Handbook of Research on Wireless Security

Yan Zhang
Simula Research Laboratory, Norway

Jun Zheng
City University of New York, USA

Miao Ma
Hong Kong University of Science and Technology, Hong Kong

Volume I

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey · New York

Acquisitions Editor: Kristin Klinger
Development Editor: Kristin Roth
Senior Managing Editor: Jennifer Neidig
Managing Editor: Sara Reed
Copy Editor: Ashlee Kunkel, Holly J. Powell
Typesetter: Jamie Snavely, Carole Coulson
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Library of Congress Cataloging-in-Publication Data

Handbook of research on wireless security / Yan Zhang, Jun Zheng, and Miao Ma, editors.

p. cm.

Summary: “This book combines research from esteemed experts on security issues in various wireless communications, recent advances in wireless security, the wireless security model, and future directions in wireless security. As an innovative reference source for students, educators, faculty members, researchers, engineers in the field of wireless security, it will make an invaluable addition to any library collection”--Provided by publisher.

Includes bibliographical references and index.

ISBN 978-1-59904-899-4 (hardcover) -- ISBN 978-1-59904-900-7 (ebook)

1. Wireless communication systems--Security measures. I. Zhang, Yan, 1962- II. Zheng, Jun, Ph.D. III. Ma, Miao. IV. Title.

TK5102.85.H35 2008

005.8--dc22

2007036301

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter VIII
Identity Management for Wireless Service Access

Mohammad M. R. Chowdhury
University Graduate Center – UniK, Norway

Josef Noll
University Graduate Center – UniK, Norway

ABSTRACT

Ubiquitous access and pervasive computing concept is almost intrinsically tied to wireless communications. Emerging next-generation wireless networks enable innovative service access in every situation. Apart from many remote services, proximity services will also be widely available. People currently rely on numerous forms of identities to access these services. The inconvenience of possessing and using these identities creates significant security vulnerability, especially from network and device point of view in wireless service access. After explaining the current identity solutions scenarios, the chapter illustrates the on-going efforts by various organizations, the requirements and frameworks to develop an innovative, easy-to-use identity management mechanism to access the future diverse service worlds. The chapter also conveys various possibilities, challenges, and research questions evolving in these areas.

INTRODUCTION

Nowadays people are increasingly connected through wireless networks from public places to their office/home areas. The deployment of packet-based mobile networks has provided mobile users with the capability to access data services in every situation. The next-generation wireless network is expected to integrate various radio systems including third generation (3G), wireless LANs (WLANs), fourth generation (4G), and others. One motivation of this network is the pervasive computing abilities, which provide automatic handovers for any moving computing devices in a globally networked environment. Fast vertical handover is considered important for managing continued access to different types of network resources in next generation networks (Li et al., 2005). Such networks will provide ubiquitous service access taking the advantages of each of these forms of wireless communications. Service intake will be increased significantly through the availability and reach of innovative and easy-to-use services. Apart from the remote service access (Web services), the introduction of near field communication (NFC) in use with a mobile phone can enable many new proximity services.

User identity solutions and its hassle-free management will play a vital role in the future ubiquitous service access. Current identity solutions can no longer cope with the increasing expectations of both users and service providers in terms of their usability and manageability. Mobile and Internet service providers are increasingly facing the same identity management challenges as services in both domains continue to flourish. Real-time data communication capabilities of mobile networks will multiply the remote service accesses through mobile networks, if efficient identity management and security is ensured over the wireless access. Personalization through customized user profiles based on their preferences will become an important factor for success of future wireless service access. In more advanced service scenarios, open identity management architecture enables the use of standard user profile attributes, like age and gender, and authorizations for service, such as location, to bring a richer user experience. Users, network operators, and service providers can make use of an open standard technology for identity management to meet their own specific requirements through customizations. There is clearly a need for such a standard for identity management that can be applied to all ubiquitous service access scenarios. As user needs are at the center in the service world from business perspective, identity management mechanism should be user-centric.

