PE-TLBS: Secure Location Based Services Environment with Emphasis on Direct Anonymous Attestation Protocol

Hanunah Othman[1], Habibah Hashim[1], Jamalul-lail Ab Manan[2]
Universiti Teknologi MARA[1], MIMOS BHD[2]
Malaysia

Abstract

Nowadays, an IT officer would normally use virtualization as a security mechanism to provide clandestine isolation environment and concurrently hope with optimism to secure the emerging of cloud computing. Indeed, virtualization offers some kind of computing defense from being attacked from the cloud infrastructure. Significantly, the proliferation of Location Based Services in mobile and wireless communication has also increased the need to address security, privacy and trust issues. Thus, this paper presents Privacy Enhanced-Trusted Location Based Services (PE-TLBS) framework which create more trusted and privacy preserving services on top of existing Mobile Location Protocol (MLP). The framework implements a simplified protocol based on Direct Anonymous Attestation (DAA) scheme supported by Trusted Platform Module (TPM) functionalities. A Trusted Group of users/clients is organized based on P2P communication concept and the trust-ability is measured by using RSA key pairs. A Privacy CA acts as an issuer organization which validates the embedded TPM before clients use an LBS service. TPM Emulator and TCG Software Stack simulate and make the accession to TPM much simpler while maintaining the functionality as well as providing Application Programming Interfaces (APIs). We have initiated a virtualized Proof of Concept (PoC) environment to validate the framework. We anticipate that the proposed framework would be able to mitigate threats, and strengthen customers' confidence on using LBSs.

1. Introduction

In a typical cloud environment, a cloud user is responsible for his/her application-level security while cloud provider is responsible for physical and virtual machine security. Malicious cloud provider may gain access to private user information which poses threats to security. A major concern is how to protect the cloud user from malicious cloud user or cloud provider. Furthermore, the increase of heterogeneity in mobile and wireless communications applications and services focusly in Location Based Services (LBS) environment has overridden security, privacy and trust (SPT) issues.

Currently, the mobile platform does not allow a local or remote user to attest their platform and has to rely on software-based security to protect these platforms. Moreover, software alone protection cannot assure its own integrity and can be easily affected by malicious codes. For this reason, trusted hardware is needed as the basis for software security mechanisms and to preserve privacy of user's information stored in trusted platform. Therefore, a trusted hardware known as Trusted Platform Module (TPM) adopted by Trusted Computing Group (TCG) technologies has been accepted worldwide as the foundation of trust for software processes within a system.

The major challenge in these systems is how to provide an unlinkable transaction in LBS and how to integrate TCG circuitry into a phone to make the technology work with the handset's software due to the limited memory, power and processing resources. Privacy Enhancing Technologies (PET) [1-3] is a set of computer tools, applications and mechanisms integrated in online services or applications which provide a trustworthy environment and allows users to protect the privacy of their personally identifiable information (PII). Consequently, by emerging the PETs and TCG technologies will result the privacy enhancement of user's identity profile and location information in mobile network services.

This paper has three main areas. In the first section, we discussed on security, privacy and trust (SPT) issues in the entire domain of mobile and wireless communications especially in Location Based Services environment. The second section emphasizes on implementing Direct Anonymous Attestation (DAA) protocol in LBS based on Trusted Platform Module (TPM) specifications and functionalities in such a way as to form unlinkable transaction and anonymously verifying the legitimacy of users. Thirdly, enhanced privacy mechanism is presented by forming virtualized secure framework called Privacy Enhanced –Trusted Location Based Services (PE-TLBS). The set up of several components and tools that must comply with TCG specifications are discussed.

We have initiated a virtualized Proof of Concept (PoC) environment to validate the framework. Virtualization Machines Monitor (VMMs) software was used to construct the secure framework virtualization. Three virtual machines are created to represent the mobile device, anonymizer and LBS

server. Anonymizer and LBS server are installed with Windows Vista SP 2 OS. For the mobile device which is the client, MS-DOS OS is installed to support Windows CE 6.0 R3 emulation. It is used because Windows CE 6.0 cannot be directly installed as an OS inside VMM since it does not run on x86 or x64 hardware. They will have their own dedicated TPM Emulator to make sure that PCRs are enough for remote attestation between the entities.

2. Security, Privacy and Trust

Security, privacy and trust issues have become paramount due to the tremendous growth in mobile communications network and mobile computing applications. Many cell phone operators' networks have offered Location Based Services to their customers. Thus, privacy threats in Location Based Services (LBS) [4-6] has become very hard to define because they could easily divulge mobile device anonymously (e.g. "nearest restaurant"), reveal any user's identity and location information to LBS server or other users (such as friend finder service) and disclose to individual (friend, other). The misuse of the user's personal data is one of the biggest concerns.

2.1. Mobile Communication Security

Mobile Communication Security has gained great attention recently mainly from the subscriber level to the network operator and service provider to protect both the physical devices and information they contain. Although all communications systems and mobile applications seems to have special requirements; many security issues with the wire-line networks such as public switch telephone and data networks; still need to be addressed. Integration of security features into wireless communication as well as security requirements in 2G and 3G systems must also be taken into account [7]. There are also limitations that may apply such as small packet size, low bandwidth, high transmission costs, limited processing and storage resources and real time constraints.

The most effective way to secure private data is not to store it on mobile devices. Traditionally, the use of *simple passwords* which are easily guessed might enforce length, complexity and timeout rules. *Strong passwords* that normally consist of six or more characters including numbers and special character are difficult to guess and *Non-text passwords* which decrypt other credentials stored on that handheld are used to allow the authenticated user access his/her company's network [8]. *Mobile authentication strategy* strives to combine strength and enforceability with usability. *Digital certificates* bind an identity to a public/private key pair and are considerably stronger than passwords, as long as the owner's private key is protected. *Smart card* used to unlock a device are security chips, embedded in a credit card, badge or MMC/SD memory to provide safe storage for cryptographic keys used by authentication and encryption algorithms.

As device capabilities became more diversified and included several wireless communication capabilities, software grew more complex, and the vulnerabilities of the corresponding software and hardware increased. Existing software security is vulnerable, not only in terms of access to the hardware of lost devices by other people but also to mobile malicious code. Thus, in order to develop an open security platform that can be used in all industrial fields and solves existing software security vulnerabilities via a hardware security module, Trusted Computing environment was organized by major IT corporations such as TCG (Trusted Computing Group) Intel, IBM, AMD, etc.,

The level of trust for a particular entity depends on the outcome of the authentication process. Ideally, user authentication should be carried out transparently, without disruption to whatever the user's task is at the moment. In current distributed systems [9], authentication is a necessary procedure for verifying an entity's identity and authority. Authentication protects the service provider from unauthorized intrusion. By mutual authentication, mobile station also authenticate with the base station. This is of great importance to prevent a malicious station from pretending to be a base station.

