A Case Study on Privacy in Mobile Computing Environment

1Dr. Mahendra Singh Bora, 2Mr. Suprabhat Joshi, 3Miss. Himani Joshi 4Komal Chandra Joshi
1Assistant Professor (CS Deptt.), Shriram Institute of Manag. & Tech., Kashipur (Uttarakhand), INDIA.
2Assistant Professor (CS Deptt.), Shriram Institute of Manag. & Tech., Kashipur (Uttarakhand), INDIA.
3Assistant Professor (CS Deptt.), Shriram Institute of Manag. & Tech., Kashipur (Uttarakhand), INDIA.
4Assistant Professor (CS Deptt.), Shriram Institute of Manag. & Tech., Kashipur (Uttarakhand), INDIA.

1mahendra.singh.bora@gmail.com, 2sup.simt@gmail.com, 3h0773@gmail.com, 4komal_joshi14@rediff.com

ABSTRACT

In the developing world it is require access to services in the financial, agricultural, business, government and healthcare sectors. Due to constraints of the existing infrastructure (power, communications, etc), it is often difficult to deliver these services to remote areas in a timely and efficient manner. Many of the applications built with mobile phone and a centralized server can exchange information and get the collected data backed up on reliable media. For this Mobile systems and applications are raising some important information security and privacy issues. This requires a mechanism for capturing user information and making it available to users. However, storing and exchanging potentially personal information raises user privacy concerns. This work describes a general framework to providing privacy and aware personalization in mobile computing environments.

Keywords- centralized server, data collection, backup, services, security, and privacy.

I. INTRODUCTION

Today, users struggle to maintain the security of their individual computing devices and have difficulty in managing their privacy in online. Tomorrow, these challenges might be unimaginably complex, as location-aware technologies embedded in both devices and environments reveal not only personal information but also location and context information.

The infrastructure and economic constraints of the developing world have resulted in a field worker based model for delivering financial, agricultural, business, government and healthcare services. By using the existing and under-utilized workforce, companies, non-governmental organizations (NGOs) and governmental organizations use these field workers asynchronously as an efficient channel for services. Beyond services, the reality of these environments is that field workers are a reliable way to transfer data.

In the developed world the set of techniques going under the name of e-Mobile is become more and more important in e-Business transactions. The use of smart mobile terminals will allow new kind of services and new business models, overcoming time and space limitations. The technological evolution in wireless data communications is introducing a rich landscape of new services relying on three main technologies:

- Personal area networks (PANs), composed by personal and wearable devices capable of automatically setting up transient communication environments (also known as ad-hoc networks).
- Wireless local area network technology (WLAN).
- 3rd Generation of mobile telecommunications (3G), gradually replacing General Packet Radio Service (GPRS) and the related set of technologies collectively called “2.5 Generation” (2.5G). 3G services are made available through technologies such as Wideband Code-Division Multiple Access (WCDMA), offering high data speeds.

User models provide a natural construct for storing, managing and communicating user information to personalize services in ubiquitous computing environments. However, maintaining user models and
releasing them to service providers, raises privacy and security concerns relating to the storage, access and processing of the information contained within the model. Users may wish to limit and control the amount of information released to the service provider. The information stored is often personal and may potentially identify the user. Protecting user identity would require providing mechanisms to allow anonymous/pseudonymous interaction with personalized services. Service providers would also need to ensure the accuracy and authenticity of the information provided by the user. Mechanisms are thus required for defining relevant subsets of the user model, allowing users to control their release, and authenticating and protecting the integrity and confidentiality of the user information released to the service provider. These topics have been extensively researched in relation to the World Wide Web [5, 6], but have received much less attention [4] in the context of ubiquitous computing. The majority of past work on privacy has focused on providing anonymity, hiding user identity and keeping personal information secret [7].

Thus, privacy needs to be seen in terms of a negotiated controlled disclosure of information. This paper addresses a wider notion of privacy that focuses on providing users with notice of data collection, choice regarding collection and informed consent, so they can make informed decisions regarding the disclosure of their personal information. User model, releasing the information to a user’s mobile device, and restricting and controlling the release of the information to service providers while protecting user privacy [3].

II. GENERAL PRINCIPLE AND REQUIREMENTS

While wireless communications provide great existence and mobility, they often come at the expense of security. Indeed, wireless communications rely on open and public transmission media that raise further vulnerabilities in addition to the security threats found in wired networks. With wireless communications, important and vital information is often placed on a mobile device that is vulnerable to theft and loss. In addition, this information is transmitted over the unprotected airwaves. 3G networks are getting smaller and more numerous, causing opportunities for hackers and other abusers to increase. 3G technologies incorporate stronger cryptographic techniques, and new authentication systems. This is probably not enough, because application areas like mobile commerce require this critical information to be decrypted by a server located somewhere in the communications chain before it is encrypted again and forwarded to a new destination. Every hop in the wireless communication chain where information is decrypted and re-encrypted represents a potential vulnerability in the overall security.