The impressive capabilities and reach of emerging next-generation networks, the abundance of services, and on-going development in user device require proper address to the user identity management issues which have yet met the stakeholders' expectations. The main goal of this chapter is to discuss these concerns. The second section discusses the background of identity management. In the third section, requirements and framework of identity management mechanism for wireless service access are given mentioning the current efforts by various organizations. Security issues are also a part of this mechanism. The fourth section provides the future trends. The chapter concludes with the summary of all discussions.

BACKGROUND

In a broadest sense, identity management encompasses definitions and life-cycle management for user identities and profiles, as well as environments for exchanging and validating such information. A service provider issues identity to its users. Identity life-cycle management comprises establish/re-establishment of identity, description of identity attributes, and at the end revocation of identity. Attributes are a set of characteristics of an identity that are required by the service providers to identify a user during service interactions. User authenticates to the service providers as real owner of the identity for accessing services. Authentication is a key aspect of trust-based identity attribution, providing a codified assurance of the identity of one entity to another.

Next-generation wireless network includes state-of-the-art intelligent core network and various wireless access networks. It is expected to offer sufficient capacity, quality of service (QoS), and interoperability for seamless service access remotely. Currently the network and thereby the remote service access are often granted through numerous user identification and authentication mechanisms, such as, usernames/passwords/PIN codes/certificates. Users have to register prior to first usage and publish private information, often more than what is strictly necessary for service access. It hampers user's privacy. There is a growing consensus among the legislators across the world that individual's rights of privacy and the protection of personal data is equally applicable in the context of the Information Society as it is in the off-line world. To address this issue, a user-centric identity management framework is expected where users having complete control over the identity information transmission.

Some services happen in the proximity of users at local access points. These services are accessed through physical interactions with physical cards or devices, for example, payment and admittance. The use of NFC with mobile phones to transfer user information from one device to another boosts the intake of proximity services. The user personal

device is often used to store his/her identity information. To protect unauthorized service access, users also need to be authenticated before accessing such devices. It is evident that a user is burdened with too many identities to access many remote and proximity services. An integrated approach is required to manage all those identities to access all these services.

Wireless service access results in more complexity to manage identities prior to accessing the services. Besides device authentications, users need to authenticate themselves before accessing the wireless networks. In addition to this, because of the size limitations, mobile devices are equipped with smaller screens and limited data entry capabilities using small keypads. For wireless services to succeed, it is critical that the mobile users are able to get convenient and immediate access to the information and services they need without going through long menus and having to enter various usernames and passwords.

In the future, one of the key issues of identity management in the wireless domain will be who the identity providers will be to the users and who will own/manage the subscriber identity module (SIM/USIM). It is because, currently, almost every service provider is also an identity provider for users to access that specific service. SIM card is in fact a smart card with processing and information storage capabilities. With the development of powerful, sophisticated as well as secure smart cards, it is now considered as the storage place for user's identity information. In current cellular models, the operator provides not only the wireless access but also owns and manages SIM/USIM. In this case, the user has little control over his/her identity. A user is having a SIM/USIM as his/her identity but is not allowed to modify or update it so that he/she cannot subscribe to new wireless providers or to whatever service providers he/she likes. A collaborative operator model has been thought where such identity module belongs to the user (Kuroda, Yoshida, Ono, Kiyomoto, & Tanaka, 2004, pp. 165-166). A third party can provide the infrastructure to manage such identity. This approach leads towards user-centric identity management and provides the user with flexibility in choosing wireless providers.