In practice most authentication protocols require the home authentication authority (or authentication server) to be contacted during the execution of the protocol.

2.2. Privacy issues in LBS

Currently, many operators of cell phone networks offer LBS to their customers. Since many operators outsource service provisioning to a third-party LBS provider and a person's location could reveal sensitive information about the person. It is imperative that the operator must comply with privacy preserving guidelines produced by the regulators, and that the service provider should process location information about the customers in a privacy-preserving way. Practically, LBSs is a mobile *Client - Server* based applications and services based on the location of mobile users that have emerged in services such as emergency services (e.g. E-911), on-line traffic jams, way-finding and friend-finding. Thus, the secured network protocol of LBS is required for *conveying location, mapping location to services* and *describing privacy requirements.*

Although privacy-preserving location based services was investigated for the three components involved in providing location-based services (i.e.

location-based service component, localization component, and communications component), nothing was mentioned about securing mobile platform and the necessary attestation required to built trusted network connection in LBS network. Most of the existing approaches primarily focused on the following directions [10]:

i. the use of access control policies that state explicitly how the subscriber's location information is treated,
ii. the use of cryptographic techniques which the communicated location information is ciphered to shield user's privacy,
iii. the use of obfuscation techniques to confuse an adversary regarding the real location of the user and
iv. the use of spatial or spatiotemporal cloaking to lower the resolution of the exact user location prior to submitting the request to the LBS provider.

Privacy in LBS can be achieved by providing anonymity or pseudonymity to the users. Users have to continuously report their locations to the database server to entertain the service. With untrustworthy LBS servers, it poses a major privacy threat on its users. To tackle this privacy threat, several centralized privacy-preserving frameworks were proposed for LBS, in which a third trusted party uses anonymizing middleware to blur user exact locations into cloaked spatial regions, such as k-anonymity, where a user is indistinguishable among other k-1 users. Due to the risk that an adversary can obtain unauthorized access to raw location data derived or computed location information [11, 12], Privacy Grid framework as mentioned in [13] supports anonymous location-based queries in mobile information delivery systems. It provides location P3P model, which allows mobile users to explicitly define their preferred location privacy requirements in terms of both location hiding measures and provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in a mobile environment.

Practically, LBS requires five basic components: *the service provider's software application, a mobile network to transmit data and requests for service, a content provider to supply the end user with geo-specific information, a positioning component such as GPS* and *the end user's mobile device*. The fast increase of location information data transaction in LBS has led into a situation where user's privacy can be compromised. Therefore, we need new privacy preserving approaches to protect the location information which is communicated during a request for LBS. Anonymization can protect privacy, but identities can sometimes be inferred from supposedly anonymous data [14]. Moreover, the service providers store and manage big amounts of personal information, mostly without the knowledge of the customers, can make users suspect the misuse of their personal data, and remove their confidence in service providers. In this situation, new technologies such as Anonymous Attestation systems are rising in demand. These schemes make use of zero-knowledge proofs and commitment schemes to allow the authentication of the users' attributes and privileges towards service providers, while preserving the user's privacy and anonymity [15].

To this end we propose an enhanced architecture for LBS based on Trusted Computing and Remote Attestation protocol functions that provide the required privacy preserving mechanisms. First, the system application lets an authorised operator to query the configuration of a location-based service. The operator will hand over user location information to the LBS Service Provider (SP) only if the service is configured and the location information is anonymized. The LBS provider will monitor information flow, and scans for any active man in the middle attacks. In the next section we discuss the role of an anonymizer and the attestation protocol in fulfilling privacy preserving requirement

2.3. Current Mobile Location Protocol

The core of location based service architecture in current GSM network is Gateway Mobile Location Center (GMLC). It is essentially a signaling node which provides the position of mobile terminals to clients that request it. This node also represents a gateway from IP network side to the mobile network. The standardized interface to communicate with GMLC from IP side is Mobile Location Protocol (MLP) [16] as depicted in Figure 1. Open Mobile Alliance (OMA) [17] including Mobile Network Operator (MNOs) and wireless vendors, mobile device manufacturers, content and service providers, and other suppliers.

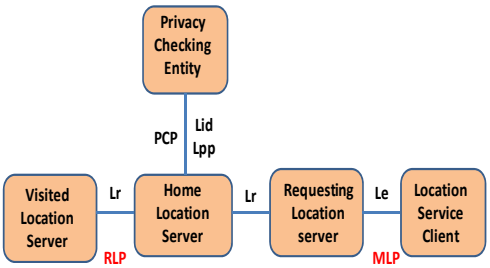

Figure 1. Open Mobile Alliance (OMA)

The OMA User Plane consists of following entities and protocols:

i. MLP: Mobile Location Protocol: MLP is a protocol for querying the position of mobile station between location server and a location service client

ii. RLP: Roaming Location Protocol: RLP is a protocol between location servers while UE is roaming
iii. PCP: Privacy Checking Protocol: PCP is a protocol between location server and privacy checking entity

MLP is mainly used by LBS to communicate from their Location Based platform to a mobile network. It is a protocol for querying the position of mobile station between location server and a location service client. An MLP library should be implemented in the way that it can be used in multiple threads to increase performance between server and client. This means that critical parts of library should be threat-safe. However the implementation of MLP library was still under development.

The motivation of our work is based on current LBS protocol issues, in such a way that the traditional approach of pseudonymity usually using a fake identity which cannot overcome such a privacy threat in LBS. Furthermore, with untrustworthy LBS providers, the revealed private location information could be abused by adversaries. On top of MLP, we will implement DAA to strengthen its privacy protection and trusted applications for LBSs and to solve anonymity issues as for Privacy Enhanced Technologies (PET) requirement. The implementation of DAA will be discussed further later.

2.4. Privacy Enhanced Technologies (PET)

Privacy Enhancing Technologies (PET) is a suitable tool for achieving advanced types of information exchange within privacy constraints [1-3] which integrated in online services or applications or when used in conjunction with such services or applications. It allows online users to protect the privacy of their personally identifiable information (PII) provided to and handled by such services or applications. The anonymity technologies field of research has become mail requirement for PET. Research in anonymity was started in the early 80's with David Chaum's paper on untraceable electronic mail [18].

PETs are designed to safeguard personal privacy by minimizing or eliminating the collection of identifiable data [19, 20] and to provide a trustworthy environment whereby users can rely on the infrastructure and system for protection of their interests. It is expected that PETs development will be widespread, especially in the areas of data minimization, privacy preferences and identity management systems [21].

