Public Opinion towards RFID Technology

F.Li and N.L.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

RFID (Radio Frequency IDentification) is an automatic identification technique. A fundamental RFID device, often know as an "RFID tag", which is a tiny inexpensive chip with built-in antenna, can be attached on an item. By using radio waves, the tag's presence and its data can be recognised by the RFID reader. RFID technology can be used in many applications to provide the fast and convenient services. As the tag broadcasts its radio signal to all the dimensions in various distances, this raises the security and privacy concerns such as sniffing and tracking when people carry RFID tagged items. This paper examines the public's security and privacy awareness towards RFID technology. A total of 365 participants completed the survey. From an analysis of the results in was found that: 55% of the participants thought that wireless technology is not secure to use although numbers of security mechanisms have already been employed and 75% of them were worried about the fact that their privacy will be compromised (such as being monitored when they use their wireless devices). What was also found is that 36% of the participants have heard RFID technology before, and compared this with past consumer survey from 2003, here with an increased 13% in result, this indicates that there is still a strong need to educate people about the RFID technology to help them familiarise with the technology; furthermore, 67% of the participants chose their personal privacy over the specialised services which would be provided by the RFID technology, this demonstrates that people were more concerned about their privacy over functionality.

Keywords

RFID, Security, Privacy, Wireless

1 Introduction

In recent years, the use of wireless technologies has been dramatically increased as they provide the ubiquitous access to the telecommunication and data networks in the daily life. Currently, there are over 2 billion mobile phone users in the world (Cellular Online, 2006) and there are more than 130,000 public Wi-Fi hotspots available in 130 countries (Jiwire, 2006). While with the increasing market demand, the security and privacy issues should also need to be concerned. In 2003, the US researchers have pointed out the security flaws on WLAN (Wireless Local Area Network) and also have demonstrated number of attacks to compromise the security such as: by using the unauthorised packet to block the legitimate users to access the WLAN (Jackson, 2003).

One member of the wireless technology family is becoming more popular than ever before. The RFID (Radio Frequency IDentification) technology is an automatic identification method that can be used in any identification systems; by using radio signals, the RFID reader detects the tag's presence and accesses the tag's data, therefore the tagged item can be located and identified. RFID technology can be used in many applications such as: identification, tracking, payment system, inventory control, access control, and supply chain management. The RFID development never stops. In the U.S. retail supply chain, the RFID implementation has been estimated at $91.5 million in 2003 and this amount is expected to grow to $1.3 billion by the end of 2008 (Boone, 2004). As RFID technology is a member of the wireless family, it inherits many common security threats such as eavesdropping. However, due to its unique character, it also faces other threats (i.e. Clone attack on the RFID based biometric passport (Young, 2006)).

Privacy threats will be concerned when people use the wireless technology, according to The Times article, "by 2016, Britain is becoming a "Big Brother" surveillance society with millions of people being tracked.", also "shopping habits, travel movements and car and train journeys are being monitored increasingly as part of the fabric daily life" (Ford, 2006). These can be achieved by tracking/monitoring people's wireless devices such as mobile phones or RFID tagged train tickets. This research is aimed to find out the public security and privacy awareness level regarding to general wireless technologies and public opinion on RFID technology. The survey was structured so that information could be collected on demographics, general security and privacy aspects on wireless technologies and in particular for RFID technology. This paper's format is to outline the general security and privacy aspect of RFID technology, followed with introducing the investigation method which was a survey and analysing its results. The paper finishes by discussing the survey outcomes and predicting future directions for RFID technology development.

2 Security and Privacy for RFID

RFID technology has been used for over the last 60 years. It was mainly deployed for the military in the Second World War: the IFF (Identification Friend or Foe) system was used to identify the aircraft (Landt, 2006). In 1960s, the technology was first utilised for the public in an anti-theft system by using 1-bit tags to detect the presence or the absence of tagged items in retail shops (Roberts, 2005). Since then, it has been dramatically developed and it has been used in many applications. In 2004, Wal-Mart began to employ RFID tags to track products in their supply chain (Roberti, 2004); recently, European countries started to deploy the new biometric passport which uses the RFID chip to store the holder's personal information such as finger prints (Hoepman *et al.*, 2006). These shows that the use of RFID technology is changed significantly from 1-bit security tags to RFID chips based passport.