In general, common identity deployment architectures can be broadly classified into three types: Silo, Walled Garden, and Federation (Altmann & Sampath, 2006, p. 496). Current identity management in the service world is mostly silo-based. Silo is a simple architecture, which requires each service provider to maintain a unique ID for each user. This approach is simpler from a service provider's point of view but it is not only laborious but also problematic for the user. Moreover, it results in a huge waste of resources due to the possession of redundant identity information in the service world. As studies show, users who register with several service providers routinely forget their passwords for less frequently used accounts. This has a significant financial effect. On average, $45 is spent on password reset each time a user forgets a password (Altmann & Sampath, 2006, p. 496). Walled Garden is a centralized identity management approach where all service providers can typically rely on one singe identity provider to manage the user's identity. The user is benefited through managing only a single set of credentials. Its inherent weakness is, once the significant barrier of protection is compromised, a malicious user enjoys unbridled access to all resources. Lastly, in identity federation management a group of service providers forms a federation. Here, each service provider recognizes the identifiers of other service providers and thereby, consider a user who has been authenticated by another service provider to be authenticated as well. However, the real distinction between Walled Garden and Federation approach is that here service providers have their own unique identifiers and credentials. Though this approach is widely accepted considering the heterogeneity of service providers, many possible service interaction scenarios and the requirements of several levels of security make such a system far more complex.

IDENTITY MANAGEMENT FOR WIRELESS SERVICE ACCESS

Designing an identity management mechanism to access both remote and proximity services, without

using numerous inconvenient identity solutions, is expected to be the main focus in the identity management for service access over wireless networks. This section also considers the selection of a user identity storage place, the role of identity provider, and various other requirements to develop such a mechanism from a wireless service access point of view.

Requirements of Identity Management Systems

Identity management system should be user-centric. It means such a system should reveal information identifying a user with user's consent. Security is one of the most important concerns of this system. The system should protect the user against deception, verifying the identity of any parties who ask for information to ensure that it goes to the right place. In the user-centric approach, the user will decide and control the extent of identifying information to be transmitted. The system must disclose the least identifying information possible. By following these practices, the least possible damage can be ensured in the event of a breach. These are some of the requirements to design a user-centric identity management system in The Laws of Identity (Cameron, 2005).

Identity management system requires an integrated and often complex infrastructure where all involved parties must be trusted for specific purposes depending on their role. Since there are costs associated with establishing trust, it will be an advantage to have identity management models with simple trust requirements (Jøsang, Fabre, Hay, Dalziel, & Pope, 2005). Success of an identity management system depends upon the ability to interoperate across a trusted network of businesses, partners, and services regardless of the platform, programming language, or application with which they are interacting. It should handle user identities for both remote (Web) and proximity service access. Above all, such a system should be user friendly.

Identity Management Solutions and Controversies

Various institutes and industries are working to develop the required identity management solutions. SXIP ("The SXIP 2.0 Overview," n.d.). identity has designed a solution to address the Internet-scalable and user-centric identity architecture. It provides user identification, authentication and Internet form fill solutions using Web interfaces for storing user identity, attribute profiles, and facilitating automatic exchange of identity data over the Internet. Windows CardSpace uses various virtual cards (mimic physical cards) issued by the identity providers for user identifications and authentications, each retrieving identity data from an identity provider in a secure manner (Chowdhury & Noll, 2007). In the Liberty Alliance Project (Miller et al., 2004), members are working to build open standard-based specifications for federated identity and interoperability in multiple federations, thereby fostering the usage of identity-based Web services. Within this, they are focusing on end-user privacy and confidentiality issues and solutions against identity theft. But these efforts are mainly focusing on identity management in the Internet domain.

Besides working for identity handling in a Web domain, Liberty Alliance (Miller et al., 2004) also provides solutions in identity management for mobile operators. It proposes single sign-on (SSO) to relieve the users from managing many usernames/passwords and for fast access to the resources. But in SSO, if a malicious attacker secures one of the user's accounts, he/she will enjoy an unbridled access to data pertaining not only to that account but also across all her accounts spread across domains. Therefore, some research approaches do not encourage such SSOs (Altmann & Sampath, 2006, p. 500). However, a current version of liberty, Shibboleth, reduces such risk by providing an attribute-based authorization system. But in wireless service access, especially for mobile devices seamless service sign-on solutions and one-click access to personalized services are key issues for successful identity management.

