Security, Privacy, and Trust in Mobile Systems

Angelo Corallo[1] **Marco Cremonini**[2] **Ernesto Damiani**[2]
Sabrina De Capitani di Vimercati[2] **Gianluca Elia**[1] **Pierangela Samarati**[2]
(1) eBMS/ISUFI - Universit'a di Lecce - 73100 Lecce - Italy
(2) Dip. di Tecnologie dell Informazione - Università di Milano - 26013 Crema - Italy
{angelo.corallo,gianluca.elia}@isufi.unile.it
{cremonini,damiani,decapita,samarati}@dti.unimi.it

Abstract

Mobile systems and applications are raising some important information security and privacy issues. This chapter discusses the need for privacy and security in mobile systems and presents technological trends which highlight that this issue is of growing concern.

1 Introduction

Access to general purpose Information and Communication Technology (ICT) is not equally distributed on our planet: developed countries represent about 70 per cent of all Internet users while its percentage of Internet hosts has raised from 90 per cent in 2000 to about 99 per cent in 2002.

Things change dramatically if we look at mobile and wireless technology: developing countries already represented about 40 per cent of mobile connections in 2000, with a foreseen growth rate that is faster for developing countries than that for the developed one in the period 2000-2005 (mainly due to India and People's Republic of China). This trend depends on the new perspectives mobile electronic technology applications offer, making in principle possible to do business with partners located anywhere on the globe by-passing the poor telecommunication infrastructure still common in many developing countries. On the other hand, in the developed world the set of techniques going under the name of *e-Mobile* is becoming more and more important in e-Business transactions. The use of smart mobile terminals will allow new kind of services and new business models, overcoming time and space limitations. The technological evolution in wireless data communications is introducing a rich landscape of new services relying on three main technologies:

- proximity (or personal) area networks (PANs), composed by personal

and wearable devices capable of automatically setting up transient communication environments (also known as *ad-hoc* networks);

- wireless local area network technology (WLAN);
- 3rd Generation of mobile telecommunications (3G), gradually replacing General Packet Radio Service (GPRS) and the related set of technologies collectively called "2.5 Generation" (2.5G). 3G services are made available through technologies such as Wideband Code-Division Multiple Access (WCDMA), offering high data speeds.

PANs is a new technology bringing the "always connected" principle to the personal space. On the other hand, 3G systems and WLANs have coexisted since long; what is new is their interconnection, aimed at decoupling terminals and applications from the access method. While 3G is generally considered applicable mainly to fully mobile wireless devices (e.g., operating from a car), WLAN is more relevant to fixed and portable wireless devices (e.g., operating from an elevator). 3G mobile networks already provide video-capable bandwidth, global roaming for voice and data, and access to the Internet rich online content.

Thanks to their increasing integration, PANs, WLANs, and 3G networks will extend the users connectivity in a complementary and hierarchical manner; in the fullness of time, they will provide all the functionalities of a *Integrated Services Multimedia Network* (ISMN), enabling a whole series of new business models and applications.

The fusion of these technologies will eventually result in a ultimate ubiquitous wireless system that will be operational from anywhere on the planet, including use in homes, businesses, land vehicles and even commercial aircrafts. Even today, WLAN and 3G can already promote each other encouraging WAN users to continue connections in the wider area, provided that security, roaming and mobility are fully supported.

1.1 Mobile and wireless security issues

While wireless communications provide great flexibility and mobility, they often come at the expense of security. Indeed, wireless communications rely on open and public transmission media that raise further vulnerabilities in addition to the security threats found in wired networks. A number of specific open issues and even inherent dangers (some of which had been already identified and described in the early stages of wireless technology adoption [Howard, 2000]) are yet to be solved.

With wireless communications, important and vital information is often placed on a mobile device that is vulnerable to theft and loss. In addition, this information is transmitted over the unprotected airwaves. Thirdly, 3G

networks are getting smaller and more numerous, causing opportunities for hackers and other abusers to increase.

Currently, 2.5G security mechanisms include 40-bit encryption, but theoretical attacks against this and the authentication mechanisms have been demonstrated [van Oorschot et al., 1996]. 3G technologies incorporate stronger cryptographic techniques, and new authentication systems. This is probably not enough, because application areas like mobile commerce require this critical information to be decrypted by a server located somewhere in the communications chain before it is encrypted again and forwarded to a new destination. Every hop in the wireless communication chain where information is decrypted and re-encrypted represents a potential vulnerability in the overall security.

Furthermore, the growing complexity of mobile terminals and the increased presence of interoperability software on them is making them vulnerable to viruses and hacking attacks. However, there is great motivation for 3G security. The boom of users demand for richer content for their mobile terminals (such as through multimedia messaging, video conferencing, voice-over-IP, m-business) is increasing the need for security solution ensuring user and data confidentiality, quality of service (QoS), billing, and protection against intruders. The challenge for industry players now is to tackle all security issues within PAN, 3G and WLAN and create a profitable integrated wireless business comprising of services and value. In this chapter we shall look into some of the main security issues within the whole hierarchy of 3G and WLAN systems, including network access security, network domain security, user domain security, and personal identity management.

1.2 Wireless applications and security testing methodologies

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

- identification of the security requirements to be satisfied;
- identification of proposed product security mechanisms;
- determination of the test objectives;
- determination of the test methodology/technique;
- determination of expected test results;
- conduct of the test;

- documentation and analysis of test results;
- feedback of test results to appropriate individuals/organizations;
- determination of the next action to be taken (e.g., additional testing, corrective actions, and so on).

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

1.3 Organization of the chapter

The chapter is structured as follows. Section 2 presents an overview of the main privacy and security issues in mobile systems. Section 3 describes the identity management issue in 3G mobile systems. Section 4 discusses the integration of different wireless technologies into ubiquitous networking. Section 5 illustrates the concept of mobile identity management. Section 6 presents some privacy and security issues in the hotspots context. Section 7 addresses the privacy and security issues that may arise by introducing recovery procedures for transactions initiated by mobile users. Finally, Section 8 reports our concluding remarks.

2 Mobile Systems Security: An Overview

Mobile systems security was conceived as a natural development of conventional POTS (*Plain Old Telephone Service*) security. Some of the objectives, therefore, were clear and well-understood: avoiding unauthorized disclosure of a user's or operator's data, repelling *denial-of-service* (DOS) attacks and preventing unauthorized access to and use of mobile service. However, as we anticipated in the previous Section, a mobile communication environment presents a number of unique challenges due to the fact that mobile terminals are easily lost or stolen and to user expectations for flexibility and ease of use. In this section we shall focus on the main authentication and identity establishment techniques which are instrumental for the more complex mobile identity management solutions that will be described in the remainder of this chapter.

