Mobile Identity Management

enisa
European Network and Information Security Agency

www.enisa.europa.eu

Editor:
Maria Papadopouli, University of Crete & FORTH, Heraklion, Greece, mgp@ics.forth.gr

Contributors:

- **André Årnes**, *Oracle Norway/ NISlab, Gjøvik University College*, Norway,
- **Jorge Aguado Bombin**, *ISDEFE Madrid,* Spain
- **Elisa Boschi**, *Hitachi Europe & ETH Zurich*, Zurich, Switzerland,
- **Sonja Buchegger**,*Technische Universität*, Berlin, Germany
- **Raul Benito Cortiñas**, *Isdefe*, Madrid, Spain
- **Francesca Gaudino,** *Baker & McKenzie*, Italy
- **Giles Hogben**, *ENISA*, Heraklion, Greece
- **Thomas Karagiannis**, Microsoft Research, Cambridge UK
- **Charalampos Manifavas**, *University of Crete*, Heraklion
- **Katerina Mitrokotsa**, *Delft University of Technology*
- **Nikos Nikiforakis**, *Katholik Universitat* of Leuven, Belgium
- **Panos Papadimitratos**, *EPFL*, Lausanne, Switzerland,
- **George Roussos**, *Birkbeck College*, *University of London*, London, UK,
- **Katerina Tsakona**, *FORTH*, Heraklion, Greece

Group members participate as individuals. This position paper should therefore not be taken as representing the views of any company or other organisation, and does not in any way bind group members when dealing with the issues it covers in other contexts.

Executive Summary

This position paper reports on information security risks and best-practice in the area of Mobile Identity Management (Mobile IDM). It also provides recommendations of systems, protocols and/or approaches to address these challenges.

Principal Risks

- **Identity theft:** Mobile devices contain a wide range of personal information (including even personal credentials, such as encryption keys or biometric data), making mobile devices a gold mine for identity thieves. An important possibility which increases the severity of this risk is the theft of the actual device. This underlines the need for a more robust identification mechanism through the digital footprint of a user or a device.
- **Eavesdropping and spyware:** Weaknesses in GSM and 802.11x encryption make such attacks relatively easy [97]. In GSM, encryption is only applied for the wireless transmissions, that is, the messages are sent in plain text from the Base Station to the gateways.

  Infrared and Bluetooth applications aiming at swift information exchange (contacts, multimedia files) among cellular phone owners offer primitive authentication and access control mechanisms while blindly trust any content received over the air.

Users pair Bluetooth-enabled devices by entering a secret PIN number. While the PIN provides an authentication, this user involvement makes the system less user-friendly. Moreover, studies have shown that Bluetooth pairing is susceptible to eavesdroppers [35,36,37].

Finally, mobile devices have been designed without appropriate defences against malware. For example, attacks may target smart-phones to obtain address books and telephone directories stored locally through physical access to the phone or by exploiting a vulnerability of its installed software.

- **Surveillance:** Even without knowledge of the content of communications, traffic data or localized EMEI (International Mobile Equipment Identity) data can be used for unauthorized monitoring or surveillance. Such an attack or unintended disclosure can potentially reveal large amounts of personal information and provide a detailed profile of an unsuspecting user, unless the network monitoring is properly secured [90-92].

  It should be noted that mobile device users could be monitored both through network monitoring and through various sensors in their physical surroundings. A network of physical sensors could potentially monitor the movement and position of thousands or millions of mobile devices, e.g., using RFID network interfaces.

- **Phishing:** Mobile identity management systems are vulnerable to phishing attacks due to their low-footprint user interfaces, which make authentication of the communication counterpart more difficult.

- **Collection and storage of private information beyond the stated purpose:** Frequently service providers obtain more personal information than necessary to perform the service. Often, a large amount of information is collected from users in case it is required in future.

- **Failure to recognize context:** As different contexts (e.g., customer of an online service, member of a social network, game player) require different identities, users possess a variety of identities in the digital world. Efficient management of a a large number of identities and deciding the extent to which identities may be shared across different service providers is important. However, the recognition and characterization of the user context in order to retrieve the appropriate identity without interrupting them from their main tasks is a challenge.

- **Inadequate device resources**: Authentication algorithms used in cellular and IEEE802.11 networks have been compromised. Several security concerns can be mitigated with the use of strong encryption for all transfers. However, stronger algorithms demand higher processing power, imposing technological challenges to the mobile devices with limited resources.
  Mobility also presents a number of unique constraints compared to fixed line systems. A mobile device may experience frequent disconnections from the Internet and/or an infrastructure, supports limited functionality, in terms of user

interaction, and has limited resources, in terms of bandwidth, processing, power, display, and storage capacity.
Many privacy protection mechanisms assume the existence of a trusted third party that can certify the credentials of a service provider. This also requires connectivity to the trusted third party or reliance on public key infrastructure. However, in a mobile context, continuous access to such infrastructures cannot always be assumed.

- **Intrusive authentication:** Authenticating the user in a non-intrusive way is still a research challenge. One approach is using biometric data, in the form of a physiological or anatomical attribute or a distinctive behaviour, which enables checking of (mostly) unique biological characteristics submitted by an individual with previous biometric reference data. However, this may not be always effective or even feasible for remote authentication. The development of biometric authentication requires the construction of biometric models for each person, which is a relatively new research area.

- **Lack of user awareness:** Users should be aware of the extent to which personal data are revealed to service providers. At the same time, it is a challenge to provide users with intuitive control mechanisms (through user-friendly GUIs) to both handle their identities and also perform operations on them, such as revocation of information and separation between domains using multiple identities.

Legal analysis

The paper presents an analysis of the most important legal considerations for mobile identity management, including:

- A summary of applicable legislation
- An analysis of provisions present in European Legislation regarding location data.
- Transparency requirements for mobile IDM–information which must be given to the data subject.
- Consent requirements for mobile IDM and their application to geo-localization services.
- The right to withdraw consent and its application in the mobile IDM context.
- Data retention considerations.
- Security measures applicable to service providers and transmission to third parties.

Recommendations and conclusions

The main conclusions are expressed as a set of design objectives, including:

User-experience: The system should provide the appropriate information to the user that allows him/her to decide about a transaction minimizing the intrusiveness and interruptions. A mobile identity management mechanism needs to identify the user and his/her context in an efficient manner: minimizing the delay, the number of false identification results, and the user interruption. This problem becomes challenging given that devices may need to process and correlate information across various devices which may be out-of-date or even false and not all devices and applications may have the same

rights to access these data. Systems should also describe in a concise manner their privacy policies. Many privacy policies and their implications of their configuration are not well-understood by end users. This involves research in domains that span from networking and systems to contextual information representation and reasoning, and graphics.

Access and authorisation: A management system must transparently handle the access rights that are pertinent to each identity and relevant to the particular service. Password or profile management must allow users to easily change passwords or handle cases of forgotten passwords. An efficient management system should assist users in creating strong passwords. Users must be provided with intuitive controls to both handle their identities and also perform operations on them, such as revocation of information. The means of control should be visible and its results verifiable. This can be especially challenging in mobile devices, in which screen size is limited and typing can be hard.

Scalability: Mobile identity management systems should not only be cost-effective and scalable from the perspective of the operators and/or service providers but also from the perspective of users. Often users are required to memorise multiple passwords for accessing different services. This may represent a minor inconvenience, when a user accesses only a few online services.

Resilient connectivity: Many attacks on mobile IDM systems rely on isolating the "target" from the rest of the network, effectively depriving it of crucial information. Such attacks can be prevented by the provision of reliable connectivity, along with more resilient networks, and the support of strong crypto mechanisms.

Malware defences: Security mechanisms should be implemented to resist compromise by malicious software. Such mechanisms include antivirus software and frequent patching. They should only allow trusted and certified software to be executed on the device. Moreover, any communication that is part of the identity management protocols must be protected through the use of appropriate encryption to ensure confidentiality and integrity.

Control over privacy settings: It is important to provide tuneable privacy protection mechanisms and tools for automatic customization and personalization of services. For example, a user may choose to reveal his/her geographic location in exchange for maps or information about local points of interest, or in a different scenario, may decide not to, because of the potential security and privacy risks.

Delegation: In general, privacy-preserving delegation mechanisms need to consider the following criteria [74]:

- Authentication without revealing identifying data
- Non-linkability of transactions
- Least privilege, in which only credentials related to the purpose of a delegation are given to the service provider/proxy (least privilege)
- Preventing misuse of delegated credentials
- Restricting re-delegation of a credential
- Revocation of a credential

Accountability: Service providers should nevertheless be able to attest the accountability of their users. A privacy preserving delegation mechanism guarantees these interests, if it fulfils the following criteria [74]:

- Non-repudiation of using a credential
- Provision of necessary identity attributes

Identity selection and composition: Another important issue is the determination of the attributes (data fields) that will compose the mobile identity and the collection mechanisms. Specifically, the collection mechanisms need to indicate which parties (e.g., network operators, government office, professional organization, employers, law enforcement agencies, and profile providers and/or service provides) in addition to the mobile user should participate in the generation of a mobile identity. Furthermore, users should be able to understand the separation of the various identities across service domains and providers.