Security and privacy was never a major issue for RFID technology before; however, with the increased applications, security and privacy issues have become more important. For the security, in 2005, the researchers from John Hopkins University and RSA security have performed a spoofing attack on an RFID system; by using the

cloned RFID tag, they successful unlocked the car with the electronic immobilisation system (Bono *et al.*, 2005). In March 2006, the researchers who are from Vrije University Amsterdam have showed the vulnerability of the RFID system under the virus attack (Rieback *et al.*, 2006). With respect to the privacy, malicious users could build a hotlist to determine exactly location of the tagged item among thousands of others; this is an extremely dangerous threat to the people's privacy when carrying tagged items (Ayre, 2004). Although people may not heard these threats before, with the dramatic development and increasing usage, RFID security and privacy aspects should be concerned by people in the near future.

3 Methodology

The method used in this research was an online survey: by analysing the survey result, to predict the public's security and privacy awareness level when people use the wireless technology and especially public's view on RFID technology. After the draft version, a number of people were invited to form a focus group giving feedbacks to improve the survey quality. Survey invitation was sent out by using emails which contained the survey link and the research background information. The data collection process started from 25/08/2006 and completed on 30/10/2006, and the participants remained anonymous.

The survey was aimed to discover the public's view on wireless security and privacy and their attitudes on RFID technology; it was designed in two main sections: backgrounds: what RFID technology is and what it can be used for, and questions section which contained three subsections: demographics which required the participants' gender, age, nationality, education level and employment, general security and privacy for wireless technology which accessed what level of security and privacy awareness participants have when they use the wireless technology, and final section to predict what their opinions are on the RFID technology.

4 Results

A total of 365 participants completed the survey. According to the result, the participants were with a mix of gender (56% male and 44% female) and 77% were in the age group of 18-30. Given the skew towards higher educated persons who have a bachelor or higher degree (96% of the participants), it is suggested the results presented in this paper might reflect a more positive perspective of wireless and RFID technology than might be expected from the general public.

4.1 Security and Privacy on wireless technology

Wireless technology has been around for years, many people may have already experienced it in one or other formats, such as mobile phone. From the finding, a significant number of participants (87%) were aware of Bluetooth and WLAN both of them have only existed for few years; 72% were aware of GPS (Global Position System), GPRS (General Packet Radio Service) and 3G; only 34% were aware of RFID technology which has been survived for more than 40 years in the commercial

world; From figure 1, it shows that: the WLAN is the most frequently used wireless technology as 57% of the participants use it on a weekly basis compared to others, and the RFID technology is the least used one . This indicates the reason why most participants were familiar with WLAN as people regularly use it; compare with it, RFID technology is much less known as it is not a widely used yet and there is not much information about it even when people do use it such as the car's electronic immobilisation system is the RFID technology based, but it is very rarely people are informed about it.

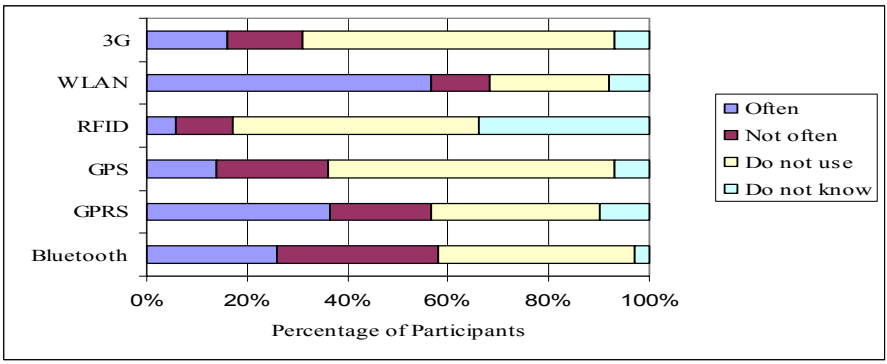

Figure 1: How often do participants use the wireless technology?

People can use many security mechanisms to protect various wireless devices. So what method(s) have been deployed by participants to protect their wireless devices? The results are shown in Table 1. On average, authentication is widely used as the ease of use and low requirement. 60% used firewalls and antivirus software to protect wireless laptops, but less usage of these methods on other devices. Due to those devices may not necessary need them at the moment and those devices have small amount of computer power to support those two mechanisms, but it is still possible for people to use these tow methods on those devices. Although biometrics method has been existed for many years, less than 5% used it as most of the devices do not support it; also, participants were aware switching off is an option, as some threats (i.e. the virus) can not harm devices when they are switched off.