2.1 2G and 2.5G Mobile Authentication

First generation analogical mobile phones relied on an electronic serial number to confirm that the terminal should be allowed access to the service [Blanchard,].[1] On the other hand, GSM systems were designed with security in mind. Each subscriber to a GSM service receives a *Subscriber Identity Module* (SIM) card which contains the user's identity (see Section 3) and a long-life authentication key (technically speaking, a shared secret key [van Oorschot et al., 1996]) supposed to last for the whole duration of the subscription. The SIM is a removable security module which is issued and managed by the users' home service operator (even when the user is roaming) and is independent of the terminal. SIM-based authentication does not require any user action, other than entering the familiar 4-digit *Personal Identification Number* (PIN) into the terminal. No more user awareness on security is needed than what they are already used to from their ATM cards. While certainly not unbreakable (e.g., it was subject to *cloning* attacks), this system was successful inasmuch it placed much of the security and authentication responsibilities with the final users holding the SIMs.[2] In GSM, after the initial access request message has been exchanged over the air back to the user's home operator, a temporary user identity is allocated which is local to the area operator where the user is located and is reassigned to another user as soon as the original requestor leaves the area. This reduces the exposure of the real user identity on the air and prevents information on a user's movements or use of a service being harvested by unauthorized eavesdroppers (e.g.,

[1] Such a naive system was doomed. However, before long, hackers learned to read these electronic serial numbers from the air and access unsuspecting users' accounts.

[2] Long life is guaranteed by the fact that the authentication key is used to enable the user terminal and is not required by the GSM network when the user is placing or receiving calls.

for traffic flow analysis). Note that the GSM authentication mechanism is one-way only: the user sending the request cannot be completely sure that she has reached an authentic service operator. In the last few years, GSM 2G technology was upgraded to 2.5G with the introduction of the *General Packet Radio Service* (GPRS) overlaying, an IP core network on the GSM transport via two additional network elements, the *Serving GPRS Support Node (SGSN)* and *Gateway GPRS Support Node* (GGSN). While a complete description of GPRS technology is outside the scope of this chapter, it is worthwile to remark that enabling IP traffic via GPRS allowed 2.5G systems to take advantage of some well-known and understood authentication techniques [Smith, 2002] used on the Internet, such as certificates based on asymmetric encryption. Such authentication is performed in addition to (and independently of) GSM PIN-based authentication. Also, the GSM infrastructure already in place allows for large-scale roaming and recognition of security information. Recently, fully fledged *Public Key Infrastructure* (PKI) techniques have been enabled for mobile terminals by using enhanced SIM cards to handle the asymmetric key protocols.

2.2 3G Authentication and on-the-air Confidentiality

In the design of 3G systems like UMTS, a new security architecture was specified. However, the approach that was taken was rather conservative. Indeed, the new approach maintained backward compatibility with GSM, while trying overcoming some perceived weaknesses of 2G systems. A main heritage of GSM still present in 3G systems is the *automatic integrated roaming*. 3G systems retain the basic idea of the GSM radio signaling system, that is, the concept that each user has a "home" cell and may be currently visiting another, operated by the home operator (telecom company) of by a local one. In order to find the location of its users (and bill them accordingly) the mobile network relies on distributed *location registers*, respectively called the *Home Location* and *Visited Location* Register (HLR/VLR). The HLR/VLR solution ensures that 3G calls can be set up with the same speed users experienced (and liked) in 2G networks. On the other hand, it preserves operator-based management of user authentication via shared authentication keys stored in SIMs.

Like in 2G systems, 3G systems' users identify themselves by providing the identity stored in their SIM and known to their home service operator, just like users accessing a computer system. 3G authentication was designed with the following requirements in mind.

- *Mutual authentication*. Both the user and the network are identified in the authentication exchange.
- *Key freshness*. Assurance that authentication information and keys are not being re-used.

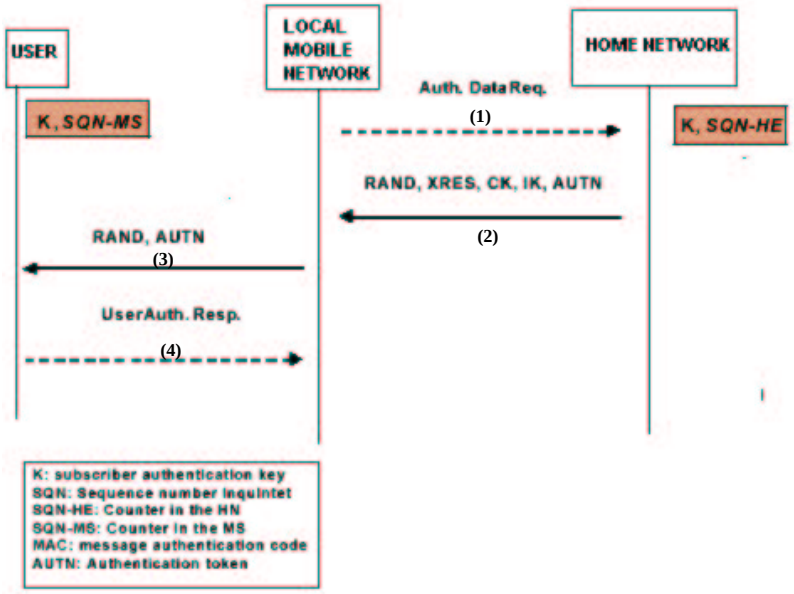

Figure 1: 3G user authentication

- *Integrity of signaling.* Protection of service messages, for example, during the encryption algorithm negotiation.

- *Strong encryption.* Strong cryptography, obtained via a combination of key length and algorithm design, is performed inside the core network rather than at the periphery.

Figure 1 shows a 3G authentication and key agreement (AKA) mechanism involving the local and home network operators. The mechanism is based on symmetric key encryption and uses a subscriber authentication key K that is shared between the user and the home network operator. The mechanism then combines a challenge-response protocol with a sequence number-based protocol to support network authentication and to provide the user with assurance of key freshness. More precisely, the AKA mechanism works as follows.

1. Upon receiving an authentication data request, the home network operator generates a fresh sequence number (SQN) from its local counter (SQN-HE).

2. The home network operator generates a challenge RAND and prepares a quintet that includes: the challenge RAND, an expected response XRES, a cipher key CK, an integrity key IK, and an authentication

token AUTN. The authentication token is obtained by combining the sequence number SQN and a message authentication code. XRES, CK, and IK are generated by applying three different key generating functions that take RAND and K as input and return, respectively, XRES, CK, and IK. The quintet is then sent to the local mobile network.

3. The local mobile network extracts from the received quintet the challenge RAND and the authentication token AUTN and send them to the user.

4. The user checks whether the authentication token AUTN can be accepted. Basically, the user verifies the integrity of the message and if the received sequence number SQN is acceptable. In case of a positive response, the user sends back to the local mobile network a response RES. The user also computes a cipher key CK and an integrity key IK. Note that CK and IK are computed by using the challenge RAND received from the local mobile network and the shared key K. Therefore, CK and IK corresponds to the keys generate by the home network operator.

5. The local mobile network compares the received response RES with XRES and if they match, the protocol is successfully completed. The local mobile network then selects the corresponding CK and IK from the quintet.

