Where's the Security in WiFi? An Argument for Industry Awareness

Dr. Glen Sagers
Illinois State University
gsagers@ilstu.edu

Dr. Bryan Hosack
Illinois State University
bhosack@ilstu.edu

Dr. RJ Rowley
Illinois State University
rjrowle@ilstu.edu

Dr. Douglas Twitchell
Illinois State University
dtwitch@ilstu.edu

Ms. Ranjitha Nagaraj
None
ranjitha.nagaraj@gmail.com

Abstract

As more and more wirelessly connected networks come online, security becomes a prominent concern. WiFi insecurity can result in detrimental effects to both individuals and organizations. To establish a greater awareness of the problems associated with wireless security and the extent to which the so-called digital divide effects such problems, we examine the relationship between wireless access points collected via wardriving and a series of US Census socio-economic variables in two communities in the United States. We found significant correlations between WiFi security race/ethnicity, which may also correlate to education levels and income. Such findings suggest that a greater awareness and/or manufacturer-driven default security for wireless access points may be necessary to ensure better security.

1. Introduction

Wireless (WiFi) networks are here to stay. It seems that every new electronic device released is WiFi capable, whether laptop or desktop PC, smart phone or tablet. Increasingly, restaurants, hotels, coffee shops, and other businesses provide Internet access to customers via WiFi networks. It can be difficult to find an area in American cities where there are not several available networks. What is not to like about WiFi? Wireless networks are inexpensive to set up, requires no drilling through walls, no skilled labor to install cable, and little in the way of maintenance. It seems a feasible solution for many Internet connectivity situations. However, not all aspects of wireless networks are ideal. Wireless networks are a broadcast technology, meaning that anyone within radio range can intercept the signal. If that signal is not encrypted, the transmission can be read by anyone with a WiFi capable device. Approximately 65% of all wireless networks use some form of encryption, but many use older, less secure standard. This insecurity has allowed wireless networks to serve as the vector for a number of high-profile attacks.

One of the most famous such attacks was perpetrated against TJX Corporation, parent company of T.J. Maxx, in 2005. In this case, the initial penetration was accomplished by breaking into a poorly-protected corporate Wireless Access Point (WAP) [3]. This break-in ultimately led to the theft of more than 94 million credit and debit card numbers. While there were other significant flaws in the company's security, it is safe to say that if they had invested in improved security for the WAP, the breach would have been much more difficult. T.J. Maxx is not the only organization to experience a WiFi attack, and there are certainly many more intrusions that have gone unreported for business, individual, or government WiFi networks.

The insecurity of WiFi, whether due to user error or ineffective standards, represents a serious threat to personal and business security. One of the real problems with WiFi is that it can be secure if configured correctly, but proper configuration seems to happen in a minority of cases. This paper calls for more awareness at both the industry and consumer levels of the need for proper use of encryption. Industry can play a large role in educating consumers about why they need security, and how to achieve it.

This study presents a large-scale attempt to collect data from thousands of WiFi networks to measure their security in two distinct geographic regions to determine what, if any, socio-economic factors affect the level of security. We further suggest a number of possible solutions to the gaps that exist in WiFi security.

1530-1605/15 $31.00 © 2015 IEEE
DOI 10.1109/HICSS.2015.641

2. WiFi insecurity

To appreciate the magnitude of the WiFi eavesdropping problem, it is necessary to understand the history of wireless networks. The 802.11 network standards were first released in 1997, and the more common 802.11b standard in 1999, followed by 802.11g and 802.11n over the next decade. The initial standards utilized an encryption method known as Wired Equivalent Privacy (WEP), which was designed to provide the user with the same privacy as could be expected on a switched Ethernet network. Flaws in the implementation of the encryption algorithm may allow publicized attacks on WEP [6]. A successful attacker retrieves the WEP key, allowing all transmissions to be decrypted and monitored. Within a few years, the time required for such an attack had dropped to only a few minutes. WEP encryption was used by T.J. Maxx at the time of the attack, even though better standards were available.