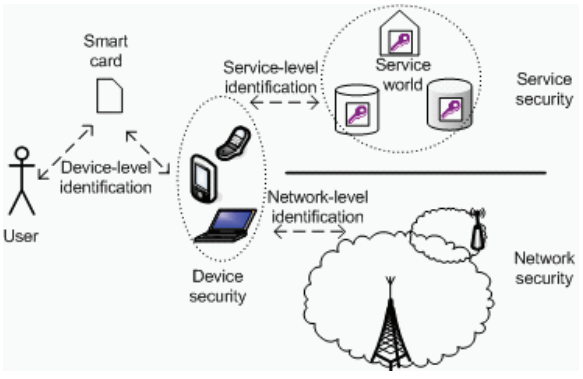
Apart from possessing numerous usernames/passwords/PIN codes for remote (Web) service access, the user is also carrying many physical identities for proximity service access. These include credit card, bank card, home/office access cards, and so forth. Many researchers working in these areas are proposing the smart cards, like SIM/USIM currently used in mobile phones, as the secure storage place for the user's identity information because it can be revoked, users nowadays can rarely be found without a mobile phone and there are possibilities of security enhancements. Custom made SIMs/USIMs having enough computational power and storage space can be used to manage users' identification information and multi-factor authentication mechanisms. Gemalto, a company providing digital security, is involved in developing sophisticated smart cards (e.g., SIM/USIM) based online or off-line identity management with associated software, middleware, and server-based solutions. NXP, a semiconductor company (formerly a division of Philips), is also offering identification products in areas like government, banking, access control, and so forth using secure innovative contactless smart cards and chips. Credit card companies are running various trials for providing user's payment identity handling solutions using mobile phones and NFC technology. *Tap N Go* is the name of a contactless payment trial powered by MasterCard *PayPass* (2007) in the U.S. started in 2006. In the same year, Visa completed contactless-based mobile pilots in Malaysia and the United States, using NFC-enabled phones, complementing existing programs in Japan and Korea. In February 2007, Visa International and SK Telecom of South Korea announced the world's first contactless payment application on a universal SIM card which is personalized over-the-air based on Visa's recently introduced mobile platform ("Visa's mobile platform initiative," 2007).

Identity providers issue identities to each user. They have a very important central role in the identity management business. The identity provider manages users' identities and their access rights to various services securely. It provides the authentication and authorization services to the users. Who can be the identity providers in future identity management systems, is a debatable issue. Liberty Alliance (Miller et al., 2004) believes that mobile operators are in a good position to become the most favored identity providers, because they possess valuable static and dynamic user information which can be transmitted to third parties in a controlled manner through open standard Web service interface. Mobile operators also have the ability to seamlessly authenticate users with the phone number on behalf of the service providers (SP). Many contradict such roles of mobile operators. Instead a more trusted third party, like financial institutes and governments are also well positioned to become preferred identity providers. They might provide identity services for their specific market and services that need stronger user identities. When a user wants to subscribe to a new wireless network, he/she asks the third party identity provider to add new identification data into his/her phone. In such a situation, it is possible that a third party can even manage SIM/USIM, which is currently done by cellular operators. It is expected that the next-generation wireless network will have such flexibility.

Components of User Identities

Identity management in wireless service access needs to address device-level security, network-level security, and service-level security (Kuroda et al., 2004, p. 169). Therefore, the over-all user identity comprises device, network, and service identities. The user's device is divided into two components, a personal smart card (e.g., SIM/USIM) and mobile devices with wireless access capabilities. The smart card includes user identification data that contains user's public or shared-secret keys, certificates for network operators, and service providers. The card and the device need to be mutually authenticated in the initial setup phase because both devices have built no relationship of trust to exchange security information from the very beginning. Afterwards, the user identifies him/herself to the card, since it stores sensitive personal information, which is used for network- and service-level authentication. The user can identify through PIN, password, or biometrics. After these authentication procedures,

Figure 1. User identifications to ensure device-, network-, and service-level security



the card delegates user identity information to the mobile device to authenticate wireless access and thereby, service access. The user expects to use services without being concerned about the individual characteristics of each wireless access. Network-level authentication verifies that the user is a subscriber and has wireless access to the right network. Service-level authentication verifies that the user is a subscribed user to the right services. In each case, service or network providers and user device mutually authenticate each other. Figure 1 depicts the overview of device-, service-, and network-level identifications to ensure the security of user-device, network, and services for wireless service access.

