User Perception of the Security & Privacy Concerns of RFID Technology

F. Li[1], N.L. Clarke[1] and C. Bolan[2]

[1] Network Research Group, School of Computing, Communications & Electronics,
University of Plymouth, Plymouth, UK
[2] School of Computer and Information Science, Edith Cowan University, Perth,
Western Australia

Abstract

The adoption of wireless technologies has undergone unprecedented growth, beginning with cellular devices and now including Wi-Fi and Bluetooth. A relative newcomer to this domain is RFID, a shortwave communications technology capable of tagging almost any physical item. Unfortunately, as with all wireless technologies, RFID based technologies face a range of security and privacy threats. Indeed, many RFID systems completely lack any security or data protection provision whatsoever. This paper presents a survey into the end user perception towards security and privacy of RFID technologies in order to establish the level of understanding and concern towards its adoption. Noticeably, users are very responsive towards the use of wireless technologies and RFID in particular, however, only to the point at which their privacy is not negatively affected. 93% of respondents considered their privacy to be important. The survey established users do have a some appreciation of security and privacy but encouragingly are also aware of limitations in this respect and are eager to learn more.

Keywords

Mobile, Wireless, Security, RFID, Privacy.

1. Introduction

The dramatic uptake of wireless technology has provided a platform for the ubiquitous access to telecommunication and data networks, now central to the modern lifestyle. According to Cellular Online (2006) there are now over 2 billion mobile phone users and more than 130,000 publicly available WiFi hotspots in 130 countries, and these numbers are increasing daily. As with any growth in technology there is a need to balance the enthusiastic uptake with due concern towards security and privacy issues. This is evidenced by the multiple published vulnerabilities of WLANs, Bluetooth and other wireless technologies (Bolan, 2005; Wong, 2005).

Radio frequency identification (RFID) technology stems back to Faradays' discovery that light and radio waves were both forms of electromagnetic energy. The first concrete step towards the modern conception of RFIDs was made by Harry Stockman in his 1948 paper Communication by means of reflected power (Stockman, 1948), although it was not until 1973 that the first direct patent on passive RFID tags was lodged in America by ComServ (Cardullo, 2005). For the present RFID systems remain too expensive to completely penetrate all possible markets, with typical transponders costing around US$0.50 – US$1.00 (Sarma *et al.*, 2002). However, with mass production coupled with an open standard, supporters aim to bring the price down to around US$0.05 – US$0.10 which would see RFID integration into almost every facet of life. This has prompted predictions such as Boone (2004) who estimates that over 1.3 billion dollars will be spent on RFID integration in 2008.

As RFID technology is a member of the wireless family, it will inherit many commonly known wireless security and privacy threats currently linked to its wireless cousins. Beyond this, new attacks and threats are being discovered such as cloning, spoofing and kill attacks (Young, 2006; Bolan, 2006a). When such concerns are coupled with warnings that by 2016 Britain will increase the level of tracking to unknown levels, and the monitoring of individual consumer behaviour will emerge as an unavoidable facet of daily life, a worrying trend emerges (Ford, 2006). While it is likely that this dystopian image of the future is overly alarmist, as with all advancements in modern life, it is better for the public to have a clear idea of the security and privacy implications before product saturation becomes irreversible. Before a reasoned discussion may take place it is important to gauge the current level of awareness and fears surrounding the technology, and how these levels may impact on RFID's uptake and acceptance.

This paper presents the findings of a survey conducted to assess the level of public awareness regarding the security and privacy aspects of RFID technology. Section 2 presents background information on the problem of privacy and security of RFID technology. Section 3 describes the aim and methodology of the study, whilst section 4 presents the key results. Section 5 puts the results into context and provides a discussion on the implications of its findings. The conclusions are presented in the final section.

2. Security and Privacy Concerns of RFID

While RFID tags are typically silicon-based microchips, functionality beyond simple identification-upon-request may be achieved through the inclusion of integrated sensors, read/write storage, encryption and access control (Weis *et al.*, 2003). The downside to such operations is the increased production cost of the RFID tag away from the ideal market penetration cost, thus RFID security is often focused on reader security ignoring the obvious avenue of attack due to tag limitations (Choi et al., 2005).

Added to this is the debate as to whether the adoption of some RFID security measures is against the original vision of the technology. Knospe & Pohl (2004) argue that, as the primary purpose of RFID technology is as a cheap automated identification, it is unreasonable to expect that standard security mechanisms be implemented, due to the complexity and constraints of the resource. Ranasinghe et al. (2004) use this as a basis to propose that RFID security be implemented at the data processing subsystem and thus leave RFID tags merely for identification. However, others argue that security is possible without affecting tag cost or the original vision for the technology (Engberg et al., 2004).