Introduction

Mobile devices, integrated with positioning systems and enhanced with more powerful hardware are entering a new era offering attractive new functionality. At the same time, they are becoming easier to use and more pervasive. In effect, people are depending more and more on mobile information wherever they are. People access local and international news, traffic or weather reports, sports, maps, guide books, music, blogs, calendars, electronic payments, video files and games via the mobile Internet. On-line collaboration and social networking tools have amplified the trend towards information sharing and online access via mobile devices. New "bio-sensors" may be linked to mobile devices to monitor various health conditions (e.g., diabetes) in the context of diagnosis in e-health environments [39, 53-56].

Studies predict that the mobile payments market (including banking transactions) will exceed $587 billion by 2011. An example of payment via mobile phones is Mobile Suica using the Edy and Sony's FeLiCa chip technology [38], mainly used for payment on the JR East railway network in Japan. Similar to FeLiCa, NFC supports banking and e-cash applications in Europe. Recently RFID-enabled mobile phones (e.g., Mobile Payment Skins [82]) have been developed for payments at RFID-enabled point-of-sale terminals.

This growing deployment of mobile services and applications results in a wealth of sensitive personal information (e.g., user's identity, payment information, user preference and usage history). Given the vulnerabilities and constraints of mobile devices and wireless communications, if the system is not designed appropriately, there is a risk that adversaries can intercept the communication of mobile devices with the infrastructure/service provider. Such threats jeopardise the penetration of mobile services.

Given that different platforms, service providers, organizations, business processes, policies and technologies may be involved as an individual performs various transactions while this user is roaming, an identity management system is required to ensure the validity of these transactions between service providers and the specific user, in a seamless way, minimizing the management overhead, protecting user data, and resources and services. For roaming users, the various domains should be able to communicate and verify the identity of the user/device at the home domain, assign a new local and often temporary identity for the foreign domain the user/device is now visiting, and perform accounting.

Sometimes, user transactions may be performed with an identity which is not linkable to the official, civil identifiers of the person, such as social security number, nonetheless, it is required that the user discloses a variety of other identity attributes that are not necessary for the transaction. In other situations, the use of certain technologies (e.g., web-based interfaces, IEEE802.11 access) can "leak" private information (e.g., about the user's

location[1]). Thus, a wealth of sensitive personal information is publicized and if the system is not designed appropriately adversaries can intercept the communication of mobile devices with the infrastructure/service provider. We now describe two examples of use cases that address important mobile identity management issues. The remaining sections discuss these issues in more detail.

"Use case 1"

Consider a government issued identifier used to provide secure access to citizen services, such as health-, tax-, and education-related services. Using such an identifier, an EU citizen could check the availability of and book health services while travelling across Europe from his/her mobile device. The application using this service could be critical, e.g., by providing emergency alerts with diagnostics and blood type information for persons with life threatening diseases. Such a service could potentially provide quick and appropriate reactions to a medical emergency with increased probability of success.

Data may be accessed across borders between EU countries. The user has to be authenticated, ideally with minimum effort, based on his/her home country user database, and then access has to be provided by the service in the country visited. Apart from authenticating the user, the system should be able to recognize his/her context (e.g. location) retrieve the appropriate information (e.g. medical records) which could be stored across various platforms (e.g., networks, databases, and organizations), and later, update the system with the newly obtained information about the patient status, diagnostics, accordingly. The system should be able to detect and prevent attempts of unauthorised use and privacy should be guaranteed.

The critical assets are the user's private information (e.g., medical records, position history), and the system's availability and responses (e.g., emergency medical alerts, reports).

"Use case 2"

A location-based service (such as Google Latitude) is integrated with a digital identity service to provide access to commercial services, such as Amazon, Facebook and Google Maps based on the user's location. As an example, user preferences are derived from his/her Amazon and Facebook profiles correlated with the user's location and Google Maps data to provide the user with an updated Google Maps overview of his/her most relevant businesses and local offers.

In this use case, the critical assets include the private information of the user, such as his/her credit card number, position history, and preferences for certain products.

Section 3 and 4 will discuss the vulnerabilities and threats relating to these use-cases in detail. Specifically, in Section 4.3, these two use cases are discussed in detail. Before that, in Section 2, we set the background by defining some important concepts, namely, mobile

[1] *Because of the wide-deployment of wireless access points, this issue should not underestimated.*

identity and mobile identity management, personal data and privacy, security, authentication, authorization, and federation of identities. Section 3 presents various threats in mobile identity management while Section 4 discusses the objectives and challenges in the design of mobile identity management. In Section 5, we review current approaches in the mobile identity management. An overview about the legislative issues and privacy can be found in Section 6. Finally, Section 7 summarizes our recommendations and conclusions.

1. Background

The following paragraphs introduce some important concepts on mobile identity management and security.

1.1 Mobile identity and mobile identity management

For the purposes of this paper, an *identity* is a set of claims about an individual in a specific application context. Identities are usually related to real-world entities, e.g., people, organisations, and devices. A digital identity fundamentally requires digital identifiers—strings or tokens that are unique within a given scope (globally or locally, within a specific domain, community, directory, application). Identifiers are used by the participating entities to establish an identification relationship to agree on the entity being represented. Identifiers may be classified as *omni-directional* and *unidirectional*; the former are intended to be public and easily discoverable, and the latter private and used only in the context of a specific identity relationship [73].

Identity systems not only maintain and manage personal electronic information (credit card numbers, biometrics, personal health records, and personal preferences) but also are the channel through which entities communicate, interact, transact, share reputations and create trust relationships with people, businesses, and devices. The operations performed to support the lifecycle of the digital identity are referred to as identity management [30].

A person, organisation or device may have zero or more identities within a given domain. For example, a person may have two identities in a school system because he or she is both a parent and a teacher at the school. The rules for registering identities within a domain determine whether multiple identities for one entity are permitted. Even if forbidden, multiple identities for the same entity may still occur in the system, e.g., in error or because of fraud. Different identities can be employed in different domains. For example, a person may have one identity associated with being a customer in a bank and another identity associated with being an employee in a company. Social networking and on-line collaborative systems also trigger the need for defining various group identities (e.g., colleagues, friends, private, family).

Mobile identity is an extension of the digital identity which may be divided into three classes (and their combinations): *device-to-device, location-to-location, and context-to-context.*

In device-to-device identity, mobile identity can be used in the certification process to attest the authority of a particular individual to gain access to a specific resource while

using different devices. Note that we distinguish the identity of a device—often related to a specific user—and the identity of an individual. This position paper emphasizes the need for a user-centric mobile identity management.

In location-to-location identity, the mobile identity can be used in the certification process to attest the authority of a particular individual to gain access to a specific resource/service while moving in a different geographic area.

In context-to-context identity, the device may need to "select" the most preferable identity depending on the context – e.g. the people in their proximity.

Contextual information can play a key role in terms of allowing the device owner to set privacy rules which depend on dynamic context data. For example, a policy can be set where access to specific information is either granted or restricted based on the location of the requesting user or device.

1.2 Personal data and privacy

Private information, ranging from identity attributes (e.g., biometric elements) to proofs of private/secret tokens (cryptographic keys, passwords) and credentials and to location, can be critical for the functionality of mobile computing and context-aware services.

In the EU data protection directive [21], **personal data** is defined to be "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".

Privacy refers to the right of persons to have control on the processing of their (personal) data and to be enabled to determine for themselves, when, how and to what extent information about them is communicated to others[2].

[2] P*rivacy viewed as an individual right constitutes a fundamental human right, although there is no universally* accepted privacy law/definition among all countries*, still, most countries have somehow recognised the right to privacy at international, European and national level by virtue of article 12 of the Universal Declaration of Human Rights, a*rticle 8 of the European Convention on Human Rights *accordingly and* article 9 of the Greek Constitution (for instance); As such s*ee Article 12 of the Universal Declaration of Human Rights "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[94]*; Article 8 of the European Convention on Human Rights guarantees the right to respect for private and family life, one's home and correspondence [95]. In terms of constitutional law, see article 9 of the Greek Constitution providing similar recognition as above. Further to the above, the right to privacy when viewed in relation to the processing of personal data, see article 1 et seq. of the Directive 95/46/EC.

1.3 Security, authentication, and authorization

Security aims at preventing attackers from violating security policies, the detection of attacker's violations of security policies, and the assessment and repair of the damages, and continuing operating even when the attack succeed.

