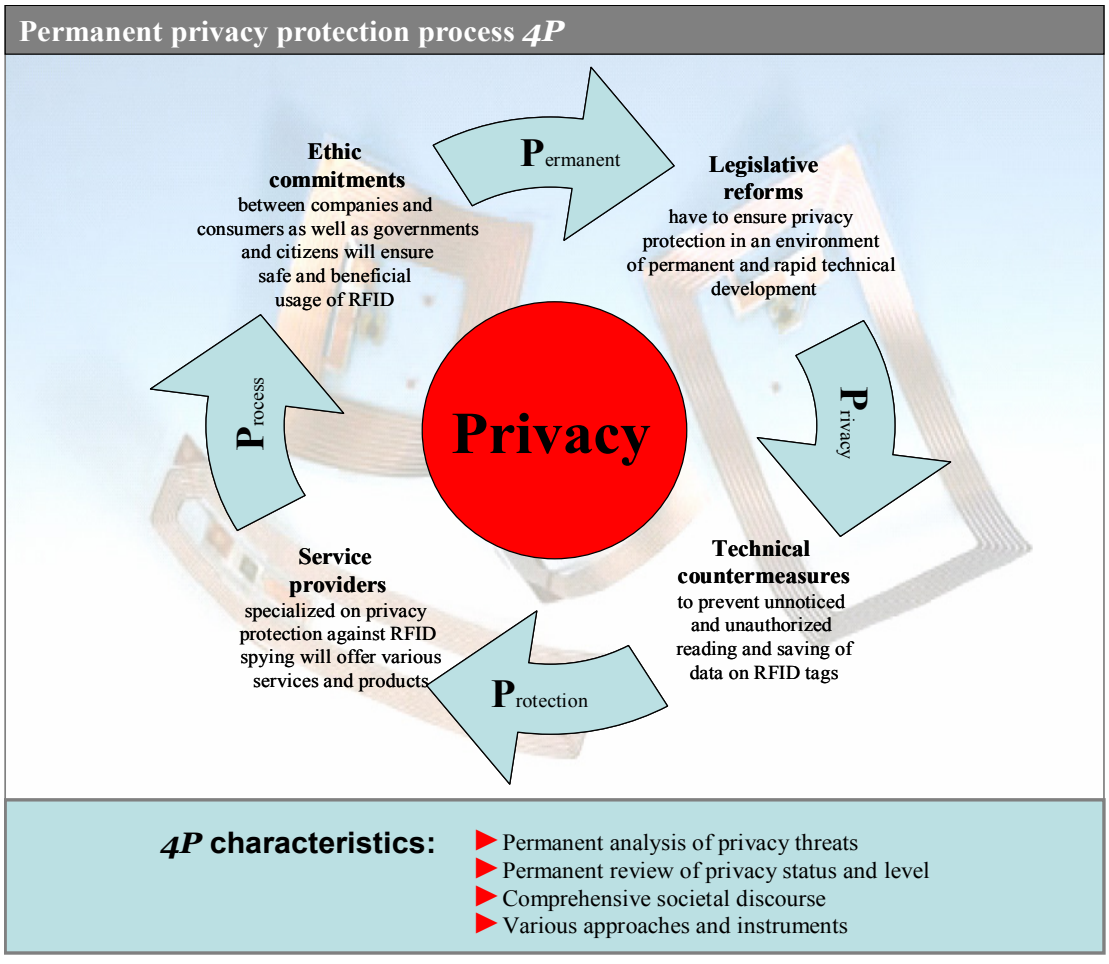
IWI Discussion Paper Series
11 (July 5, 2004)[1]

ISSN 1612-3646

Privacy Protection against RFID Spying: Challenges and Countermeasures[2]

Marcel Heese[3], **Günter Wohlers**[4] und **Michael H. Breitner**[5]



---

[1] Copies or a PDF-file are available upon request: Institut für Wirtschaftsinformatik, Universität Hannover, Königsworther Platz 1, D-30167 Hannover, Germany (www.iwi.uni-hannover.de).

[2] Paper submitted to the „7. Internationale Tagung Wirtschaftsinformatik 2005", Bamberg, February 23 – 25, 2005, see http://www.wi2005.de.

[3] Graduate Student (marcel.heese@web.de).

