Near Field Communications Handbook

Edited by

Syed A. Ahson and Mohammad Ilyas

CRC Press
Taylor & Francis Group

Near Field Communications Handbook

Edited by

Syed A. Ahson and Mohammad Ilyas

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
Version Date: 20110804

International Standard Book Number: 978-1-4200-8814-4 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Preface

Near Field Communication (NFC) is a short-range, high-frequency wireless communication technology that has emerged from the convergence of contactless identification such as RFID and networking technologies such as Bluetooth and Wi-Fi. An NFC communication can be initialized by as simple a means as "touching" or "tapping" one NFC device to another. Two NFC-compatible devices communicate (exchange data) over a distance of a few centimeters. Such a short transmission range makes eavesdropping inherently hard, and thus helps achieve better communication security. NFC enables direct interaction between mobile devices such as phones or cameras as well as allowing access to RFID-tagged items and contactless smart cards. Massive growth in the industry started in the late 1990s with the possibility of fabricating low-cost RFID tags in high volume. NFC allows access to those tags not only from dedicated reader devices, but on the basis of devices we carry with us every day (e.g., a mobile phone or camera); it will represent therefore the major interface between our daily life and tagged objects. The basic principle of RFID technology is that a device called a "reader" or "interrogator"—in our case a mobile phone with NFC interface—provides an RF field. It transmits data to the tag, which is also known as the transponder, by modulating the field. The tag is an integrated circuit that is attached to an antenna. It receives requests and transmits data to the reader.

Over the last 15 years, the growing availability of wireless communication technologies, as well as the miniaturization of electronic components inside consumer devices, has enabled the possibility of creating a so-called ubiquitous computing environment, as foreseen by Mark Weiser at the beginning of the 1990s. In a Weiser article titled "The Computer for the 21st Century," the researcher from XEROX PARC hypothesized a world of interconnected objects by means of information and communication technologies. NFC technology enables local communication between entities in our everyday environment. These features facilitate creating a network of interconnected objects known as the "Internet of Things." NFC focuses on user-initiated communication, due to the short reading distance a user has to bring a reader and a tag near each other. As NFC technology becomes common, various electrical devices can be equipped with NFC readers. These readers can then be used to read and write RFID tags and even to communicate with other devices equipped with similar readers.

In the meantime, another important process related to ICT has appeared. It deals with the convergence of different communication technologies inside one single device, the mobile phone, nowadays spread among 61% of the worldwide population, according to the International Telecommunication Union (ITU). Suitable to be used with a variety of devices, NFC technology is mainly aimed at mobile phones. The computational power of modern mobile phones and NFC wireless connectivity technology has become the enabler of various mobile-based applications, such as electronic ticketing for public transportations, mobile payment, and bootstrapping Wi-Fi or Bluetooth-pairing processes. The convergence of a number of communication interfaces (Bluetooth, Wi-Fi, W-CDMA, and NFC, just to mention some) inside the mobile phone, makes this device the most qualified for accessing different types of services into an interconnected environment such as the one predicted by Mark Weiser. The centrality of the mobile phone inside everyone's life is one of the reasons why NFC technology has caught the attention of different industries and research institutions. In fact, NFC can be seen as the integration of Radio Frequency Identification (RFID) technology inside the mobile phone, potentially allowing more than a half of the worldwide population to interact with smart environments via RFID technology.

NFC will enable a range of applications and services: proximity services such as getting information by touching smart posters or sharing information between phones or any NFC devices, being the boarding pass in an airport, functioning as a remote controller or a key, advertising services, location-based services, and so forth. To achieve these services and many more we may not yet have even thought of, it should be highlighted that PCs, TVs, other computing devices and noncomputing devices should become NFC enabled. We believe in the long-term potential of NFC to make a significant difference in the quality of life and comfort for many people and for our environment. This technology can be woven itself into our environment according to Weiser's vision of Ubiquitous Computing, and it can be the key technology for the Internet of Things.