Due to the failures of WEP, the WiFi alliance released the WiFi Protected Access (WPA) encryption standard in 2003, closely followed by WPA2 in 2004. Today, both the WPA and WPA2 protocols have some vulnerability, which allow attackers to authenticate to the network, and, in some cases, to inject packets into the bit stream or decrypt traffic [2]. The latter attacks can be avoided by using AES encryption as used in WPA2. It should be noted that the WPA2 protocol is generally considered secure, as long as good passphrases or RADIUS authentication are used.

In short, WiFi networks can be vulnerable to attack, but defending against these infiltrations can be accomplished by utilizing the security features of the 802.11 standards included with WAPs. However, according to wigle.net, a website which tracks and maps the location and encryption status of WAPs, about 65% of WAPs are configured with encryption. Of these, about half use the older WEP and WPA standards [19]. Many newer devices using the otherwise secure WPA2 standard likely use another technology called WPS (WiFi Protected Setup), which can be cracked extremely easily. The use of WPS actually negates any security advantage of using WPA2.

WPS was released to address the complexity of setting up WiFi, allowing users to enter a short PIN (Personal Identification Number), push a button, or use other simple methods to pair two devices. However, WPS is trivially easy to crack via brute-force, and from there, the WPA2 passphrase can be cracked. Even worse, on some models, WPS can't be turned off, or pretends to turn off but doesn't. Thus, even when a technically sophisticated user is aware of the vulnerability, it may not be possible to mitigate. Unfortunately, some of the data in this study was gathered before the advent of WPS, and the rest before tools were available to detect whether WPS was in use, so no data exists yet as to how many access points use the protocol. So, while vendors have made strides in shipping WiFi APs in a secure default configuration, the true security level may have worsened in some cases.

Valid reasons for not encrypting an access point may exist; often, public hotspots are left open to allow easy access. Many unencrypted residential and business wireless access points remain open, putting owner's information at risk. As of 2009, 80% of survey respondents used WiFi to connect some device to the Internet, and 39% use wireless access to connect their computers to the Internet [14], and this number has certainly increased. With such a level of WiFi penetration into the residential space, it is imperative that users understand the importance of using wireless encryption.

Individuals may have several reasons for not encrypting their WAPs properly. Some users may not know security is necessary. Others may not understand how to set up proper security given its complicated nature, and so do not activate it, even if they know they should. Given these factors, there seems to be a plausible link between the concept of the digital divide and WiFi security use. The digital divide may be summed up as the "information haves vs. information have-nots". A strong, positive relationship exists between access to information technology, such as Internet and computer access, and the economic wealth and democracy of people [16]. The wealthiest countries are accruing digital technology much faster than those in poorer nations [13]. Early digital divide literature found economic factors to be prime contributors to this disparity, but more recent research suggests that various political and social variables also contribute [13]. This means that digital divides exist not only between nations, but also within countries; between races, genders, and those of different socioeconomic status [9],[12],[20]. Just as some classes of individuals have less access to technology, it may be that some have less opportunity to develop skills, such as those needed to set up WAPs securely.

To date, few studies have systematically correlated surveys of security in WAPs with other data, such as socioeconomic status, to find patterns that may explain the lack of encryption in many wireless networks [10]. The question guiding this research is whether socioeconomic factors contribute to the lack of use of wireless encryption. If user knowledge is to blame, education may be in order. If, on the other hand, the interfaces are cryptic and difficult to use, manufacturer redesign might be suggested.

3. Propositions

In this study, we propose several socio-economic factors that will impact whether WiFi security is used. The proposed factors are income, age, education, ethnicity and workforce type. These factors are derived from US Census data and are spatially compared with the WAP position at the census block group level.

3.1. Race and ethnicity

A number of research studies have shown that in the US, the white population has more access to and awareness of new technologies than minorities. For example, the white population owns more computers and uses the Internet more often than the African-American or Hispanic populations [18]. As different ethnic groups have different access to technology, it is likely that their expertise with the technology also varies. Proposition 1 states:

Census block groups with higher white populations are more likely to contain WAPs utilizing wireless security compared to block groups with high minority populations.

