Predictors of Home-Based Wireless Security

Matthew Hottell
Indiana University

Drew Carter
Indiana University

Matthew Deniszczuk
Indiana University

March, 2006

Abstract

Wireless routers are appearing in increasing numbers in homes. Many of these routers are left in a default, wide-open configuration, while even more of these routers can be considered unsecured. What are the factors that contribute to the general state of insecurity in home-based wireless networks? We examine the following factors: education, income, and housing density. If education is the critical factor then increased public education on the risks will increase security. If income is a better indicator of wireless security then wireless security and privacy could be considered a luxury good and is therefore consumed disproportionately by wealthy consumers. Thus, forcing this luxury good on other populations may be an inappropriate policy. For example, low income consumers may need to share wireless connectivity across households and may lack the ability to implement fine-grained access controls. If housing density is the dominant factor then users are arguably responding appropriately to the risk of local free riding. A series of wardrives was conducted to examine the relative state of security of wireless access points in neighborhoods representing key demographics with a collection of nearly 2500 data points.

After a comprehensive study of these thousands of points we discovered that the only statistically significant indicator of security is router type. Routers with default security configuration were found to be secure 97% of the time, while identifiable Linksys Secure Easy Setup routers were secure 88% of the time. The percentage of secure routers found for the entire study was 61%.

The surprising results of this extensive wardriving effort are that interface and ease-of-use dominate demographic factors including income, population density, and education.

Introduction

In this paper we report on the factors that tend to predict implementation of security measures in wireless access points from a privacy perspective.
Section 1, Theory and Motivation, describes consumer privacy and security concerns at a high level. Section 2 provides more detail on the specific motivation for the exact experiment conducted, while Section 3 describes the wardriving experiment. We review the results of the study in Section 4, and discuss the implications of our findings in Section 5. We provide a summary, a direction for further research, and concluding remarks in section 6.

1. Theory and Motivation

In this section we describe our motivation. We begin with a basic discussion of privacy and security theory, moving later into specific work on the economics of security that motivated our hypotheses.

The advent of the Information Age has created a new set of economic factors that have hastened the erosion of personal privacy. Computing systems have increasingly become more interconnected, while computing devices have been integrated into practically all aspects of our lives. This tendency towards connection and integration creates an environment where private personal information can be collected and traded, intrusive spam email can reach us in our homes, and web sites can track our every surfing move online. Clearly these are just some of the new privacy threats we face specifically as citizens of the online world

But what exactly is privacy? Jim Harper of the Cato Institute defines privacy as "the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values." In this definition, acceptable privacy levels depend on the judgments of individuals, not society as a whole. Furthermore, this view does not treat privacy as a right per se, but as a personal condition that must be maintained by "exercising personal initiative and responsibility"[11]. In other words, each individual is responsible for being vigilant in protecting her personal level of privacy in the face of privacy-eroding efforts such as customer loyalty cards.

We can view privacy as consisting of three dimensions: secrecy, autonomy, and seclusion. Secrecy refers to the right to control the proliferation of personal information, autonomy is the right to be free from observation, and seclusion is the right to be left alone.[5] Each of these aspects of privacy is threatened by participating in online activities. For example, secrecy can be negatively impacted when a website shares personal information it acquires from clients with outside third parties. Seclusion can be violated by spam, spim, or pop-up advertisements, and autonomy is impacted when advertising companies use cookies to follow surfers as they view pages across multiple sites.

What impact does this erosion of privacy have on the consumer? One potential use of personal information is price discrimination, the practice of charging different prices for the same good based on the consumer's willingness to pay, allowing a seller to sell goods at several points along the demand curve.[1, 14, 17, 18] In order for sellers to effectively price discriminate, accurate personal information is required. The seller therefore has an economic incentive to gather enough personal information to be able to set a price for a consumer that is closer to the price that they are willing to spend on a good.

A combined security and privacy risk is identity theft. Identity theft, which is also known as impersonation fraud, is the capture and use of personally identifying information for the purpose of conducting financial fraud. The true cost of such an attack to the consumer is not measured in terms of the money stolen using the fraudulent credentials as liability in fraud cases is limited in many jurisdictions. The actual cost to the victim is measured in loss of credit standing and resources spent to fix financial records, which can often take years.[8, 9]