The problem on which more work has been performed is the study of technologies that can anonymize the communication layer. With the aid of PET, it is possible to protect information about a person, such as identity and personal details. PET comprises all the technological controls for guaranteeing privacy. For instance, PET can be used to detach identification details from the other data stored about the person. The link between the identification details and the other personal details can only be restored with the use of specific tooling. Another option offered by PET is to prevent the registration of personal details altogether, for instance, once the identity has been verified. Software can also be used to enforce the condition that personal data are always disclosed to third parties in compliance with the prevailing privacy policies.

Therefore, new approach to curtail anonymity issues in Privacy Enhancing Technologies (PETs) [22, 23] based on Trusted Computing technologies [24-26] will result in increased privacy enhancement of user personal data and location information in mobile network services.

2.5. Trusted Computing Group (TCG)

The Trusted Computing Group (TCG) is an organization created to develop and promote open industry standards for trusted computing across diverse computing platforms, such as PCs, PDAs, mobile phones, servers, gateways and various other network devices and peripherals. The convergence of various mobile access technologies like UMTS, WLAN, and WiMAX necessitates the need for newer supporting security infrastructure. By integrating Trusted Computing into mobile & wireless networking, mainly in LBSs network, it offers secure technical applications and business environments. TCG standardizes a hardware-based security module as a security function for trust computing; known as TPM (Trusted Platform Module) for general PC (Personal Computer) environments and MTM (Mobile Trusted Module), for applying TPM in mobile environments.

Since mobile phones are much smaller than PCs and already have full circuitry, they have limited space for another chip. The most challenge is how to integrate TCG circuitry into a phone to make the technology work with the handset's software because most mobile devices have limited memory, power, and processing resources. A mobile device stores a high volume of private information and makes it high risk. A secure migration scheme is necessary for the secret key (TPM Based). Some other security services need also be migrated or updated after migration, for example, u*ser authentication, platform authentication*, c*ommunication confidentiality, data integrity, efficiency, consistency and completeness* [27].

In practice, user would prefer their privacy protected and therefore requires that the verifier only learns that she/he uses a TPM but not which

particular one – otherwise all her transactions would become linkable to each other. Currently, Trusted Computing have been deploying Privacy CA scheme which is a very sensitive entity, and must be carefully protected because it is involved in every attestation process and requires a trusted third party (TTP) during the verification and validation process. Moreover, every time TPM generates an AIK, it needs to request Privacy CA to issue corresponding AIK certificates, which could make the Privacy CA a bottleneck when serving a massive number of TPMs. Attestation of a platform as depicted in the example of a typical one in Figure 2 is an operation that provides proof of a set of the platform's integrity measurements.

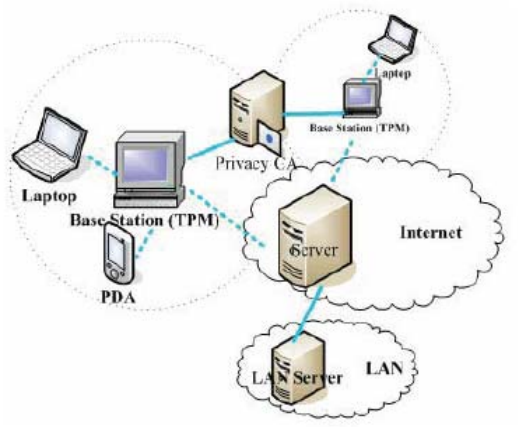

Figure 2. Trusted Computing technology enabled mobile environment

A software-based TPM essentially cannot provide the same security guarantees (tamper-resistance, trust anchor) like a hardware chip. However, TPM emulator has been proved to be useful in various ways:

i. to run more than one TPM instance per platform (e.g. virtualisation), e.g. Hewlett-Packard: Trustworthy Virtualisation Environment, VMKnoppix (Xen Hypervisor), patch for QEMU,
ii. to restore previously stored or artificially created states (e.g. testing, debugging, and educational purposes), e.g. TU Graz: class "AK IT-Sicherheit 1 / Trusted Computing"
iii. to simulate new TPM commands and vendor extensions (e.g. research and development), e.g. Princeton University, NEC, Texas Instruments: energy and execution time analysis of ECC algorithms (DATE 2007) Nokia: Validation of MTM specification (MTM Emulator).

3. Implementation

We consider the unique features of mobile phone devices, coupled with trusted services provided by DAA protocol will create more conducive LBS environment with better security, privacy and trust. Ideally, our work is based on two main parts; firstly to build a conducive anonymized environment for LBS and secondly to emphasize trust in mobile platform and the necessary attestation required to form trusted LBS network connection by giving a high level overview of DAA protocol.

3.1. Anonymization in LBS

Since mobile systems succumb more easily to eavesdropping and tapping compared to fixed networks, making it easier to unauthorized access user information, preserving anonymity in LBS systems has become a greatest concern. Current mobile communication systems store a lot of their user related information on network databases to assist in user mobility support as well as authentication and billing. This makes the user information more widespread and highly available. It is also uncertain whether the environment where this data is stored is safe and trustworthy. The following issues should be considered to solve the eavesdropping and tapping problems:

i. Preventing any association of the user with messages that he sent or received.
ii. Preserving the privacy of location and movement information of users.
iii. Preventing the disclosure of the relationship between a user and his home domain.
iv. Preventing any association of the user with the foreign domains that were visited.
v. Disallowing the exposure of a user's activities, by hiding the relationship between him and the visited domains.

Most of the existing approach utilizes anonymizer between the users and the LBS server. The above problems can be resolved through implementation of an Anonymizer. The anonymizer will act as a middleware, having several security mechanisms to defend against passive and active attacks. The privacy-aware query processor is embedded inside the LBS database server to tune its functionality to deal with anonymous queries. There are many proposed anonymization techniques that are considered as great privacy tools that preserve users' private information. Our proposed solution is shown in Figure 3 where the Anonymizer server behaves as the following:

i. receive exact location information from mobile users along with a privacy profile of each user.

ii. anonymize exact location information into cloaked spatial areas based on each user privacy profile.
iii. send cloaked spatial areas to the location-based database server. The privacy-aware query processor is embedded inside location-based database server to tune its functionality to deal with anonymous queries.