The AKA mechanism provides mutual entity authentication and the establishment of a shared secret cipher key and integrity key between the involved parties. Indeed, after authentication took place, the established keys CK and IK are transferred to the entities that perform ciphering and integrity functions. On-the-air encryption performed at the radio interface can be used by the network operator to prevent *session hijacking*, maintaining the validity of the authentication throughout the call.[3]

3 Personal Identity Management in 3G Mobile Systems

In the previous Section, privacy and security issues of mobile systems have been described mainly from the perspective of technological security research (access control, integrity, authentication, non repudiation, availability, and confidentiality). Recent developments in ICT-based business models reveal the necessity to approach the concept of privacy and security

[3]On-the-air encryption is not mandatory in 3G networks due to concern about restrictions on the use of encryption in some countries.

more broadly, embracing not only the technical aspects, but also the socio-economic, the policy and business points of view. This approach could represent a useful attempt to create a common basis from which users' trust in mobile world can arise, opening new business opportunities, launching new services and goods (i.e., mobile payment and finance, mobile ticketing, mobile voting), sparking new social and economic dynamics, and generating new life styles [Tsalgatidou et al., 2000]. The on-going transition from monolithic and localized systems, mainly based on single technology and weakly opened to integration with heterogeneous systems, towards multi-application, multi-access, multi-players, distributed and heterogeneous scenarios, is generating a context in which mobile applications and systems could play a strategic role. This event will occur if these kinds of scenarios will be wisely managed, taking into account both a set of internal elements and a group of context drivers that constitute important levers to enhance the users' trust in mobile systems and applications [Kagal et al., 2001, Kagal et al., 2003, Matskin and Tveit, 2003]. In other words, this means that technological potentialities, business opportunities and joining industries complex dynamics have to be strongly internetworked with users' social dynamics, standards, policy, and regulation to create a sort of digital identity management framework where digital identity is conceived as "an electronic representation of individuals' or organizations' sensitive information" [Damiani et al., 2003]. Support offered by this framework is crucial for building and maintaining trust relationships in today's globally interconnected society because:

- it offers adequate security and availability;
- it strikes the right balance between protection of privacy and convenience;
- it allows to present different subset of the users' identity depending on the on-going and perceived application and communication context;
- it guarantees that identity, personal data, and user profile (including location based information) are safeguarded and no thefts will happen.

Starting from the late '80s, many examples of *identity management system* (IM) have been proposed. In 1985, David Chaum considered a device that helps the user with payment transactions and upholds the user's privacy [Chaum, 1985a, Chaum, 1985b]. In 1993, Roger Clark proposed the *digital individual*, that is, the individual's data shadow in the computer system which can be compared to user's identity [Clark, 1993]. In 1995, John Borking published a report about the *Identity Protector* to protect the user's data [van Rossum et al., 1995]. In 1999, Martin Reichenbach proposed the reachability manager applied to telephone reachability [Herbert et al., 1999].

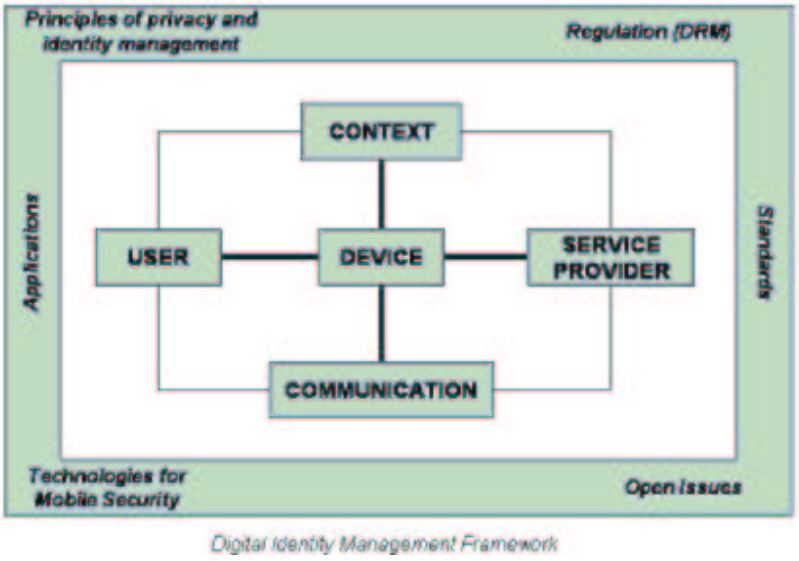

Figure 2: Our reference digital identity management architecture

Starting from 2001, Uwe Jendrike et al. [tom Markotten et al., 2001] proposed the concept of generic identity management to provide the users with usable and secure way to protect their privacy when using the Web.

Digital security and, more generally, digital identity management has been growing fastly in recent years, especially in mobile scenarios where personal communication and new computing devices will generate new security and integrity requirements for user and service information [Jendricke et al., 2002].[4] New trends include general ubiquity, new context-aware applications and services, new network and terminal technologies, flexible spectrum management and dynamic reconfiguration of terminals and networks in response to user mobility, user behavior and capacity optimization. Most of these trends have surely an impact on the user's privacy (both in terms of access control and of published data), due to the additional user profile attributes that should be added in a mobile context (e.g., location, context, and terminal capability). Users are thus more and more aware of the impact of these developments on their personal privacy. Having a framework that gives a systemic view of the digital identity management represents a step to be explored to reinforce users' mobile trust in mobile systems, enhancing the penetrability level of mobile applications, and services in today society.

As it is visible from Figure 2, a *Digital Identity Management Framework* is realized by taking into consideration both the real internal dynamics char-

[4]We will talk more about mobile digital identity in Section 5.

acterizing a use-case scenario, and the main external elements that may influence the architecture of an identity manager (e.g., regulations, standards, and so on). In particular, with respect to the internal dynamics we have identified the following five main elements.

User. The service requestor associated with a profile. According to application and communication context, a subset of personal data is extracted from the user profile to create the user's *personal identity*. The digital identity management framework should allow the user to keep her desired level of privacy depending on the situation, presenting multiple user "appearances" in different circumstances. In a mobile scenario, a portable user identity might include the following information:

- *profile information* that consists of a number of static (e.g., date of birth, place of birth) and dynamic attributes (e.g., technical skills and role);
- *preferences in system usage* (e.g., browser settings) and other personal preferences that do not depend on the system (e.g., UK or US English spelling);
- *behavioral information* that may be derived by an history of previous interactions with the system.

Service Provider. The supplier of network services and applications.

Context. The particular situation in which user interacts with the system. It includes the channel information (i.e., device and network features), the location information (i.e., cell, country, town) and time information.

Communication. It is based on well-known secure mechanisms to enable anonymity and confidentiality like *Secure Socket Layer* (SSL) [Freier et al., 1996].[5] Referring to anonymity, it is interesting to see that there are some possibilities for users to remain anonymous even in a world of SIM-based authentication, since the authentication step is not repeated when roaming; rather the users hold a reusable, temporary identification provided by the local mobile network. At the network level, therefore, mobile users have no fixed device address and, in principle, are identified only by the location. Location-based addressing ensures that no information that can be traced back to a specific device is required for communication on the datalink and network level of the protocol stack.[6]

[5] These mechanisms work at the packet level and sit on top of the on-the-air encryption mechanism offered by some 3G networks.