A *security risk* is defined as the potential that a given threat will exploit the vulnerabilities of a system. In general, vulnerability is defined as a weakness which leads to a threat. A security risk is measured by the impact multiplied by the probability of the threat to occur.

1.4 Identity federation

Various services depend on authentication mechanisms that enable smart and automatic user registration and ensure smooth identity transition across service providers (e.g., mobile operators). *Identity federation* can be defined as the set of agreements, standards and technologies that enable a group of service providers to recognise user identifiers and entitlements from other service providers within a federated domain. These agreements include policy and technology standards, resulting in a single virtual identity domain. *Federation* refers to mechanisms for cross-domain authorization, while *provisioning* refers to the provisioning of users from authoritative systems to subsidiary systems. In addition to federation, provisioning may be necessary in the backend systems. The automatic registration initiated by an authoritative system is provisioning.

Federation is essential in both use cases in order to provide authorization and govern access control. In the first use case, federated access has to be provided cross-border, i.e., access control mechanisms have to be able to access citizen databases for each participating country.[3] In the second case, federated access has to be provided across corporations with different user policies. The corporations involved will have to have a trust relationship that governs the federation policies. The technical challenges involve the sometimes daunting task of integrating proprietary and non-standard systems with federated authorization systems. In order for users to exist in, e.g., hospital services and applications (as in the first use case) or in customer databases (as in second use case), users have to be registered either manually or automatically. In the case of federation, the systems involved are required to have trust relationship that governs the provisioning processes. Provisioning can also be technically challenging from an integration perspective, as automated identity management on proprietary and non-standard systems may be hard.

[3] *In Norway, for example, federated authorization for citizens is provided by the "MinID-service" [28], but this is not specifically aimed at mobile services.*

2. Threats to mobile identity management

2.1 Identity theft

Identity theft is a serious and widespread crime. The Federal Trade Commission reports that over a quarter of a million identity theft complaints were received in 2005, in addition to over 430,000 other fraud complaints. Internet-related complaints accounted for almost half of those [66].

A mobile device can be targeted for identity theft by malicious attackers. Identity theft can be performed by stealing permanently or temporarily security credentials, by using the trusted mobile device as a proxy for performing the attack, or by stealing the actual device. This threat can potentially be used to access public and government services in order to get access to private data or to breach the integrity of private data (e.g., through unauthorized address changes).

In the case of mobile identity management systems, the devices in question may contain a wide range of personal information (including even personal credentials, such as encryption keys or biometric data), making mobile devices a gold mine for identity thieves. The severity of this threat underlines the need for a more robust identification mechanism through the digital footprint of a user or a device.

2.2 Eavesdropping and spyware

Due to the vulnerable nature of wireless communications, eavesdropping is one of the most challenging threats against mobile identity management. In many cases, communication can be intercepted without authorization. Users are not aware that eavesdropping can occur (or has occurred) while they are communicating. Infrastructure deployed by other providers or for completely different purposes (e.g., IEEE802.11 WLANs in the form of mesh or city-wide networks) can be used by their owners or by wire-tappers to eavesdrop other communications. Weaknesses in GSM and 802.11x encryption now mean that data can be read by an attacker relatively cheaply [97].

Information at risk includes geographical locations, communications, financial transactions, purchases, preferences, critical personal information—such as medical data—and profile information. Information related to the position of an individual or her association with specific objects can be exploited by adversaries to enable other more direct type of attacks.

Infrared and Bluetooth applications aiming at swift information exchange (contacts, multimedia files) among cellular phone owners offer primitive authentication and access control mechanisms while blindly trust any content received over the air, resulting in emerging threats, such as Bluetooth-propagating worms.

Mobile devices have been designed without appropriate defences against malware. For example, attacks may target smart-phones to obtain address books and telephone directories stored locally through physical access to the phone or by exploiting a vulnerability of its installed software.

2.3 Surveillance

Even without knowledge of the content of communications, traffic data or localized EMEI data can be used for unauthorized monitoring or surveillance. Such an attack or unintended disclosure can potentially reveal large amounts of personal information and provide a detailed profile of an unsuspecting user, unless the network monitoring is properly secured [90-92].

It should be noted that mobile device users could be monitored both through network monitoring and through sensors in their physical surroundings. A network of physical sensors could potentially monitor the movement and position of thousands or millions of mobile devices, e.g., via RFID interfaces.

Recent studies have analyzed the human behaviour and daily routines using real-life data collected with mobile phones [57-59]. This analysis shows that wireless communication can be easily used to track people and create patterns of human behaviour regarding their physical location or their social activities.

2.4 Phishing

Phishing is the process of acquiring and/or manipulating private or confidential information through masquerading as a trustworthy entity. Phishing can be performed through the use of malicious software, network attacks, or the use of forged emails. User and bank accounts worldwide have been compromised through the use of simple phishing techniques.

Mobile identity management systems counter phishing attacks through the use of sound authentication and cryptographic mechanisms. Raising the user awareness can also have a prominent impact.

2.5 Man in the middle attacks (MITM)

An attacker operates as a man-in-the-middle between a mobile device and its trusted services. The attacker can use this to monitor users or, even, launch an identity theft attack against users.

2.6 Illegitimate utilization of interception software

Providers of communication services are required to have in place appropriate technical measures that allow lawful interception of communications.

The legislation on lawful interception is differently implemented in the various countries. However, as a general principle, usually the communication service provider is not necessarily the one expected to perform interception activities itself, rather it is the one expected by law to allow the competent enforcement authority to intercept the communication that is generated by the services of the providers. However, if the competent authority is unable itself to perform interception activities, the authority may delegate the service provider to perform interception and then to provide the authority with the relevant data.

With regard to the latter scenario, there have been cases where service providers, or malicious intruders working for the service provider, have used the data collected on behalf of the competent authority for their own interests, or have used the technical means in place to perform interception activities out of the scope of the requests of the authority.

The CSO of Telecom Italia was accused of having unlawfully gathered information and personal data on a wide number of individuals by using the technical device in place at Telecom Italia [93]. Another example is the Vodafone Greece case [83], centering on the collection of the conversations of specific government and military officials.

2.7 Collection and storage of private information beyond the stated purpose

Frequently service providers obtain more personal information than necessary to perform the service. Moreover, appropriate security mechanisms are not always taken to ensure privacy or anonymity of information. Existing services may use software in which security is obtained by speculative collection of data, that is, a large amount of information is collected from users in case it is required in future.

2.8 Vulnerable software

Applications running on mobile devices may contain program errors that could potentially allow an attacker to compromise the mobile device (e.g., buffer overflow, code injection).[4]

2.9 Failure to recognize context

As different contexts (e.g., customer of an online service, member of a social network, game player) require different identities, users possess a variety of identities in the digital world. A challenge in managing a large number of identities is deciding the extent to which identities could be shared across different service providers, in order to identify architectures and abstractions suitable to store, retrieve and manage efficiently this common set of identities.

The recognition and characterization of the users' context in order to retrieve the appropriate identity without interrupting them from their main tasks is an important challenge.

2.10 Inadequate device resources

Authentication algorithms used in cellular and wireless networks have been compromised. Several security concerns can be mitigated with the use of strong encryption for all transfers. However, stronger algorithms demand for higher processing power, imposing technological challenges to the resource constrained mobile devices.

---

[4] *This threat has already materialized on a large scale for online banking on the Internet. Millions of Euros have been lost to online bank fraud performed through the use of malicious software.*

Mobility also presents a number of unique constraints compared to fixed line systems. A mobile device may experience frequent disconnections from the Internet and/or an infrastructure, supports limited functionality, in terms of user interaction, and has limited resources, in terms of bandwidth, processing, power, display, and storage capacity. This requires the use of seamless identity management solutions with high usability as well as solutions that support low-connectivity and off-line use with limited resource usage.

Many privacy protection mechanisms assume the existence of a trusted third party that can certify the credentials of a service provider. This also requires connectivity to the trusted third party or reliance on public key infrastructure. However, in a mobile context, continuous access to such infrastructures cannot be assumed. Finally, the system architecture design needs to also address the scalability issues, given the growth of various service providers.

2.11 Threats to protocols

Devices that would support such mobile electronic identification mechanisms are vulnerable to different types of threats, such as impersonation, eavesdropping on personal data, and dissemination of false information, viruses, and spam. These vulnerabilities and constraints make the provisioning of privacy, confidentiality, and security a challenging task, especially given the resource constraints of mobile devices. For example, users pair Bluetooth-enabled devices by entering a secret PIN number. While the PIN provides an authentication, this user involvement makes the system less user-friendly. Moreover, studies have shown that Bluetooth pairing is susceptible to eavesdroppers [35-37].