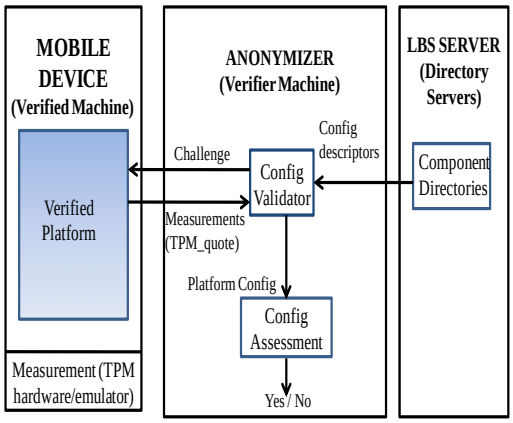

Figure 3. Anonymization in LBS Architecture based on TCG Spec

One of the purposes of remote attestation is to attest whether the remote platform is trustworthy but not revealing actual identity of the platform. To guarantee the trustworthiness and freshness, description of characteristics needs to be signed by the TPM. Usually this signature is generated by using Endorsement Key (EK) of TPM, which is a cryptographically unique and bounded to TPM and develops a solution using a trusted third party called Privacy Certificate Authority (CA). The Privacy CA acts as a Validator and it needs to be involved in all the transactions of the attestation. When a challenger requests the proof of trustworthiness of an attesting platform, it also requests the responding PCR value from that platform. An agent on the attesting platform will collect the proof data and request the built-in TPM for Attestation Identity Key (AIK) signed PCR and returns to the challenger as well as credentials that vouch for the TPM. The challenger verifies the proof and other information returned by the platform agent and determines the trustworthiness of the attesting platform[28].

We emphasize the necessity of using attestation mechanism in our proposed solution in which a trusted agent is assured to measure and report to the service provider the state related information of its resided platform. In the following section we present the implementation of anonymous attestation protocol in LBS that is being used together with the Trusted Anonymizer described above.

3.2. Direct Anonymous Attestation

Trusted Computing Group (TCG) is responsible to develop an enhanced security and privacy platform known as Trusted Platform Module (TPM) which capable of deploying a simplified protocol known as Direct Anonymous Attestation (DAA) protocol. DAA acts as a core component to remotely convince a communication partner. It is a kind of group signature scheme which is adopted by Trusted Computing Group in the specification 1.2 which involves several zero-knowledge proofs to guarantee the trustworthiness and privacy of an appropriate platform.

Furthermore, DAA is the process of using certified credentials by the Client to do DAA with Identity Provider (Prover) that produces anonymous or pseudonymous identification will make it difficult for man in the middle attacks to trace and linking back to the client. Indeed, allows trusted TPMs to obtain an anonymous attestation credential on a secret value from an issuer and use this to authenticate to a verifier. In practice, TCG proposes to use a genuine and different Endorsement Key (EK) in each trusted TPM. If we assume that the issuer knows all valid EKs, then the issuer is able to recognize trusted TPMs. The way of performing such authentication can be seen in [15, 29]. The following entities are involved in the DAA scheme as virtualised in Figure 4:

i. *The issuer* is a trusted third party functioning as a Privacy Certification Authority (Privacy CA). It grants certificates to users to allow them to authenticate themselves towards a verifier.
ii. *A user* consists of a TPM and a host, which are both needed for authentication. In particular, the host is not able to authenticate without being connected to a valid TPM. Together, the host and TPM can authenticate by proving they have a certificate and know all the secret values the certificate was built on.
iii. *A verifier* is the entity to whom the user wants to authenticate.

In order to distinguish between valid and fake TPMs, we only need to ensure an authenticated channel between the TPM and the issuer send only one initial certificate. Before a user can authenticate towards a verifier, he/she first has to obtain valid credentials from an issuer. DAA scheme basically consists of two protocols which known as *Join protocol* and *Sign protocol.* During *DAA Join protocol*, the TPM (under TPM Owner control) interacts with an Issuer to generate a set of DAA credentials. This can be done multiple times.

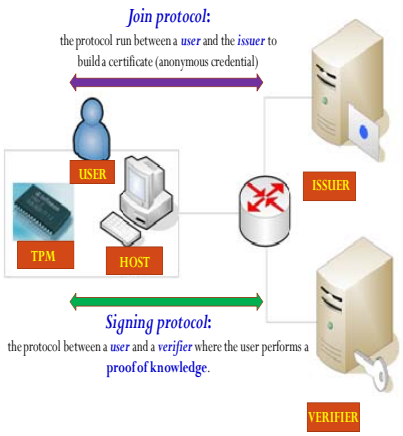

Figure 4. Architecture of the DAA scheme

In this protocol, the Issuer must also verify the endorsement, platform, and conformance credentials. A secure channel between TPM and Issuer has to be established (based on the EK) in order to prevent an attacker from simulating the TPM. AIKs based on one set of DAA credentials obtained in a single execution of the Join protocol. The DAA credentials are used during an interaction defined by the *DAA Sign protocol* with a second party called the Verifier (normally this is a server). The goal of the protocol is that the Verifier can determine if the TPM contains a valid set of DAA credentials from a particular Issuer, but does not have specific knowledge that might help to identify the TPM from among others that also have valid DAA credentials from the same Issuer. The DAA Sign protocol can also be used to sign AIKs. A Verifier can then check the signature, which confirms that this is a valid TPM to DAA credentials from the given Issuer. Therefore a TPM can create and sign an arbitrary number of AIKs based on one set of DAA credentials obtained in a single execution of the Join protocol.

TPM (embedded in mobile device or TPM Owner control) interacts with an Issuer to generate a set of DAA credentials. This can be done multiple times. In this protocol, the *Issuer* must also verify the endorsement, platform, and conformance credentials. A secure channel between TPM and *Issuer* has to be established (based on the EK) in order to protect it from misbehaving users. The purpose of the protocol is that the *Verifier* can determine if the TPM contains a valid set of DAA credentials from a particular *Issuer*, but does not have specific knowledge that might help to identify the TPM from among others that also have valid DAA credentials from the same *Issuer*. A *Verifier* can then check the signature, which confirms that this is a valid AIK from a TPM with DAA credentials from the given *Issuer*. Therefore a TPM can create and sign an arbitrary number of AIKs based on one set of DAA credentials obtained.

It must be taken into account that the DAA protocol is the heart of our framework to measure the trust ability, anonymity and anonymous attestation while running the LBS service. The basis part in our framework is to form a group of trusted users and to manage the communication link between members as well as making use of Privacy CA for the framework establishment.

4. PE-TLBS Framework

Based on PETs requirement [20, 22] we propose an information sharing scheme based on P2P environment called Trusted Group to enable mobile users to share their gathered peer location information with nearby trusted peers. If the mobile user can get enough peer location information from a peer, he/she does not need to search the network; and therefore, the information sharing scheme can reduce communication overhead. Consequently, the proposed of forming Privacy-Enhanced Trusted-LBS (PE-TLBS) protocol is necessary for preserving anonymity, detecting rogue users and possible linkability, conveying location, mapping location to services and complying with privacy requirements.