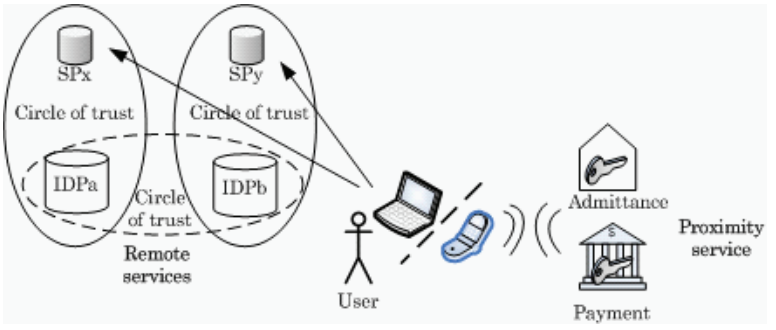
Integrated Identity Management Mechanism

Every human being is playing numerous roles in life to live. To organize the user identities in a more structured way, all user identities can be broadly categorized into three areas based on the roles he/she exercises in real life (Chowdhury & Noll, 2006). These are personal identity (PID), corporate identity (CID), and social identity (SID). PIDs can be used to identify a user in his/her very personal and commercial service interactions. CIDs and SIDs can be used in professional and social, interpersonal interactions respectively. For example, PIDs include bank/credit card, home/office access card/code, and so forth. According to Dick Hardt (keynote speech at OSCON 2005 conference), founder and CEO of SXIP Identity, individual's interests, fondness, preferences, or tastes are also part of his/her identity. These roles can be dealt with by user's SIDs. Some of these identities are having very sensitive user information therefore very strict authentication requirements have to be met. Some others require less secure infrastructure as they possess not so sensitive user information.

Considering all these aspects, instead of storing user's vast identity information into a single place (a user device), these can be distributed into two places. The less sensitive user identity information, especially his/her SIDs can be stored in a secure network identity space. The most sensitive identity information like user's PIDs will be stored in user's personal device. The mobile phone (more correctly the SIM card) has been proposed as the user's personal device (Chowdhury & Noll, 2006). When the user subscribes to the identity services, the identity provider (IDP) issues a certificate to him/her. It will be stored in the device. At the same time, a secure identity space in the network will be allocated for the user too. The device identifies and authenticates the user to access his/her network identity space. When the user authenticates to the device and the network, he/she can also gain access to the network identity space (if it requires, an optional password can also protect such access). The user device holds the most sensitive user identity information. Depending on the security requirements of the services, the possession-based authentication (e.g., having a personal device) can be enhanced by a knowledge factor (e.g., PIN code). An additional knowledge-based authentication mechanism can be used here to grant access to sensitive PIDs stored in the device. This is how user identities can be stored in a distributed manner and multi-factor authentication mechanisms can protect the security of user's identities.

In future service access scenarios, the user expects a hassle-free use of identities. In this regard an approach is expected to integrate all user's identities to access every remote and proximity services into a single mechanism. The distributed identity infrastructure just being described can also

Figure 2. A generic diagram for integrated identity mechanism and service access



provide an integrated mechanism to handle the use of identities for every possible service access over the wireless network. For example, by using public key infrastructure (PKI) built in SIM card user can access services of banks remotely; with the NFC capable mobile phone user, can access home premises transferring the stored admittance key from user device. This is how a proximity service access can also be handled. Figure 2 shows a generic diagram for integrated identity mechanism to handle remote and proximity service access.

In a significant move towards providing secure ubiquitous digital credentials management; the banking industry of Norway with a partnership of a mobile operator initiated PKI-based BankID (Cybertrust Case Studies Library, 2005) for identification and signing agreement on the move. BankID for mobile phones will initially be used in four areas: (1) logging on to Internet banks, (2) mobile banking, (3) electronic service for business and the public sector, and (4) account-based payment service for the Internet and mobiles.

