Broader privacy issues

Yvo Desmedt
Department of Computer Science, Florida State University
Tallahassee, FL 32306-4530, USA
desmedt@cs.fsu.edu

Abstract

In RFID, identification takes place in an overt way, even though the user may be unaware of its consequences. Although RFID is getting a lot of attention, other technology may undermine privacy as much as RFID by using covert identification. Privacy enabling solutions based on disabling RFID may unfortunately be bypassed.

The issue that passive or active RFID or ubiquitous computers in general can be used to identify the reader of a book, has already been pointed out several years before September 11. We reflect back on some of the earlier predictions.

Finally we also propose some limited solutions to increase privacy.

1 Introduction

Lately, RFID technology has received a lot of criticism. Already 7 years ago the author pointed out the potential privacy problem of embedding chips (Thinks that Think) in such objects as shoes, belt buckles, tie clasps, etc. [9]. He basically wrote a "black paper against Things That Think and to a certain extent a black paper against Ubiquitous Computing" by pointing out that these can be used for identification purposes.

Some have suggested that RFID technology will replace bar codes, see e.g. [13]. If this would happen, it *seems* that the potential abuse of privacy may be quite extensive. The author already warned 7 years ago that

> modern technology replaces after a while — when it is no longer an expensive exclusivity — the old and the old technology is

> no longer produced, even if the new has several disadvantages. ... So, if ubiquitous computing and Things That Think become more popular they will replace old technology such that it will be inevitable to wear clothing with chips, which may enable covert identification.

So, it is important to try to foresee the new versions of the technology decades before it even exists in order to understand a potential evolution towards the natural extinction of an older technology. There are several problems with this need:

- the new technology, or in this case renewed[1] technology, may have several advantages which make its acceptance natural, regardless of the dangers to society.
- scientists and engineers are very bad in predicting the progress of technology (see e.g. the many claims made by the AI community in the 1950-1960's).

We now discuss the goals and organization of the paper. We first reflect back in Section 2 on the feasibility of some attacks on privacy that were proposed 7 years ago. We also try to learn some lessons. A weakness of the author's 7 year old paper is that the author did *not* predict other types of technologies to achieve covert identification, besides using covert circuits. Some that have been discovered in the meanwhile are briefly surveyed in Section 3. We end by suggesting some research issues.

2 Privacy issues before September 11

The author already pointed out some privacy concerns when using ubiquitous computers 7 years ago. We first briefly survey those. The main goals of this section are to:

- check whether the 7 year old predictions for "future" technology are feasible,
- learn some lessons, and
- analyze the impact of September 11 on these predictions.

[1] Since IFF (Identification of Fried or Foe) can be regarded as a first form of RFID, it can be considered as actually quite old.

2.1 The concern, as expressed

Three methods in which covert techniques can be used to covertly identify a certain part of the population and/or to monitor their behavior were described by the author 7 years ago [9]. The first was on using covert technology to identify the author of a document. The prediction of this danger came true three years afterwards [7]. Since this is not related to RFID, the covert identification of authorship is not discussed further.

We now focus on the two predictions [9] made that are relevant to RFID like technology. Although these were discussed in the context of Thinks That Think, they obviously also apply to active RFID. We now quote relevant parts of the text [9] (the footnotes are also 7 years old):

> we can indeed envision that in the future books will have a chip embedded in the cover to give the buyer access to a private multimedia environment while maintaining copyright, in a similar way as chipcards do today. To interact with their environment, communication equipment, such as an antenna[2], will be in the cover of the book. Suppose that an agency wants to find out, secretly, who buys books about a topic considered of interest to national security. ... The Global Positioning System (GPS) [18] allows pinpointing one's location with an accuracy of a few meters. Since the aforementioned hardware has an antenna built-in, it may be used[3] to obtain the positioning of the book on earth ... This may enable one to trace the location of the owner. Observe that in countries where one has to register where one lives, this identifies the owner of the book. ...
>
> Our next illustration is similar to the last one. Instead of using chips embedded in the cover of a book, we use the Things That Think scenario in which chips are in sneakers, belt buckles, tie clasps, etc. We also use the GPS system in this example and if enough chips are at fixed locations in the "environment" a higher accuracy can be achieved than with normal GPS and the need to

[2]For example, flexible antennas that have the thickness of paper and are used to protect medium priced merchandise against theft in shops, can easily fit in a fraction of the cover of a book.