[6] Also, service discovery relies on a broadcast message on the part of the service provider. Terminals do not have to become active, and can avoid revealing their presence just for discovering services the user may not be interested in.

Device. The terminal that provides the physical layer services (e.g., a radio interface) used to communicate data and to interact with context and service providers. Moreover, the device becomes the physical place in which user profile, context and communication could be revealed and analyzed. For this reason, the terminal must be able to change the information it discloses much in the same way as the user.

Interactions among the five elements of the internal subsystem is aimed at enabling users to express and enforce their privacy and security needs, according to their specific requirements.

We are now ready to describe some of the external aspects that may influence the Digital Identity Management Framework.

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

- *Confidentiality.* The guarantee that information is read only by the intended receiver. In turn, confidentiality can be split into three main elements: integrity of message content, protection of location information (location-based information should be related to a specific user and device only with her consent) and support for sender/receiver anonymity. The latter element can be seen as relying on mobile terminals being capable of revealing SIM authentication data only in well-defined situations and to well-defined partners; in all other cases, users are capable to act under a pseudonym without revealing the true identity.
- *Integrity.* Transmission of information is executed by using cryptographical mechanisms (symmetric and asymmetric) to identify and detect eventual manipulation of information.
- *Accountability.* Information exchange by using encryption techniques and digital signatures is very important for security and trust.
- *Notice.* An alert service must be available to draw the user's attention to situations in which privacy and security could be affected. Notice mechanisms should be manual whenever automatic solutions could compromise user's security.
- *Data collection.* Users should be able to actively manage their own data, deciding whether and which identity presented to device and applications [Ceravolo, 2003]. Data collection must be inspired to the principle of data minimization, by which data should only be collected for a specific purpose.

Technologies for Mobile Security. As we have seen in the previous Section, technologies for 2G mobile security provide standard functions

for checking the subscriber identity authenticity, for protecting the subscriber anonymity and for encrypting user and signaling data. 3G, while retaining SIM-based authentication, enhances security features organizing the issue in four domains: access, network, user and application, and adding auxiliary information on visibility and configurability. For packet data traveling over the mobile network layer, conventional security technologies apply. Two main areas can be identified:

- *Security Network Domain.* When Mobile IP is used at the network level over a mobile infrastructure, the most salient security issue is the problem of how to authenticate the registration messages that inform the server about a mobile node's current IP address, in order to avoid spoofing and IP impersonation attacks [Cheswick et al., 2003].[7]
- *Security Transport Domain.* The well-known Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols provide entity authentication, data confidentiality, and data authentication.

Trust Management. In the previous Section we saw how SIM-based authentication is the main technique for linking a terminal to a user identity. To secure this mechanism, however, specifical mobility-related threats must be addressed. As they get smaller, mobile terminals become more and more susceptible to theft. Stolen data is often regarded as being more valuable than the terminal itself. Thus, the need to protect user data and secrets is of paramount importance in a 3G mobile computing environment. Since 1999, the *Trusted Computing Platform Alliance* (TCPA) [Trusted Computing Platform Alliance,] was created to foster industry participation in the development of an open specification for a trusted computing platform focused on two areas: ensuring privacy, and enhancing security. The TCPA provides for a platform root of trust, which uniquely identifies a particular platform, and provides various encryption capabilities, including hardware-protected storage.

Digital Rights Management (DRM). DRM mobile networks rely on two crucial standards: the *Open Mobile Association* (OMA) DRM [OMA DRM Requirements - Vers and OMA Download (OMA 2004) [Generic Content Download Over The Air Specification - Versio OMA DRM is the Digital Rights Management standard language for mobile phones published by the Open Mobile Alliance, while OMA Download is the application-level protocol that enables reliable and

[7]Mobile IPv4 and Mobile IPv6 solve this issue by using a protocol specific authentication extension based on a secret key shared between mobile node and home agent, and by reusing IPSec protocol to secure the binding updates, through Internet Key Exchange (IKE) protocol, respectively.

secure downloading to mobile terminals of digital content whose access rights are specified using OMA DRM. OMA Download can be integrated to other channel-specific services such as billing, and management of premium priced. However, OMA DRM and OMA Download are different technologies designed for independent purposes. Taken together, they enable secure downloading of digital content to mobile terminals and improve the consumer's experience of mobile content. Content protected by OMA DRM can be delivered using the OMA Download or other channel-specific protocols such as the *Multimedia Message System* (MMS).

4 Wireless heterogeneous environments: toward ubiquitous networking

We are now ready to discuss the integration of different wireless technologies, like 2.5 or 3G cellular networks and WiFi (IEEE 802.11b and 802.11g) [Board,] into the more general landscape of *ubiquitous networking*. Ubiquitous networking is aimed at addressing the users' need of seamlessly roaming from one connection mode to the other without impairing their on-going operations. Accordingly, multi-mode cards (e.g., LAN-WLAN-GPRS cards) have been launched on the market and are becoming increasingly affordable. In particular, the advent of 3G is likely to make those multi-mode cards rapidly evolve to the LAN-WLAN-3G setting thus transforming portable devices - cellular phones, laptops, and PDAs - in *multi-mode devices* equipped with cards that permit connections to multiple heterogeneous networks.

However, to foster effective mobility and ubiquitous computing through networks built on different wireless technologies, many fundamental issues need to be taken into consideration. An important one is the integration at link level between WiFi and GPRS/3G, which could result in a uniform network level. Realizing a uniform network layer between WiFi and GPRS/3G, in turn, may facilitate *transparent mobility*, that is, the possibility for users to automatically switch from one wireless network to another (possibly based on a different technology) without any detriment to on-going Internet transactions or application service provision. There are many high-value mobile application services that will greatly benefit from transparent mobility such as Tele-Medicine, Intelligent Transport Systems (ITS), and mobile Geographical Information Systems (mGIS).

As an example, we could imagine a mobile user connected to a certain WLAN that is performing an Internet transaction or is interacting with complex application services. In the course of such a transaction, the user could be moving close to the physical limit of the WiFi Access Point range of transmission.[8] Before loosing network connection, the user's device may,

[8]The available physical range might be limit by other parameters other then the pure

for example, switch to a GPRS/3G cell. Transparent mobility should permit to keep the Internet transaction alive (this could be a logical property, since physically the user connection with the first provider must be terminated and a new one established with the second). Finally, the same user that keeps moving, could enter into the range of a new WLAN and switch back to WiFi. To achieve features like the one described, the user should use several devices (e.g., laptops, PDAs, and Cellphones) or a unique multi-mode device.

Transparent mobility is characterized by successfully migrating live TCP connections during the handoffs through different wireless technologies (WLAN $\rightarrow$ GPRS/3G handoff and GPRS/3G $\rightarrow$ WLAN handoff). To do this, it is not only sufficient a seamless inter-network handoff mechanism, but also the connectivity (as devices keep moving across environments while still minimizing any disruption to ongoing flows during switchovers) is another important aspect.