4.1. Virtualized Secure Framework

Virtualization is needed to improve the utilization of existing computing resources and to reduce hardware. The survey and research in virtualization was started over 30 years ago. Computer's core peripherals such as processor, memory are much faster nowadays where it can allow a normal personal desktop computer to host multiple virtual machines (VM) concurrently. VMware, Xen and OpenVZ are examples of Virtual Machine Monitor's (VMM) software which controls the operation of the VMs hosted. Every single devices found in a physical machine will be virtually created by these software to act like a physical devices in the VMs. With this, any software running inside the VM will not recognize devices found as virtual devices but as physical devices. Virtualization helps server administrator to ease the burden to administrate numbers of machine where its entire are virtualized in a single computer. By having a "sandbox-like" environment, administrator should not be worried if the guest operating system (OS) infected to malware or virus because it will not be spread throughout the whole machine.

Therefore, we present a virtualized secure framework called Privacy Enhanced Trusted Location Based Services (PE-TLBS) providing trusted mobile devices, trusted entities and trusted services while protecting the client privacy. This framework contributes the desired privacy and trust level on top of existing Mobile Location Protocol (MLP). One of the objectives of virtualization is to

reduce the existence of physical machines to run several operating systems. By using virtualization, operating systems can concurrently exist in just a single physical machine where those operating systems will share the physical machine's processors, memory resources and more. Referring to Figure 5, it shows the flow of our virtualized secure framework where it is applied in a virtualization environment. There are three main components which need to be complied based on TCG Spec which are:

i. Support for Trusted Platform Boot.
ii. Platform Security Kernel.
iii. Virtual Machines.

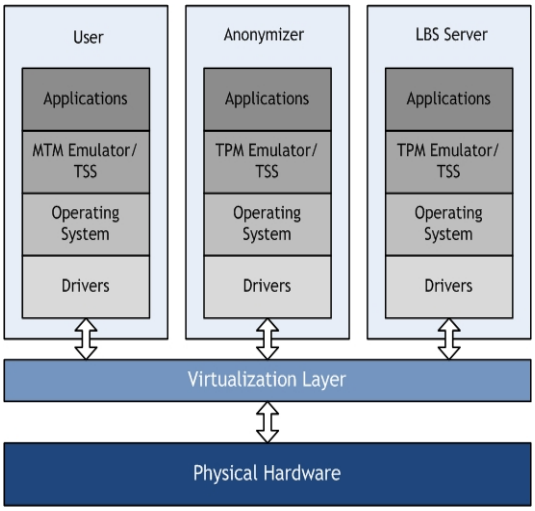

Figure 5. Our Approach on Virtualized Secure Framework based on TCG Spec

During system boot up, the integrity metrics of the system will be generated and the corresponding values will be hashed using SHA-1 to be stored inside the PCR. Next, during the platform initialization, the integrity metrics of the affected components will also be generated and the corresponding values will also be stored inside the PCR as well. Prior to the execution of virtual machines installed, their integrity metrics might be checked as well and the process is similar to the platform trusted boot process. Those integrity metrics stored in PCR will be then used for remote attestation purposes..

4.2. The Used of Privacy CA and Trusted Group of Clients

The key idea behind the system is to hierarchically encrypt location information under different key pairs in RSA which are Endorsement Key (EK) and Attestation Identity Key (AIK), and distribute those appropriate keys only to trusted group members with the necessary permission given by the Group Leader in a respected Trusted Group of clients. A terminal platform, hosted by TPM, can attest to its description of characteristics to a remote party. To guarantee the trustworthiness and freshness, the description of characteristics needs to be signed by the TPM. Usually this signature is generated by using the Endorsement Key (EK) of TPM, and the Endorsement Key of TPM is the Root of Trust for Reporting (RTR) which is the cryptographically unique and bound to the TPM.

For guaranteeing the accuracy of the information and protecting the privacy of the host of the TPM, TCG develops a solution using a trusted third party (Privacy CA). TPM gets an Attestation Identity Key (AIK) certificate from Privacy CA by securely negotiating with the Privacy CA, and signs the message by using the AIK instead of EK. The AIK is an asymmetric key pair only used for signing, and is never used for encryption. It only signs information generated internally by the TPM, e.g., PCR values. The AIK must never sign arbitrary external data, since it would be possible for an attacker to create a block of data that appears to be a PCR value.TPM can create an unlimited number of AIKs.

The enrolment with a Privacy CA requires the TPM to prove AIK keys are exclusively bound to the TPM. The platform accomplishes this by decrypting the AIK credential using the EK private key in the TPM. Only the TPM with the EK private key will be able to perform the decryption. CA must also check endorsement, platform and conformance credentials. The Privacy CA then distributes a credential certifying the AIK. Hence, every time TPM generates an AIK, it needs to register with Privacy CA and request to issue corresponding AIK certificates, which could make the Privacy CA a bottleneck when serving a massive number of TPMs. DAA indeed is a method that should solve this bottleneck issue in AIK creation and to achieve enhanced privacy by eliminating the need for a Trusted Third Party (TTP - which is initially managed by Privacy CA).

Although DAA practically reduced the need for TTP, and in the number of parameters required, there are still problem in its operation. The main problem in the existing DAA implementation is the vulnerability of the system in case of one TPM can be compromised and its secret published. In this case, the verifier is not able to distinguish between trusted and fake TPMs since all of them use the same secret value. In order to overcome the problem, we make use of Privacy CA at the very beginning of establishment of the LBS environment. Figure 6 below shows our PE-TLBS framework which adopted P2P communication device process to form Trusted Group. Privacy CA will act as a trusted third party and an issuer organization at the beginning stage of validating TPM before clients use an LBS services.

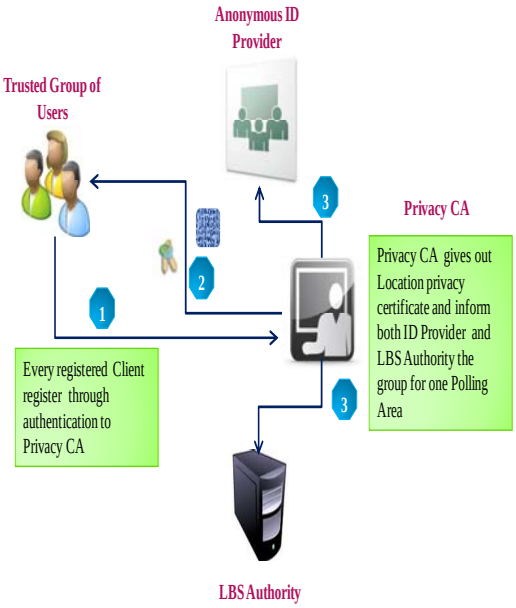

Figure 6. Registration through Privacy CA

Before providing the user with an EK certificate, the issuer needs to check whether or not the TPM is valid. Thus, it is required that the issuer is able to distinguish between fake and trusted TPMs. The need of validating TPM with Privacy CA is to grant the certificate required by the user to authenticate itself towards the verifier. After the user is granted an EK certificate, she is able to authenticate herself by proving she has the certificate and the secret values on which the certificate is built. To protect the privacy of the client identity, the true identity of the client is only known to the privacy compliant Identity Provider, which must comply with a legislative privacy agreement. The prover will then check with the Verifier whether the client is registered and authorised to get the service. Once proven to be true, the LBS Server will be able to provide service to the client, without actually knowing who the client is.