Irrespective of these arguments, no single security or encryption standard for tags or readers has been adopted and thus many systems remain insecure (Weis, 2003; Henrici & Müller, 2004). Noting such issues, Hennig et al. (2004) voice the following concerns:

∉ “*Worldwide unique IDs enable tracking*” – the adoption of unique Electronic Product Code (EPC) tags will allow anyone who carries at least one of these tags to be tracked worldwide.

∉ “*Unnoticed remote reading without line-of-sight*” – the very nature of RFID technology allows RFID tags to be read without line-of-sight or any overt suggestion that they are being engaged. Such features make unauthorised access more likely.

∉ “*Small hidden tags and readers*” – As tag sizes decrease the ease with which it becomes possible to install hidden tags and readers increases.

∉ “*Tracking and profiling through sporadic surveillance*” – with a sufficient spread of strategically placed RFID readers it is possible to track and profile without the need for continual activation. Also, through the use of natural bottlenecks such as doorways it is further possible to ensure an individual passes within range of a reader.

3. Research Methodology

Although RFID systems have existed for some time it is only recently, with advancements in technology, the demand for RFID-based technology has begun to thrive. Organisations are utilising RFID technology for a variety of purposes with inventory control being one of the most popular. To date, many of the applications of the technology have been developed for business use, with few real large scale consumer RFID products. As such, it is suggested that public awareness of RFID technology is fairly low. Some people might be using the technology but unaware of its inner workings and classification as a RFID product – for instance, remote central locking devices for cars, the Oyster card, anti-theft devices in supermarkets and biometric passports. Nevertheless, as the popularity of RFID technology increases it is inevitable that consumers will begin to interact and directly utilise RFID technology. However, the nature of RFID introduces a number of additional concerns regarding the security and privacy of individual’s information. As such, a survey was conducted to provide some preliminary insight into consumer’s awareness of RFID, its possible applications, and the threats posed by the technology. The purpose of the survey was to assess the degree to which consumers would accept the benefits/additional services provided by RFID when facing threats to the privacy of their information.

Compared to other wireless technologies, such as cellular, Wi-Fi and Bluetooth, RFID is relatively unknown technology. Therefore, in order to maximise the usefulness of the survey findings and to provide a context/point of comparison, the survey asked a series of questions regarding the general topic of wireless technology, in addition to specific questions regarding RFID technology and its applications. This assisted in judging whether respondents were more or less concerned about security and privacy when compared to other more familiar wireless technologies. In addition, to ensure the survey received informed opinions from respondents, the survey included a paragraph of text describing RFID technology and how it can be used.

The survey comprised of four sections:

∉ Demographic questions to establish an understanding of the respondent population

∉ General security questions to gauge the level of awareness of security across wireless technologies

∉ General privacy questions to understand the privacy concerns of respondents regarding wireless technologies

∉ Specific RFID questions to assess the degree to which respondents are concerned over the use of the technology

4. Survey Findings

A total of 365 completed surveys were received. An analysis of the demographic questions reveals a fairly even gender split, with 54% male respondents compared to 44% female. The age of respondents, however, was found to be skewed heavily (77%) towards the 18-30 age group. There is also a notable bias in the level of education, with 96% of respondents declaring a university level education. Although both the age and education are clearly not representative of the general population, it is felt this bias would only serve to provide a more informed opinion. Prior surveys have demonstrated the 18-30 age group as having amongst the highest market penetration of mobile devices (Competitive Commission, 2003).

4.1 Awareness of Wireless Security

Prior to assessing the level of concern about wireless technologies it is prudent to establish the degree of awareness that exists within the respondent population. Figure 1 illustrates a breakdown of the principal consumer wireless technologies. The table clearly shows a lack of awareness of RFID technologies with only a third of respondents registering a positive awareness. Respondents were very aware of all other wireless technologies, receiving well over three quarters of the response, with the slight exception of the newer 3G telephony networks. It is interesting to note however, that 77% respondents stated they were aware of GSM/GPRS. Given the market penetration in Europe and the respondent population, the number of respondents actually using a GSM/GPRS mobile phone is likely to be greater than this, perhaps highlighting a lack of awareness of the underlying technology.