A mechanism that enables this has to exhibit a low handoff latency, incur little or no data loss (even in highly mobile environments), scale to large internetworks, adapt to different environments, and act as a conjuncture between heterogeneous environments and technologies without compromising on key issues related to security and reliability [Vidales et al., 2003]. For all these reasons, transparent mobility is indeed one of the most challenging goals of ubiquitous computing in wireless heterogeneous environments.

Network technologies that are actively used for such systems are [Chakravorty et al., 2003]: *Mobile IPv4* (MIPv4) and *Mobile IPv6* (MIPv6). MIPv4 is the network technology traditionally used to foster seamless roaming for ubiquitous computing systems, mainly due to its compatibility with the wired IP-based network infrastructure. Nevertheless, MIPv4 limitations have forced the development of overly complex systems and protocols. MIPv6 promises to overcome some of MIPv4 limitations and improve security, although it has other disadvantages in high mobility scenarios [Chakravorty et al., 2003, Perkins and Johnson, 1996]. Some current studies are then actively exploring the possibility to make use of approaches similar to those used in micro-mobility protocols that are aimed at improving the transparent roaming of mobile hosts at the subnet level of a network domain. Such protocols reduce the handoff latency and improve performance under high mobility scenario [Campbell and Gomez-Castellanos, 2001]. An IETF working group, called Seamoby [Kempf, 2002], has been formed aiming to resolve complex interaction of parameters and protocols needed for seamless handoffs and context transfers between nodes in an IP access network.

Ubiquitous computing in wireless heterogeneous environments needs operational features and security requirements to be provided [Vidales et al., 2003]. For instance, two interesting and fundamental open issues are the following.

transmission range, such as the Quality of Service (QoS).

- *Link-Switch Decision Rule-base.* Current schemes that regulate handoffs operate based on link layer information, such as signal strength. However, this could be insufficient to assist the handoff process in heterogeneous environments. Signal quality, overall link characteristics and robustness, link cost, as well as security considerations might be other parameters that need to be evaluated to decide the handoff. In particular, with respect to the security-related information, it has to be taken into consideration the *trust relationship* or the *reputation of the network provider* (WiFi or GPRS/3G), and the technical provisions put in place to guarantee a certain security level (e.g., *message security* mechanisms or *mobile identity management*).

- *Context-Awareness.* A mobile device context involves aspects such as physical context variables (e.g., device location, movement direction, velocity, and so on), application characteristics and, of course, user-based preferences. Context-awareness is necessary to take informed decisions about switching to a different network and provider. For instance, based on the exact position (e.g., available from a GPS system) and velocity available to a mobile host (e.g., speed sensors), a given proxy in the infrastructure can assist mobility by tracking and accurately predicting when a handoff should occur. This may let a user anticipate the link-switch decision before reaching the physical network connectivity limit. The user may then evaluate whether the next network provider is reliable and secure with respect to her on-going Internet transactions.

4.1 Multilateral Security

Multilateral security is an important factor to consider for wireless heterogeneous environments. Traditional security approaches assume that the whole set of actions that could be legally performed on corporate IT resources can be fully described in a security policy. Consequently, corporate security is achieved by enforcing the security policy throughout a secure and trusted entity. *Multilateral security*, instead, considers different and possibly conflicting security requirements of different parties that cannot be efficiently regulated through a static security policy [Rannenberg, 2000, Rannenberg et al., 1999]. Some examples of conflicting security requirements of different parties in networks are the following.

- *Service requesters* cannot fully trust service providers (e.g., network operators) because they could perform unsolicited actions such as monitoring, profiling, and, in general, collecting data from the service offered to the users.

- *Service providers* might be victims of frauds or malicious service misuse caused by service requestors.
- *Network operators* could be harmed by breaches caused by network intrusions, sabotage, or other risks that could lead to network failures and downtime periods.
- *Users* of network connections might be harmed by other users.

Multilateral security copes with these competing security requirements of different parties and aims to strike a balance among them. *Open communication systems* (e.g., networked services based on the telephone or on the Internet) often exhibit these characteristics and an high degree of untrustworthiness. A possible approach for multilateral security consists in taking into consideration the security requirements of all parties involved and, at the same time, considering the parties as potential attackers.

Two technical areas are considered especially important in multilateral security [Rannenberg, 2000, Rannenberg et al., 1999]:

- *Negotiation.* Negotiating security requirements is a natural way to set common security practices and foster cooperation among communicating parties. A related approach, although developed for a different technology, has been proposed by the Platform for Privacy Preferences (P3P) project of the Word Wide Web Consortium [Consortium, 1998]. The P3P project, as well as multilateral security, aims to set a standard for reaching agreements with service providers about the collection and use of personal information.
- *Secure Architectures.* Security measures located on devices are not sufficient alone to satisfy all security requirements. For instance, transaction recovery after an handoff between WLAN and 3G/GPRS has associated security risks that cannot be prevented with device-based countermeasures only. Hence, architectural security measures must be put in place protecting communication functions and network operations.

A number of technical design principles that support the development of multilateral security architectures and solutions have been proposed and they can be summarized as follows.

- *Data Economy.* Data economy states that the only way to keep confidential data on which users have no control, is to avoid those data. For instance, in communication protocols only data under the control of users should be transmitted. This principle is particularly important for identification data. The strategy of data economy aims at minimizing data transmitted and at transmitting only those personal data

that were explicitly authorized by the owner. This prevents security risks and reduces the cost and complexity of data protection.

- *Careful allocation.* Data that are needed to conduct Internet transactions or to obtain networked services must be carefully allocated. This means that systems must permit a strict control over both the ownership and the location of such data.

- *User ability to control.* Negotiating security requirements between communicating parties often results in trade-offs that strike a balance among conflicting requirements. Users should keep the control of the outcome of the trade-off and actively monitor how the security context evolves. This might be achieved by means of monitoring consoles, tools providing status information and the access to configuration/administration interfaces.

- *Usability of security mechanisms.* Lack of usability in security mechanisms is a well-known problem that has impaired many security solutions. Multilateral security prescribes the adoption of usable mechanisms only. This is a challenging principle since usability is a dynamic notion that may vary for different users at different stages of interest, understanding, and competence.

- *Opportunities for individual negotiation.* Negotiation can only work if there are real options and opportunities to negotiate on. This may need economic and regulatory frameworks to balance the usually different power of communicating parties or network operators.

5 Mobile Identity Management

Wireless heterogeneous environments present many challenges in the area of *digital identity management*. As previously mentioned, digital identities are the electronic representations of individuals' or organizations' sensitive information [Damiani et al., 2003]. In everyday life experiences, the personal identity is not a unique, monolithic concept. Instead, the identity is a complex concept made up of many different attributes and each one manages her own identity according to the circumstances that ask for personal identification data. Normally, only those personal information that are needed to access a certain service are disclosed. *Digital identity management* is then defined as the ability to selectively disclose only those personal information related to the service, while preserving and enforcing privacy and security needs, such as protection from possible theft of identities for later illegal usage, requirements of anonymity, and use of pseudonyms. These security and privacy-related issues have contributed to the develop-

ment of the notion of *mobile identity management* [Jendricke et al., 2002, Roussos and Patel, 2002].