[3]The design should take into account that antennas do not capture all frequencies equally and that antennas have been designed that are able to capture several frequencies simultaneously.

> rely on GPS can be diminished. It should be noted that a global positioning (with a precision of 2 meters) only requires 6 bytes, as one can easily verify. This means that it only takes roughly 1.5 Gbytes to store the global positioning of the whole U.S. population (approximately 250 million) while an inexpensive 8 mm "videotape" can store (roughly) 5 Gbytes. If one is not interested in recording such travel as commuting between home and work, but only to track who travels further away and to where, and who approaches sensitive locations which may be targets for terrorist activities or places where one can buy material to make bombs, etc., then the data can easily[4] be compressed significantly. The things-that-think need communication equipment, as mentioned in Section 1. So they could covertly sensor the positioning of its bearer, as explained in the previous example and covertly transmit it to the computers in the "environment". These send the data to their intended destination and/or could replace the need to rely on GPS. If the things-that-think know the identity of its bearer (as in the examples we overviewed in Section 1), the identification is straightforward, otherwise it might be deduced when correlating the data with other databases.

To deal with environments that do not have the equipment to receive such communication, the following variant was proposed, quoting from [9]:

> Even if one travels to remote locations that do not have an abundance of ubiquitous computers, at regular time intervals the things-that-think could store the exact positioning of the bearer under compressed form and transmit this at a later time. It is clear that the sooner a high bandwidth network is installed and the more omnipresent computers become, the more frequently the global positioning of persons can be updated. This then facilitates the more detailed monitoring of individuals. Traffic monitoring which nowadays mainly monitors who communicates electronically with whom can then be extended to its full power.

[4] One could question whether such gigantic amount of data could easily be processed. However, one should know that several laboratories in the world have computers each having several Gbytes of RAM, so that the task is rather easy.

2.2 Relevance and relation to active RFID

While the 7 year old paper was primarily focusing on how covert technology can be abused by a so called "Big Brother," it is obvious that the same concern applies to overt technology. Moreover, the role of GPS can be replaced by RFID readers to some degree when one knows their location. GPS (or similar methods) are still required if there are not enough RFID readers for more detailed tracking purposes.

2.3 Technological feasibility

So far we know, nobody has attempted to design the aforementioned technology proposed 7 years ago. We now discuss the issue whether the technology that was predicted is feasible today.

A problem is that the required bandwidth to receive GPS signals (1575.42 MHz and 1227.6 Mhz are currently used) is different from the RFID's high frequency range, which is between 850-950 Mhz and 2.4-2.5 Ghz. Progress on multi-frequency antennas however solves this problem (see e.g. [16]).

Another problem with the proposed use of GPS receivers, is that 7 years ago these required relatively high power. Today, chips have been developed that are low power GPS receivers (see e.g. [15]). The size of the chip is 7mm×7mm and can be put into standby. However, seeing the size of the chip this does not easily fit within a small "covert circuit."

2.4 Lessons

2.4.1 A positive note

The predictions seem to warn against deploying a combined use of active RFID and GPS. However, the opposite may be true, as we now discuss.

A well known problem with some RFID is that these will leak the identity of the user even when undesired. A solution to avoid undesired use of RFID is to couple it with user programmable technology based on GPS. Let us explain this while focusing on the typical example of toll booths on a toll road.

One could use GPS technology to find the location of the car. The list of toll booths could contain the information of their GPS coordinates. Only when the car is near a registered toll booth will the user's technology allow the RFID to respond. Evidently, to remain economical such combined use

assumes that a GPS receiver is already installed in the device. The example evidently is not limited to cars, but the idea applies to any device with a GPS. A positive or negative list could be used of where to enable the RFID to respond.

So, although GPS technology can be used to identify the owner of goods, it can also be used to prevent abuse.

2.4.2 A negative note

Although, it seems unrealistic that in the near future cover circuits can be used to covertly run a GPS receiver, there are other potential dangers of covert circuits, as we now illustrate.