Security Infrastructure in Identity Management Systems

The wireless network along with the user device (mobile phone) can serve as the underlying secure infrastructure for exchanging user identity information and authentication messages. The next generation network will integrate 3G and WLAN to offer subscribers high-speed wireless data services as well as ubiquitous connectivity (Siddiqui et al., 2005). Users are expected to access countless services seamlessly over the wireless network. Hence, secure identity information handling is a crucial issue in wireless service access. In the mobile domain, the security of 3G mobile systems has already been strengthened by introducing longer cipher keys; mutual (network, user) authentication; signaling and data traffic integrity; and the extension of ciphering back into the network (Boman, Horn, Howard, & Niemi, 2002, pp. 192-200). WLAN security has been improved significantly with the adoption of IEEE 802.11i. It was created in response to several serious weaknesses researchers had found in the previous system, wired equivalent privacy (WEP). There have been discussions to accomodate both 3G and WLAN security frameworks on the IP layer or based on 3rd Generation Partnership Project (3GPP), but the resulting solution does not offer fast vertical handover which is critical for session continuity (Kuroda et al., 2004, p. 166). EAP-TLS and EAP-AKA have been proposed to provide strong end-to-end security and authentication to the user in such integrated network environment (Kambourakis, Rouskas, & Gritzalis, 2004, pp. 287-296). Due to the various weaknesses of Bluetooth/Infrared communications, NFC is considered as the secure technology to transfer user identity information between a user's mobile phone and the devices at service points. Its short range should mitigate the risk of eavesdropping by other reader devices. It is practically impossible to do man-in-the-middle attack on NFC link (Haselsteiner

& Breitfuss, 2006). Moreover, a secure channel can be established using cryptographic protocol between the two NFC devices.

Identity management and associated security infrastructure will play a vital role for seamless service interaction in the next generation wireless network. There are several important requirements of a successful identity management system. Such a system should be user centric rather than service centric. The user expects an integrated identity management mechanism that can handle identities for both remote and proximity service access. Security of the underlying infrastructure is also a crucial issue in wireless service access. This section has discussed all these aspects in brief.

FUTURE TRENDS

3G networks are covering a wide service area and providing ubiquitous connectivity to mobile users with low-speed data rates which is sufficient for most real-time communications. WLAN/Wi-Fi networks cover smaller areas and provide high data rates to static users. There exists a strong need for integrating WLANs/Wi-Fis with 3G networks to develop a hybrid of data networks capable of ubiquitous data services and very high data rates at strategic locations called "hotspots." The future wireless network is expected to attain this goal and thereby, seamless service access. Next generation wireless network architectures envisaged to constitute of an IP-based core network, whereas the access network can be based on a variety of heterogeneous wireless technologies depending on the nature of the access cell. In this environment, people can access many new innovative services from anywhere and anytime. Service intake will be increased significantly. Instead of current identity provisions, a new identity management mechanism is expected, especially in wireless service access.

People no longer use many usernames and passwords for remote service access. Instead SSO will become popular with the provisions of additional authentication levels to meet higher security requirements. In future identity management, the role of an identity provider will be very critical. The key issue will be who can be the identity provider? Whoever will be the identity provider, the user SIM/USIM card is in a good position to become a secure storage place for user identity information. Researchers are working to develop high capacity sophisticated smart cards to meet such demand in various service access scenarios. In this regard, it is very important to decide who will be the owner of such a user identity device (e.g., SIM/USIM). For acceptability of a SIM card as a secure identity storage place and to develop a user-centric identity management mechanism, the user should have rights to update or modify the SIM card. It is expected that the business model of the next generation network will have such flexibility. Mobile networks or other wireless access networks will play a vital role to ensure security for identity information exchange. Therefore, numerous efforts are going on to enhance the security infrastructure of access network's air interface and provide strong end-to-end protection for secure service access.

Introduction of NFC adds intelligence and networking capabilities to the phone and creates many new opportunities to add product and service capabilities to handset-like digital transactions in very good proximities. It can make the mobile phone an ideal device for payments and gaining access. Financial institutes like credit card companies and mobile manufacturers are running various trials with NFC-enabled mobile phoned in service access scenarios like admittance and payment. User identities for admittance and payment services are very sensitive in nature. Therefore, an integrated identity mechanism is expected to deal with these proximity services and as well as remote services.