In this book, we guide the reader through the numerous NFC applications that have evolved over the years or that are expected to come in the near future. We provide glimpses of a future where NFC technology has fully become part of our lives and serves as source of endless inspiration for anticipating the richness of the NFC world. This book also introduces a set of guidelines to design future NFC applications with a high user acceptance in consumer markets.

Technical information about all aspects of NFC technology is provided here. The areas covered range from basic concepts to research-grade material including future directions. This book captures the current state of NFC technology and serves as a source of comprehensive reference material on this subject. It has a total of 12 chapters authored by 50 experts from around the world. The targeted audience for the handbook includes professionals who are designers or planners for NFC systems, researchers (faculty members and graduate students), and those who would like to learn about this field. Although the book is not precisely a textbook, it can certainly be used as a textbook for graduate courses and research-oriented courses that deal with NFC. Any comments from readers will be highly appreciated.

Many people have contributed to this handbook in their unique ways. The first and foremost group that deserves immense gratitude is the group of highly talented and skilled researchers who contributed 12 chapters to this book. All of them have been extremely cooperative and professional. It has also been a pleasure to work with Rich O'Hanley and Stephanie Morkert of CRC Press, and we are extremely grateful for their support and professionalism. Our families have extended their unconditional love and strong support throughout this project, and they all deserve very special thanks.

Contributors

Manfred Aigner
Graz University of Technology
Styria, Austria

Elisabeth André
Augsburg University
Augsburg, Germany

B. Benyó
Sapienza University of Rome
(CATTID)
Budapest University of
Technology and Economics
Budapest, Hungary

Elisa Bertino
Qualcomm
San Diego, California

Abhilasha Bhargav-Spantzel
Intel
San Francisco, California

Thomas Bingel
Hochschule Darmstadt
University of Applied
Sciences
Darmstadt, Germany

Francisco Borrego-Jaraba
University of Cordoba
Cordoba, Spain

Pilar Castro Garrido
University of Cordoba
Cordoba, Spain

U. Biader Ceipidor
Sapienza University of Rome
(CATTID)
Rome, Italy
and
Budapest University of
Technology and Economics
Budapest, Hungary

Marta Cortés Orduña
University of Oulu
Oulu, Finland

Martin Feldhofer
Graz University of Technology
Styria, Austria

Miguel Ángel Gómez-Nieto
University of Cordoba
Cordoba, Spain

Eric Gressier-Soudan
Conservatoire National des Arts et Métiers
Paris, France

Rosa Iglesias
Ikerlan Technological Research Center
Mondragon, Spain

Felix Köbler
Technische Universität München
Munich, Germany

Philip Koene
Technische Universität München
Munich, Germany

Helmut Krcmar
Technische Universität München
Munich, Germany

Karin Leichtenstern
Augsburg University
Augsburg, Germany

Jan Marco Leimeister
Kassel University
Kassel, Germany

Irene Luque Ruiz
University of Cordoba
Cordoba, Spain

Michael Massoth
Hochschule Darmstadt University of Applied Sciences
Darmstadt, Germany

Guillermo Matas Miraz
University of Cordoba
Cordoba, Spain

C. M. Medaglia
Sapienza University of Rome (CATTID)
Rome, Italy
and
Budapest University of Technology and Economics
Budapest, Hungary

Philipp Menschner
Universität Kassel
Kassel, Germany

A. Moroni
Sapienza University of Rome
(CATTID)
Rome, Italy
and
Budapest University of
Technology and Economics
Budapest, Hungary

Romain Pellerin
Ubidreams
La Rochelle, France

Andreas Prinz
Universität Kassel
Kassel, Germany

Mikko Pyykkönen
University of Oulu
Oulu, Finland

Florian Resatsch
Servtag GmbH
Berlin, Germany

Jukka Riekki
University of Oulu
Oulu, Finland

Iván Sánchez Milara
University of Oulu
Oulu, Finland

Ning Shang
Qualcomm
San Diego, California

Michel Simatic
Institut Telecom
Telecom Sud Paris
Evry, France

Kevin Steuer Jr.
Qualcomm
San Diego, California

Juan Pedro Uribe
Ikerlan Technological Research
Center
Mondragon, Spain

A. Vilmos
Sapienza University of Rome
(CATTID)
Rome, Italy
and
Budapest University of
Technology and Economics
Budapest, Hungary