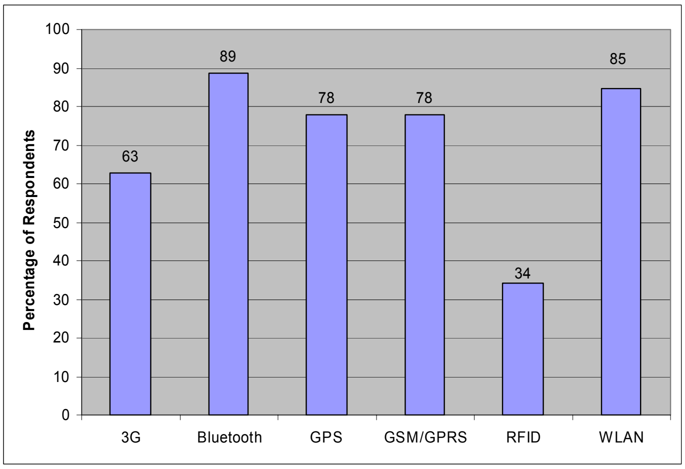

Figure 1: Respondent Awareness of Wireless Technologies

Respondents' use of the technology would also be a useful indicator as to the practical experience and subsequent relevance of responses they provide. Table 1 provides a breakdown of the usage of wireless technologies. The most frequently utilised technologies include WLAN and GSM/GPRS, although similarly to the earlier question, the percentage of the latter is surprisingly low. All wireless technologies have some level of usage from respondents, with RFID being the least utilised technology. Interestingly, although respondents were made aware of what RFID technology is with example applications, 34% of respondents were unsure if they used the technology. This lack of understanding regarding what technology they are utilising could have a significant impact upon the user, as they would either not understand, or misunderstand, what the security and privacy threats against the technology are.

	Very often (daily) (%)	Often (few times a week) (%)	Not very often (few times in two weeks) (%)	Few times a month (%)	Do not use it (%)	Do not know (%)
3G	11	5	5	10	62	7
Bluetooth	12	14	10	22	39	3
GSM/GPRS	30	13	6	12	30	9
GPS	8	6	6	16	57	7
RFID	3	3	4	7	49	34
WLAN	46	11	5	7	24	8

Table 1: Frequency of Usage of Wireless Technologies

Given the medium of communication, wireless systems exhibit additional security threats when compared to more traditional wired networks. War driving in particular is one well known example of such misuse. The perception of how secure a technology is will be essential to the successful widespread adoption of a technology. When asked how secure they consider wireless technologies to be, the largest proportion of respondents indicated "secure" – which if technically true and not a misconception is a reassuring statistic. It is however, also worth noting that over 55% of respondents indicated they felt wireless technologies to be only a little secure or not secure at all. Figure 2 presents theses findings and illustrates a skew towards feelings less secure overall.

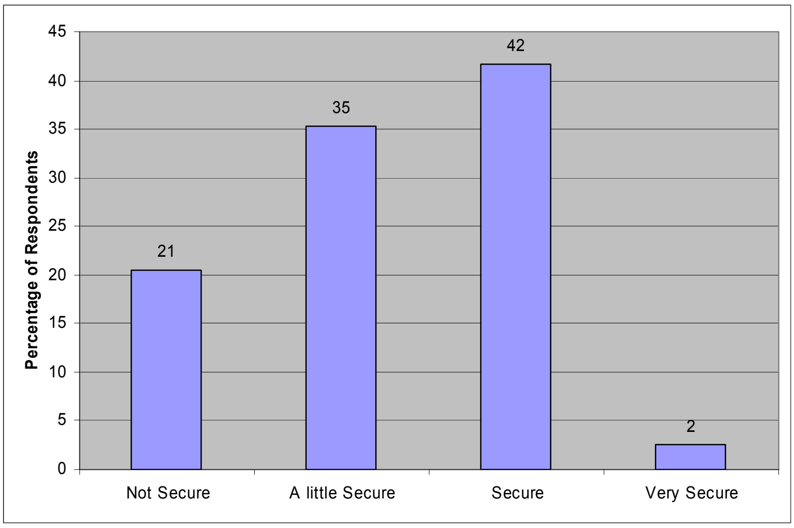

Figure 2: User Perception of the Security Wireless Technologies

Upon analysing respondents' use of security controls, it certainly seems that a good majority of users are aware of the typical countermeasures. As illustrated in Table 2, 79%, 78%, 72% of respondents use Antivirus, Firewalls and password authentication respectively on their laptop. Notably, the use of such controls is less on other types of mobile device, however, given the level of threat to date against these technologies (when compared to their laptop/desktop counterparts) and the maturity of the controls that exist for these platforms, it is not unexpected.