Currently, the user expects and technology demands service personalization, including adaptation to personal preferences, terminal, and network capabilities. Rule-based personalization algorithms become too complex when handling user context and preferences, thus asking for new mechanisms allowing dynamic adaptability of services. Semantic descriptions of user preferences and user relations with the combination of current developments in security and privacy issues

can create more dynamic service provisions and personalization. Semantic Web is seen as the next generation of the Internet where information has machine-readable and machine-understandable semantics.

CONCLUSION

Current reporting from the World Factbook states 1.5 to two times as many mobile users as Internet users for developed countries like UK, France, and Germany and roughly three times as many mobile users as Internet users in China (The World Factbook, 2006). Taking into account that mobile users are available 24/7 as compared to an average PC usage of 137.3 min/day for male (134.2 min/day for female) shows the importance of mobile service access. The emerging next generation network is expecting to integrate various access networks including 3G and WLAN/Wi-Fi networks. Ubiquitous access for seamless service interaction will be a reality soon.

The current identity provisions will not allow this to happen. Users possess many identities in various forms and identity information is stored in a scattered way in networks. Most of the recent developments are focused towards identity management in Internet domain to access remote services. However, some efforts also target service access located in the proximity of users. The success of future service access asks for an integrated identity mechanism to deal with both remote and proximity service access. The creation of a user's role-based identity in a dynamic way and use of Semantic Web technology will enhance user experience in service interaction. Such a dynamic and integrated identity mechanism together with mobile, sensor networks, and NFC-enabled mobile terminal can improve the healthcare system for better handling of patients, especially elderly and disabled people. Semantic descriptions of user preferences and relations can also improve user experience in social interactions.

The user personal wireless device along with a sophisticated smart card will play a key role for identity management for wireless service access in terms of user identity information storage and providing secure network and service authentication. With strong encryption, privacy, and data integrity mechanisms, mobile networks have the capability to provide the underlying security infrastructure for sensitive identity information exchange for mobile users. Mobile phones equipped with custom-made high capacity SIM cards can act as a secure user identity storage place. New developments in security mechanisms to protect mishandling of user identities over the air interphase as well as over the IP-based core network can make the identity management for wireless service access secure enough.

REFERENCES

Altmann, J., & Sampath, R. (2006, April). UNIQuE: A user-centric framework for network identity management. In *Proceedings of IEEE/IFIP Network Operations and Management Symposium, NOMS 2006* (pp. 495-506). Vancouver, Canada.

Boman, K., Horn, G., Howard, P., & Niemi, V. (2002, October). UMTS security. *Electronics and Communication Engineering Journal, 14*(5), 191-204.

Cameron, K. (2005). *The laws of identity.* Retrieved December 29, 2006, from http://identityblog.com/

Chowdhury, M. M. R., & Noll, J. (2006, November). *Service interaction through role based Identity.* Paper presented at Wireless World Research Forum Meeting 17, Heidelberg, Germany.

Chowdhury, M. M. R., & Noll, J. (2007, March). Distributed identity for secure service interaction. In *Proceedings of the Third International Conference on Wireless and Mobile Communications, ICWMC'07,* Guadeloupe, French Caribbean.

Cybertrust Case Studies Library. (2005). *BankID: Delivering bank-common trust for Web-based transactions*. Retrieved November 15, 2006, from https://www.cybertrust.com/intelligence/case_studies/

Damiani, E., De Capitani di Vimercati, S., & Samarati, P. (2003, November). Managing multiple and dependable identities. *IEEE Internet Computing, 7*(6), 29-37.

Haselsteiner, E. & Breitfuss, K. (2006). *Security in near field communication (NFC) strengths and weaknesses.* Paper presented at the Workshop on RFID Security—RFIDSec 06, Graz, Austria.

Jøsang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, S. (2005). Trust requirements in identity management. In *Proceedings of the Australasian Information Security Workshop (AISW'05),* Newcastle, Australia.