A relatively new factor in the online privacy equation is the emergence of wireless networking technologies. IEEE 802.11 wireless technologies have made participating in the online world easier and more convenient. Initially confined to business use due to prohibitive costs, recent years have witnessed a large increase in the home adoption of wireless devices. While this technology allows for easier access to networked resources, wireless security can be problematic. Instead of requiring a physical connection to a home network, anyone with the proper hardware and software can connect to the wireless device and access both the private internal network and any WAN the device is connected to. The intruder need only be in fairly close proximity to the wireless device. Security mechanisms such as encryption are available for wireless devices, but the efficacy of many of those measures is questionable at best.[4,8]

Unsecured wireless presents cybercriminals a de facto "get out of jail free card." Anyone can drive near an open point, connect to the Internet, and then engage in a variety of activities ranging from sending spam emails to downloading child pornography to launching hacking attacks. Once done, the attacker can simply drive away leaving little trace. Perhaps an even more likely scenario is a neighbor using an open point to share and download copyrighted material. Each of these actions carries clear economic costs that can potentially be borne by the actual victim of the crime (loss of property, system damage, etc) as well as the owner of the open access point (lawsuits, criminal investigation).

Other risks impose costs that fall more squarely on the owner of the access point. These costs can include loss of information stored on computing devices connected to the wireless node, including financial and personal information that could be used in an impersonation fraud attack. If the node is left in a completely default state, an attacker can access the router administration panel, poison the DNS settings, and engage in a pharming attack that can reveal account username and password information for websites that contain financial information. In addition, an attacker can collect and decipher wireless packets and in so doing track the activities of computers using that wireless node.[4,8]

Home-based wireless access points are usually installed by non-technical consumers and are often left in a default, insecure configuration. There are a variety of reasons why consumers might leave their wireless access points unsecured. One reason is that the owner may wish to share an existing Internet connection as a public good. Many coffee shops use this strategy to attract and retain customers.

Another reason consumers do not secure their wireless access points is a lack of knowledge. Effectively securing a wireless router without assistance requires understanding several basic concepts in encryption and networking, and many consumers simply lack any form of training in these disciplines. An access point will generally work in a default, open configuration by plugging in the correct cables and turning it on, which may encourage owners not to make an effort to secure it.

Some wireless consumers do not secure their devices because they do not understand the risks associated with an open node, while others understand the risk but judge the risk to be small enough to accept. A problem here is that many consumers do not know what can be done with the information they make available, or they do not understand the complicated nature of the impact of the threat.[15] A recent study of Facebook.com showed that many consumers willingly placed sensitive private information online that when asked they would want to remain private.[10] Another issue is that many users have the wrong mental model of what their expected contribution to security should be.[6] For example, if the metaphor used for security is "information warfare", then the average citizen of the Internet might believe that fighting back against cyber-guerillas should be left up to the security professionals, while they simply pay their "Internet taxes" to their ISP.

Whatever the case may be, wireless consumers may perceive that the cost of implementing and maintaining wireless security measures lowers the benefits of wireless consumption.[12] For example, implementation of an access control list security mechanism requires that any new devices connected to the router must first be registered. Assuming the owner knows how to accomplish this task, the process of finding the MAC address of the new device, logging in to the wireless router, and finally entering the new MAC address into the database must be performed each time the owner wishes to enable a new device. The cost of performing this series of steps may be too high, particularly for the naïve user.

2. Predictors of Wireless Security

In this section we examine more closely the factors that may impact the configured security of wireless devices.

2.1 Is Education the Problem?

One factor that may predict wireless security is education level. As noted above, implementing wireless security requires a basic level of networking knowledge that most consumers do not have. Effective education could give consumers this basic knowledge and allow them to better make choices about protecting their privacy. Higher education might create an environment where consumers are exposed to more information about wireless networks. Concurrent study results indicated that wireless security rates in predominately student populations increased 9% after a university launched a security awareness campaign.[7]

One could also argue that one of the benefits of higher education is a better understanding of the risks of privacy erosion. Varian et al found that education was a significant predictor of people who signed up for the national do-not-call list.[16] This suggests that more highly educated people understand the inherent risks and are more likely to take steps to protect their privacy. On the other hand, Wathieu and Friedman found that individuals generally are already aware of privacy risks[19] and need no prompting to be concerned.

If education is found to be a predictor of wireless security, then an obvious response to that finding is a call for better educational initiatives to empower naïve consumers as they attempt to make decisions about wireless security and privacy risks.
Hypothesis 1: higher education level is a predictor of higher levels of wireless security.

2.2 Are Privacy and Security luxury goods?

By definition, a luxury good is one that is consumed disproportionately or solely by the wealthy.[3] Can security and privacy be considered luxury goods? Varian et al found that consumers at the highest income level (>$100,000 household income) were the most likely to sign up for the do-not-call list[16], this may indicate that people who are wealthier are more likely to either value their privacy or understand the potential risks for privacy erosion. Shostack and Syverson point out that consumers often pay for goods or services that enhance privacy[15], and the wealthy should be better able to pay for such.