In general, as described in [Jendricke et al., 2002], the strategic impact of mobile identity management can be evaluated along three major areas: increasing *operational efficiencies* without compromising security, increasing degree of *personalization of services* as well as active consumer management, and finally increasing rate of *development of novel services* thus increasing revenue streams.

Therefore, the ultimate goal of mobile identity management is to increase trust between businesses, consumers, and trading peers, so as to enable a wider adoption and access to network services. In the context of mobile users roaming through heterogeneous environments and accessing critical corporate resources and possibly exchanging sensitive data, mobile identity management benefits represent certainly a strong incentive to its development.

Mobile identity management systems support a collection of different *interaction modes*. The simplest mode of interaction is *peer-to-peer*. In this case, identification and credential exchange is performed without the mediation of a third party (e.g., a Certification Authority) in a distributed, and decentralized manner. Significantly more complicated is the support by mobile identity management systems of *nomadic* and *ad-hoc conferencing*. To do so, it is necessary to provide mechanisms for group member identification, membership control and access to common resources, either within the context of a single organizational unit. Finally, the last operational mode we present is a fully deployed mobile identity management system in *intra-organization* or even *global scale*, which requires a global mobile identity infrastructure that should be open, fully interoperable, and distributed.

However, current mobile identity management systems have to cope with the extra requirements of an heterogeneous context. Areas that are likely to require improvements are interoperability, roaming and self-configuration, as well as privacy protection and security. For instance, many mobile identity management systems are based on Public Key Infrastructure (PKI) technologies that have proved not to scale well and have shown many interoperability problems in practical contexts. These limitations may impair the development of mobile computing in wireless heterogeneous context, which in turn are heavily based on strong interoperation requirements for authentication. Modern trust management systems exhibit better characteristics that may well support mobility. Moreover, whether interactions between nomadic users and wireless network providers are carried out in a peer-to-peer style, centralized solutions (e.g., PKIs) could not be adopted: in the case of ad-hoc interactions the peers cannot resolve certificate chains without incurring in high latencies due to the indirect access to verification resources.

It has been widely recognized the relevance of requirements exposed

in multilateral security for the foundation of mobile identity management. Clauss and Kohntopp have explicitly developed the SONET system for identity management on the basis of multilateral security principles [Clauss and Kohntopp, 2001]. Jendricke et al. [Jendricke et al., 2002] have derived the following relevant privacy principles for mobile identity management directly from multilateral security requirements.

- *Confidentiality and Integrity.* A mobile identity management system must support cryptographic techniques and key exchange protocols to achieve confidentiality and message integrity.

- *Anonymity and Pseudonymity.* There are situations where Internet transactions should not be linked to individuals. Users should have the possibility to conceal their own true identities by using pseudonyms or even by accessing services anonymously. High mobile users equipped with multi-modal wireless cards should have the ability to selectively disclose personal information or use pseudonyms.

- *Availability.* Wireless connections are by nature more prone to network failures than wired systems. Handoffs between WiFi and 3G/GPRS providers might introduce new failure possibilities. On the contrary, although handoffs are critical operations, multi-mode network access might be used for alleviate disconnection problems if a backup recovery mechanism exists. For instance, a WLAN connection may experience connectivity problems and an on-going Internet transaction could unexpectedly terminate. In this case, if the 3G/GPRS mode was used as a backup to save some safe state of the user session, switching to the 3G/GPRS link, the transaction could be recovered from that safe state. Transaction recovery is indeed an extremely important area for multihop mobility in heterogeneous environments that should be integrated with mobile identity management. Security risks may arise if recovery features could be misused by attackers that impersonate other digital identities and reclaim the recovery of transactions belonging to different users.

- *Accountability.* Wireless service providers, such as hotspot providers and 3G/GPRS telco, would probably offer their network connection facilities at a market price. Billing systems, linked to digital identities or pseudonyms, are likely to be the target of subversion attacks and need to be carefully protected.

- *Security-awareness.* A basic security principle that even mobile identity management systems have to satisfy is that users must always be fully informed of security-related action performed on their behalf by devices. In this way, an informed user must ultimately do evaluations

about the security risk associated with the switch to a certain wireless network provider and decide how to negotiate security requirements. Those decisions cannot be taken automatically and transparently by the device on its own and based, for example, on PKI certificate chains or reputation mechanisms. Techniques and tools are of extreme value when effectively assist users to take an informed decision, but they may turn out to be harmful when they substitute users or even make them incapable of enforcing their own decision.

- *Data Collection.* A basic principle of identity management that should always been enforced is that users must be able to decide which personal data disclose to whom. It is not sufficient that users were fully informed of which data have been disclosed and collected. Minimizing disclosed personal data actually represents the main task of an identity management system.

6 Multihop Hotspots

Hotspot providers in public area represent key components of an heterogeneous wireless infrastructure for mobile users, which could be used to access WLAN services while moving. *Multihop hotspots*, in particular, are hotspots through which users could roam seamlessly. Considering heterogeneous environments, users could hop through hotspots that are either physically contiguous, thus directly switching from one hotspot to another, or through a sequence of multi-mode handoffs between hotspots and GPRS/3G cells [Balachandran et al., 2003].

With respect to security, hotspots have still significant open issues. One is *authentication* that is currently implemented with different and incompatible techniques by commercial WiFi networks. For instance, since hotspots are often under the control of different providers, users will have to repeat the authentication procedure (possibly different for each hotspot) at each hotspot location. Also, some commercial hotspot providers offer access to users through pre-established accounts, while others offer scratch-off cards containing a one-time login and password.

A uniform and shared authentication infrastructure is fundamental for effective multihop mobility since highly mobile users cannot be required to cope with different authentication schemes, mechanisms, and configurations at each handoff. Clearly, the goal of providing fast and seamless authentication, while simultaneously ensuring user accountability, raises several research problems that are today still unsolved.

- *Ease of Access.* Single-Sign-On (SSO) features encompassing multihop hotspots are needed to support transparent mobility and reduce the latency.

- *Mechanism.* What authentication mechanisms are best suited in such an environment? Is it adequate for the network to authenticate the users through software mechanisms such as identity certificates or digital tokens or are hardware mechanisms, such as SIM cards, needed?

- *Identity Management.* The mobile identity a user presents to each network provider could change according to context-related information such as provider reputation, QoS, location or other contextual attributes. Which mechanism can permit an effective context-awareness and negotiation of identity attributes and at the same time minimize the latency of the handoff?

- *Third-Party Authenticators.* Should authentication be delegated to dedicated third parties offering such a service for the whole multihop infrastructure?