Contents

1

Secure Mobile Identity

Concepts and Protocols

ABHILASHA BHARGAV-SPANTZEL

Contents

Digital Identity Overview

The emerging information infrastructure connects remote parties worldwide through the use of large-scale networks, and through a diverse and complex set of software technologies. Activities in various domains, such as commerce, entertainment, scientific collaboration, healthcare, and so forth, are increasingly being carried out based on the use of remote resources and services. These resources and services are engaged at various levels within those domains. The interaction between different parties at remote locations may be (and sometimes should be) based on only little knowledge about each other.

To better support these activities and collaborations, information technology (IT) infrastructure and systems are needed that are more convenient to use. We expect, for example, that personal preferences and profiles of individuals will be readily available when shopping over the Internet or when running jobs on a computing grid, without requiring the individuals to repeatedly enter them. In such a scenario, digital identity management (IdM) technology is fundamental in customizing user experience, underpinning accountability in transactions, and complying with regulatory controls. For this technology to fully deploy its potential, it is crucial that strong *protection of digital identity* be achieved. IdM systems must assure that such information is not misused and individuals' privacy is guaranteed.

In this section, we describe the basic concepts related to digital identity followed by describing some key challenges in digital identity management and use. We also provide an overview of federated digital identity management systems.

Basic Concepts

Digital identity can be defined as the digital representation of the information known about a specific individual or organization. More specifically, our notion of digital identity refers to two different, not necessarily disjoint, concepts: nyms and partial identities. A *nym* gives an individual an identity under which to operate when interacting with other parties; an example of a nym is a login name or a pseudonym. Nyms can be strongly bound or linked to an individual, or be meaningful only in the context of a specific application domain. Weakly bound or unbound nyms are useful in contexts such as chat rooms and online games. *Partial identities* encompass a set of properties, such as name, birth date, credit card numbers, patient record number, which are referred to as *identity attributes* or *identifiers*, that are associated with individuals. We use an identity attribute as a synonym of an identifier. Each subset of identifiers represents the partial identity of the individual. Partial identities may or may not be bound to the human identity of one or more actual individuals.

It is important to note the issue of *identity ownership* as the identity attributes of individuals are stored and shared among various entities in IdM systems. By *owner of an identity attribute*, we mean the individual to whom this identity attribute is issued by a trusted authority or an individual who is authoritative with respect to the claiming of the identifier. In the former case, the trusted issuer of the identifier is also responsible for providing information about the *validity* of that identifier. The validity of an identifier encompasses several notions (some of which are derived from the field of data quality [24]). Examples of such notions are (1) correctness; the identifier is correct (possibly with respect to the real world); and (2) timeliness; that is, the identifier is up to date.

When talking about identifiers, it is also important to distinguish between weak and strong identifiers. A strong identifier uniquely identifies an individual in a population, whereas a weak identifier can be applied to many individuals in a population. Whether an identifier is strong or weak depends on the size of the population and the uniqueness of the identity attribute. The combination of multiple weak identifiers may lead to a unique identification [5,30]. Examples of strong identifiers are an individual's passport number or social security number (SSN). Weak identifiers are attributes such as citizenship, age, and gender. This distinction is significant because misuse of strong identifiers can have more serious consequences, such as identity theft, as compared to misuse of weak identifiers.

Our notion of identity verification deals with verifying that the identity attributes claimed by an individual are also owned by that individual. Identity verification is coupled with the concept of identity assurance. The notion of identity assurance deals with the confidence about the truth of the claims related to the identity of an individual. Successful identity verification with high assurance about an identifier claimed by an individual means that the identifier is considered valid and the verifier is confident that it is owned by that individual.