GSM faces also several weaknesses: For example, the encryption is only applied for the wireless transmissions, that is, the messages are sent in plain text from the Base Station to the gateways. It is necessary for a Mobile Station to transmit its current location in short periods to the Base Station. This can be abused to track and record the movement profile of a subscriber.

2.12 Intrusive authentication

Authenticating the user in a non-intrusive way is still a research challenge. One approach is using biometric data, in the form of physiological or anatomical attributes or a distinctive behaviour, which enables checking of (mostly) unique biological characteristics submitted by an individual with previous biometric reference data. However, this may not be always effective or even feasible for remote authentication. The development of biometric authentication requires the construction of biometric models for each person, which is a relatively new research area.

An important issue that opens up several challenges is the problem of compromising certain unique biometric data of an individual: once such data are compromised (e.g., stolen), it is not possible for that individual to obtain "new" ones [76]. In general authentication using biometric data may involve a number of risks (e.g., spoofing and mimicry attacks, face reference template, intercepting transmission, data alteration during enrolment, brute-force attack, injection, users' rejection due to its invasive nature). However, a parallel evolution of the attacks may also occur. Attacks against a person to

obtain his fingerprints or retinal scan (coercion or worse) are much more dreadful than stealing passwords with a keylogger or brute force.

2.13 Lack of user awareness

Increasing user awareness and educating users is also a challenge. For example, studies in online social networks have shown that users do not really comprehend the extent to which their private information is disclosed to their "friends" [41]. Users should be able to understand the separation of the various identities across service domains and providers. Furthermore, users should be aware of the extent to which personal data are revealed to service providers.

4. Current approaches to mobile identity management

This section describes various approaches to address various issues related to mobile identity management.

4.1 EU projects

The PRIME (Privacy and Identity Management for Europe) project [17] focused on privacy enhancing identity management with an emphasis both on identity management on the Internet, as well as, on active protection of privacy. Example applications of PRIME include location- and eGovernment-based services and social networking-based applications running on mobile devices. Their objective is the development of a framework and working prototypes related to collaborative eLearning, location-based, and airline and anonymous. A white paper with a use-case analysis and discussion of issues related to human-computer interaction, public awareness, and economics can be found in [77].

The FIDIS Network of Excellence [18] is a consortium of partners with a long-term objective to develop a deeper understanding of how appropriate identities and identity management can progress the way to a fairer European information society. They focused on methods/frameworks for identifying individuals and digital identities, and investigated interoperability, ID theft, privacy, security, profiling and forensic implications.

The MODINIS project [78] studied identity management in eGovernment, held five workshops, and published several reports and newsletters related to the topic. It aimed to assess the impact of identity management initiatives related to eGovernment [79], provide a prospective analysis of possible initiatives and solutions (e.g., various identity technologies), and propose a methodology with actual use cases of good practices in identity management. It also published a comprehensive glossary [80].

4.2 Identity management in cellular networks and GSM

Considering identity management and privacy protection, it can be useful to look at standardized wireless communication technologies. At first, we take cellular networks and GSM as an example. GSM supports two forms of identity management, namely (a) the International Mobile Subscriber Identity (IMSI), and (b) the International Mobile Equipment Identity (IMEI). The IMSI identifies the subscriber and is stored in the SIM

card. However, these two attributes are identifiers and not an identity, as defined in this paper. The cell phone providers keep a database—Home Location Register (HLR)—which associates these IMSI with the subscriber data, composing the identity. The IMEI uniquely identifies the GSM equipment. Similarly to the HLR, a provider maintains an Equipment Identity Register (EIR) that stores the IMEIs of banned or monitored mobile phones. All the identity management within a network is completely managed by the provider, including authentication and revocation. In case of roaming between providers, they grant access to their HLR so authentication can take place. In cellular networks, the mobile nodes only attach and authenticate with the base stations of own or foreign providers (in case of roaming). Therefore authentication and especially generation and resolution of pseudonyms are straight-forward: the base station plus core network is considered to be trusted. In other heterogeneous and/or ad hoc infrastructures provided by multiple organizations which may not all be trusted this approach is not feasible.

In order to protect privacy by preventing tracking of devices, the Temporary Mobile Subscriber Identity (TMSI), a form of pseudonym, is assigned to a mobile device when it connects to a Location Area and replaces the IMSI. In the case of eavesdropping during the initial handshake, an attacker will be able to track the device by its TMSI later on. Mechanisms, such as the IMSI-catcher, reveal the vulnerabilities and concept failures of the system [81].

4.3 Identification in mobile ad hoc networks

To perform identification in mobile ad-hoc networks—that face intermittent connectivity to the Internet and to a trustee entity—the user's identities can be based on certificates, public/private key pairs or anonymous credentials. A taxonomy of these proposals can be found in pages 53-84 of [74].

4.4 Use of federated identity management tools

The management of identity could be performed with federated identity management models. Such models can be identity management "meta-systems", such as the Windows CardSpace [31] or the OpenID [32].

4.5 Biometric authentication

Authentication can be performed using biometric tools, including ones based on face, hand geometry, voice and iris recognition, keystroke dynamics, gait, retina, hand and finger veins, footprints, DNA, facial thermogram. For example, Motorola’s Mobile Automated Fingerprint Identification System (AFIS) is a handheld biometric tool that can capture fingerprint and facial images, analyze the data, and match this information against databases stored locally on the device, in centralized biometric matching systems, or on smart cards.

4.6 Secure hardware on mobile devices

Mobile devices with a high level of end-to-end security need a ‘secure element’ (SE) where private or secret keys are stored. The Mobey Forum identifies three categories of SEs: removable hardware, non-removable hardware, and software [18,29]. Depending on the

category, the SE could therefore be the mobile device's memory or an internal card, such as a Universal Integrated Circuit Card (UICC), containing the Subscriber Identity Module (SIM) application, or a secure digital (SD) or microSD card [29]. Secure Digital (SD) is a non-volatile memory card format developed for portable devices.

5.1 Legislative Issues and Privacy

5.1 Introduction and scenario

Recent technology advances in the area of hand-held devices are bringing about an increasing possibility of monitoring and tracking in the field of communications services, sensing technologies, location and context-aware solutions and services. These new services increase the possibility for the user to receive specifically fine-tuned information and services upon request. However, the same services are also posing the basis for monitoring and surveillance solutions that may represent a serious threat to the privacy of users. The gathering of personal and also of contextual data, in particular when they are combined with other various information stemming from different sources, combined to the fact that this information may also be disclosed to various infrastructure operators and service providers, poses a threat to the right to data protection of users.

The scenario from a privacy perspective is made more problematic by the circumstance that the user is often not even aware of the amount and kind of information that is gathered. Not being aware of the fact that his/her data are being collected, the user is prevented from ascertaining and defending his/her privacy rights.

The right to privacy has been clearly defined and ruled by data protection laws and regulations throughout Europe. The competent national data protection authorities together with the EU Commission have embraced the view that the technology solutions should be turned out from possible infringement of privacy rights to means to defend said rights. Indeed, the argument held is that technologies and related services should be technically structured and designed as of the very beginning, the initial stage of the relevant process, in a way that they allow to comply with the applicable data protection legislation.

5.2 Location data

Article 9 of the Directive 2002/58/EC[5] provides specific rules for the processing of location data other than traffic data, namely data that "*May refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal*

[5] *Directive 2002/58/EC of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication), O.J. L 201/37, 31 July 2002 (which has replaced Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector, O.J. L 53, 14 January 1998.*

equipment is located at a certain point in time and to the time the location information was recorded"[6].

The aim of the provision is to protect private life and confidentiality of the individual as to movements in relation to communications services based upon localization of users. Location data may be processed if the following requirements are met.

First of all, the user has to be informed of the processing of location data, including information on the type of location data that will be processed, the purposes and duration of the processing and the extent of data communication, notably if data will be transmitted to a third party providing the value added service or other third parties.

Further, location data may be processed only if they are made anonymous or with the data subject's consent. As to the consent, the data subject must be given the possibility to withdraw the relevant consent at any time, and must also be enabled to temporarily refuse the processing of location data for each connection to the network or for each transmission of a communication, at any time, through simple means and free of charge.

This might appear in contrast with the provision on the data subject's consent specified under the Directive 95/46/EC where one of the exemptions to the necessity to obtain the data subject's consent prior to starting the data processing is that the consent of the data subject is not required when the data processing is necessary to perform contractual obligations[7]. The reason of the different approach that requires the data subject's consent in case of processing of location data has to be identified in the circumstance that the legislator wanted to avoid lessening the level of data protection guaranteed to the individual in a sector deeply linked to a fundamental right such as the freedom of expression regarded as right to communication.

Without the consent requirement, the situation would have been as follows: when the data subject communicates to another person, it necessarily leaves traces (the traffic and location data). Once formed, these traces might be accessed and used by the providers of value added services for the provision of said services, without the data subject being informed or having consented to the data processing. Requiring the data subject consent avoids that the prior traffic and location data, formed as a result of the first communication of the data subject, could be used for providing further services[8].

