers. To ensure the security of the authentication, passwords must not be easily guessable, i.e. they should not be chosen from dictionaries nor should they be names or birth dates. Instead, passwords should contain capital letters, numbers and even non-ASCII characters. Strong passwords increase security but they are not easy to keep in mind and thus decrease usability. In spite of feeling uncomfortable about it, many people nevertheless use weak passwords.

Another trade-off example is digital certificates. When the lifetime of a certificate is over, it does no longer guarantee the authenticity and validity of its content. When a mobile device receives an invalid certificate from a service provider or the broker, it should warn the user in a suitable manner. Users, on the other hand, have different sensitivity for security. While invalid certificate warnings are annoying and therefore usability-decreasing for some users, others may find such warnings inevitable.

As both examples show, the m-business framework should allow users to balance usability and security according to their personal needs and not enforce fixed security policies.

A dynamically configurable security policy management system is a possible solution. Such a security policy management system can consist of the following components and mechanisms:

1. *Password Manager*: A password manager creates strong passwords for different services, encrypts and stores them on a local storage medium.

Users then do not need to worry about remembering all strong passwords or using weak passwords. They only have to keep in mind a master password for the authentication by the password manager and to retrieve passwords at any time.

2. *Single-Sign-On (SSO) Mechanism*: With the help of SSO, as discussed in Section 3.6, not all service providers need to authenticate a particular user. Instead, a central authentication server performs this task on behalf of the service providers.
3. *Security Level Manager*: The security level manager presents different security levels (e.g. high, medium, low), and each level is bound to a set of security policy options. Users can easily and dynamically switch from one security level to another and also enable or disable any policy option individually for each level.
4. *Identity Manager*: An identity manager, as explained in Section 3.3, provides full control over the disclosure of personal data in each transaction and therefore increases usability as well as security. Since location information is generally considered very sensitive, the client could trade-off security and quality of the returned service by adjusting the accuracy of the location information that is transmitted to the service provider, e.g. instead of transmitting exact GPS-coordinates, the mobile client could send only the district or even only the city that he is currently located in.

3.10. Secure Mobile Payment and Fair Exchange

Mobile payments involve transactions in which monetary values are transferred from mobile clients to service providers in order to pay for services offered. Suitable monetary values for mobile payments are digital coins which can be stored on either the mobile device itself or smart card devices (e.g. Geldkarte). Alternatively, monetary values stored on a remote trusted party (e.g. a credit card or an account in a bank) can also be used for payments.

Credit card numbers and other payment media can be stolen during message transmissions of payment protocol and misused by adversaries. Misuses can sadden both users and service providers. It saddens users, because their credit cards are used on behalf of them. It also saddens service providers, because in case the users prove that they were charged due to misuse of their credit cards, the money is taken back from the providers. Hence, the mobile payment protocol (or protocols) that would be deployed in the m-business framework should consider strong encryption methods to provide confidentiality of monetary values transmitted over unreliable networks.

Mobile users expect service providers to play fair when they exchange service and monetary values. Otherwise, they

may complain about an unfair exchange and argue that they were charged more money than the expected value, more than once, although they did not get a service, although they got a wrong service, although they did not request any service or although they are unhappy with the quality of the received service.

Similarly, service providers also expect mobile users to play fair when they exchange services and monetary values. Service providers can also have different arguments to claim against users, e.g., that they are not paid although they presented a service, they are not paid in time, or they are paid less than the agreed amount.

In payment schemes, if any dispute comes up between client and merchant, they need a trusted third party to solve the dispute. In the m-business framework, the broker can take the role of such a trusted party.

In order to provide evidence in cases of dispute, the payment protocols of the m-business framework should be able to account all actions of both parties.

The payment protocol should provide anonymous payment (in case possible), accountability (*non-repudiation*) of both users and service providers as well as mechanisms verifying authenticity and integrity of protocol messages.

There exist many mobile payment protocols based on monetary value types and methods to pay [26]. The m-business framework requires a flexible payment architecture that supports different payment protocols with different monetary values to pay. Analyzing existing mobile payment protocols and designing such an architecture is an important field of future research.

3.11. Rogue Access Points and forged GPS-signals

Mobile devices can discover their current geographical positions with the help of a special hardware device. Computing the location can be categorized into outdoor and indoor computing according to the underlying communication infrastructure. Outdoor computing most often relies on the availability of satellite-based positioning systems like GPS (Global Positioning System) [2]. In indoor areas, existing wireless network infrastructure like WLAN enables a cheaper and more accurate computation of the location [27]. They can help mobile devices to determine their location relatively to the location of access points in indoor areas.