	Mobile phone (%)	**PDA (%)**	**Wireless Laptop (%)**
Antivirus software	7	25	79
Biometrics	2	8	7
Firewall	6	25	78
Password/PIN	45	56	72
Switch off when not using it	32	35	68

Table 2: Security Controls Implemented

Switching the device off when not in use has the potential to prevent exposure to a wide variety of threats, particularly if the threat is utilising Bluetooth. Typically, with the exception of laptops which have an obvious power consumption problem, the majority of respondents do not switch off their device when not in use. Interestingly, when asked specifically with regards to Bluetooth, a larger proportion of respondents (58%) did state they switched it off when not it use. It is unclear whether this is due to respondents' security awareness of for example Bluejacking, Bluesnarfing and Bluebugging, or perhaps simply through a lack of use of Bluetooth, or just to conserve power.

When asking respondents to rate their security awareness, the largest group of respondents chose the middle ground (40%). In fact, an analysis of the findings illustrated in Figure 3, show a fairly Gaussian distribution, with a very slight left skew towards poor. On average, respondents do feel they have a level of security awareness, which is reinforced when analysing the security controls they have put in place. It is worth pointing out, 32% of respondents felt they have a 'poor' or 'very poor' level of security awareness.

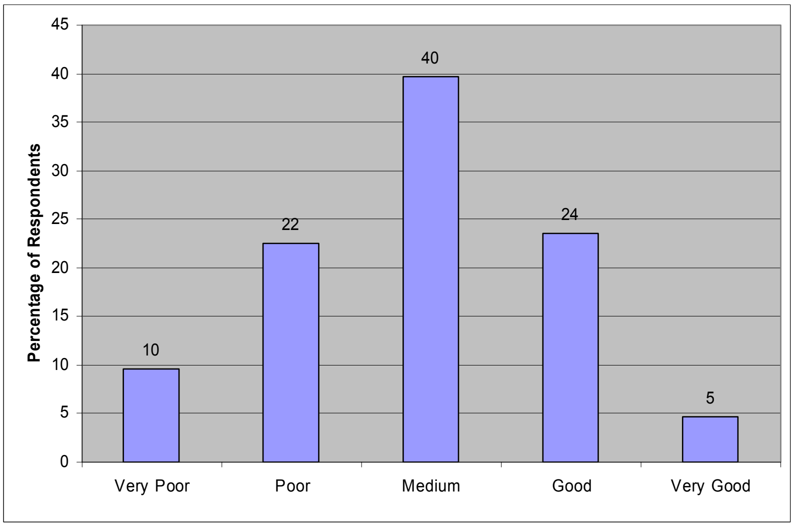

Figure 3: Respondents' Level of Security Awareness

Even though 68% of the respondent population felt they had 'medium' to 'very good' awareness of security for their devices, an overwhelming 86% stated that they would benefit from learning more about security. This figure shows how much more work needs to be undertaken in successfully educating the public regarding not only the security threats but also the implications of the technology they utilise.

4.2 Wireless Privacy Concerns

Personal privacy is becoming an increasingly important concern. As our use of technology continues to expand, the amount of personal information we have increases. The nature of the information can vary from direct sources such as corporate files, personal expense records, contact lists, personal and business messages, to more indirect sources or side-channel information, such as a person's location both past and present, frequency of use and shopping habits. Each of the different wireless technologies has its own unique properties and threat vectors.

However, what is clear from the respondents' perspective is their privacy is an important consideration. 93% felt their privacy to be at least important or greater, with the largest group of 41% selecting 'extremely important' as the most appropriate category.