	Mobile phone	PDA(personal digital assistant)	Wireless laptop
Physical secure(e.g. locks)	25%	7%	20%
Biometrics (e.g. finger print)	2%	2%	5%
Authentication(e.g. password/pin)	41%	16%	55%
Firewall	5%	7%	60%
Antivirus software	6%	7%	61%
Switch off when not using it	29%	10%	48%

Table 1: Security methods for various wireless devices

Although various methods have been used, there are still 55% of the participants thought it is not secure to use the wireless technology with two thirds of the population felt their security awareness level was medium and above. In addition, a significant number of participants (86%) felt that they could be benefited from learning more about security.

As the wireless technology uses radio waves by transferring data through the ether, it becomes to a potential privacy threat when people use it. 75% of the participants were worried that they may be tracked or monitored by other people when they use wireless technology. Furthermore, participants were asked "which of the following wireless technologies do you believe can be used to monitor\track you?" and the result shows in Figure 2: 70% chose WLAN; around 55% believed GPS, GPRS, Bluetooth and 3G; only 38% picked RFID technology. In fact, all these technologies can be tracked\monitored; this result indicates that people are very familiar with the WLAN as they use it fairly often and they do not know about RFID technology that well as they do not use it that much.

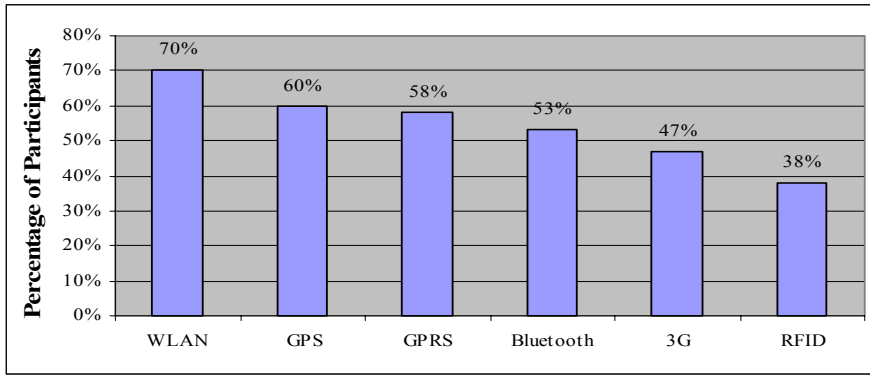

Figure 2: Wireless technologies they believe they can be tracked by.

In order to predict the public's privacy awareness level, a question was asked to scale their privacy awareness level when they use wireless technologies. From the Table 2, it shows that the skew towards to the very poor privacy awareness level (10%) from the very good privacy awareness level (4%), it may reflect that more participants do not know how to protect their personal information privacy, and even more they may not know whether their privacy is vulnerable or not when they use the wireless technology.

Privacy Awareness Level	Very poor	Poor	Medium	Good	Very good
Number of participants	10%	26%	41%	19%	4%

Table 2: Privacy awareness level when people use wireless technologies

4.2 RFID technology

RFID technology has been utilised by people for more than half century, much longer compared to other wireless technologies (e.g. WLAN). From the survey result, only 36% of the participants have heard about it before; this shows that actually participants' awareness of RFID technology is very low at this time, as it was mainly used for the military and then moved on for the business usage such as in the supply chain management. Further more, 37% of those who have heard about RFID technology have a job in I.T./Computing, 24% were full time students, and participants in education and engineering also took big portion of the total population; moreover, the result shows that individual's background does have an impact on their answers.

RFID technology has been deployed in many applications and it will be used in more areas. Figure 3 shows that applications which participants currently use and they would try with RFID technology in future. Only small portion of the participants use inventory control compares with majority of the population use the library system, passport, bus tickets and Visa debit card; on average, 38% of the population would use the RFID technology in aforementioned applications, this indicates that those participants would try new technology does not matter whether they use the current applications or not.