The state-of-the-art peer-to-peer (P2P) communication technology adds a new dimension to the privacy-preserving techniques in LBS. We adopt the concept of P2P communication devices process as illustrated in Figure 7 as the user's ability to collaborate with one another but with the ability to blur their exact locations into spatial regions without any help from centralized third trusted parties

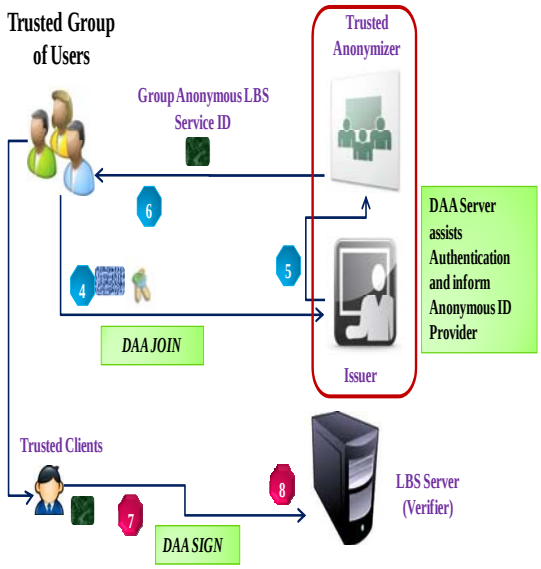

Figure 7. The Usage Of DAA Protocol in Privacy Enhanced Trusted LBS (PE-TLBS) framework including Trusted Group of clients.

With respect to Figure 6 and Figure 7, we show the attestation flow between client and server in our virtualized Proof of Concept (POC) environment Figure 8 below.

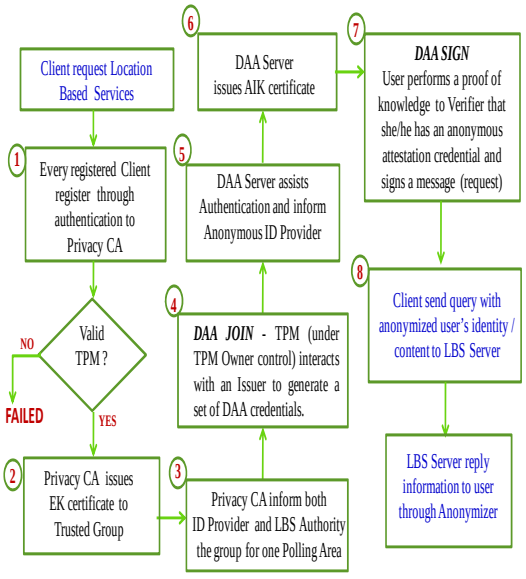

Figure 8. Attestation Flow between Client-Server in the virtualized POC environment

A number of clients/devices in the particular Trusted Group co-located at a geographic location can broadcast and receive a token called Group anonymous ID. The tokens or Group anonymous ID can be exchanged using a communication link having limited communication range in a particular duration to remain the privacy. Tokens that are received by a device can be stored locally on the

device and/or transmitted to a trusted service operating remotely on a network. Furthermore, the tokens can be stored with corresponding timestamps to assist a trusted service in matching the tokens with tokens provided by other devices.

A group can be created based on results of the analysis. Trusted users of valid TPM can be invited to join the trusted group. User interfaces, filters and search engines can be provided to the users to enable users to search and manage groups. The groups can be used with various applications to provide additional content and services to the users. If the geographic location of the group at the contact time is known, then members of the group can be targeted to receive location-based services (LBS) and content. The size or membership of a group can be defined by the transmission range provided by the communication technology employed. For example, Bluetooth technology can provide a transmission range of about 10 meters (30 feet). To reduce the amount of tokens that are stored by a given device, a filter can be implemented on the receiving device to allow every n^{th} token to be stored. Alternatively, or in addition to filters, the repetition rate for broadcasting tokens can be reduced on the broadcasting device. Thus, token counts can be used to generate a score that indicates a level of quality of the contact which can be used for organizing and managing Groups.

4.3. Proof of Concept

The main goal of implementing DAA in this PoC environment is to demonstrate that we can provide both trusted services and at the same time provide client privacy. It is anticipated that this POC system can be used in providing the flexibility to add on more enhancement features and security services for Location-Based network and applications.

Our POC is mainly focuses on implementing a simplified protocol based on a group signature scheme called Direct Anonymous Attestation (DAA) scheme supported by Trusted Platform Module (TPM) functionalities in such a way for preserving anonymity, detecting rogue users/TPM and possible linkability complying with privacy requirements. The POC is essentially privacy preserving a trusted user from a respected Trusted Group of clients who are dealing with Trusted LBS through DAA protocol by validating several parameters in TPM. Since software-based security applications cannot defend users against cybercrime threats and cannot assure its own integrity, hence, by providing a hardware based security such TPM, we could against those threads and preserve important and sensitive information especially in mobile environment.

For our implementation, we set up a Virtualized Secure Framework with several components as suggested in Table 1. To have a secure framework, several components must be complied based on TCG specs.

Table 1.
Several Components for Virtualised Secure Framework Development

Tools	Specifications
Physical Server	- CPU HP Compact dc 7800 - Quad Core 2.4 GHz - RAM : 8 GByte - QEMU Wrapper
Entity (DAA Mobile Client)	- MSDOS 6.22 with 512MB RAM - TPM Emulator - TrouSerS (TCG Software Stack)
Entity (DAA Server)	- Windows Vista SP 2 with 1GB RAM - TPM Emulator - TrouSerS (TCG Software Stack)
Entity (LBS Server)	- Windows Vista SP 2 with 1GB RAM - TPM Emulator - TrouSerS (TCG Software Stack)
Entities (User1, User2, User3)	- Windows Vista SP 2 with 1GB RAM - TPM Emulator (Each entity will have different EK) - TrouSerS (TCG Software Stack)
Development Tools	- Visual Studio 2005 with Service Pack 1 - Window CE 6.0 R3 - Embedded visual C++ 4.0 SP4 - Marvell C++ Compiler for Windows CE - Window embedded CE 6.0 platform builder SP 1.