Limitations relating to the persons that may process traffic and location data[9] and more generally the attention paid by the legislator to the processing of traffic data may be explained considering the peculiar nature of the data itself. Retention and processing of traffic and location data allow determining behaviours, preferences, activities, and

---

[6] *Recital 14 of the Directive 2002/58/EC.*

[7] *Article 7 of the Directive 95/46/EC.*

[8] *RICCARDO IMPERIALI, ROSARIO IMPERIALI, "Codice della Privacy Roma, Il Sole 24 Ore, 2005.*

[9] *Traffic data may be processed only by persons acting under the authority of the service or network providers and who are in charge of billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or value added services.*

movements of the data subject. Moreover, the amount of information that electronic communications services allow to gather and store is significant; hence the relevant processing encroaches forcefully into the private sphere of the individual and exposes the individual to serious privacy risks. Indeed, data relating to the activities performed on the Internet have regard to *"Not only the freedom to surf on the Internet, and thus the new and electronic version of the right to circulation, but also the freedom of thought and that of association, considering the increasing vocation of the Internet to represent an instrument of expression and organization for millions of persons"*[10].

Location data may moreover be processed only to the extent and for the duration necessary for the provision of the value added service. The processing of location data must be further limited to persons acting under the authority of the service or network provider or of the third party providing the value added service. Moreover, the processing that may be carried out is exclusively the one that is functional and necessary to the purposes of providing the value added service.

In principle location data may be processed only if made anonymous. Location data in identifiable form may be processed only with the consent of the data subject, which must be preceded by an information statement particularly strict as to content requirements. The consent may always be withdrawn, also temporarily, by the data subject. The persons accessing and using location data must be limited in number, clearly identified, and must act under the supervision of the service or network provider or third party providing the value added service.

New technologies allow precise localization and tracking of the movements of the individual that uses electronic communications services and go beyond geographical boundaries. The risk is that such a tracing might result in invasive surveillance of the individual's life. The Directive 2002/58/EC has thus provided for special safeguard for the processing of location data.

With regard to the processing of location data for providing value added services, the Article 29 Data Protection Working Party ("Working Party")[11] issued a document on the use and processing of location data for value added services in its opinion adopted on 25 November 2005[12]. The Working Party holds the view that the issue of location data is very topical, since the development and sharp spread of new technologies capable of gathering and processing 'traces' left by the individual, such as satellite and mobile telephone technologies, have increased enormously the possibilities of gathering location data. In the

---

[10] *Presentation of S. RODOTA' to the 2002 Annual report of the Italian Data Protection Authority to the Italian Parliament, page 15, available at the following address: http://www.garanteprivacy.it/garante/document?ID=128285.*

[11] *For more information on Article 29 Data Protection Working party see : http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm.*

[12] *Opinion on the use of location data with a view to providing value added services adopted on 25 November 2005; 2130/05/EN; WP 115; available at the following address: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.*

meantime, new ways of commercial exploitation of location data have come to light, providing a multifarious range of services based on location data.

The Working Party expresses concerns as to the possible use, or rather misuse, of location data also in light of the path followed by provision of value added services. At the beginning, the services were based on one-off use of location data giving information at a specific moment in time, offering for example information required by a user on the nearest location of a certain place, such as restaurant or shop, to the user's position. Further, these services were integrated by services based on use of the data on a continuous basis (assistance in navigation). *"This first stage has now given way to a second stage, with the development of services that are no longer based on locating people at their own request (users wishing to avail themselves of a service), but on their being located (at the request of a third party). Tracking and search services have developed whereby individuals can be located via their mobile phones even if they are not using them, but provided that are switched on. The key issue for the processing of location data has thus moved on from being a question of storage (essentially: on what conditions should location data be stored by electronic communications operators?) to being a question of use (how can we ensure that data are used for supplying value-added services in accordance with the principles applicable to the processing of personal data?)"*[13].

The gathering and processing of location data fall within application of the Directive 95/46/EC and the Directive 2002/58/EC and their use is considered as a matter deserving specific attention as it involves the freedom of movement of the individual. The Working Party recognizes that the Directive 95/46/EC and the Directive 2002/58/EC provide for satisfactory legal framework for the processing of location data, and intends to spell out specific modalities of application of the provisions contained in the aforementioned Directives.

The Working Party first of all specifies that all the various parties involved in the provision of value added services have to comply with the privacy law requirements, meaning that not only the electronic communications operator but also possible third parties providing the value added services are subject to the privacy law provisions.

The Working Party has identified the following as the general conditions ruling on the use and processing of location data for the provision of value added services.

5.3 Applicable law

The starting point is to determine the law applicable to the provision of value added services. Indeed, it is usual that the service provider is not located in the same place as the person benefiting from the service (namely the data subject), as it happens for example for services provided through a website. In this case, the place of establishment of the Controller is the criterion to be followed in order to determine the applicable privacy law. The privacy law of the Member State where the Controller is established will apply, while that of the Member State of which the data subject is national is irrelevant. In case

[13] *The Article 29 Data Protection Working Party, Opinion adopted on 25 November 2005, above quoted.*

the Controller is established out of the boundaries of the Community or even if their headquarters are located outside the EEA, the specific requirements set forth in the Directive 95/46/EC as to the transfer of data towards third countries should be complied with. It may also be the case that the Controller is established out of the Community and processes data making use of equipment located in one Member State. In said circumstance the privacy law of the Member State where the equipment is based applies[14] since the Article 29 Working Party suggests the issues of establishment and use of equipment to be "*the determinants for the applicability of the Data Protection Directive and the rules subsequently triggered by the processing of IP addresses and the use of cookies*."[15]

5.4 Information to the data subject

The data subject has to be given a detailed set of information on the processing of location data[16]. The Working Party specifies that the information requirement should be fulfilled by the subject collecting the location data to be processed, which may be either the electronic communications provider or the third party providing the value added services. In any case, the information on the service offered should be "*clear, complete and comprehensive*".

5.5 Consent

Under Article 9 of the Directive 2002/58/EC the data subject's consent is necessary for the processing of location data functional to performance of value added service.

Given the features that the consent must have under the Directive 95/56/EC (freely given, specific and informed), the Working Party expressly state that the consent may not be regarded as validly given when it is considered part of the acceptance by the data subject of the general terms and conditions of the value added services.

In case the provision of the value added services entails processing also of sensitive or judicial data, the higher requirements set forth in the Directive 45/96/EC for these special categories of data have to be complied with.

---

[14] *Article 4, paragraph 1, letter c) of the Directive 95/46/EC. For a throughout analysis on the extra-territorial dimension of the Community data protection law please refer to the Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, adopted on 30 May 2002 by the Article 29 Data Protection Working Party; 5035/01/EN/Final; WP 56; available at the following address: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf.*

[15] *See Article 29 Data Protection Working Party, WP 163, "Opinion 5/2009 on online social networking", at p.5 and the WP 148 "Opinion 1/2008 on data protection issues related to search engines".*

[16] *Under Article 10 of the Directive 95/46/EC and Articles 6 and 9 of the Directive 2002/58/EC the following information has to be given to the subject of location data: identity of the Controller and of his representative, if applicable; purposes of processing; type of location data processed; duration of the processing; whether data will be transmitted to a third party for the purpose of providing the value-added service; rights of access to the data, to rectify and to cancel them; right of users to withdraw their consent at any time or temporarily refuse the processing of such data, and the conditions on which this right may be exercised.*

As to the entity required to obtain the data subject's consent, this may be the electronic communications operator or the third party service provider. It depends upon what is the entity actually providing the service in each specific case.

The circumstance that the number of service providers is continuously increasing led the Working Party to suggest centralization by operators of the requests to access value added services, so that the further transfer to the service provider of the location data necessary to provide the requested services may be made in a way that preserves identification of the data subject requesting the services, for example using an alias. In this way, the data subject might benefit of the services without being known to the service provider, but only to the electronic communications operator.

The Working Party also notes that another way to protect identity of the data subject may be exploiting the end-user terminal location capability embedded in the terminal itself in combination with use of pseudonyms to identify the terminal with the service provider. The forgoing example has been proposed by the Working Party for highlighting "*the need to consider Privacy Enhancing Technologies as efficient and complementary elements in providing a high and satisfactory degree of protection to users of geo-localization services*".

The Working Party also urges providers of value added services to take appropriate safeguards in order to guarantee validity of the consent, namely that the person giving the consent to the data processing is indeed the same person whose location data will be processed. To this purpose, the service provider must first give to the user a confirmation of the subscription to the service through a message sent to the user's terminal equipment upon receipt of the relevant consent. Further, if necessary, the service provider must also require that the user confirms his/her subscription. Considering the person whose consent must be obtained, it is necessary to obtain the consent of the person whose location data are to be processed.