Furthermore, the growing complexity of mobile terminals and the increased presence of interoperability software on them is making them vulnerable to viruses and hacking attacks. The boom of users demand for richer content for their mobile terminals (such as through multimedia messaging, video conferencing, voice-over-IP, m-business) is increasing the need for security solutions ensuring user and data confidentiality, quality of service (QoS), billing, and protection against intruders. The challenge for industry players now is to tackle all security issues within PAN, 3G and WLAN and create a profitable integrated wireless business comprising of services and value. They will provide all the functionalities of an Integrated Services Multimedia Network (ISMN), enabling a whole series of new business models and applications [2]. With a number of available services a privacy beacon (1) announces the data collections of each service and their policies using a wireless communications channel such as Bluetooth or IrDA. In order to save energy, the mobile privacy assistant (2) the user is carrying delegates this information to the user’s personal privacy proxy residing somewhere on the Internet (3), which contacts the corresponding service proxies at their advertised addresses (4) and inquires their privacy policies. After comparing those privacy policies to the user’s privacy preferences, the user proxy decides to decline usage of the tracking service, which results in disabling the location tracking service. [10]

III. WIRELESS APPLICATIONS AND SECURITY TESTING METHODOLOGIES

As the complexity of mobile and wireless applications increases rapidly, importance of manufacturing security test becomes more critical. The main requirements of an effective security test methodology are the establishment of functional completeness and compliance with appropriate security requirements, and minimum test execution time. Activities associated with testing include the following:

- identification of the security requirements to be satisfied;
- identification of proposed product security mechanisms;
- determination of the test objectives;
- determination of the test methodology/technique;
- determination of expected test results;
- conduct of the test;
- documentation and analysis of test results;
- feedback of test results to appropriate individuals/organizations;
- Determination of the next action to be taken (e.g., additional testing, corrective actions, and so on).

The Open Source Security Testing Methodology Manual (OSSTMM) [Open Source Security Testing Methodology Manual] is a need for an open, free security testing methodology in response to the numerous security testing companies who claimed to have an internal
and corporate methodology for testing. The OSSTMM has become the most widely used security testing methodology in existence. In particular, the OSSTMM provides testing methodologies for the following six security areas: Information Security, Process Security, Internet Technology Security, Communications Security, Wireless Security, and Physical Security. The methodology is used by IT consultancies, institutions, government, and legal firms worldwide because it offers low-level tests for many international laws on privacy and security. We now focus our attention on the wireless security testing section. This section includes ten modules (e.g., electromagnetic radiation testing, 802.11 wireless networks testing, Bluetooth network testing, and so on) that in turn include one or more tasks. Each module has an input, which is the information used in performing each task, and outputs a dataset, which can then be classified in terms of Risk Assessment Values (RAV). RAVs serve to quantify the results of each module, which in turn tells security testers how long information remains useful and ‘current’. Basically, a relative risk value is assigned to systems under test, and each user is willing to accept different levels of risk. This allows end users to determine how often they want regular testing to be carried out and how much risk they are willing to support. The output of a module may then be the input for one or more sections, or in certain cases, may be the input for a previous module.

As pointed out in the introduction, anonymity, pseudonymity, and security (i.e., secure communication and access) are useful tools when being a supportive part of the infrastructure, but should not be taken as isolated solutions. Consequently, our system employs anonymous and secure connections, as well as reasonable access controls, whenever possible to prevent unwanted data spills and trivial data sniffing. Our main focus, however, lies on implementing the other four principles for use in a ubiquitous computing (mobile) environment:

- **Notice:** Given a mobile environment where it is often difficult for data subjects to realize that data collection is actually taking place, we will not only need mechanisms to declare collection practices (i.e., *privacy policies*), but also efficient ways to communicate these to the user (i.e., *policy announcement*).
- **Choice and consent:** In order to give users a true choice, we need to provide a selection mechanism (i.e., *privacy agreements*) so that users can indicate which services they prefer.
- **Proximity and locality:** The system should support mechanisms to encode and use *locality information* for collected data that can enforce access restrictions based on the location of the person wanting to use the data.
- **Access and recourse:** Our system needs to provide a way for users to access their personal information in a simple way through standardized interfaces (i.e., *data access*). Users should be informed about the usage of their data once it is stored, similar to call-lists that are often part of monthly phone bills (i.e., *usage logs*).