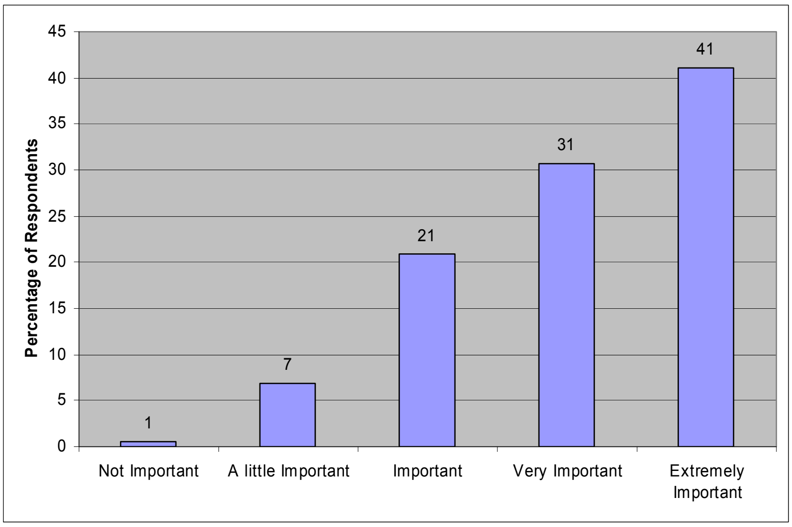

Figure 4: The Important of Privacy to Respondents

Respondents were particularly concerned (75%) about the possibility of being tracked via wireless technologies. Upon being presented with a list of wireless technologies that could possibly be used in tracking, only 5% of respondents felt none of the technologies could be used for tracking, as illustrated in Figure 5. Obviously, the degree to which these technologies can be utilised for tracking is somewhat dependent upon the technical capabilities of the adversary, with some technologies (such as WLAN) being far simpler to monitor than others (such as GSM/GPRS). Nevertheless, the perception and awareness of the respondents is on the whole quite high, with 4 of the 6 technologies listed eliciting a response of over 50%. A pattern again can be seen with the newer 3G and RFID technologies both receiving less attention. Although it is unlikely to have a direct impact currently given the fairly low penetration of the technology, both these technologies inherently offer a finer level of tracking through location-based services of 3G and inventory control of RFID than other wireless technologies traditionally have (with the exception of GPS of course). These services will provide an opportunity for an unprecedented level of personal tracking.

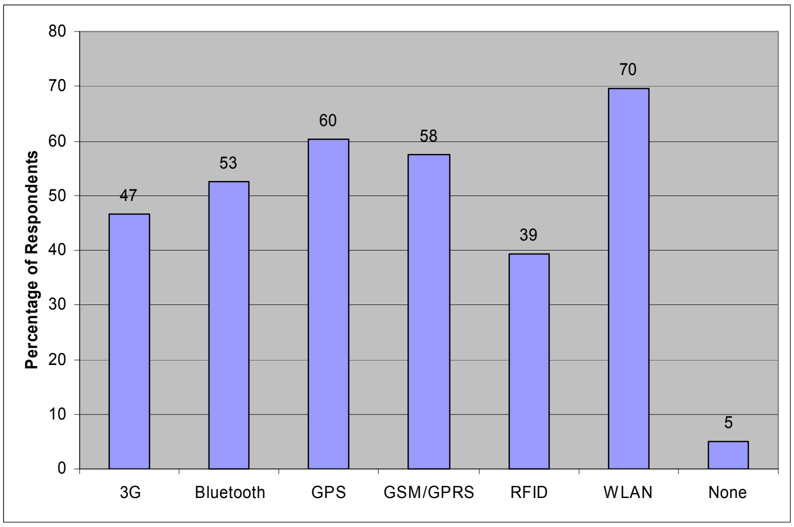

Figure 5: Respondent Perception of Tracking Technologies

Although respondents are clearly concerned about privacy and have some awareness of one key threat to privacy, tracking, it is clear that this knowledge and awareness is certainly not uniform across the respondent population. In fact, upon analysing the results from the level of privacy awareness the majority of respondents only feel they have a 'medium' level of awareness, with an overall skew towards a poor level (as illustrated in Figure 6).