The used of Virtualization technique due to the capability of utilization of existing computing resources and to reduce hardware. By having this technique, the burden to administrate numbers of machine is reduces. This privacy mechanism represents the actual entities topology by having several virtual machines running on a physical machine.

In practice, there are some limitations in the personal computer environment compared to the real mobile device environment. Our goal is to create a working software-based TPM emulator that is compliant with TCG TPM specification version 1.2 and supported by operating systems including GNU/Linux, Open/FreeBSD, (ebuild script for Gentoo Linux available) Third-Party Libraries GNU Multiple Precision Arithmetic Library support for RSA and DAA). Referring to Table 1, we mainly use QEMU wrapper for our physical server which acts as Virtual Machine Monitor's (VMM) software that controls the operation of the VMs hosted. Every single device found in a physical machine will be virtualized in the VMs. With this, any software running inside the VM will not recognize devices found as virtual devices but as physical devices.

Three virtual machines are created to represent the mobile device, anonymizer and LBS server. QEMU was selected because it can emulate a working PCI Ethernet driver from Advanced Micro Devices (AMD) for Windows CE 6.0 R3 emulation which runs on top of MS-DOS operating system.

Each of the entity except mobile client is installed with Windows Vista SP 2 OS. For the mobile device which is the client, MS-DOS is installed to support Windows CE 6.0 R3 emulation. This method is used because Windows CE 6.0 cannot be directly installed as an OS inside QEMU since it does not run on x86 or x64 hardware. They will have their own dedicated TPM Emulator to make sure that PCRs is enough to do the remote attestation between the entities. This TPM Emulator was adapted from and compiled under Windows platform using software MinGW with arbitrary precision arithmetic library and CMake 2.6. There is a limitation in Windows platform where the TPM Emulator is not recognized as a driver like in Linux platform but it is recognized as a Windows pipe. Hence, Windows TPM Base Services (TBS) could not recognize this TPM Emulator like TPM hardware.

An open-source TSS, named TrouSerS was used to talk to the TPM Emulator to overcome the problem stated above. There is an issue where TrouSerS can only work with TPM hardware and not with an emulator. To overcome this, the TCG Device Driver Library (TDDL) for TrouSerS was edited to let it recognize the emulator as hardware. This Windows based TrouSerS can support both hardware and emulator where it will first detect the present of hardware. TBS must be disabled to let the TrouSerS talk to the emulator rather than talk to the hardware. In order to support the remote attestation process, TSS Application Programming Interface (TSS API) is used where it support TPM services which are:

i. RSA key pair generation.
ii. RSA encryption and decryption using PKCS v1.5 and OAEP padding.
iii. RSA sign/verify.
iv. Extend data into the TPM's PCRs and log these events.
v. Seal data to arbitrary PCRs.
vi. Random Number Generation.
vii. RSA key storage.

For the programming part, several software and header files are needed which are Visual Studio 2005 with SP1 and Marvel C++ Compiler for Windows CE. The header files are required to make sure that the compilation successful since a specific library of file is needed by the compiler to recognize the entry point of TPM programming. To create and configure an image for Windows CE 6.0 R3, there are several software required which are :

i. Microsoft Visual Studio 2005 with SP1
ii. Microsoft Windows CE 6.0 until Microsoft Windows CE 6.0 R3 MSI package.
iii. Windows Embedded CE 6.0 Platform Builder with SP1.
iv. Specific drivers for PCI Ethernet for Windows CE.

The drivers for PCI Ethernet should be loaded into Microsoft Visual Studio 2005 after successfully installed the other software requirements as stated above. After that, MS Visual Studio will create an image named NK.bin which will be emulated under MS-DOS. For this study, MS-DOS version 6.22 is used since it is the only version which able to do the emulation. To implement this, MS-DOS initially will be installed inside QEMU as one of the Virtual Machines and from the command line interface, the image named NK.bin is loaded by using a specific command line.

Solving the security, privacy and trust issues as well as forming our PE-vTLBS framework, is extremely hard especially how to make the service components trustworthy; composing services leads to new subtle and dangerous vulnerabilities due to interference between component services and policies, the shared communication layer, and application functionality.

We initially discuss how the TPM Resource Manager performs sharing of resources through TPM authorization delegation without exposing privacy of other VMs. Secondly we show a simulation of an application running in VMs that shows the attestation process. We then analyze the speed performance and measure the integrity of the running application. Thirdly, we run replication of Multiple Virtual Machines (MVMs) by deploying TPM functionalities to simulate the virtualized secure framework. We anticipate that our proposed framework would be able to mitigate threats, and strengthen customers' confidence on using LBSs.

In practice, any services (as well as LBSs) need to be securely combined according to evolving trust and security requirements and policies. A rigorous demonstration that a composed Service-Oriented Architecture (SOA) meets the security requirements and enforces the application policy will significantly increase customers' confidence and also enable them to fully exploit the benefits of service orientation.

5. Conclusion

Our Privacy Enhanced virtualized Trusted LBS (PE-TLBS) framework implements a Direct Anonymous Attestation (DAA) protocol based on group signature scheme. We make use of Privacy CA which acts as an issuer organization at the beginning stage of validating TPM before clients may use an LBS services. We adopt the concept of trusted P2P communication devices process as for user's trust ability to collaborate with one another to form Trusted Group members with valid TPM. The Proof of Concept is actually validating a trusted user from respected Trusted Group of clients who are dealing with Trusted LBS through DAA protocol. The location information is hierarchically encrypted using

key pairs known as Endorsement Key (EK) and Attestation Identity Key (AIK), and distributes the appropriate keys only to trusted group members with the necessary permission. We use TPM Emulator and TCG Software Stack (TSS) to simulate and make the accession to TPM much simpler while maintaining the functionality as well as provide Application Programming Interfaces (APIs). We believe that this framework would fulfill the desired privacy and trust level to help create more trusted and privacy preserving in LBS.

In future, we will continue our work on the Proof of Concept for PE-TLBS framework development with the implementation of DAA protocol and examining in greater detail the TPM functionalities in terms of processing resources, privacy performance and verifying the system behaviors in a large system, in which each mobile user terminal has different security requirements.

7. Acknowledgements

This paper was prepared for Universiti Teknologi MARA (UiTM), Malaysia. The material in this paper was presented in part at The 2nd International Workshop on Network Assurance and Security Services in Ubiquitous Environments 2010 (NASSUE 2010-WiMob 2010) Niagara Falls, ON, Canada, October 12, 2010, The 5th International Conference for Internet Technology and Secured Transactions (ICITST-2010), November 8-11, 2010, London UK and 2010 International Conference on Computer Applications and Industrial Electronics - Trusted Computing & Secure Systems (ICCAIE2010), December 5-7, 2010, Kuala Lumpur, Malaysia.