## IV. SECURITY REQUIREMENTS AND MECHANISM

Security in user modeling is not a goal in itself, but an auxiliary means for realizing privacy [8]. The same principle applies to ubiquitous computing; security measures are designed to protect the privacy of the data exchanged and the entities involved in the system. Requirements for security comprise requirements for implementing the four key attributes of security, i.e., authentication, confidentiality, integrity and no repudiation [9]. Another key attribute of security is availability. Within the context of user modeling, availability refers to the amount of user modeling functionality available to user model client (in this case, the service provider) [8]. Since the functionality is adjustable depending upon user preferences, as expressed in (A Platform for Privacy Preferences Exchange Language) APPEL, availability cannot be guaranteed. Similarly, ubiquitous computing applications depend on the availability of networking infrastructure (such as Wi-Fi) and thus, availability of a particular ubiquitous system cannot be independently guaranteed. Thus, availability is not included as a security requirement. The security requirements discussed here apply only to securing the communication between the participants of the system. Service providers would be responsible for securing the storage of personas and templates on their systems. The system also does not provide mechanisms for securing personas and templates stored on the user’s mobile device. A solution may be to store encrypted personas along with a one way keyed hash of the persona. On a PDA, however, this may introduce additional processing delays. Similarly, the authorizing entity is expected to provide its own methods for securing the data storage. Requirements for communication security are discussed below:

- **Confidentiality:** personas may contain personal information and thus their content needs to be kept secret from entities other than the participants in the system. Secrecy of exchange can be achieved through SSL.
- **Integrity:** personas and templates need to be protected against tampering during communication. This may again be achieved by using secure message digests and communicating over SSL. Users would be responsible for ensuring the integrity and confidentiality of personas stored on their mobile devices.
- **Authentication:** users need to authenticate personas and templates released by the authorizing entity. Similarly, service providers need to authenticate the templates released by the authorizing entity and the personas released by the user.
Additionally, users need to authenticate the service provider prior to releasing their personas. Thus there are two kinds of authentication that is required:

- **Entity authentication** to authenticate the participant in the exchange and **data authentication** to authenticate the personas and templates exchanged. Note that users do not authenticate themselves while communicating with service providers. This allows them to preserve their anonymity. Entity authentication can be achieved through X.509 certificates and communicating over SSL while data authentication can be achieved through RSA signatures together with a Certification Authority. Note that data authentication implicitly provides data integrity (for if a message has been modified, the source has changed) [9].

- **Non-repudiation**: refers to preventing an entity from denying previous commitments or actions [9]. Non-repudiation is not a core security requirement of the system but may be required to prevent a service provider from denying data collection.

**V. TECHNOLOGIES FOR MOBILE SECURITY.**

As we have seen in the previous Section, technologies for 2G mobile security provide standard 12 functions for checking the subscriber identity authenticity, for protecting the subscriber anonymity and for encrypting user and signaling data. 3G, while retaining SIM-based authentication, enhances security features organizing the issue in four domains: access, network, user and authentication, enhances security features organizing the issue in four domains: access, network, user and authentication, enhances security features organizing the issue in four domains: access, network, user and authentication, enhances security features organizing the issue in four domains: access, network, user and authentication, enhances security features organizing the issue in four domains: access, network, user and authentication. For packet data traveling over the mobile network layer, conventional security technologies apply. Two main areas can be identified:

- **Security Network Domain**: When Mobile IP is used at the network level over a mobile infrastructure, the most salient security issue is the problem of how to authenticate the registration messages that inform the server about a mobile node's current IP address, in order to avoid spoofing and IP impersonation attacks [18].

- **Security Transport Domain**: The well-known Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols provide entity authentication, data confidentiality, and data authentication.

**VI. USER PRIVACY**

Privacy and security are major issues that must be addressed. In health applications, it is important that patient data remain secure when transferring between devices. Using a standard public key infrastructure would be a good solution. Each device can encrypt data with a public key of the centralized server. When the data is received, it can be decrypted using the private key. The privacy concern of sharing location profiles raises questions about tracking people. To introduce a sufficient amount of plausible deniability, we imagine introducing variable granularity of location. For example, locations could be reported on village level instead of precise locations of connectivity. Depending on the application, it may be that field workers wish to be tracked so they can be managed more efficiently by their organizations. Being able to tell where field workers are can reduce overlap and duplication of data collection. This is especially important for transport workers mulling data [2].