One of the most likely outcomes of privacy erosion is price discrimination[14]. Price discrimination requires good information to be effective, and price discrimination more adversely affects those who have the means to pay more for a good. Therefore, we would expect that the wealthy would have greater incentive to protect their information assets knowing that the release of that information could bear a real cost in terms of a higher price paid for goods.

Income could be highly correlated with education; therefore these wealthier consumers might also have a better understand of the risks and be more able to mitigate them. In our regression we treated these variables a separable. This is feasible due to the demographics of the neighborhoods chosen.
Hypothesis 2: Higher income indicates a greater likelihood of secured wireless access points.

2.3 Is Risk Awareness an Indicator of Wireless Security?

There are many reasons why population density may be a good predictor of higher levels of wireless security. One such reason is that it may be easier to identify local experts when population density is high. These experts may help increase the general level of security in the area by sharing their knowledge with others or by actually configuring other access points.

Another consideration is that some apartment complexes provide free Internet access to their residents. These complexes often engage in education campaigns to encourage residents to secure their access points, therefore raising awareness of security and privacy issues in the complex.

Perhaps another reason to expect higher population density to result in better security is risk identification. For someone living in a remote location the identification of potential attackers is fairly easy as it might involve recognizing that there is a strange vehicle sitting in that consumer's driveway. Identifying potential attackers in a highly populated area is not straightforward. There could be dozens of people who have the ability to access the wireless device from the privacy of their own home without giving the naïve consumer any clues. The sheer number of potential attackers who can access a wireless

device in a densely populated area may create an incentive for the consumer to invest more resources to implement secure wireless.
Hypothesis 3: Higher population density predicts better levels of wireless security.

3. Experimental Design

Data about the state of individual wireless access points was collected in a "wardrive" of 62 neighborhoods in a small college town. The neighborhoods surveyed represented a wide range of economic and educational demographics, and included both apartment/condominium complexes as well as single-family homes. The data was collected using two different laptop computers, one with a GPS unit attached for accurate plotting of access points. The software utilized for the data collection was NetStumbler, available from http://www.netstumbler.org.

Initially, over 3000 access points were identified during 5 five separate wardriving sessions lasting a total of 12 hours. Any commercial access points, identifiable either by SSID or wireless router maker, were purged from the data set. All unique access points appearing in more than one neighborhood were also discarded. Three neighborhoods in which less than 8 access points were present were dropped from the data set as well, giving us a final total of 59 neighborhoods surveyed and 2443 individual access points recorded.

Once access point data was collected, each neighborhood was given a score reflecting the percentage of wireless access points that were identified as secure in that area. For purposes of this study, a secure wireless access point is defined as one that utilizes any form of encryption technology. A variable named *edlevel* representing percentage of residents with at least a bachelor's degree as determined by US Census Track (2000 Census) data was added to each neighborhood to test Hypothesis 1. For Hypothesis 2, a variable named *income* representing consumer income level was approximated using rental rates for apartments and a calculated mean mortgage payment (10% of home value down, amortization over 30 years at 7% interest) for homes. Finally, a dummy variable named *pdensity* representing high or low population density was assigned to each neighborhood to test Hypothesis 3. A regression was then run using the following equation:

$$\%\text{secured wireless points} = \beta_0 + \beta_1 * \text{edlevel} + \beta_2 * \text{income} + \beta_3 * \text{pdensity}$$

4. Results

The results of the regression can be seen in Tables 1 and 2 below. None of the variables were found to be significant; therefore we must reject all three of our hypotheses and conclude that income, education level, and population density all are not predictors of increased wireless security.

Table 1: Regression statistics

Regression Statistics	
Multiple R	0.1181
R Square	0.0140
Adjusted R Square	-0.0398
Standard Error	0.1342
Observations	59

Table 2: Parameter estimates

	Coefficients	*Standard Error*	*t Stat*	*P-value*
Intercept	0.665802	0.067813	9.818	0.00000
edlevel	-0.000815	0.000998	-0.817	0.41736
income	-0.000008	0.000047	-0.162	0.87170
pdensity	-0.002968	0.038681	-0.077	0.93911