Access points that are illegally attached to WLAN networks are called rogue access points. If a rogue access point is attached to the m-business framework, mobile devices may fail location determination, or sensitive user data would be transmitted over rogue access points, which is dangerous in terms of privacy.

To prevent illegal attachments of access points, infrastructure providers should make regular checks in order to

determine rogue access points. Common detection techniques are based on only wireless (e.g. sniffers for packet analyzing, enterprise-wide scan from a central location), only wired (e.g. MAC address filtering) and hybrid approaches [19].

As well as access points, GPS-satellites can be forged by ground stations transmitting GPS-signals in order to disturb the location determination of the clients. Since authentication of civilian GPS-messages is not yet available [34] and will only be included in next-generation location determination systems like GPS III and Galileo, particularly critical applications should not trust the location information provided by GPS.

4. Next Step and Research Focus

We have so far specified the security requirements and possible solutions in the m-business framework. The next step is to design an open security architecture which can easily be integrated within the described m-business application framework and to implement its components. The security architecture should be flexible enough that one can easily adapt it for both mobile devices and high-end PCs and servers.

The security architecture should support an identity manager which manages pseudonyms and personal data. To handle issues arising from payments, m-Wallet (for mobile devices) and e-Wallet (for the broker and service providers) components should be implemented. A crypto provider which offers many cryptographic libraries for encryption, digital signatures, SSL-based protocol support, strong password generation etc. is also required. Other components in the architecture interact with the crypto provider to implement specific security functions. Spam managers, password managers, certificate managers and policy managers are additional components to be implemented.

Our research focus is therefore to build an open, scalable and flexible security architecture supporting many possible solutions to overcome the challenges that can arise in different location-aware mobile business applications. In addition, the architecture should be easily configurable on both mobile devices and high-level servers of the broker and service providers.

5. Related Work

There are several existing research projects on context-aware systems, but they are not specifically m-business oriented. Hence, their security focus is mostly restricted to privacy, confidentiality and anonymity.

The Nexus project [7] aims at modeling a spatial world for mobile context-aware applications. Unlike in the m-business framework, location information of mobile ob-

jects is stored by a central location service provider, and other objects and service providers can query location information of a particular object. Security-wise, Nexus focuses mostly on privacy problems. To control location information, a certificate-based access control system based on SPKI is enforced. To be able to query the location of an object, requesters must hold an authorization certificate which is issued and digitally signed by this particular object. Nexus uses virtual IDs for managing personal data. To handle the virtual IDs, the identity manager from [25] is suggested.

The WASP project [14], which aims at developing a context-aware service platform using web services, proposes a P3P-based (*Platform for Privacy Preferences*) [9] architecture to provide privacy. The P3P protocol enables web users to be aware of what kind of information is collected when they communicate with web servers. Users' web requests are managed by user agents that are mostly integrated within browsers. Upon getting requests, agents request web servers to send their P3P policy, more specifically, what kind information they intend to get from the user. Agents then compare the returned P3P policy and the user preferences, and if there is no conflict, agents send the relevant data to the servers, get responses and forward them to users. In the m-business framework, the P3P protocol as well as the identity manager solution should be supported to keep the security architecture open to web-oriented business applications.

The Nimbus project [8] provides a framework to support developers of location-based services. But from the security point of view, the focus is especially on network and communication security [18].

6. Conclusion

In this paper, we discussed security challenges of a location-aware mobile business framework. Mobile users, the broker and service providers are the main principals in the framework. Since their security concerns slightly differ, we analyzed the challenges from the perspective of each principal.

The analysis shows that privacy and confidentiality are not the only security issues in the framework. They are still inevitable, but challenges like anonymous and unlinkable services, usability with security, integrity of services, fair exchange, location-based spamming and network security also directly affect the user acceptance of the m-business framework.

Having specified the challenges and possible solutions, the next step is to design an open and flexible security architecture that can be integrated within the m-business application framework.

7. Acknowledgment

We would like to thank to Henning Pagnia for his valuable comments on the proposed security challenges and their solutions.