The privacy policy is evaluated against the user’s privacy preferences and the user may configure these to prompt for action, release data or block data release based on the contents of the privacy policy. Default privacy preferences are provided for usability purposes but users can also define their own privacy preferences and are thus not restricted to choosing the least intrusive of a set of preferences. This provides users with choice regarding data collection thus allowing them to make informed decisions regarding the release of his information it is easy to conclude that tamper-proof technical protection mechanisms such as strong anonymization and encryption are the only solutions to such privacy threats. However, we argue that such perfect protection for personal information will hardly be achievable, and propose instead to build systems that help others respect our personal privacy, enable us to be aware of our own privacy, and to rely on social and legal norms to protect us from the few wrongdoers. We introduce a privacy awareness system targeted at ubiquitous computing environments that allows data collectors to both announce and implement data usage policies, as well as providing data subjects with technical means to keep track of their personal information as it is stored, used, and possibly removed from the system. Even though such a system cannot guarantee our privacy, we believe that it can create a sense of accountability in a world of invisible services that we will be comfortable living in and interacting with [10].

**VII. POLICY-BASED DATA ACCESS**

Once data has been solicited from the user (either actively by receiving a data submission via the privacy proxy, or implicitly by receiving sensor data such as video or audio feed), it is stored in a back-end database (not shown in figure 1 above). In order to prevent accidental use of information that is in disagreement with the previously granted privacy policy, the database not only stores the data collected, but also each individual privacy policy that it was collected under. By combining both data elements and their respective policy into a single unit managed by the database, we can have the database take care of observing that the promises made in a privacy policy with respect to the lifetime, usage, and recipient of a certain piece of information are kept, as well as provide users with a detailed “usage log” of their personal data (recourse). Note that since policies are often invariant for a large number of collected data elements, storing an
additional pointer to such a policy only adds a small overhead for storage requirements [10].

VIII. MACHINE-READABLE PRIVACY POLICIES

Privacy policies are an established principle in legal domains to codify data collection and usage practices. Within the “Platform for Privacy Preferences Project (P3P),” the World Wide Web Consortium (W3C) recently finalized work that allows the encoding of such privacy policies into machine-readable XML, allowing automated processes to read such policies and take actions on them [16]. Figure 2 shows an abbreviated example of such a P3P privacy policy. It contains XML elements. For a more detailed explanation of the XML syntax see [16]. Using a similarly machine-readable preference language such as APPEL [15], users can express personal preferences over all aspects of such policies and have automated processes judge the acceptability of any such policy, or prompt for a decision instead. Since it might be cumbersome to manually create such preferences from scratch, a trusted third party (e.g., a consumer interest group) could provide preconfigured preference specifications that would then be downloaded and individually adjusted by each user. Together with some domain-specific extension (e.g., location), these mechanisms allow data collectors in a mobile environment to specify data collection, storage and distribution parameters that can be automatically processed by user clients (choice and consent). It is important to note that typical environments will involve a reasonably small number of policies, even though a large number of sensors and data exchanges might be present, since policies are typically on a per realm or task basis. This means that the setup of a mobile environment with P3P policies is quite feasible.

IX. POLICY ANNOUNCEMENT MECHANISMS

While P3P is a Web technology and thus uses HTTP-headers as well as well-known URI-locations on each Web server to help user clients locate such policies, we need an alternative mechanism in a mobile environment. We can differentiate between two types of data collection that will need different ways of communicating such privacy policies to the data subject (notice):

Implicit announcement: In many cases, the user client is actively locating and using a service offered by the environment. In this case, we embed links to the P3P policy (or even the policy itself) into the service discovery protocol, such as the one in Jini [17].

Active policy announcement: Some services such as audio or video tracking might work continuously in the background, without the need for user interaction in order to gather data. In this case, a privacy beacon must used that constantly announces the privacy policies of implicitly running data collections, using a short-range wireless link.

X. PRIVACY PROXIES

Privacy proxies handle privacy relevant interactions between data subjects and data collectors (i.e., policy access and data collection) but also provide access to specific user control capabilities disclosed in the privacy policy such as data updates and deletes, or querying usage logs. Privacy proxies are continuously running services that can be contacted and queried by data subjects anytime, allowing them instant access to their data. Each mobile environment either features a single such service proxy to handle all its data collections, or multiple service proxies for each individual service it offers. Similarly, each user is expected to have a corresponding personal privacy proxy, which handles all interaction between service proxies in order to exchange user data or query their usage logs (in case of disconnects, a mobile device could temporarily act as a substitute for a personal privacy proxy residing on the network). Privacy proxies are configured using a preference language such as APPEL, described above, and typically involving small set of general rules (which could be created by a trusted third party and downloaded by the user) and a larger set of specific rules incrementally created by the user. As part of such an interaction between user and service proxies, an agreement is made in form of an XML-document containing the data elements exchanged and the privacy policy applying to them (both is encoded in the P3P policy). Such an agreement document also contains an explicit agreement-id for later reference, as well as detailed information on how the user proxy can access the service proxy (see our extensions to the ACCESS element. Should the user decide to update her email address with all places that have it on file, her privacy proxy contacts each service’s update function to transparently update the changed data (access).