[4] Senior Lecturer (wohlers@iwi.uni-hannover.de).

[5] Full Professor for Information Systems Research and Business Administration (breitner@iwi.uni-hannover.de).

Table of contents

Privacy Protection against Ubiquitous RFID Spying: Challenges and Countermeasures

Marcel Heese, Günter Wohlers, Michael H. Breitner
University of Hannover

Abstract: The privacy threats of Radio Frequency Identification (RFID) as inevitable ubiquitous computing technology require new approaches to avoid scenarios as the "Orwell 1984 State" or the "transparent citizen". This paper introduces a new comprehensive approach: A permanent privacy protection process named "4P" or also "Fo(u)r P(rivacy)", here. The process 4P consists in a holistic societal discourse including individuals as well as business and government. Beyond technical countermeasures, specialized service providers will gain in importance. RFID using companies may be forced to establish ethic commitments and the legislative is supposed to protect privacy by law adapting technological developments.

Keywords: Radio Frequency Identification, RFID, privacy protection, ubiquitous computing, pervasive computing

1 Introduction

Headlines as "Bugging operation on cereals" or "Your products are watching you" are descriptive statements of many international consumer and privacy protection organizations. Privacy threats can result from the widespread usage of RFID as ubiquitous computing technology. The 20th century was characterized by many economical crises and wars between nations. Will the diffusion of ubiquitous devices in our daily environment result in an informational war within the society of the 21st century? The battlefield of the 21st century could be the supermarket of our neighborhood.

After mainframe computing and personal computing, "ubiquitous computing" names the third wave in computing [Weis96] and stands for the actual trends of information processing. In 1991 M. Weiser had the vision of an invisible technology, embedded in the devices of our everyday life that would be able to remove annoyances from the daily routine. The technology should be used as means to an end, indistinguishable from the device itself, allowing the human to concentrate on the essential basics of his action [Weis91, pp. 66-75]. The industry adopted the

expression “pervasive computing” as a more pragmatic approach for the penetration of all branches with the omnipresent information processing already today, by using today’s technology of mobile computing [LangMat03]. Because of the fast developments in microelectronics, the internet and wireless technologies, a permanent presence of smallest, networked computers in our “everyday devices” is likely in a short term. These “smart devices”, also called “things that think (3T)”, can autonomously share information, have access to resources in the internet and can operate adapted to their environment [Mat+03].

In this paper we discuss the characteristics and applications of RFID as ubiquitous computing technology and we evaluate privacy offenses, violations and intrusions. RFID allows the contact-less reading and writing of data stored on tiny tags. It will be used in various applications like product tracking in warehouses or logistic chains, but could also be realized in passports and banknotes. Business sees a high potential of efficiency increase by closing the gap between reality and information processing. That will make RFID an inevitable bulk commodity and will anchor it in our everyday devices. International consumer and privacy protection organizations raise an alarm and proclaim ubiquitous RFID will have direct impact on privacy. Without considerations of data and information security RFID will offer a perfect surveillance infrastructure. Approaching are, e. g., the scenarios of the “transparent consumer” in retail trade [MeySchü04] and a state creating complete movement schemes of its citizens. The latter may be provoked by the evident threads of today’s global terrorism including massive assaults with ABC-weapons.

A new comprehensive approach is necessary to decrease these technological dangers: A permanent privacy protection process named “4P” or also “Fo(u)r P(rivacy)”, here. 4P includes a holistic societal discourse including individuals as well as business and government. Beyond technical countermeasures, specialized service providers will gain in importance. RFID using companies may be forced to establish ethic commitments and the legislative is supposed to protect privacy by law adapting technological developments. 4P is characterized by a permanent analysis of privacy threats, an execution of various and adequate countermeasures and a review of the privacy status and level.

2 RFID and privacy

2.1 Function and technology of RFID systems

RFID is a technology for the contact-less reading and writing of data. It is used in automated identification applications that can provide information systems with the identity of a physical object. RFID describes a whole technological infrastructure including the RFID tag, a read/write device and the integration with servers, services or other systems, for example payment or resource planning systems [Fi02, p.7; FarShe03, p. 8].

velopment (OECD) published the "Fair Information Practices" in the beginning of the 80ies. They most important principles can be summarized as follows: data quality, use limitation, purpose specification, and individual participation [Lang04, pp. 3-13; OEC80]. The international RFID privacy conference 2003 published a resolution that generally says these privacy regulations have to be applied as well to RFID applications [ICDP03].