References

- [1] Fleet management.
URL: <http://www.fleetonline.ch>.
- [2] Global positioning system.
URL: <http://electronics.howstuffworks.com/gps.htm>.
- [3] Indoor & outdoor routing.
URL: <http://www.falk.de>.
- [4] Locating people in emergency.
URL: <http://www.sintrade.ch>.
- [5] Location-based chat and games.
URL: <http://www.vodafone.de>.
- [6] The mobile business research group.
URL: <http://www.m-business.uni-mannheim.de>.
- [7] The Nexus project.
URL: <http://www.nexus.uni-stuttgart.de/index.en.html>.
- [8] The Nimbus project.
URL: http://dreamteam.fernuni-hagen.de/nimbus/nimbus_eng.html.
- [9] P3P (platform for privacy preferences initiative).
URL: <http://www.w3.org/P3P/>.
- [10] RSA secureid cards for two-factor authentication.
http://www.rsasecurity.com/products/secureid/datasheets/SID_DS_0804_lowres.pdf.
- [11] Simple public key infrastructure.
URL: <http://www.ietf.org/html.charters/spki-charter.html>.
- [12] Tracking of kids.
URL: <http://www.trackyourkid.de>.
- [13] Tripwire.
URL: <http://www.tripwire.org>.
- [14] The WASP project.
URL: <http://www.freeband.nl/kennisimpuls/projecten/wasp/ENindex.html>.
- [15] ISO99 IS 15408.
URL: <http://www.commoncriteriaportal.org>, 1999.
- [16] Tough penalties for mobile phone theft. *BBC News*, 3. May 2002.
- [17] R. Anderson. *Security Engineering*. Wiley Computer Publishing, 2001.
- [18] Hagen Barlag and Stephan Drautz. Concept and implementation of security architecture (in german). Master's thesis, University of Hagen, October 2003.
- [19] Raheem Beyah, Shantanu Kangude, George Yu, Brian Strickland, and John Copeland. Rogue access point detection using temporal traffic characteristics. In *Proceedings of IEEE GLOBECOM*, December 2004.
- [20] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–90, 1981.

- [21] N. Diezmann. *Report Mobile Business - Neue Wege zum mobilen Kunden*, chapter Payment - Sicherheit und Zahlung per Handy, pages 155–178. 2001.
- [22] Andreas Pfitzmann et al. Anonymity, unobservability, and pseudonymity: A proposal for terminology, July 2000.
- [23] S. L. Jarvenpaa et al. Mobile commerce at crossroads. *Communications of the ACM*, 46(12):41–44, 2003.
- [24] Oded Goldreich. A tutorial about zero-knowledge. URL: <http://www.wisdom.weizmann.ac.il/~oded/zk-tut02.html>.
- [25] Uwe Jendricke and Daniela Gerd tom Markotten. Usability meets security - the identity-manager as your personal security assistant for the internet. In *Proceedings of the 16th Annual Computer Security Applications Conference*, pages 344–353, December 2000.
- [26] D. O’Mahony, M. Peirce, and H. Tewari. *Electronic Payment Systems for E-Commerce*, chapter Mobile Commerce, pages 308–316. Computer Security. Artech House Inc., 2nd edition, 2001.
- [27] P. Prasithsangaree, P. Krishnamurthy, and P. Chrysanthis. On indoor position location with wireless LANs, 2001.
- [28] Phillip Rogaway. Authenticated-encryption with associated-data. In *CCS ’02: Proceedings of the 9th ACM conference on Computer and communications security*, pages 98–107. ACM Press, 2002.
- [29] Deborah Russell and G.T. Gangemi Sr. *Computer Security Basics*. O’Reilly & Associates, Inc., 1992.
- [30] Bill Schilit, Norman Adams, and Roy Want. Context-aware computing applications. In *IEEE Workshop on Mobile Computing Systems and Applications*, pages 85–90, Santa Cruz, CA, US, December 1994.
- [31] S. Schwiderski-Grosche and H. Knospe. Secure mobile commerce. *Electronics Communications Engineering Journal: Special issue security for mobility*, 14(5):228–238, October 2002.
- [32] Sarah Spiekermann. *Location-based Services*, chapter General Aspects of Location-Based Services. Morgan Kaufmann, 2004.
- [33] Rüdiger Weis and Stefan Lucks. Standardmässige Wave-LAN Unsicherheit. *Datenschutz und Datensicherheit*, 25(11), 2001.
- [34] C. Wullems, O. Pozzobon, and K. Kubik. Trust your receiver? enhancing location security. 2004. <http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=128320>.
- [35] Erik Zenner, Rüdiger Weis, and Stefan Lucks. Sicherheit des GSM-Verschlüsselungsstandards A5. *Datenschutz und Datensicherheit*, 24(7), 2000.