XI. SHARED PRINCIPLES

Mobile privacy and identity management is realized to implement the following main principles.

• Confidentiality: The guarantee that information is read only by the intended receiver. In turn, confidentiality can be split into three main elements: integrity of message content, protection of location information (location-based information should be related to a specific user and device only with her consent) and support for sender/receiver anonymity. The latter element can be seen as relying on mobile terminals being capable of revealing SIM authentication data only in well-defined situations and to Well-defined partners; in all other cases, users are capable to act under a pseudonym without revealing the true identity.
- **Integrity**: Transmission of information is executed by using cryptographically mechanisms (symmetric and asymmetric) to identify and detect eventual manipulation of information.
- **Accountability**: Information exchange by using encryption techniques and digital signatures is very important for security and trust.
- **Notice**: An alert service must be available to draw the user's attention to situations in which privacy and security could be affected. Notice mechanisms should be manual whenever automatic solutions could compromise user's security.
- **Data collection**: Users should be able to actively manage their own data, deciding whether and which identity presented to device and applications [18]. Data collection must be inspired to the principle of data minimization, by which data should only be collected for a specific purpose.

**XII. SUMMARY AND FUTURE WORK**

The idea of combining data with metadata governing its use is already popular for enforcing digital copyright [11]. Successful implementation of this concept, however, requires use of so-called “trusted systems” [12] along the whole distribution chain, otherwise it would be fairly easy to separate data and metadata again. In contrast to digital media systems, we are not aiming for hacker-proof data protection but instead assume that the added-value of our trusted system pawDB (i.e., having the system make sure that data collector honors privacy policy without costly manual verification) will make its usage popular among data collectors. Of course, it will still be important to add legal requirements to that effect that provide a reasonable recourse mechanism for the few abusers present. pawS can also be combined with popular privacy solutions currently developed for the Internet, such as anonymizing proxy, such as anonymizer.com, thus masking the proxy’s identity on the network level and decoupling it from the user’s identity. Other popular tools such as Mix-based networks [13] could easily be employed for all wired network communications. If available, pawS components could also use anonymizing techniques on the physical layer as well (e.g., transient MAC-addresses, etc.). Similarly, it should also be possible to incorporate identity management techniques [14] into this framework: every time a data exchange is requested, the user’s system can respond with different data set. However, one needs to remember that anonymity and pseudonymity in general might be less useful in a mobile environment than on the Internet, simply because real-world data is much more difficult to anonymize completely. With privacy proxies and pawDB, two important components of our pawS architecture have been implemented. Our next step is to fully integrate the two components, as well as implementing privacy announcement mechanisms such as privacy beacons or Jini-integrated policy links. Using the P3P extension framework, a mechanism for describing dissemination practices based on the location of the data collection (i.e., the locality and proximity principle from section 2) needs to be incorporated into privacy proxies and pawDB. Once a corresponding user interface has been devised, a user-study will finally need to show how useful a tool such as pawS will be. In any case, the scope of pawS will remain deliberately limited at providing users of ubicomp environments with a privacy-enabler, not with a tamper-proof privacy protector. As we move around in a ubicomp environment, our personal privacy assistant will keep track of all data collections happening with and without our help. Whenever possible, our assistant will enable or disable optional services, based on our preferences.

Instead of alerting us to unwanted data collections, however, it might be more useful as a silent but watchful transparency tool keeping track of whom we leave our personal data with. While the actual inspection of its large logs, as well requests for data deletion or updates might be less frequent for the individual user, it is the few cases when we need to know what is going on where it will prove invaluable to us or any consumer interest group, trying to hold data collectors accountable to their privacy statements [10].

**REFERENCES**


[15]. Lorrie Cranor, Marc Langheinrich, and Massimo Marchiori. “A P3P preference exchange language 1.0 (APPEL1.0)”, www.w3.org/TR/P3P-preferences, 2002
[16]. Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, and Joseph Reagle. “The platform for privacy preferences 1.0 (P3P1.0) specification”, www.w3.org/TR/P3P1/, 2002