Strong and weak identity assurances exist regardless of the linkability of the identifier to the identity of the actual individual. Additionally, linkability among identifiers may exist with or without being bound (or linked) to the actual individual.

Example 1.1 Consider an individual whose real-world name is Bob Smith who has a digital pseudonym Homer07. In a digital interaction, when Homer07 claims to have SSN=123456789 and the verifier has strong

> assurance that the claim is correct (i.e., the SSN is valid and owned by the user Homer07) and linked to the real-world individual Bob Smith, then this corresponds to the case where one has strong identity assurance and strong linkability to the real-world individual.
>
> Consider another scenario in which Homer07 claims to have citizenship=U.S.A. and the verifier does not know which real-world individual the claim belongs to, but at the same time, is confident that the claim is correct. Such a scenario corresponds to strong identity assurance and weak linkability. Notice that for a party to make a decision, such as in access control, linkability to a human identity of the actual individual is not always required.

In addition to the traditional identifiers, there also exist *biometric* identifiers that are increasingly included as an integral part of an individual's identity. Biometric verification occurs when an individual presents a biometric sample, and possibly some additional identifying data such as a password, which is then compared with the stored sample for that individual. Biometric verification provides some inherent advantages as compared to other nonbiometric identifiers because biometrics correspond to a direct evidence of the personal physical characteristics versus possession of secrets which can be potentially compromised. Moreover, most of the time biometric enrollment is executed in person and in controlled environments, making it reliable for subsequent use [23].

An interesting extension to the traditional identity attributes is the incorporation of the history of an individual's activities. The *transaction history-based identifiers* or *mobile identifiers* can be encoded as receipts from e-commerce or m-commerce transactions. This concept is especially relevant when considering mobile client systems such as cellular phones that are enabled with Near Field Communication (NFC)-type communication capabilities. This is elaborated further in the section titled "Mobile Identity Concepts."

Federated Identity Management Systems

The goal of identity management systems (IdMs) is to provide individuals with protected environments to share identities among organizations by managing individuals' identity attributes. Federations provide a controlled method by which federation members can provide more integrated and complete services to a qualified group of individuals. The members of a federation have trust relationships among themselves to share and use individuals' identity attributes.

Federations are usually composed of two main entities: IdPs that manage identities of individuals, and service providers (SPs) that offer services to registered individuals. In a typical federated IdM, the individual registers with his or her local IdP and is assigned a login name. Based on this information a registered individual can submit additional attributes and corresponding attribute release policies that are stored at the IdP. From then on, the IdP is contacted whenever the individual interacts with any SP in the federation and additional identity information is needed. The IdP is then in charge of sending the SP the submitted attributes of the individual in accordance with the attribute release policies. Note that there are several social, economic, and legal requirements to realize an IdM system. For example, the legal requirements would have to dictate how the contracts for transactions limited to the physical world get adopted when these transactions are performed electronically. Those nontechnical requirements are important to address when building an IdM system. In such *federated systems*, multiple IdPs are distributed and can store partial identity information of individuals, if required.

Mobile Identity Concepts

In this section, we present *history-based* or *mobile* identity attributes that are related to users' past transactions that can be used by users, together with other identity attributes, to perform identity verification and enabling SPs to make trust-based decisions concerning current transactions. One category of such systems is represented by *reputation systems* [18,14]. Several e-commerce SPs have built reputation systems so as to give a better idea of how trustworthy both the buyers and the sellers are. This is because the sellers are typically SPs but could also be users in a peer-to-peer (P2P) environment. Sellers benefit from the use of such systems because a good reputation score is likely to attract more customers. Similarly, buyers may qualify for better deals and services if they have a good reputation. However, most reputation systems have a major limitation in that the only information they maintain are scores, and they do not typically provide information about the actual transactions a seller or buyer has made. Therefore, it is important that trust be established also according to the transaction history–based attributes. Examples include the behavior of