In contrast to that, the USA is gone furthest on the way to a specific RFID privacy law so far. In several states, for example California and Utah, concrete RFID laws are discussed in the senate or already passed. The main intention in the discussion is not to ban the RFID technology or to limit its potential positive uses for the companies, but definitely to protect consumer privacy [Rob04]. The laws of California require companies and governmental agencies to inform consumers whenever RFID systems are used. The companies must obtain consumer's consent before they can use RFID to track purchases and collect information about them. Also it requires the RFID tag to be detached or destroyed before consumers leave the shop with it [Rob04; Gil04]. Introduced to the senate in February 2004 by Senator Debra Bowen, the "bill 1834" passed the senate with 22:8 majorities in May. Next steps will be the decision of California's parliament about the bill in June. [16] Utah's House of Representatives passed the first RFID privacy law in February 2004 and the law will take effect from May 2005. It requires all products containing RFID tags to be labeled as such.[17]

5 Conclusions and outlook

The discussion of this paper clearly shows that it is too early to accept the scenarios of the "transparent citizen" or the "Orwell 1984 state" as inevitable. The "information war" can be controlled by a comprehensive societal discourse supported by privacy protection processes. A permanent evaluation of upcoming privacy threats and the timely execution of countermeasures will minimize the impacts caused by new technological developments. Various societal institutions like governments, business and individuals must be involved. With various countermeasures split in different fields, a broad set of instruments against the penetration of everybody's privacy is available today. Besides acts and laws also technical instruments and specialized services as well as ethic commitments can be part of a permanent privacy protection process, e. g. 4P presented here. 4P allows companies and governments, e. g., to realize efficiency increases and launch new products without threatening privacy.

[16] Download the RFID bill of California: http://www.leginfo.ca.gov/pub/bill/sen/sb_1801-1850/sb_1834_bill_20040220_introduced.pdf.

[17] Download the RFID Right to Know Act of Utah: http://www.le.state.ut.us/~2004/bills/hbillamd/hb0251.pdf.

IWI Discussion Paper Series

ISSN 1612-3646

Michael H. Breitner, *Rufus Philip Isaacs and the Early Years of Differential Games*, 36 p., #1, January 22, 2003.

Gabriela Hoppe and Michael H. Breitner, *Classification and Sustainability Analysis of E-Learning Applications*, 26 p., # 2, February 13, 2003.

Tobias Brüggemann and Michael H. Breitner, *Preisvergleichsdienste: Alternative Konzepte und Geschäftsmodelle*, 22 p., # 3, February 14, 2003.

Patrick Bartels and Michael H. Breitner, *Automatic Extraction of Derivative Prices from Webpages using a Software Agent*, 32 p., # 4, May 20, 2003.

Michael H. Breitner and Oliver Kubertin, *WARRANT-PRO-2: A GUI-Software for Easy Evaluation, Design and Visualization of European Double-Barrier Options*, 35 p., #5, September 12, 2003.

Dorothée Bott, Gabriela Hoppe and Michael H. Breitner, *Nutzenanalyse im Rahmen der Evaluation von E-Learning Szenarien*, 14 p., #6, October 21, 2003.

Gabriela Hoppe and Michael H. Breitner, *Sustainable Business Models for E-Learning*, 20 p., #7, January 5, 2004.

Heiko Genath, Tobias Brüggemann and Michael H. Breitner, *Preisvergleichsdienste im internationalen Vergleich*, 40 p., #8, June 21, 2004.

Dennis Bode and Michael H. Breitner, *Neues digitales BOS-Netz für Deutschland: Analyse der Probleme und mögliche Betriebskonzepte*, 21 p., #9, July 5, 2004.

Caroline Neufert and Michael H. Breitner, *Mit Zertifizierungen in eine sicherere Informationsgesellschaft*, 19 p., #10, July 5, 2004.

Marcel Heese, Günter Wohlers and Michael H. Breitner, *Privacy Protection against RFID Spying: Challenges and Countermeasures*, 21 p., #11, July 5, 2004.