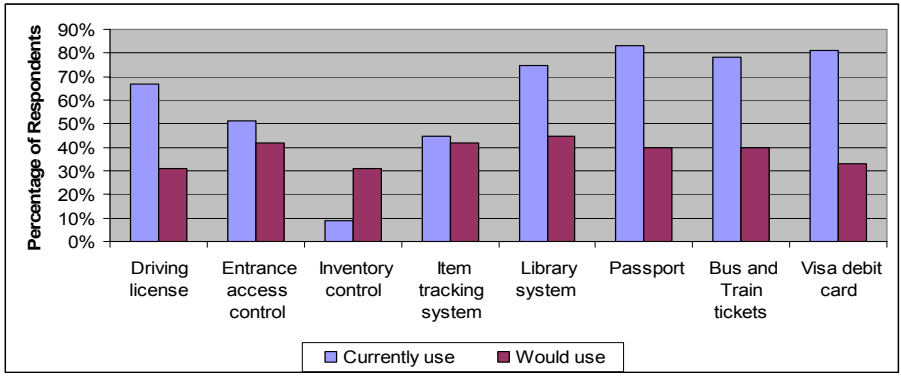

Figure 3: Applications people currently use, and they would try with RFID technology.

Various security and privacy threats are associated with RIFD technology such as sniffing, tracking, spoofing, replay attack, DoS (Denial of Service), man in middle attack and virus (Rieback *et al.* 2006). Participants were asked if they have heard those threats before, 68% said they have and the rest have not; for those who have heard the threats before, their answers were further analysed which is showed in Figure 5: among those who have heard the threats, 71% thought tracking may associate with RFID technology, around 30% thought the rest threats may relate with the technology and 8% thought none of the threats may have association with the RFID technology. As all these threats are related to the RFID technology, but

participants' responses are so different, it can be explained each participant has a different view about each threat for the RFID technology: participants understood more about tracking threat compare to others threats.

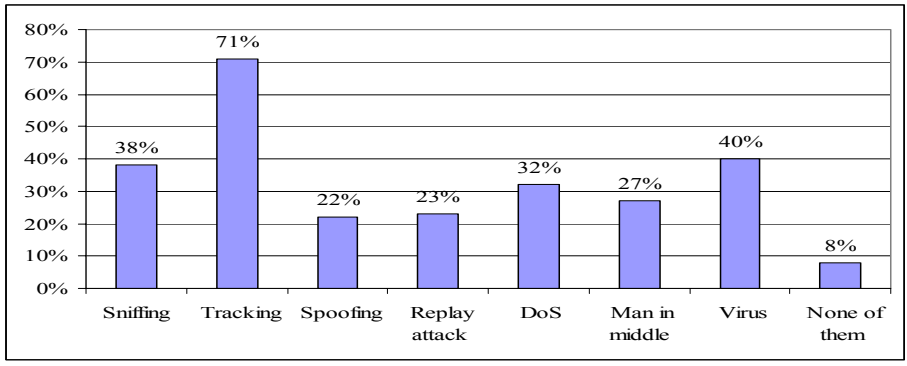

Figure 4: Attacks on RFID technology

RFID technology has some special futures such automatic warning which would be use in the daily life to provide the convenient, but at the same time, these futures may cause the personal privacy leakage. Participants were asked to give their opinions on these services and views about their information privacy when they use the services; for the services which would provided by RFID technology, 64% would like be informed by their washing machine if two different colour clothes cannot be washed together and 53% would like to be informed if the milk is low in their fridge. On the other hand, regarding to the privacy, 64% do mind that people know what they have in the fridge when others pass their home and 66% do mind taking off an item(s) such as jewelleries to protect their information against tracking. From these results, it shows that on average 59% liked the services and 65% wanted to keep their information privacy safe, this points out that there are some participants would like to have both at the same time; obviously, the participants can not have both at the same time at the moment; therefore a trade of question was asked to choose between personal specialised services (e.g. automate warning) and personal privacy information (e.g. current location). 67% of the responders chose their privacy and the rest prefer to the specialised services; this indicates that more people are concerned about their privacy than the services they would get.

5 Discussions

From the results, it shows that participants have a good level of understanding about wireless security. Participants use varies security mechanisms to protect their wireless devices to meet different security requirements: generally, authentication is used as it provides minimal protection; as the computer is vulnerable to the virus, therefore that is why 61% of the participants use antivirus software to provide with an extra level of security; in future, if the virus threats other devices, the antivirus software will be designed to fit them in order to protect the devices. It is very

interesting that although majority participants have a medium and above level of awareness on the wireless security, there are still 86% of participants thought they would gain more if they learn more about security, this indicates that how important people consider about the wireless security is.

Compared with the participants' security awareness, participants do have low privacy awareness level, as 77% of participants' privacy awareness level is the medium and below. 75% of participants were concerned that they would be tracked\monitored by their wireless devices; this indicates generally people are unfamiliar with the privacy impact when they use wireless technology, and they certainly do not know how to protect their privacy information. Therefore, relevant privacy protection methods should be introduced to erase people's fears when they use the wireless technology, this may take some time to develop as currently the systems' main concern is the security issue rather than people's privacy.