5.6 The right to withdraw

The person who has given the consent to the processing of location data has the right to withdraw said consent at any time, and has also the right to temporarily refusing the processing through simple means and free of charge[17]. These rights may be regarded as implementation of the right to object to the processing, and are essential if one considers the peculiar and sensitive nature of location data. Taking into account the foregoing, the Working Party holds that information to the data subject is an essential prerequisite to effective exercise of the above referenced rights, and that the information requirement should be satisfied not only at the time when the service is subscribed, but also through constant reminder on an ongoing basis, notably each time that the data subject uses the value added service.

[17] *Article 9 of the Directive 2002/58/EC.*

5.7 Data storage time

Location data may be used and processed only for the time strictly necessary to perform the value added service[18]. When the service has been performed, location data may be retained only if they are necessary for billing and interconnection payment reasons, or if they are made anonymous.

5.8 Security measures and transmission to third parties

Electronic communications operators and service providers should adopt technical and organisational security measures that protect and guarantee confidentiality and integrity of the location data processed, taking into account the risks represented by the processing and the nature of the data involved. As to transmission of location data to third parties, the transmission is allowed only towards third parties providing the value added services[19].

Taking into account access to and processing of location data, these may be authorized only in relation to persons that act subject to the third party service provider's authority, and should be curtailed to the extent and the time functional to the service performance. Moreover, access to location data should be registered.

6. Recommendations and conclusions

6.1 Recommendations for interoperability

The use of standards for security interoperability and identity management for the backend systems and also the mobile devices, following best practices for security-hardening trusted mobile devices is recommended. Open standards have been developed in consortiums of major vendors in the industry with a high degree of peer review. Two such standards are SAML (Security Assertion Markup Language) and WS-Security. SAML is an XML-based framework for "describing and exchanging security information between on-line business partners", and for providing single sign-on, federated identity, specifically for web services [22]. WS-Security is a protocol for providing security for web services through protecting the confidentiality and integrity of SOAP messages [23].

Open standards form the basis for interoperability between different products and services. For example, Google's Android platform for mobile applications is a step in the right direction. Android makes the mobile application development environment publicly available so that it becomes easier for application developers to apply security to programs designed for smart-phones. Moreover, several researchers support a layered approach to security on mobile devices that encompasses carriers, manufacturers and application developers [67].

---

[18] *Article 9, paragraph 1 of the Directive 2002/58/EC.*

[19] *Article 9, paragraph 3 of the Directive 2002/58/EC.*

6.2 User awareness

Public awareness of the privacy and security implications related to mobile identity management should be a key policy to defend against and requires long-term effort. ENISA has published several documents with guidelines on how to raise information security awareness [47,48]. Organizations like ENISA should continue playing a dominant role in educating people about privacy and security concerns and requirements. The activities of these organizations include awareness raising campaigns, organization of consultation platforms and complaint centres, technical-related activities aiming to the enhancement of information security standards and innovative techniques. The customer confidence can be enhanced by the existence of trustee authorities/organizations, supported or provided by ENISA, that would evaluate service providers and assess their security and privacy guarantees.

Competent National Regulatory Authorities (NRAs), such as the Hellenic Authority for the Information and Communication Security and Privacy (ADAE) are also aware of this need. In Greece, for instance, although regulatory authorities are not obliged *stricto sensu* to inform citizens on what kind of privacy self-protection measures they could employ in their communications, still, they have started publishing user awareness documents for consumers' privacy protection, as well as codes of conduct for services providers' use [70]. Similarly, in the UK, the Information Commissioner's Office (ICO), a privacy and data protection regulator, has published a guide to help organisations decide if information they hold is caught by the Data Protection Act (DPA) [71].

6.3 Design objectives for mobile IDM

User-experience: One of the most important challenges in mobile and pervasive computing is the unobtrusive but secure user experience. To achieve that, user identification and authentication as well as the registration in various services need to take place in a "transparent" manner, minimizing the user input and intervention and the delay overhead. The system should provide the appropriate information to the user that allows him/her to decide about a transaction, minimizing the intrusiveness and interruptions. At the same time, the provisioning of mechanisms for detecting the various attacks or threats (e.g., compromised identities and identity thefts) and also dealing with incidents ex post facto is critical.

A mobile identity management mechanism needs to identify the user and his/her context in an efficient manner: minimizing the delay, the number of false identification results, and the user interruption. In general, this is a challenging task, given that devices may need to process and correlate information collected from various devices which may be out-of-date, incomplete, or even false, while not all devices and applications have the same rights to access these data.

Systems should describe in a concise manner their privacy policies. Many privacy policies and their implications of their configuration are not well-understood by end users. Some researchers have also proposed systems that allow users to query their policies and investigate further their information dissemination mechanisms. Such "feedback-" and "feedforward-" based mechanisms should be developed and evaluated.

This involves research in domains that span from networking and systems to contextual information representation and reasoning, and graphics. It opens up exciting challenges in computer science, demanding interdisciplinary research and innovative paradigms. An example is the positioning, a mechanism crucial for the support of various location-dependent and context-aware services. In several cases, position traces can be obtained by intercepting communications and location privacy can be a serious issue.

Access and authorisation: A management system must transparently handle the access rights that are pertinent to each identity and relevant to the particular service. Password or profile management must allow users to easily change passwords or handle cases of forgotten passwords. An efficient management system should assist users in creating strong passwords. Users must be provided with intuitive controls to both handle their identities and also perform operations on them, such as revocation of information. The means of control should be visible and its results verifiable. These can be especially challenging in mobile devices, in which screen size is limited and typing can be hard.

Scalability: Mobile identity management systems should not only be cost-effective and scalable from the perspective of the operators and/or service providers but also from the perspective of users. Often users are required to memorise multiple passwords for accessing different services. This may represent a minor inconvenience, when a user accesses only a few online services. However, the impact on the user experience increases with the number of services that are used. As the number of services increases, the problems in managing multiple passwords and access rights are exaggerated, especially in the context of mobile computing. Thus, it becomes important to provide user-friendly, flexible, expressive, and efficient mechanisms to manage the access rights, control, and passwords.

Resilient connectivity: On the physical layer, many attacks rely on isolating the "target" from the rest of the network, effectively depriving it of crucial information. Such attacks can be prevented by the provision of reliable connectivity, along with more resilient networks, and the support of mechanisms that allow devices to select the appropriate network interface or access point based on security-related criteria. The support of strong crypto mechanisms is necessary.

Malware defences: Apart from attacks on connectivity and other shared resources, a user device can also be a physical target. Often a mobile device is tightly associated with its owner. The compromise of such a device or its trusted communications can have negative consequences for its owner. Thus, attention should be given to strengthen the security of the device, its operating system, and network layers, during their development phase. Security mechanisms should be implemented to resist compromise by malicious software. Such mechanisms include antivirus software and frequent patching. They should only allow trusted and certified software to be executed on the device. Moreover, any communication that is part of the identity management protocols must to be protected through the use of appropriate encryption to protect confidentiality and integrity.

Control over privacy settings: In some situations, customers may choose to give up some privacy for the benefits they gain. For example, a user may choose to reveal his/her geographic location in exchange of maps or information about local points of interest or choose to run third-party applications which in one hand they provide to the user

additional functionality but on the other hand they could introduce security and privacy risks. Thus, it is important to provide tuneable privacy protection mechanisms and tools for automatic customization and personalization of services.

Delegation: Another important aspect is the privacy protection when various delegation mechanisms are employed. For example, in several advanced markets, Near Field Communication-based mobile phones, enabled with e-wallet mechanisms, are used for electronic payments. A desirable feature of such systems is the privacy preservation, in that the e-wallet/account holder is not required to reveal his/her shopping list and history but allows the bank and merchant to communicate in order to prevent un-approved transactions. Service providers (via proxies) may request more attributes and more rights than necessary for a service. Only credentials related to the purpose of a delegation are given to the service provider/proxy (least privilege). In general, a privacy-preserving delegation mechanism needs to consider the following criteria [74]:

- Authentication without revealing identifying data
- Non-linkability of transactions
- Least privilege
- Preventing misuse of delegated credentials
- Restricting re-delegation of a credential
- Revocation of a credential

Accountability: Service providers should be able to attest the accountability of their users. A privacy preserving delegation mechanism guarantees these interests, if it fulfils the following criteria [74]:

- Non-repudiation of using a credential
- Revealing of identity

Identity selection and composition: The determination of the type of data that will compose the mobile identity is of primary importance. Specifically, the collection mechanisms need to indicate which parties (e.g., network operators, government office, professional organization, employers, law enforcement agencies, and profile providers and/or service provides) in addition to the mobile user should participate in the generation of a mobile identity. Furthermore, users should be able to understand the separation of the various identities across service domains and providers.