Another challenge to multihop mobility is *wireless hop security.* Traditional security mechanisms - like SSH, SSL or VPN - provide end-to-end data privacy to communicating parties. These mechanisms are not always well suited for multihop mobility because intermediaries - like network providers, gateway or proxies - might need to access and inspect message-specific information. This could be asked for security reasons as well as for routing, accountability, or recovery.

To this end, novel approaches, for example realized in the area of Web services, have developed per-message security solutions that permit to selectively disclose information carried by messages to specific intermediaries. In this way, information carried by a network message could be targeted to different destinations. For instance, some control information could be disclosed to intermediaries for authentication, access control, or routing. Other information could be delivered to the final endpoint of the communication and then kept private during the whole multihop session.

7 Security and Privacy Issues in Mobile User Recovery

Recently, an important contribution to mobile computing has been published by VanderMeer et al. [VanderMeer et al., 2003]. In their work, the authors address the problem of recovery Internet transactions initiated by mobile users. The issue is new and relevant since it presents many differences with respect to classical database transaction recovery. Also, it appears extremely important in the context we have considered, since there is not only the case of recovery after a network failure, but there is the peculiar situation of recovery user activity after an handoff. This aspect is an additional novel issue to the most general problem of mobile user recovery.

This issue has also significant links with security and privacy since mobile user transactions and mechanisms for recovery could become critical points of security risk and been targets of network attacks and subversion attempts. If network attacks would eventually succeed, it will be possible for an intruder, for example, to subvert the recovery mechanism and then recover transactions of other users possibly gaining their privileges. By attacking a recovery mechanism could also be possible to access transactions' state information that still could let intruders impersonate users or gathering sensitive information. Denial-of-service attacks towards the recovery systems is another threat that might severely impairing the benefits of the infrastructure for ubiquitous computing and transparent mobility.

Security researches in this area are still at the beginning since even operational features, like mobile user recovery, are in their initial stages. Despite this, the issue looks extremely important for future evolution of ubiquitous computing and transparent mobility. In the following the characteristics of mobile users recovery are presented, according to [VanderMeer et al., 2003].

Firstly, consider a simple case study to describe the peculiarities of mobile user recovery. A user is buying an airline ticket over his wireless Internet connection. She may execute typical Web operations like: logging on to the airline site with her frequent flier number, entering travel dates and destination, selecting the preferred seat, and finally entering credit card information and receiving a confirmation of the purchase. Typically, this interaction spans multiple sites, that is, at least the travel agency and the company in charge of processing payment information. In wireless heterogeneous environments, mobile users may have switched several times on different links and modes through the life of the described Internet transaction. The flow of operations executed by the user during her ticket purchase should proceed seamlessly after each handoff.

Considering the underlying mechanisms that support transparent mobility, it has many elements in common with Internet user recovery since in both cases a transaction state has to be stored somewhere and then recovered when the new connection is established.

As a consequence, requirements in terms of efficiency, performance and transparency have an increased importance.

In the scenario described above, the goal is to be able to avoid the repetition of work (computation, communication, I/O) required after a connection disruption, thus minimizing the cost for recovery. Solutions for recovery of such interactions are quite different from classical system transaction recovery. In recovering database transactions, the focus is on ensuring that the status of the underlying database system is consistent: if a transaction prematurely aborts, the transaction is rolled back and is resubmitted after the database system recovers.

In mobile computing, in addition to the classical recovery problem, we need to minimize (or to completely avoid), the user task of resubmitting

the transaction again. The recovery infrastructure should permit users to efficiently and quickly restart from an appropriate point prior to disconnection. For this reason VanderMeer et al. have proposed the expression *user recovery* in place of the traditional *system recovery*.

Therefore, the first goal is to define the *user state* during her flow of operations. The proposed approach observes the sequence of operations as they occur, logs state information corresponding to each operation, stores the state information, and utilizes it to recover the user to a useful point in her interaction. User state information may span through multiple Web sessions and multiple service providers. For this reason, along with user recovery, the notion of *user session* was introduced to encompass all active Web sessions included in the on-going user transaction. A user state, after the execution of a given action, has been define as a 4-tuple composed by: the set of *cookies* valid after the given action; the *HTTP request* corresponding to the given action; the *site's response* to the user HTTP request; and a *function* denoting the validity of the user state.

Based on the notion of user state, a *recovery protocol for Internet transaction* should have the ability to: *store user states* to be used in the case of connection failure; and *return a recent and valid state* to the user upon reconnection after failure.

Intuitively, the recovery protocol that has been proposed works in the following way. It logs user states for each action in *action logs* and maintain a *failover map* of various sub-transactions. This information is needed to recover after and handoff too.

According to this proposal, several important issues that may affect security arise.

- *The secure storage and access to action logs, failover maps, and recovery logic.* There could be different choices, from storing them locally to the device, to storing them at network gateways or specialized recovery hosts. Indeed, a support to recovery features from the network infrastructure is needed. This introduces security issues related to trust relationships with third parties or networked components in charge of recovery user sessions. Also, distributed authentication mechanisms should be in place because users that switch from some links (e.g., from WiFi providers), might reconnect later to different network providers with different modes (e.g., to 3G/GPRS telcos).

- *Trustworthy generation of action logs and failover maps.* The generation of state information must be secured and trustworthy. State information must be protected from tampering and disclosure since network components in charge of generating and store state information are probable points of attacks. Moreover, the usage of cookies to simulate HTTP sessions is traditional target of intrusions for gathering information that let attackers impersonate Internet users. Secure

management of session state information is important to secure hand-offs and transactions management.

- *Trustworthy management and usage of users action logs and failover maps.* User authentication is another important aspect for the security of user session's recovery. For instance, imagine a user that disconnect from a certain link and only after a certain time frame reconnects to a different wireless network. What if while she is disconnected someone else reclaim the recovery of that user session? How the recovery system recognizes that this is a malicious attempt? Recall that for ubiquitous computing we need to strike a balance between ease-of-use and security to foster transparent mobility and mobile device always have to deal with the problem of power consumptions, therefore current strong authentication mechanisms might be unfeasible in this context.

8 Conclusions

The amount of mobile computing is expected to increase dramatically in the near future. As the user's demands increase with the offered services of mobile communication systems, the main expectation on such systems will be that they provide access to any service, anywhere, at anytime. Indeed, in today's highly connected, and highly mobile environments, the secure transmission of information is imperative for every enterprise, and will grow in significance as mobile devices, networks, and applications continue to advance. However, the promise of mobile computing technologies further increases privacy and security concerns. In this chapter we have discussed the need for privacy and security in mobile systems and have presented technological trends which highlight that this issue is of growing concern.

References

[Balachandran et al., 2003] Balachandran, A., Voelker, G. M., and Bahl, P. (2003). Wireless Hotspot: Current Challenges and Future Directions. In *Proceeding of the ACM WMASH'03*.

[Blanchard,] Blanchard, C. Security for the third generation (3G) mobile system. http://www.isrc.rhul.ac.uk/useca/OtherPublications/3G_UMTS%20Security.pdf.