The result also shows that: only 36% of the participants have heard the RFID technology and the majority of them were IT/Computing professional and full time students; this compares with the 2003 US consumer survey (Capgemini, 2004) with an increased 13% in result. The result should be increased as most of the participants were higher educated persons whom received more knowledge compares to those general publics; this means that the public's view of the RFID technology has not changed much during the pass three years radically RFID development. Furthermore, for those who have heard the security and privacy threats before, 40% of them thought that virus associates with RFID technology; as the world's first virus infected RFID tag was created in earlier 2006 (Rieback *et al.*, 2006), this strongly indicates that those people presumed this only based on the virus is one of the common threats for IT systems, therefore it could be a threat for RFID technology as well.

From the results, it demonstrates that people are not familiar with the RFID technology although it has been around for very long time; there is certainly a need to educate those who have not got knowledge about it in order to help the RFID development; as from the survey result shows that 49% of those who have heard about the technology would use the RFID technology, in contrasts with 32% who have not heard about it before would use it. Once people start to use the RFID technology, then they can be informed with which security and privacy threats with the according protection methods. Also, from the survey results, 67% of the participant chose their personal information privacy over personal specialised services; this shows that although RFID technology would provide the convenient services, people still consider about their personal information as more important; this means in future, it will be desirable if the public's privacy is protected while they use the services.

6 Conclusions

Most of the participants do have a good level of security awareness on wireless technology, not only because what they have said, but also because people do use the

correct method to protect the right devices with the security needs; this still could be improved if they were informed more about security; On the other hand, participants' privacy awareness level is fairly low as people are not sure what the privacy threats are and how to protect themselves from these privacy threats; in order to improve this situation, people should be educated on what the privacy issues are and the industry should produce the according protection methods for the public to use. For the RFID technology, it shows that people's awareness level about it is pretty low as it was mainly used in the military and business, but not for the consumers, people should be informed about it before it is widely used by the consumers, as this can certainly boost the RFID development. Overall, as the increasing development of the wireless technologies especially for the growth of the RFID technology, both the security requirement and privacy impact should be considered by people and the sooner people receive the relevant information about them, the better for system security and the public's privacy.

7 References

Ayre, L.B (2004), "RFID and Libraries", http://galecia.com/included/docs/position_rfid_permission.pdf, (Accessed 02 October 2006)

Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A. and Szydlo, M. (2005), "Security Analysis of a Cryptographically-Enabled RFID Device", *In 14th USENIX Security Symposium*, pages 1–16, Maryland, USA, July-August 2005

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

Capgemini (2004), "RFID and Consumers: Understanding Their Mindset", http://www.nrf.com/download/NewRFID_NRF.pdf, (Accessed 14 November 2006)

Cellular Online (2006), "Stats Snapshot", http://www.cellular.co.za/stats/stats-main.htm, (Accessed 09 November 2006)

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)

Hoepman, J.H., Hubbers, E., Jacobs, B., Oostdijk, M. and Schreur, R.W. (2006), "Crossing Borders: Security and Privacy Issues of the European e-Passport", *In Advances in Information and Computer Security*, vol 4266 of LNCS, pages 152-167, Springer Berlin / Heidelberg, 2006.

Jackson, W. (2003), "Wireless network attacks get a public airing", http://www.gcn.com/online/vol1_no1/23053-1.html, (Accessed 29 November 2006)

Jiwire (2006) Worldwide Wi-Fi Hotspots Hits the 100,000 Mark Online at: http://www.jiwire.com/press-100k-hotspots.htm date accessed: 14/11/2006

Landt, J. (2001), "Shrouds of Time The history of RFID" http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf, (Accessed: 02 October 2006)

Rieback, M.R., Crispo, B. and Tanenbaum, A.S. (2006), "Is Your Cat Infected with a Computer Virus?", *PerCom 06: 4th Annual IEEE International Conference on Pervasive Computing and Communications*, in Pisa, Italy, 13-17 March 2006

Roberti, M. (2004), "Wal-Mart Begins RFID Rollout", http://www.rfidjournal.com/article/articleview/926/1/1/, (Accessed 21 June 2006)

Roberts, C.M.(2005), "Radio frequency identification (RFID)", *Computer & Security*, Vol. 25, pp18-26

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