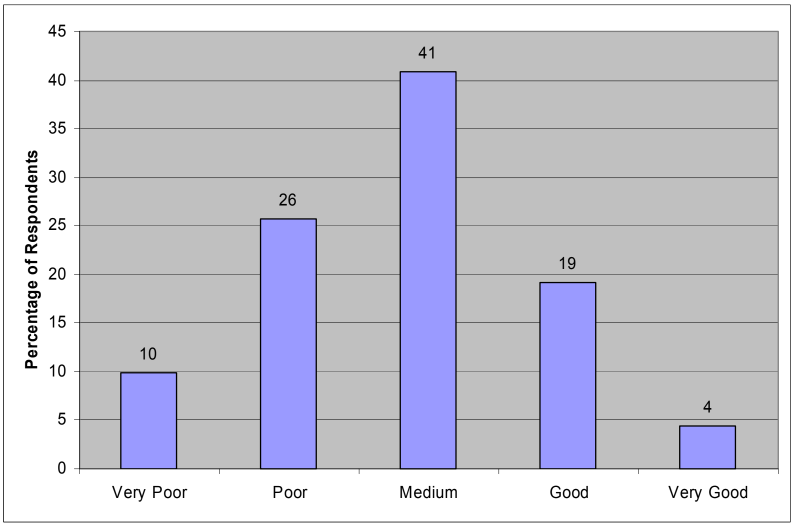

Figure 6: Respondents' Level of Privacy Awareness

4.3 Applications of RFID

In order to establish the degree of threat people might be open to, it is useful to understand the level to which they would be willing to use various types of RFID application. Respondents were asked to indicate what services they used from a prescribed list and which they would be willing to use with RFID based technology. The list of services/applications was compiled based upon their current applicability to RFID. As Figure 7 illustrates, respondents use a wide range of the services, with only inventory control resulting in a low percentage. This is expected, as the use of inventory control is not something that has particularly been adopted by consumers and resides as more of a business service. However, with the increasing widespread use of RFID, inventory control applications such as fridges understanding when the milk needs replacing or whether the butter has run out will become far more commonplace. This concept is not lost on the respondents with more positive responses towards its future use than current. That said, however, the overall response towards utilising these services when based upon RFID technology was not overly supportive, with the library system receiving the highest proportion of respondents (46%). It is unfortunately unclear why this is the case. It could be a result of the lack of understanding of how RFID technology can be applied, or moreover, perhaps a clear understanding and fear of using the technology because of potential security and privacy concerns. It is clear, however, that should these services look for widespread deployment, significant education and awareness training will be required before the technology becomes more acceptable to the general public.

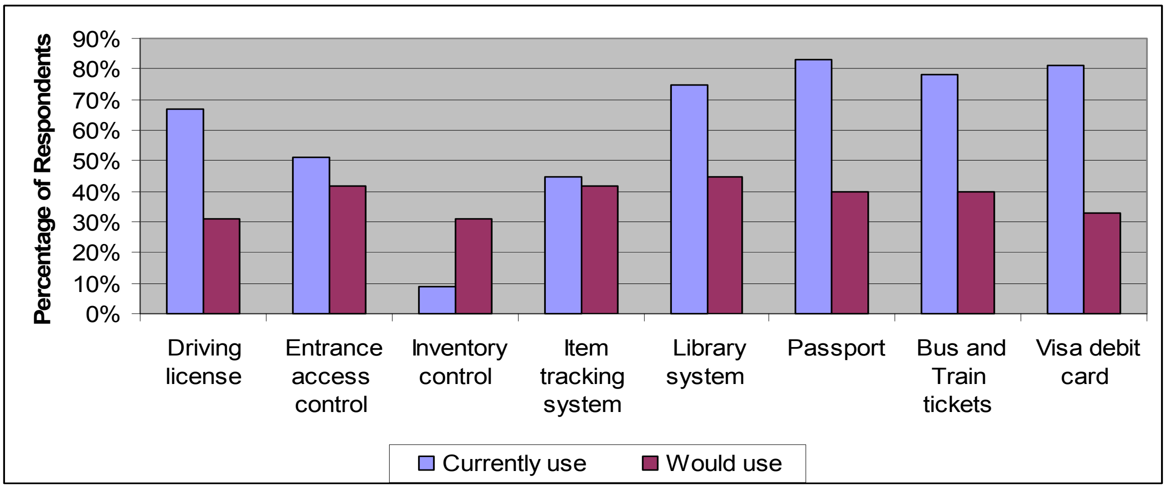

Figure 7: Services Respondents Currently Utilise and Would Utilise with RFID

The respondents were also given a couple of specific examples of how RFID technology could be implemented in the future. The examples given were the tagging of clothes, so that a washing machine could identify if an item of clothing was in avertedly included in the wash (e.g. a black sock in a white wash), and the tagging of food, for automated notification or ordering of food. As illustrated, in Table 3, respondents have conversely responded more positively towards these types of service, with over 60% in favour of tagged clothes and just over 50% in favour of tagged food. When compared to previous response (illustrated in Figure 7), this suggests perhaps that their responses were more based upon a lack of understanding of how the technology would be used.