[Board,] Board, I. S. 802 part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications.

[Campbell and Gomez-Castellanos, 2001] Campbell, A. T. and Gomez-Castellanos, J. (2001). IP Micro-Mobility Protocols. *ACM Mobile Computing and Communications Review (MC2R)*, ACM SIGMOBILE.

[Ceravolo, 2003] Ceravolo, P. (2003). Managing identities via interactions between ontologies. In *Proc. of the Workshop on Metadata for Security*, Catania, Italy.

[Chakravorty et al., 2003] Chakravorty, R., Vidales, P., Subramanian, K., Pratt, I., and Crowcroft, J. (2003). Practical Experiences with Wireless Integration Using MobileIPv6. In *Proceedings of the ACM MOBICOM 2003*.

[Chaum, 1985a] Chaum, D. (1985a). Security without identification: Transaction systems to make big brother obsolete. *Communications of ACM*, 28(10):1030–1044.

[Chaum, 1985b] Chaum, D. (1985b). Showing credentials without identification. signatures transferred between unconditionally unlinkable pseudonyms. In *Proc. of a Workshop on the Theory and Application of Cryptographic Techniques*, Linz, Austria.

[Cheswick et al., 2003] Cheswick, W., Bellovin, S., and Rubin, A. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison Wesley.

[Clark, 1993] Clark, R. (1993). Computer matching and digital identity. In *Proc. of the Conference on Computers, Freedom & Privacy*, San Francisco, CA, USA.

[Clauss and Kohntopp, 2001] Clauss, S. and Kohntopp, M. (2001). Identity Management and its Support of Multilateral Security. *Computer Networks*, Elsevier Science, 37:205–219.

[Consortium, 1998] Consortium, W. W. W. (1998). P3P Guiding Principles. http://www.w3.org/TR/1998/NOTE-P3P10-principles.

[Damiani et al., 2003] Damiani, E., di Vimercati, S. D. C., and Samarati, P. (2003). Managing Multiple and Dependable Identities. *IEEE Internet Computing*, pages 2–10.

[Freier et al., 1996] Freier, A., Karlton, P., and Kocher, P. (1996). The SSL Protocol - Version 3.0. http://ftp.nectec.or.th/CIE/Topics/ssl-draft/INDEX.HTM.

[Generic Content Download Over The Air Specification - Version 1.0, 2003] Generic Content Download Over The Air Specification - Version 1.0 (2003). Generic content download over the air specification - version 1.0. http://www.openmobilealliance.org/tech/release.html.

[Herbert et al., 1999] Herbert, D., Ulrich, P., and Martin, R. (1999). *Personal Reachability and Security Management - Negotiation of Multilateral*

Security, chapter Technical Building Blocks, pages 95–112. Addison Wesley Longman.

[Howard, 2000] Howard, P. (2000). 3G security overview. In *Proc. of the IIR Fraud and Security Conference*. http://www.isrc.rhul.ac.uk/useca/OtherPublications/IIR-overview.pdf.

[Jendricke et al., 2002] Jendricke, U., Kreutzer, M., and Zugenmaier, A. (2002). Mobile Identity Management. In *Proceedings of the Workshop on Security in Ubiquitous Computing (UBICOMP2002)*.

[Kagal et al., 2001] Kagal, L., Finin, T., and Joshi, A. (2001). Trust-based security in pervasive computing environments. *IEEE Communications*.

[Kagal et al., 2003] Kagal, L., Parker, J., Chen, H., Joshi, A., and Finin, T. (2003). *Security, Privacy and Trust in Mobile Computing Environments*, chapter Security and Privacy Aspects. CRC Press.

[Kempf, 2002] Kempf, J. (2002). Problem Description: Reason for Doing Context Transfers Between Nodes in an IP Access Network. *IETF Request for Comments*, RFC 3374.

[Matskin and Tveit, 2003] Matskin, M. and Tveit, A. (2003). Software agents for mobile commerce services support. In Siau, K., editor, *Advanced Topics in Database Research*, volume 2, chapter 11, pages 246–266. Idea Group Inc.

[OMA DRM Requirements - Version 2.0, 2003] OMA DRM Requirements - Version 2.0 (2003). OMA DRM requirements - version 2.0. http://member.openmobilealliance.org/ftp/Public_documents/BAC/DLDRM/2003/OMA-DRM-REQ-v2_0-20030515-C.PDF.

[Open Source Security Testing Methodology Manual,] Open Source Security Testing Methodology Manual. *Open Source Security Testing Methodology Manual*. http://www.isecom.org/projects/osstmm.shtml.

[Perkins and Johnson, 1996] Perkins, C. E. and Johnson, D. B. (1996). Mobility Support in IPv6. In *Proc. of the ACM MOBICOM*.

[Rannenberg, 2000] Rannenberg, K. (2000). Multilateral Security - Concept and Examples for Balanced Security. In *Proceedings of the 9th ACM New Security Paradigms Workshop*.

[Rannenberg et al., 1999] Rannenberg, K., Pfitzmann, A., and Muller, G. (1999). *Multilateral Security in Communications - Technology, Infrastructure, Economy*, chapter IT Security and Multilateral Security. Addison-Wesley Longman.

[Roussos and Patel, 2002] Roussos, G. and Patel, U. (2002). Mobile Identity Management. In *Proceeding of Mobile Business 2002*.

[Smith, 2002] Smith, R. (2002). *Authentication: From Passwords to Public Keys*. Addison Wesley.

[tom Markotten et al., 2001] tom Markotten, D., Jendricke, U., and Müller, G. (2001). *Benutzbare Sicherheit – Der Identitätsmanager als universelles Sicherheitswerkzeug*, chapter 7, pages 135–146. Springer-Verlag Berlin.

[Trusted Computing Platform Alliance,] Trusted Computing Platform Alliance. Trusted computing platform alliance. http://www.trustedcomputing.org/home.

[Tsalgatidou et al., 2000] Tsalgatidou, A., Veijalainen, J., and Pitoura, E. (2000). Challenges in mobile electronic commerce. In *Proc. of the 3rd International Conference on Innovation through E-Commerce*, Manchester, UK.

[van Oorschot et al., 1996] van Oorschot, P., Menezes, A., and Vanstone, S. (1996). *Handbook of Applied Cryptography*. CRC Press.

[van Rossum et al., 1995] van Rossum, H., Gardeniers, H., and Borking, J. (1995). Privacy-enhancing technologies: The path to anonymity.

[VanderMeer et al., 2003] VanderMeer, D., A, D., Dutta, K., Ramamritham, K., and Navathe, S. B. (2003). Mobile User Recovery in the Context of Internet Transactions. *IEEE Transactions on Mobile Computing*, 2(2):132–146.

[Vidales et al., 2003] Vidales, P., Patanapongpibul, L., and Chakravorty, R. (2003). Ubiquitous Networking in Heterogeneous Environments. In *Proceedings of the 8th IEEE Mobile Multimedia Communications (MoMuC 2003)*.