University of Bielefeld

RVS
Rechnernetze und
Verteilte Systeme

Statement on Digital Wireless Technologies Prepared for the EU 6th Framework Consultation

RVS-S-04-01

Networks and Distributed Systems (RVS) Group,
Faculty of Technology
University of Bielefeld

2004-04-08

Digital radio-frequency communication technology (which we refer to below simply as Digital Wireless or DW) has been available for many years. Recently, miniaturisation and the application of mass production techniques have led to new uses such as RFID tagging, which interests the retail industry and distributors. Such non-traditional uses of RF communication brings DW technology into increasing contact with ordinary citizens. The problems which arise have been insufficiently analysed. To enable appropriate use of RFID and related DW technology, these social and ultimately political problems must be specified and analysed more thoroughly.

Transmission Power

Very-high-energy RF transmissions are known hazards to health as well as interference with other essential infrastructure. This is already legally controlled, but certificates of exemption from these legal limits are also issued [1]. However, the effects on health (for example, interference with externally-programmable implanted heart pacemaker devices) and other infrastructure of pervasive high RF energy are still poorly known in detail. One could anticipate more research in this area.

Data Mining

Issues arise from the wide introduction of DW technology in combination with other technologies that were better resolved before large scale operations start.

The unique serial number (ID) from RFID tags makes it easy for database and archiving companies to store and associate data by linking to this ID. Information previously only available, if at all, through complex data mining is becoming available through fast database queries.

While very helpful to logistical planning undertaken by retail companies and distributors, the easy availability of such information enables also its misuse, whether undesigned or designed, inadvertent or intentional. In Germany, there is some degree of legal protection against such misuse through the Right of Informational Self-Determination derived from the Basic Constitutional Law [2]. Data from and about a person may only be collected, stored and processed with the expressed and revocable consent of that person. Processing and utilisation of the information must be transparent and comprehensible. False data or incorrectly-linked data must be corrected or deleted on demand.

However, de jure protection is not the same as de facto protection. There is a danger that these important and established rules for privacy protection may easily be violated through misuse and abuse of RFID technology. Not only that, but some features of the technology may inadvertently weaken the protections afforded by transparency and comprehensibility: for example, a customer may well not be able easily to determine when and where data is being collected from RFID tags and exactly what conclusions are being drawn from this data. For example, personal or accounting data may be stored directly on RFID tags to enable quick proofs of purchase history for refund and return purposes. But this data may equally be used by other tag readers for other purposes, for example to infer information about a customer's lifetime purchasing profile over many retailers.

Such conflicts between the intention of the law and DW technology are intrinsic to the technology and should be resolved before wide-area introduction of the technology [3]. We suggest there is a role here for the EU in identifying such conflicts.

Introduction of such technology without appropriate consultation with stakeholders has already led to protests in Germany and to a cost-intensive recall of a series of customer payment cards [4, 5]. Some of this was organised by a Bielefeld info-technology public-interest group, FoeBuD e.V. While we regard such interventions as occasionally appropriate according to the situation, we do not regard these kinds of processes as the optimal way to introduce and control technology. A stakeholder-consultation process with early resolution of concerns and a goal of reaching consensus would have been more appropriate in this specific case. However, it would not have been easy for the retailer to identify or approach appropriate interlocutors; a "try it and see what happens" approach may well have been the most easily-available option. We suggest that the EU could usefully consider what sorts of stakeholder-involvement processes it wishes to encourage, and how these might be structured.

Security concerns arise not only with customer data, but may also arise with trade secrets and other privileged business and political information. Imagine, for example, that one could detect the presence of senior government figures at a meeting with terrorists through RFID interrogation of clothing. Such occurrences may be avoided by sufficiently close attention paid to security, but this may not be effectively possible with lesser organisations than government. It would be possible to trace the movements of potentially every citizen, and such possibilities could be used by people wishing to discredit a citizen for any reason (for political or business reasons, or for purposes of determining a divorce settlement, for example). With suitable placement and combination of multiple reading devices, exact surveillance and tracking becomes technically feasible at some distance and without line-of-sight constraints.

We suggest that these possibilities must be analysed in detail and ways found to implement the technology in such a way as to render impossible such nefarious uses and to render feasible only those uses legitimated for the purpose of the tags, such as inventory assessment and automated transactions at points of sale.

Standardisation and Interoperability

Particular problems such as those mentioned directly above arise through standardisation and through interoperability. Since tag readability is de facto more or less standardised, improperly-secured data may be read by persons or companies that legally should not be able so to do. Other potential examples come to mind. Here are three:

- Were currency to be equipped with RFID tags, not only banks and stores could check its authenticity quickly, but thieves could determine how much cash a potential target was carrying in hisher purse.
- Or store A could read customers' tags upon entry and determine whether they had been shopping at competitor store B and thereby treat the customer in some way that he or she would not desire. For example, the owner of store A may, in Germany, legally prohibit entrance to any customer for any reason - such as that he or she is carrying a RFID blocking device.
- Or an inadequately-protected customer ID number stored in a rebate card could be intentionally changed by third parties, and the rebates accounted to another person. Bank ATMs have been and still are being compromised by similar exploits that have been known and documented for years, despite that the ways to guard against the exploits are also known and documented.

The social problems of exploitation through standardisation and interoperability in digital communication technologies are perhaps most starkely illustrated through problems with Internet viruses and the hindrances to productivity and the detriment to quality of life that they cause. Most of this malware is targeted at a specific vendor's software products, and the risks of such homogenisation have been studied in the professional literature for more than a decade. Those of us who use other products from different providers have not been affected by the malware to anything like the same extent (except insofar as the problems affect our interlocutors).