Chart 1: % Secure Wireless vs. Education Level

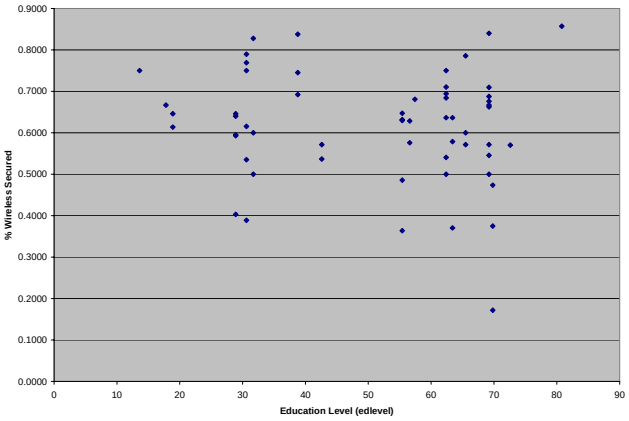
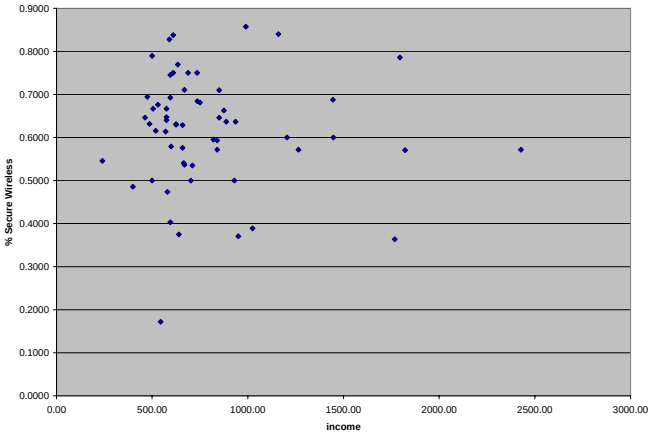


Chart 2: % Secure Wireless vs. income



5. Discussion and Future Research

None of our hypotheses, all of which were supported to some extent by the literature, were found to be significant in this study. We cannot say with any certainty that income, population density, or education level have any effect on the expected level of wireless security.

These findings indicate that investing resources in large-scale educational campaigns to raise awareness of wireless security may be a bad decision since education seems to have little effect. They also suggest that increasing levels of wireless security should not be expected to correlate with increasing wealth. Also indicated is that users cannot be expected to protect themselves more effectively against increased risk to the extent that population density indicates risk of misuse.

One interesting result that was found was an abnormally high percentage of access points with a default SSID but with encryption enabled from vendor 2Wire (http://www.2wire.com). Upon further research, it was found that their wireless product comes with an installation wizard that walks a user through the setup and secure configuration of their access point. There were 340 2Wire routers with default SSIDs, or 13.9% of the total access points polled. However, 330 of those routers were secure, a 97% lockdown rate. Another set of 57 routers identifiable as Linksys Secure Easy Setup models were found to have an 88% security rate. According to the Linksys website (http://linksys.com), these SES routers can be automatically configured to use encryption by pressing first a hardware button on the router and then a software button on a connected computer, eliminating the need for any decision making or manual configuration by the user. Removing these two types of routers from the data we find that only 55% of the other routers are configured by users to be secure. These figures are summarized in Table 3 below, and they correspond closely with findings from a recent study that found that default settings on wireless routers are powerful indicators of security[20].

Table 3: Wireless security levels by vendor

Router	*n*	*Secure*	*% Secure*
2Wire	340	330	0.971
Linksys SES	57	50	0.877
All others	2046	1116	0.545
total	2443	1496	0.612

An obvious response to this observation is a call for interfaces that are better designed to provide scaffolding for naïve consumers as they attempt to make decisions about wireless security and privacy risks. One possible scaffolding option might be a configuration wizard that walks a user through the process of locking down their router, just as the 2Wire routers provide. Term this as the “usable security” approach, allowing for assisted decision making and potentially more flexible outcomes.

Another option is that of the Linksys SES method, which is removing all configuration responsibilities from the user completely and reducing the process to the push of two

buttons. Term this as the “security as default” method, where all routers are configured to the same general security profile and consumer choices are severely limited.

The usable security paradigm would enable meaningful consumer choice and flexibility, for example allowing internet sharing in lower income neighborhoods in a secure manner. The initial data indicates that this approach is slightly more effective than the security as default method, but further studies should focus on the relative merits of each approach.

One of the limitations of this study is that many of the locations in the study were college student locations, and age was not taken into account in the study. Future research will include looking at age as a possible factor, with age cohorts representing years of computer use. However, obtaining this information is an as yet unsolved research problem.