	Yes	No
Tagged Clothes	64	36
Tagged Food	53	47

Table 3: Popularity of Future Applications of RFID

4.4 Privacy Versus Service

Given the specific concerns raised by RFID technology it was decided to establish the level to which people preferred the use of an application or service over the potential loss of privacy. Respondents were asked to comment on the same applications scenarios (tagged clothes and tagged food), but this time with respect to the level of privacy concern they would feel. The idea of other people knowing what is contained in your fridge appears to be a concern for respondents (59%). Respondents were a less concerned with people knowing what brand of clothing they wear, however, interestingly a large proportion of respondents didn't know if they are concerned, suggesting perhaps a lack of understanding towards the impact of such an application.

	Yes	No	Don't Know
Tagged Clothes	36	23	41
Tagged Food	59	22	19

Table 4: Privacy Concerns of Future RFID Applications

When comparing the results from Tables 3 and 4 it certainly presents a mixed distribution of responses. Tagged clothes are a more popular service with smaller concerns over privacy than tagged food. This mixed response illustrates that not all RFID based applications will necessarily receive the same level of acceptance, and a careful analysis of what the service will provide and how it will effect individuals (in terms of the information is provides to third parties) is imperative.

Further analysis also shows that a reasonable percentage of the respondents are neither interested in using these services and are concerned about the privacy aspects that might result from them. Businesses wishing to implement such services must be aware of these concerns and provide truly effective mechanisms for ensuring personal privacy. Recent literature has demonstrated simply killing the tags is completely ineffective (Bolan, 2006b).

The respondents were finally asked to assess what their preference was towards personal privacy versus the use of personalised services – based on the assumption that personal privacy could not be achieved if RFID based personalised services were in use. As illustrated in Table 5, two thirds of the respondent population chose personal privacy over personalised services. This reinforces the importance of ensuring RFID technology can provide a sufficient level of security and privacy before looking to implement personalised services.

	% of Respondents
Personal Privacy	67
Personalised Services	33

Table 5: Respondents' Preference between Privacy and Services

5. Discussion

The results have demonstrated that respondents are broadly aware of wireless technologies and well over half of them use one or more wireless technologies on a fairly regular basis. Although, respondents' knowledge of RFID technology lagged behind other consumer popular technologies, their prior experience and knowledge of wireless technologies will enable them to comment usefully on their perception of security and privacy for wireless and RFID technologies.

It would appear that respondents generally perceive wireless technologies to be secure, with a large proportion of them using more traditional security controls such as anti-virus, firewalls and authentication. However, even given this perception and usage, users' perceived level of security awareness is only average, with 86% stating they would benefit from learning more about security. It is interesting to note their acknowledgment of a lack of awareness and willingness to learn more about security. This is certainly a positive attribute, as a lack of awareness and education would make the deployment of any potentially harmful technology extremely difficult.

This understanding of how important security is to them is also reflected in how important they perceive their privacy to be. Overwhelmingly, respondents felt their privacy to be extremely important. However, as with security, respondents did not feel they have a good level of privacy awareness. With increasing wireless devices and services it is important that users perceive they are in control of their technology and have a good understanding of the possible threats when using it.

The popularity of possible RFID applications certainly suggests RFID technology has the potential to be as successful as many of the popular consumer wireless technologies. Indeed, recent years have already seen a number of larger consumer based application being successfully deployed. However, respondents have clearly indicated a preference towards privacy of their information over more useful or convenient applications. With 98% of respondents considering privacy to be at least an important consideration, it is imperative that RFID technology is embedded with security and privacy at all levels: the tag, the reader and backend systems.

6. Conclusions

It can be concluded from the survey that the most important considerations to users of wireless technology are security and privacy. Although wireless technologies have become successful independently of these to date, with the increasing popularity of these technologies, and increasing functionality and amount of information, it will only take a serious breach against personal information to make users aware of the real dangers to them and for them to subsequently refrain from using it.

The pervasiveness of RFID technology, and real lack of any degree of security, raises a question about its appropriateness as a consumer technology. Although it has been suggested by some authors (Kumar, 2003; Floerkemeier, Schneider &

Langheinrich, 2004) that the security and privacy concerns with RFID systems may be, in part, addressed through the creation of suitable policy and through organisational and legislative policies, it is unlikely that such measures will assuage concerns or deter an attacker. It is also notable that policy based approaches, including governmental and self regulation, have failed to prevent privacy or security concerns over other similar technologies. As such, Ranasinghe *et al.* (2004a, p.4) notes that all that RFID policy can really focus on is who may collect information, how it may be used, and ultimately who has ownership.

It is clear that, like many systems, in order to provide an effective and secure RFID system, a multi-facetted approach to security is required. Policies and legislation alone will not be a solution, but rather a series of measures including policy, legislation, technical controls and user education will be essential to ensure all stakeholders benefit from adopting the technology, not simply those looking to deploy it.