Consumer trust: Addressing user aspects of mobile identities should take place on the micro level of individual users and their devices as well as on the macro level of the environment in which mobile identities are used. To enable mobile business, the development of a trust relationship between the consumer and supplier is crucial. The main benefits of mobile commerce, namely, convenience, low search costs, and potentially lower prices, need to be balanced by costs associated with risk taking and loss of privacy; in particular, the economic risk arising from potential monetary loss could be significant [44]. While high costs associated with risk taking can impede the use of systems for mobile business, poor privacy protection can dissuade them in the long run. The appropriate legal scheme regarding protection of personal data, privacy and security in the area of telecommunications and e-commerce services, irrespective of the type of environment, platform or media used, is required to be established for a harmonised

protection of identification data not only in a national but also European level. Policy definition and enforcement can significantly strengthen the systems, offering the users the appropriate flexibility they wish for.

Acronyms

2FA	Two-factor Authentication
3GPP	Third Generation Partnership Project
BAC	Basic Access Control
eID	Electronic Identity
EPC	Electronic Product Code
LTE	Long Term Evolution
NFC	Near Field Communication
MNO	Mobile Network Operator
PDA	Personal Digital Assistant
PIN	Personal Identification Number
RFID	Radio Frequency Identification
SE	Secure Element
SIM	Subscriber Identity Module
SMS	Short Message Service
TAN	Transaction Authentication Number
TRC	Transport Revenue Collector
UICC	Universal Integrated Circuit Card
UID	Unique Identification Number
USSD	Unstructured Supplementary Service Data
WiMAX	Worldwide Interoperability for Microwave Access

References

[1] Thibault Candebat, Cameron Ross Dunne and David T. Gray, "Pseudonym management using mediated identity-based cryptography," DIM '05: Proceedings of the 2005 workshop on Digital identity management, November 2005

[2] Oliver Jorns, Gerald Quirchmayr and Oliver Jung , "A privacy enhancing mechanism based on pseudonyms for identity protection in location-based services," ACSW '07: Proceedings of the fifth Australasian symposium on ACSW frontiers – Vol. 68, January 2007

[3] Landon P. Cox, Angela Dalton, and Varun Marupadi, "SmokeScreen: flexible privacy controls for presence-sharing," MobiSys '07: Proceedings of the 5th international conference on Mobile systems, applications and services, June 2007

[4] Janne Lindqvist and Laura Takkinen, "Privacy management for secure mobility," WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society, October 2006

[5] George Roussos and Theano Moussouri, "Consumer perceptions of privacy, security and trust in ubiquitous commerce," Personal and Ubiquitous Computing, Volume 8 Issue 6, November 2004

[6] Leopoldina Fortunati, "The Mobile Phone: An Identity on the Move," Personal and Ubiquitous Computing, Volume 5 Issue 2, Springer-Verlag, January 2001

[7] Long Nguyen Hoang, Pekka Laitinen, and N. Asokan, "Secure roaming with identity metasystems," IDtrust '08: Proceedings of the 7th symposium on Identity and trust on the Internet, March 2008

[8] Alfredo Matos, Susana Sargento, and Rui Aguiar, "Embedding identity in mobile environments," MobiArch '07: Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture, August 2007

[9] Audun Jøsang, John Fabre, Brian Hay, James Dalziel, and Simon Pope, "Trust requirements in identity management," ACSW Frontiers '05: Proceedings of the 2005 Australasian workshop on Grid computing and e-research, Volume 44, January 2005

[10] Samir Saklikar and Subir Saha, "User privacy-preserving identity data dependencies," DIM '06: Proceedings of the second ACM workshop on Digital identity management, November 2006

[11] Audun Jøsang, Muhammed Al Zomai, Suriadi Suriadi, "Usability and privacy in identity management architectures," ACSW '07: Proceedings of the fifth Australasian symposium on ACSW frontiers, Volume 68, January 2007

[12] Pascal Urien and Guy Pujolle, "Security and privacy for the next wireless generation," International Journal of Network Management, Volume 18, Issue 2, March 2008

[13] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Communications Magazine, November 2008

[14] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for Secure and Private Vehicular Communications," Seventh International Conference on ITS Telecommunications, Sophia Antipolis, France, June 2007
[15] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles," Workshop on Embedded Security in Cars (ESCAR), Berlin, Germany, November 2006
[16] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: A Position Paper." Workshop on Standards for Privacy in User-Centric Identity Management, Zurich, Switzerland, July 2006
[17] PRIME EU project, https://www.prime-project.eu/
[18] FIDIS EU project, http://www.fidis.net/resources/deliverables/hightechid/int-d3300/
[19] Identity Management Group, http://www.opengroup.org/idm/
[20] eMobility, http://www.emobility.eu.org/
[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Offical Journal of the European Communities, No L 281/31, 23.11.95, http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm
[22] N. Ragouzis et al., *Security Assertion Markup Language (SAML) V2.0 Technical Overview.* OASIS Draft, February 2007. Document ID sstc-saml-tech-overview-2.0-draft-13, http://www.oasis-open.org/committees/download.php/22553/sstc-saml-tech-overview-2%200-draft-13.pdf
[23] Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard Specification, 1 February 2006
[24] D3.3: Study on Mobile Identity Management, FIDIS NoE "HighTechID", deliverable D3.3, http://www.fidis.net/resources/deliverables/hightechid/#c1786
[25] Kai Rannenberg, Identity Management in Mobile Cellular Networks and Related Applications, Information Security Technical Report, volume 9, issue 1, 2004, http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VJC-4BXN4BK8&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_version=1&_urlVersion=0&_userid=10&md5=692fe18d9c7208887ddb84ddb1efd500
[26] Johansen, Jørstad, Do van Thranh, "Identity Management in Mobile Ubiquitous Environments", ICIMP 2008, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4561345
[27] Do Van Thanh et al, "Identity Management", Telektronikk 3/4.07, http://www.telenor.com/telektronikk/volumes/index.php?page=seksjon&id1=73&id2=202&select=
[28] MinID-service http://www.norge.no/minside/
[29] Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID), ENISA, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_mobile_eid.pdf
[30] Mobile Identity Management: An Enacted View, George Roussos, Don Peterson, and Uma Patel Int. Jour. E-Commerce, Vol 8, No 1, pp. 81-100. http://www.dcs.bbk.ac.uk/~gr/pdf/ijec-mid.pdf
[31] Microsoft, Introducing Windows CardSpace,http://msdn.microsoft.com/en-us/library/aa480189.aspx.
[32] OpenID, http://openid.net/.

[33] Markus Jakobsson, Steven Myer, Phishing and Counter-Measures: Understanding the Increasing Problem of Electronic Identity Theft, Wiley-Interscience, 2006.
[34] Data Mining Methods for Anomaly Detection Workshop, KDD, 2005.
[35] H. Cheung, "How to: Building a bluesniper rifle - part 1, http://www.tomsnetworking.com/2005/03/08/how to bluesniper pt1," March 2005.
[36] Yaniv Shaked and Avishai Wool, "Cracking the bluetooth pin," in *Proc. of Mobisys*, 2005.
[37] Enabling Secure and Spontaneous Communication between Mobile Devices using Common Radio Environment, Alex Varshavsky Anthony LaMarca Eyal de Lara, Hotmobile 2007, http://www.seattle.intel-research.net/pubs/varshavsky_hotmobile2007.pdf
[38] Mobile Suica, http://en.wikipedia.org/wiki/Mobile_Suica
[39] Wikipedia, Biometrics, http://en.wikipedia.org/wiki/Biometrics
[40] Maria Papadopouli and Henning Schulzrinne, Peer-to-Peer Computing for Mobile Networks: Information Discovery and Dissemination, Springer.
[41] Balachander Krishnamurthy, Craig E. Wills. Characterizing Privacy in Online Social Networks, in ACM SIGCOMM WOSN, 2008.
[42] Zack Anderson, RJ Ryan, and Alessandro Chiesa. Anatomy of a subway hack, DefCon16, Las Vegas, 2008.
[43] Black Hat USA 2008. https://www.blackhat.com/html/bh-usa-08/bh-usa-08-speakers.html
[44] Amin Tootoonchian, Kiran K. Gollu, Stefan Saroiu, Yashar Ganjali, Alec Wolman. Lockr: Social Access Control for Web 2.0, in ACM SIGCOMM WOSN, 2008.
[45] Saikat Guha, Kevin Tang, Paul Francis. NOYB: Privacy in Online Social Networks, in ACM SIGCOMM WOSN, 2008.
[46] ENISA - The new users' guide: How to raise information security awareness, ENISA, http://www.enisa.europa.eu/doc/pdf/deliverables/new_ar_users_guide.pdf
[47] ENISA - Information security awareness in financial organisations, ENISA http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
[48] Wikipedia, http://en.wikipedia.org/wiki/Digital_divide
[49] Community wireless networks-yesterday's technology tomorrow, Henning Schulzrinne, Panel at IEEE LANMAN'08, http://www.ieee-lanman.org/presentations_2008/schulzrinne_panel.pdf
[50] Secure cards, wikipedia, http://en.wikipedia.org/wiki/Secure_Digital_card
Network forensics and fraud detection
[51] http://www.panoulu.net/
[52] http://www.ieee-lanman.org/presentations_2008/polyzos_panel.pdf
[53] L. Ho, M. Moh, Z. Walker, T. Hamada, and C.-F. Su, "A Prototype on RFID and Sensor Networks for Elder Healthcare: Progress Report", In Proceedings of the 2005 ACM SIGCOMM Workshop on Experimental Approaches to Wireless Network Design and Analysis, Applications, Technologies, Architectures, and Protocols for Computer Communication, Philadelphia, Pennsylvania, USA, 2005, pp. 70-75.
[54] E. Dishman, "Inventing Wellness Systems for Aging in Place", IEEE Computer Magazine, Vol. 37, No. 5, May 2004, pp. 34-41.
[55] S. J. Kim, S. K. Yoo, H. O. Kim, H. S. Bae, J. J. Park,K. J. Seo and B. C. Chang, "Smart Blood Bag Management System in a Hospital Environment", Personal Wireless