Further studies will also focus on the usability differences between the two styles. Formal usability analysis of wireless router installation and configuration is currently being undertaken by researchers in the Human-Computer Interaction program at the Indiana University School of Informatics. Use of those findings will allow us to better investigate our emergent hypothesis that only usability and default configuration predicts use of security in home-based wireless devices.

6. Conclusion

The most effective predictor for secure wireless configuration is not factors such as income, education level, or population density as indicated by early research in the economics of security. The best predictor is the type of router purchased by the consumer. Default settings and effective usability seem to be the driving forces behind wireless security. The production of devices that enable security by default or scaffold consumers in their security decision making process is the key to a more secure system of home-based wireless.

Bibliography

1. Acquisti, A. and Varian, H. R., "Conditioning Prices on Purchase History" (September 25, 2002). SIMS Working Paper. Available at SSRN: http://ssrn.com/abstract=336684 or DOI: 10.2139/ssrn.336684
2. Acquisti, A. and Grossklags, J. "Privacy Attitudes and Privacy Behaviors" in Camp, L. Jean and Lewis, Stephen (editors.) *Economics of Information Security* (2004) Springer/Kluwer
3. Ait-Sahalia, Y., Parker, J. A. and Yogo, M., "Luxury Goods and the Equity Premium" (August 19, 2002). Princeton University, Economics Discussion Paper No. 222. Available at SSRN: http://ssrn.com/abstract=385243 or DOI: 10.2139/ssrn.385243
4. Bosworth, B. and Kabay, M.E. (editors) *Computer Security Handbook, Fourth Edition* (2002) J. Wiley and Sons
5. Camp, L. Jean and Osorio, Carlos A, "Privacy-Enhancing Technologies for Internet Commerce" (August 2002). KSG Working Paper No. RWP02-033. Available at SSRN: http://ssrn.com/abstract=329282 or DOI: 10.2139/ssrn.329282
6. Camp, L. Jean "Mental Models of Information Security" (2006) in *Technology and Society*, forthcoming
7. Deniszczuk, Hottell, and Carter "Does Education Work? A Quantitative Evaluation of the Behavioral Effects of Security Education" (2006) forthcoming
8. Denning, Dorothy *Information Warfare and Security* (1999) Addison-Wesley
9. Federal Trade Commission - Identity Theft Survey Report (September, 2003) available at http://www.consumer.gov/idtheft/pdf/synovate_report.pdf
10. Gross, R. and Acquisti. A. "Information Revelation and Privacy in Online Social Networks" (2005) *ACM WPES Workshop*
11. Harper, J (2004) "Understanding Privacy – and the Real Threats to It" in Policy Analysis no. 520 pp 1-17(Cato Institute)
12. Hui, Kai-Lung and Png, Ivan P.L., "Economics of Privacy" in *Handbook of Information Systems and Economics*, Terry Hendershott, ed., Elsevier, June 2005 Available at SSRN: http://ssrn.com/abstract=786846
13. Lundblad, N. "Privacy in a Noise Society" in Wahlgren, P (ed) *IT-Law Scandinavian Studies of Law* vol 47(Stockholm 2004)
14. Odlyzko, Andrew, "Privacy, Economics, and Price Discrimination on the Internet" (July 27, 2003). Available at SSRN: http://ssrn.com/abstract=429762 or DOI: 10.2139/ssrn.429762
15. Shostack, A. and Syverson, P. "What Price Privacy?" in Camp, L. Jean and Lewis, Stephen (editors.) *Economics of Information Security* (2004) Springer/Kluwer
16. Varian, Wallenberg, and Woroch "Who Signed Up for the Do-Not-Call List." The Third Workshop on Economics of Information Security(WEIS04), Minneapolis available at http://www.infosecon.net
17. Shapiro, C. and Varian, H *Information Rules.* (1999) Cambridge, MA: Harvard Business School Press.
18. Wathieu, Luc, "Privacy, Exposure, and Price Discrimination" (October 2002). HBS Marketing Research Paper No. 02-03. Available at SSRN: http://ssrn.com/abstract=347440 or DOI: 10.2139/ssrn.347440

19. Wathieu, L. and Friedman, A. “An Empirical Approach to Understanding Privacy Valuation”, Fourth Workshop on Economics of Information Security (WEIS05), available at http://www.infosecon.net
20. Sandvig, C. & Shah, R. (2005). “Defaults as De Facto Regulation: The Case of Wireless Access Points.” Paper presented at the 33rd Telecommunications Policy Research Conference (TPRC) on Communication, Information, and Internet Policy, Arlington, Virginia, USA.