References

Bolan, C. (2005). Radio Frequency Identification - A Review of Low Cost Tag Security Proposals. *Proceedings of the 3rd Australian Computer, Network & Information Forensics Conference*. Perth, Western Australia: School of Computer and Information Science, Edith Cowan University.

Bolan, C. (2006a). *Strategies for the Blocking of RFID Tags.* Paper presented at the Sixth International Network Conference, Plymouth, UK.

Bolan, C. (2006b). *The Lazerus Effect: Ressurecting Killed RFID Tags.* Paper presented at the 4th Australian Information Security and Management Conference, Perth, Western Australia.

Boone, C. (2004), “RFID: The Next Big Thing?”, http://www.ftc.gov/bcp/workshops/rfid/boone.pdf, (Accessed 14 November 2006)

Cardullo, M. (2005). Genesis of the Versatile RFID Tag. *RFID Journal, 2*(1).
Cellular Online (2006), “Stats Snapshot”, http://www.cellular.co.za/stats/stats-main.htm, (Accessed 09 November 2006)

Choi, E. Y., Lee, S. M., & Lee, D. H. (2005). Efficient RFID Authentication protocol for Ubiquitous Computing Environment. In T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai & L. Yang (Eds.), *International Workshop on Security in Ubiquitous Computing Systems - SECUBIQ2005* (Vol. 3823, pp. 945-954). Nagasaki, Japan: Springer-Verlag.

Competition Commission. (2003). “Vodafone, Orange and T-Mobile. Reports on references under section 13 of the Telecommunications Act 1984 on the charges made by Vodafone, O2, Orange and T-Mobile for terminating calls from fixed and mobile networks”. Competition Commission. http://wwwcompetition-commission.org.uk/rep_pub/reports/2003/475mobilephones.htm

Engberg, S. J., Harning, M. B., & Damsgaard-Jensen, C. (2004). Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer

Convenience. *Proceedings of the Conference on Privacy, Security and Trust - PST*. New Brunswick, Canada

Floerkemeier, C., Schneider, R., & Langheinrich, M. (2004). Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols. *Proceedings of the International Symposium on Ubiquitous Computing Systems - UCS*. Tokyo, Japan: Springer-Verlag.

Ford, R. (2006), “By 2016, they'll be able to watch you everywhere”, http://www.timesonline.co.uk/article/0,,2-2433304_1,00.html, (Accessed 03 November 2006)

Hennig, J. E., Ladkin, P. B., & Sieker, B. (2004). *Privacy Enhancing Technology Concepts for RFID Technology Scrutinised* (No. RVS-RR-04-02). Bielefeld, Germany: University of Bielefeld.

Henrici, D., & Müller, P. (2004). Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In A. Ferscha & F. Mattern (Eds.), *Pervasive Computing* (Vol. 3001, pp. 219-224). Vienna, Austria: Springer-Verlag.

Knospe, H., & Pohl, H. (2004). RFID Security. *Information Security, 9*(4), 39-50.

Kumar, R. (2003). Interaction of RFID Technology and Public Policy. *Proceedings of the RFID Privacy Workshop*. Cambridge, Massachusetts

Ranasinghe, D., Engels, D., & Cole, P. (2004). Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In *Auto-ID Labs Research Workshop*. Zurich, Switzerland.

Sarma, S. E., Weis, S. A., & Engels, D. W. (2002). RFID Systems and Security and Privacy Implications. In *Workshop on Cryptographic Hardware and Embedded Systems* (Vol. 2523, pp. 454-470).

Stockman, H. (1948). Communication by Means of Reflected Power. *Proceedings of the IRE*, 1196-1204.

Weis, S. (2003). *Security and Privacy in Radio-Frequency Identification Devices.* Unpublished Masters, Massachusetts Institute of Technology (MIT), Massachusetts, USA.

Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In D. Hutter, G. Muller, W. Stephan & M. Ullmann (Eds.), *International Conference on Security in Pervasive Computing - SPC 2003* (Vol. 2802, pp. 454-469). Boppard, Germany: Springer-Verlag.

Wong, L.W. (2005). Potential Bluetooth Vulnerabilities in Smartphones, In Proceedings of the 3rd Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, pp.123-132.

Young, T. (2006), “Biometric passports cracked”, http://www.computing.co.uk/computing/news/2161836/kacers-crack-biometric, (Accessed 15 August 2006)