Communications, Springer Berlin/Heidelberg, Vol. 4217/2006, September 2006, pp. 506-517.

[56] T. Ativanichayaphong, J. Wang, W.-D. Huang, S. Rao, H.F. Tibbals, S.-J. Tang,S.J. Spechler, H. Stephanou and J.-C. Chiao, "Development of an Implanted RFID Impedance Sensor for Detecting Gastroesophageal Reflux", In Proceedings of IEEE International Conference on RFID, Grapevine, TX, 26-28 March 2007, pp.127-133.

[57] K. Farrahi and D. Gatica-Perez, "What Did you Do Today? Discovering Daily Routines from Large-Scale Mobile Data", In Proceedings of the 16th ACM International Conference on Multimedia (MM'08), Vancouver, British Columbia, Canada, October 26-31, 2008, pp. 849-852.

[58] K. Farrahi and D. Gatica-Perez, "Discovering Human Routines from Cell Phone Data with Topic Models", In Proceedings of the IEEE International Symposium on Wearable Computers (ISWC'08), Pittsburgh, September 2008.

[59] K. Farrahi and D. Gatica-Perez, "Daily Routine Classification from Mobile Phone Data", In Proceedings of the 5th Joint Workshop on Machine Learning and Multimodal Interaction (MLMI), Utrecht, The Netherlands, 2008.

[60] A. Mitrokotsa, M. Rieback, A. S. Tanenbaum, "Classification of RFID Attacks", In Proceedings of the 2nd International Workshop on RFID Technology – Concepts, Applications, Challenges (IWRT'08), 10th International Conference on Enterprise Information Systems, pp. 73-86, June 2008.

[61] International Organization for Standardization, "ISO/IEC 9798: Information Technology – Security Techniques – Entity Authentication", www.iso.org.

[62] European Commission, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of such Data", Official Journal of European Communities (1995).

[63] C. Floerkemeier, R. Schneider and M. Langheinrich, "Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols", In Proceedings of the Interational Worksop Series on RFID: Information Sharing and Privacy, Tokyo, Japan (2004).

[64] Abdullahi Arabo, Qi Shi, Madjid Merabti, David Llewellyn-Jones, "Identity Management in Mobile Ad-hoc Networks (IMMANets): A Survey" http://www.cms.livjm.ac.uk/pgnet2008/Proceeedings/Papers/2008070.pdf

[65] Search security, "What is authentication", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html

[66] Consumer Fraud and Identity Theft Complaint Data, Federal Trade Commission, 2006.

[67] Emerging Cyber Threats Report for 2009 Georgia Tech Information Security Center http://smartech.gatech.edu/bitstream/1853/26301/1/CyberThreatsReport2009.pdf

[68] Shibboleth Project. *Shibboleth Architecture Protocols and Profiles.* Working Draft 05, 23 November 2004. Internet2/MACE, 2004.

[69] Steve Riley, "Mitigating the Threats of Rogue Machines—802.1X or IPsec?" http://technet.microsoft.com/el-gr/library/cc512611(en-us).aspx

[70] ADAE 10/4/2008 http://www.adae.gr/adae/viewarticle.html?langid=el&articleid=129

[71] ICO, "Data Protection Guidance"

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialistguides/what_is_data_for_the_purposes_of_the_dpa.pdf
[72] EU-FIDIS project, "D4.2: Set of requirements for interoperability of Identity Management Systems" http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.2.set_of_requirements.pdf
[73] Kim Cameron's Identity Weblog http://www.identityblog.com/stories/2004/12/09/thelaws.html
[74] EU-FIDIS project, "D11.1: Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity", http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp11-del11.1.mobility_and_identity.pdf
[75] EU-FIDIS project, " D12.7: Identity-related Crime in Europe – Big Problem or Big Hype?", http://www.fidis.net/fileadmin/fidis/deliverables/5th_workplan/fidis-wp12-del12.7_identity_crime_in_Europe.pdf
[76] EU-FIDIS project, "D3.10: Biometrics in identity management" http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.10.biometrics_in_identity_management.pdf
[77] EU-Prime project, Ronald Leenes, Jan Schallaböck, Marit Hansen (white paper)https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf
[78] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi
[79] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.5_Identity_Management_Initiative_Report_1_IIR1.pdf
[80] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf
[81] Daehyun Strobel. "IMSI-catcher "http://www.crypto.rub.de/imperia/md/content/seminare/itsss07/imsi_catcher.pdf
[82] RFID-Enabled Phone Skins for Mobile Payments http://www.rfidjournal.com/article/view/5021/
[83] Vassilis Prevelakis and Diomidis Spinellis. The Athens affair. *IEEE Spectrum*, 44(7):26–33, July 2007. http://www.spinellis.gr/pubs/jrnl/2007-Spectrum-AA/html/PS07.html
[84] Schneier B., "RFID Passports", "Schneier on Security" blog, Retrieved from http://www.schneier.com/blog/archives/2004/10/rfid_passports.html on September 2009
[85] Schneier B., "The ID Chip You Don't Want in Your Passport", "The Washington Post" newspaper - Electronic Edition, Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/09/15/AR2006091500923.html on September 2009
[86] Schneier B., "Fatal Flaw Weakens RFID Passports", "The Wired" magazine - Electronic Edition, Retrieved from http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69453?currentPage=2 on September 2009

[87] Flexilis Security Group, "RFID Passport Shield Failure Demo - Flexilis", "YouTube" video sharing site, Retrieved from http://www.youtube.com/watch?v=-XXaqraF7pI on September 2009
[88] Cristofaro Mune Roberto Gassira' Roberto Piccirillo Hijacking Mobile Data onnections http://www.blackhat.com/presentations/bh-europe-09/Gassira_Piccirillo/BlackHat-Europe-2009-Gassira-Piccirillo-Hijacking-Mobile-Data-Connections-whitepaper.pdf
[89] Christoph Schuba. Addressing weaknesses in the domain name system protocol. M.Sc. Thesis, Purdue University, August 1993. http://ftp.cerias.purdue.edu/pub/papers/christoph-schuba/schuba-DNS-msthesis.pdf
[90] Lasse Øverlier, Tønnes Brekne, André Årnes, "Non-Expanding Transaction Specific Pseudonymization for IP Traffic Monitoring", 4th International Conference on Cryptology and Network Security (CANS 2005), Xiamen, China, December 2005, published in Springer LNCS Vol. 3810.
[91] Tønnes Brekne, André Årnes, "Circumventing IP-Address Pseudonymization", The third IASTED International Conference on Communications and Computer Networks (CCN 2005), Marina del Rey, USA, October 2005.
[92] Tønnes Brekne, André Årnes, Arne Øslebø. "Anonymization of IP Traffic Monitoring Data -- Attacks on Two Prefix-preserving Anonymization Schemes and Some Proposed Remedies''. Workshop on Privacy Enhancing Technologies (PET 2005), Kavtat, Croatia, May 2005, published in Springer LNCS 3856.
[93] Telecom Italia wiretapping scandal http://www.edri.org/edrigram/number4.15/italy
[94] http://www.un.org/en/documents/udhr/index.shtml#a12
[95] http://conventions.coe.int/treaty/EN/Treaties/html/005.htm
[96] http://brage.unik.no/people/josang/papers/JPH2002-AUUG.pdf
[97] http://www.engadget.com/2008/02/21/researchers-claim-gsm-calls-can-be-hacked-on-the-cheap/