A solution some have proposed to deal with privacy concerns of RFID is to disable these, e.g. by incorporating a switch off command. The problem with this solution, is that a covert circuit may exists that can be used to partially reactivate the RFID. Such covert circuits can obviously be relatively small.

2.5 Impact of September 11

The author's 7 year old example that agencies may be interested in tracking who reads what book is now reality. The recent Patriot Act may require libraries to release such information (see e.g. [22]). However, the Attorney General of the US claims that this provision of the Patriot Act has never been used [2].

Note that after September 11, some corporations have been pushing RFID claiming it will stop terrorists [3].

3 RFID not that unique in endangering privacy

Currently the media is giving a lot of attention to the abuse of RFID technology. While the identification capability is clearly overt, the user may not be aware of its power. The goal of this section is to state that non-RFID technology can also be used to reduce privacy rights.

RFID, is a technology that has been designed to overtly identify an object or a user. Can such identification be done under other circumstances? There are two other scenarios. In the first one, the identity must be inferred

from other information. In the second, the technology has been designed to covertly achieve identification. We now discuss both approaches.

3.1 Deducing the identity

Triangulation is an old technology that has been used, e.g. during World War II to track those that "illegally" listen to broadcast communication.

A problem with electronic equipment is electromagnetic emanation (see e.g. [21]). Even if this emanation has not been designed to identify the equipment, it is known that electronic devices, or parts of it, have a electromagnetic resonance frequency. This resonance frequency is sufficiently unique to pick a single monitor out of several others [21].

So, if one takes a handheld/handless device, then observing the location over time, using triangulation, one can identify who its owner is. This then allows later on to locate and track the user. Evidently, the technology to do this is currently not installed. However, if the desire of society to track people continues to grow, one should not exclude this in the future.

Although this scenario sounds far fetched, one should not forget that cell phones have never been designed to allow tracking the user with quite some precision. Today, by adapting the cell towers, such triangulation is now possible [5]. A relevant question evidently is whether RFID privacy advocates turn off their cell phones?

3.2 Covert technology

RFID overtly identifies the device and so possibly its user. The author pointed out [9] that covert circuits, covert sensors and covert computation in Things-That-Think and other ubiquitous computers could covertly identify the owner. However, as already discussed, a covert GPS is currently infeasible. So, the technology to set this up must be organized in a different way.

In the meanwhile, other forms of covert identification have been found that use very different technologies. Methods that have been suggested rely primarily on biometrics and pattern matching, see e.g.[5] [1, 12, 11]. In some countries legal aspects of covert identification are being considered, see e.g. [6].

[5]Note that Google finds 160 matches of "covert identification."

Although face recognition technology has been deployed to covertly identify whether known criminals are in a certain area of the city, a question remains whether the false positive rate is high [4]. License plates can also be identified in a covert way. Using cameras and artificial intelligence, error rates of roughly 6% were reported and only 2% for non-moving cars [14].

4 Conclusions and Research Issues

4.1 Research

While a lot of unclassified work has been done on covert communication (see e.g. [19, 10, 17, 20]), very little seems to have been done on covert circuits and covert devices. When we move towards ubiquitous computing, it seems we should seriously start studying this issue more deeply.

Covert devices have primarily been developed by secret agencies. To protect society against such devices, an open research study seems to be necessary. Except theoretical studies (e.g. [8]), there is almost no unclassified research on covert circuits. Interesting questions in this area are:

- what logical methods can be used to design a covert circuit hidden inside an overt one?
- what hardware methods can be used to trigger/activate the covert one?

4.2 Conclusions

There are several methods today to identify and trace individuals, e.g. using covert identification. License plate of cars and cell phones carried by individuals can be used for such purposes. The use of covert devices and covert circuits may further aggravate the problem. The existence and the ease of deploying such technologies relativizes the privacy implications of RFID. The main concern about RFID seems to be that it may enable third parties to track individuals that buy certain goods, e.g. books.

Although some predictions made 7 years ago by the author came true, the covert use of GPS needs to rely on a covert device instead of on the use of a covert circuit.

Acknowledgment

The author thanks Simson Garfinkel and Henry Holtzman for suggestions on how to reflect back on [9] in this paper. The author also thanks one of the anonymous referee who suggested to add more references. It allowed the author to find several recent publications on covert identification.