We suggest that the EU could usefully consider the social consequences both of standardisation and interoperability, and of their converses, technical and data diversity and protection. We also suggest that the development and application of appropriate technology, such as cryptologic and cryptographic technology, in service of data diversity and protection in the use of RFIDs may be a suitable area of study.

The Fragmentation of Technical Customer Protection

Two technical measures have been proposed by the DW industry and developed to enable consumers to protect themselves from the unwanted effects of RFID technology.

First is a deactivation device [5], which shall disable RFID tags after the point of sale. It is not proposed that such devices be used by retailers, thus adding a burden to a customer to ensure deactivation him- or herself. Further, it is technically not possible for a customer to ensure that the RFID tag is truly disabled, or has merely become dormant or partially-functional. Any such deactivation technology, to be effective, must prove to the customer that permanent deactivation has occurred. No such technology has yet been offered [6].

Second is a blocker tag, which is supposed to inhibit the communication between RFID tag and reading device by transmitting jamming signals. This technology is also not yet ready (see the information page on blocker tags at [7]). It may also interfere with legitimate and desirable uses of RFID tags (inventory assessment; automated transactions). Furthermore, there are technical holes in the protection thus offered. As with deactivation devices, the onus to provide blocker-tag protection will likely lie with the customer.

When the onus lies with a customer to provide protection technology, it is also open to a store owner in Germany to deny entrance to a customer possessed of such technology. So apart from the technical immaturity of the proposed protection, there could be strong social pressures inhibiting people from employing such protection, even though they might wish to do so.

We suggest that the EU could devise appropriate technical protection and develop the means, legally or otherwise, to secure its use as appropriate.

Technological Impact Protection

Not only the potential for easy misuse raises concerns about RFID technology. The proposed normal use raises concerns also, not just with DW technology alone but in combination with other technologies.

In general, it must be ensured both now and for the future that normal use does not, and cannot, lead to a violation of existing social protections, especially those dealing with security, privacy and civil rights.

Studies so far of the impact of RFID technology have mainly focused on the interests of the introducers and users of such technology, rather than on the interests of all stakeholders, many of whom may be negatively affected by its use. We therefore see a significant role for the EU in supporting impact studies which focus on all stakeholders, including not just industrial users but also consumers of retail products, those who wish to maintain their privacy to at least the current extent, and so on.

Unless significant study of impact followed by appropriate actions and measures is undertaken, we can envisage abuse levels of RFID technology reaching the levels of abuse of current Internet technology, which to all accounts is unacceptably high. (We note that much abuse of digital communication technology is known to be underreported, especially embezzlement through financial institutions.) We regard the proposals we have made above as the minimum necessary to avoid such an outcome with RFID technology.

Summary

We have suggested that the EU could:

- Further study the impact on health (particularly implanted electronic equipment) and existing infrastructure of increasing levels of moderate- to high-energy RF transmissions.
- Identify conflicts between the intention of the law and DW technology which are intrinsic to the technology, and propose resolution of such conflicts before wide-area introduction of the technology.
- Usefully consider what sorts of stakeholder-involvement processes it wishes to encourage for the resolution of the conflicting interests of stakeholders in RFID use, and how these processes might be structured.
- Analyse possibilities for intentional and unintentional abuse of RFID technology in detail and find ways to implement the technology so as to render impossible such nefarious uses and to render feasible only those uses legitimated for the purpose of the tags.
- Consider the social consequences both of standardisation and interoperability, and of their converses, technical and data diversity and protection.
- Develop means, say through development and application of appropriate cryptologic and cryptographic technology, to ensure the acceptable degree of technical and data diversity, whatever that should turn out to be.
- In general, devise appropriate technical protection for stakeholders in RFID technology and develop the means, legally or otherwise, to secure use of this protection.

References

[1] FoeBuD e.V., Public Domain 128: “Spy Chips in the Yoghurt Mug – RFIDs - coming soon!”,
`http://www.foebud.org/pd/pd128/index-gb.html`

[2] Dr. Benda, Dr. Simon, Dr.Hesse, Dr. Katzenstein, Dr. Niemeyer, Dr. Heußner, Niedermaier, Dr. Henschel: “BVerfGE 65, 1 - Volkszählung: Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden”,
`http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm`

[3] Jan E. Hennig, Networks and Distributed Systems (RVS) Group, Faculty of Technology, University of Bielefeld: “Preserving Privacy in RFID Deployment”, RVS-Occ-04-01, 2004-03-23,
`http://www.rvs.uni-bielefeld.de/publications/Papers/RFID/preserving_privacy_in_rfid_deployment.pdf`

[4] Jane Black, Business Week: “Shutting Shopping Bags to Prying Eyes”, 2004-03-05,
`http://www.businessweek.com/technology/content/mar2004/tc2004035_8506_tc073.htm`

[5] Metro AG, Future Store Initiative Website: “Position paper Subject: The use of RFID in the Future Store in Rheinberg”, 2004-02-28,
`http://www.future-store.org/servlet/PB/menu/1002376_l2/index.html`

[6] Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN): “Scandal: The ’Undead Machine’ RFID Tag Deactivation Station that does not Deactivate Tags”, 2004,
`http://www.spychips.com/metro/scandal-deactivation.html`

[7] Jan E. Hennig and Harald Manninga, FoeBuD e.V.: “What are RFID blocker tags? Should I go and get such a thing?”, 2004-03-27,
`http://www.foebud.org/texte/aktion/rfid/blocker_tags/index.html`