Kambourakis, G., Rouskas, A., & Gritzalis, D. (2004). Performance evaluation of certificate based authentication in integrated emerging 3G and Wi-Fi network. In S. K. Katsikas et al. (Eds.), *EuroPKI 2004* (LNCS 3093, pp. 287-296). Berlin/Heidelberg, Germany: Springer.

Kuroda, M., Yoshida, M., Ono, R., Kiyomoto, S., & Tanaka, T. (2004). Secure service and network framework for mobile Ethernet. *Wireless Personal Communication, 29,* 161-190.

Li, M., Sandrasegaran, K., & Huang, X. (2005, July). Identity management in vertical handovers for UMTS-WLAN networks. In *Proceedings of the Internationl Conference on Mobile Business, ICMB'05* (pp. 479-484). Washington DC: IEEE Communication Society.

Mastercard PayPass. (n.d.). *The NYC mobile trial.* Retrieved February 09, 2007, from http://www.mastercard.com/us/paypass/mobile/

Miller, P. et al. (Eds.). (2004). *Tier 2 business guidelines: Mobile deployments.* Retrieved November 1, 2006, from http://www.projectliberty.org/liberty/resource_center/papers

Noll, J., Carlsen, U., & Kalman, G. (2006, August 7-10). *License transfer mechanisms through seamless SIM authentication.* Paper presented at the International Conference on Wireless Information Systems, Winsys 2006, Setubal, Portugal.

Noll, J., Lopez Calvet, J. C., & Myksvoll, K. (2006, July 29-31). *Admittance services through mobile phone short messages.* Paper presented at the International Conf. on Wireless and Mobile Communications ICWMC'06, Bucharest, Romania.

Park, D.-G., & Lee, Y.-R. (2003). The RBAC based privilege management for authorization of wireless networks. In G. Dong et al. (Eds.), *WAIM 2003,* Berlin/Heidelberg, Germany (LNCS 2762, pp. 314-326). Springer-Verlag.

Siddiqui, F., Zeadally, S., & Yaprak, E. (2005). Design architecture for 3G and IEEE802.11 WLAN Integration. In P. Lorenz & P. Dini (Eds.), *ICN 2005* (LNCS 3421, pp. 1047-1054). Berlin/Heidelberg, Germany: Springer.

The SXIP 2.0 Overview. In specifications of SXIP 2.0 protocol. (n.d.). Retrieved December 15, 2006, from http://sxip.net/Specs

Visa's mobile platform initiative. (2007). *Payment news.* Retrieved April 27, 2007, from http://www.paymentsnews.com/2007/02/visas_mobile_pl.html

KEY TERMS

Authentication: Authentication is to prove as genuine.

Biometrics: Biometrics is the biological identification of a person which may include characteristics of structure and of action such as iris and retinal patterns; hand geometry; fingerprints; voice response to challenges; the dynamics of hand-written signatures, and so forth.

Circle of Trust: Circle of trust is a trust relationship through agreement among various service providers.

EAP-TLS and EAP-AKA: EAP-TLS and EAP-AKA are authentication frameworks frequently used in wireless networks.

Federation: Federation is the joining together to form a union through agreement.

IDP: Identity providers.

Life Cycle: Life cycle is the progression through a series of different stages of development.

PIN: Personal identification number.

Personalization: Personalization is when something is customized or tailored for the user, taking into consideration that person's habits and preferences.

Pervasive Computing: Pervasive computing is the use of computing devices everywhere and these devices communicate with each other over wireless networks without any interactions required by the user.

Proximity Service: Proximity services are those available close to the users.

Revocation of Identity: Revocation of identity is the act of recalling or annulling the identity.

SP: Service providers.

Single Sign-On (SSO): SSO on is the ability for users to log on once to a network and be able to access all authorized resources within the domain.

Smart Card: Smart card is a card containing a computer chip that enables the holder to perform various operations requiring data stored on chip.

Ubiquitous: Ubiquitous is being or seeming to be everywhere at the same time.