7. References

[1] White Paper Privacy.-Enhanced Technologies Dec2004, “Privacy Enhanced Technologies White Papers for Decision Makers,” Privacy-Enhancing Technologies White Paper for Decision-Makers Written for the Dutch Ministry of the Interior and Kingdom Relations Directorate of Public Sector Innovation and Information Policy (DIIOS).

[2] J. Z. E. Kosta, T. Scherner and J. Dumortier, “Legal Considerations on privacy-enhancing Location Based Services using PRIME Technology,” Computer Law & Security Report 2008.

[3] C.-Y. C. Mohamed F. Mokbel, and Walid G. Aref., “The new Casper: query processing for location services without compromising privacy,” Proc. Of the 32nd International Conference on Very Large Data Bases (VLDB), pp. 763-774, 2006.

[4] C. Y. Chow, “Privacy-Preserving Location-based Services” A DISSERTATION SUBMITTED TO THE FACULTY OF THE GRADUATE SCHOOL OF THE UNIVERSITY OF MINNESOTA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF Doctor Of Philosophy May, 2010

[5] M. F. M. Chi-Yin Chow “Privacy in location-based services: a system architecture perspective ” SIGSPATIAL Special vol. Volume 1 no. 2 pp. 23-27, July 2009, 2009.

[6] M. C. Claudio A. Ardagna[20] , Sabrina De Capitani di Vimercati[20] and Pierangela Samarati[20] “Access Control in Location-Based Services” Book Series Lecture Notes in Computer Science, Publisher Springer Berlin / Heidelberg, Book Privacy in Location-Based Applications, Subject Collection:Computer Science , SpringerLink DateThursday, July 30, 2009, vol. Volume 5599/2009, ISBN 978-3-642-03510-4, pp. 106-126, 2009.

[7] H. I. M. G. Rahman, “Security in Wireless Communication Full text,” Source Wireless Personal Communications: An International Journal Kluwer Academic Publishers Hingham, MA, USA, vol. Volume 22, no. 2, pp. 213 - 228, 2002.

[8] “SUBJECT: Effective Date: Policy Number: Security of Mobile Computing, Data Storage, and Communication Devices,” Responsible Authority:Vice Provost for Information Technologies & Resources, vol. Policy Number 4-007, pp. Supersedes: Page Of 1 - 5, July,15 2007.

[9] S. i. W. Communication, “Wireless Personal Communications,” Publisher:Springer Netherlands, Subject Collection:Engineering, SpringerLink Date : Tuesday, November 02, 2004, vol. Volume 22, no. Number 2, pp. 213-228, August, 2002.

[10] A. Gkoulalas-Divanis, V. S. Verykios, and D. Eleftheriou, "PLOT: Privacy in Location Based Services: An Open-Ended Toolbox." pp. 62-71.

[11] J. A. Pang, “Quantifying and Mitigating Privacy Threats in Wireless Protocols and Services,” School of Computer Science, Carnegie Mellon University, PhD thesis, 2009, 2009.

[12] X. Fei, H. Jingsha, W. Xu et al., "A Method for Privacy Protection in Location Based Services." pp. 351-355.

[13] L. L. Bhuvan Bamba, Peter Pesti, Ting Wang, “Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid” WWW 2008, April 21–25, 2008, Beijing, China, 2008.

[14] P. Golle, and K. Partridge, “On the Anonymity of Home/Work Location Pairs,” in Proceedings of the 7th International Conference on Pervasive Computing, Nara, Japan, 2009.

[15] B. ERASMUS, P. D. I. B. Preneel, D. Supervisors: et al., “Implementation of an Anonymous Credential Protocol” Thesis for the Engineer's degree of Telecommunications 2007 - 2008.

[16] R. B. Petr Vlacil, "Implementing Mobile Location Protocol," Czech Technical University in Prague. Department of Telecommunications Engineering 2009.

[17] Mobile Location Protocol. OMA-TS-MLP, draft v3.3, Open Mobile, and Alliance.

[18] C. DIAZ, "Anonymity and Privacy in Electronic Services" PhD thesis KATHOLIEKE UNIVERSITEIT LEUVEN FACULTEIT INGENIEURSWETENSCHAPPEN DEPARTEMENT ELEKTROTECHNIEK-ESAT Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, December 2005,
Promotors:
Prof. Dr. ir. Bart Preneel, Prof. Dr. ir. Joos Vandewalle

[19] A. S. Gajparia, "On User Privacy for Location-based Services" Thesis submitted to the University of London for the degree of Doctor of Philosophy Information Security Group Department of Mathematics Royal Holloway, University of London 2007

[20] W. P. P.-E. T. P. P.-E., and Technologies_Dec2004.

[21] a. I. f. P. T. S. I. Joint Research Centre (DG JRC)J. R. C. D. JRC), "Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview," Technical Report Series for the European Parliament Committee on Citizens Freedoms and Rights, no. Justice and Home Affairs (LIBE) EUR 20823.

[22] X. Fei, H. Jingsha, W. Xu et al., "A Privacy-Enhanced Access Control Model." pp. 703-706.

[23] S. Yan, T. F. La Porta, and P. Kermani, "A Flexible Privacy-Enhanced Location-Based Services System Framework and Practice," Mobile Computing, IEEE Transactions on, vol. 8, no. 3, pp. 304-321, 2009.

[24] M. P. <martin.pirker@iaik.tugraz.at>, "TPM - Trusted Platform Module," Trusted Computing Labs, IAIK TU Graz, 2009.

[25] S. Balfe, E. Gallery, C. J. Mitchell et al., "Challenges for Trusted Computing," IEEE Security and Privacy, vol. 6, no. 6, pp. 60-66, 2008.

[26] A. M. a. M. M. Daqing Zhang, "A trustworthy framework for impromptu service discovery with mobile devices" International Conference On Mobile Technology, Applications, And Systems, Proceedings of the 4th international conference on mobile technology, applications, and systems and the 1st international symposium on Computer human interaction in mobile technology, Singapore pp. Pages: 254-260 Year of Publication: 2007

[27] H. M. I. S. A. (Intel), F. M. N. DoCoMo) et al., "Trusted Mobile Platform," Trusted Mobile Platform Protocol Specification Document 04/05/2004 Trusted Mobile Platform NTT DoCoMo, IBM, Intel Corporation File Name: tmp_protocol_spec_rev1_00__20040405.doc, 04/05/2004.

[28] S. C.-X. LI Xiao-Yong, "An Efficient Attestation for Trustworthiness of Computing Platform," Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), 2006.

[29] J. C. Ernie Brickell, Liqun Chen, " Direct Anonymous Attestation," In Proceedings of 11th ACM Conference on Computer and Communications Security, ACM Press, 2004.(CCS'04), October 25-29,
2004.