References

[1] Active laser imaging system. http://www.continuityofgovernment.org/, 2002.

[2] K. Arena, K. Bohn, and T. Frieden. Justice document: Patriot act provision never used. `http://edition.cnn.com/2003/LAW/09/17/ashcroft.patriot/index.html`, September 18, 2003.

[3] M. Baard. Claim: Rfid will stop terrorists. `http://www.wired.com/news/privacy/0,1848,59624,00.html`, August 8, 2003.

[4] Biometrics under scrutiny. `www.nao.gov.uk/intosai/edp/intoit_articles/16p45top56.pd` October, 2002.

[5] J. Borland. Wireless phone tracking plans raise privacy hackles. `http://news.com.com/2100-1033_3-248442.html`, November 10, 2000.

[6] Jeremy Dein. Identification - the way forward. Criminal Bar Association Winter Lecture, http://www.criminalbar.co.uk/lectures/lec18.cfm, November 26, 2002.

[7] Y. Desmedt. Re: Lack of anonymity in microsoft word. *Forum On Risks To The Public In Computers And Related Systems*, 20(24), March 11, 1999. See also `http://catless.ncl.ac.uk/Risks/20.24.html#subj16`.

[8] Y. Desmedt. Is there an ultimate use of cryptography? In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto '86 (Lecture Notes in*

Computer Science 263), pp. 459–463. Springer-Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15.

[9] Y. Desmedt. Establishing Big Brother using covert channels and other covert techniques. In R. Anderson, editor, *Information Hiding, First International Workshop, Proceedings (Lecture Notes in Computer Science 1174)*, pp. 65–71. Springer-Verlag, 1996. Cambridge, U.K., May 30–June 1.

[10] J. T. Haigh, R. Kemmerer, J. McHugh, and W. D. Young. An experience using two covert channel analysis techniques on a real system design. *IEEE Transactions on Software Engineering*, SE-13(2), pp. 157–168, February 1987.

[11] S. T. Kent and L. I. Millett, editors. *Who Goes There? Authentication Through the Lens of Privacy.* The National Academies Press, Washington, D.C., 2003.

[12] S. Liu and M. Silverman. A practical guide to biometric security technology. *IT Professional*, 3(1), pp. 27–32, January-February 2001.

[13] A. Martin. Radio chip to rival bar code security. http://www.computerweekly.com/Article103732.htm, July 6, 2001.

[14] J. Molina, M. Mossi, and A. Albiol. Development of a plate reader for a surveillance system. In *Sixth Annual Scientific Conference on WEB technology, new media (EUROMEDIA 2001)*, pp. 209–211, Valencia (Spain), 2001.

[15] Motorola unveils latest in family of single chip GPS devices. `http://www.motorola.com/ies/GPS/docs_pdf/singlechip.pdf`, September 22, 2002.

[16] D O'Shea. Skycross transmits funding news. `http://telephonyonline.com/ar/telecom_skycross_transmits_funding/`, August 25, 2003.

[17] P. A. Poras and R. A. Kemmerer. Covert flow trees: a technique for identifying and analyzing covert storage channels. In *Proc. of the 1991 IEEE Symposium on Security and Privacy*, pp. 36–51. IEEE Computer Society Press, May 1991. Oakland, California.

[18] N. F. Ramsey. Precise measurement of time. *American Scientist*, 76, pp. 42–49, January–February 1988.

[19] G. J. Simmons. The prisoners' problem and the subliminal channel. In D. Chaum, editor, *Advances in Cryptology. Proc. of Crypto 83*, pp. 51–67. Plenum Press N.Y., 1984. Santa Barbara, California, August 1983.

[20] G. J. Simmons. The history of subliminal channels. In R. Anderson, editor, *Information Hiding, First International Workshop, Proceedings (Lecture Notes in Computer Science 1174)*, pp. 237–256. Springer-Verlag, 1996. Cambridge, U.K., May 30–June 1.

[21] W. van Eyck, J. Neesen, and P. Rijsdijk. On the electromagnetic fields generated by video display. In *Proc. Symp. EMC*, Zürich, March 1985.

[22] H. Yi. Cmu librarians going by the book on patriot act. *The Tartan, Carnegie Mellon's Student Newspaper*, 97(25), April 28, 2003.