3.2. Income

One of the most commonly researched variables used in the digital divide literature is income level. People with higher income levels tend to have more access to technology. As individuals have more access to technology, they will likely use it for more purposes and more frequently. As an individual uses wireless technology more, opportunities for a security breach increase. Further, those with higher incomes may be more conscious of the security of their information systems, as they perceive that they have more to lose. Proposition 2 is:

Census block groups with higher per-capita income will have more WAPs that utilize encryption to secure their online communications.

3.3. Age

Younger individuals have been shown to be more tech-savvy than older generations. They accept new concepts and changes in technology more rapidly and more favorably [8]. They also may have more access to high-tech resources in schools, and feel considerable peer pressure to try out new technologies. As the younger generation uses such technologies, they may understand the security implications involved. Proposition 3 is:

Census block groups with a younger demographic will have more WAPs with encryption turned on.

3.4. Education

As new technologies develop, individuals must learn the skills necessary to utilize them [15]. It is believed that education plays a critical role in differentiating the level of computer-based work skills, with higher education leading to higher skill levels [1]. When an individual has a college education, even in a non-technical field, they are more likely to be aware of the need to use technology properly, and to consider all implications of using a new technology [5]. Further, people with college educations tend to work in white-collar jobs, exposing them to new technologies. For example, they may have a wireless network at their workplace requiring authentication and encryption, leading them to consider why this precaution is necessary, which may carry over to their personal networks. Proposition 4 claims:

Census block groups with higher levels of education will be more likely to have WAPs using encryption.

3.5. Workforce Type

In the last few decades, information workers have become much more common in many sectors of the economy. Almost sixty percent of the US gross national product comes from the information and knowledge sectors. These knowledge workers—including scientists, engineers, and IT staff—are more likely to be exposed to advanced technologies, including wireless technologies, and to use this knowledge when configuring their own networks. Proposition 5 suggests:

Census block groups with higher proportions of knowledge workers will be more likely to use WiFi encryption than block groups with other types of jobs such as manufacturing or agriculture.

4. Data Collection

Data in this study was collected from a variety of sources. The approach for WiFi data collection is described in detail, followed by the description of the data collected using wardriving and the publicly available socioeconomic data.

4.1. Wardriving

The WAP data used in this study was gathered via wardriving. Wardriving is defined as locating WAPs

and logging their position by registering the location of the broadcast signal. The term wardriving was coined by Peter M. Shipley around 1999-2000. Shipley was one of the first to automate the entire wardriving process of using dedicated software and GPS. Although logging WAP locations was not new, until then it was done manually by using laptops to collect data and then write down location and access details using pen and paper.

Contrary to popular belief, wardriving does not include connecting to or "hacking into" wireless networks, both of which are illegal activities. In fact, location information is commonly determined by everyday devices using WiFi, including the geolocation services on the iPod Touch, iPad and various Android devices. Skyhook and Google, respectively, have provided large databases for these services, which are used to find a user's location, based on proximity to a known WAP. These databases were compiled using wardriving data.

The first recorded wardriving efforts took place in September 2002, and included about a hundred wardrivers in six countries. Approximately 9000 access points were located and about 30% of these were encrypted with WEP. About 30% of WAPs (not mutually exclusive of whether WEP was implemented) used the default SSID [11]. Several more worldwide efforts took place in the next few years, culminating in June 2004. This larger study logged 228,000 access points in 17 countries; with 38% using WEP encryption, and 31% using the default SSID [11]. Currently, organized wardriving activities take place around the annual DEFCON conference. A number of websites have been created to log this information; the largest is wigle.net, which has a current database of over 89 million access points.

4.2. Wireless Access Point Data

For the wardriving effort used to collect data for this study, an integrated system of a laptop with several wireless cards and a consumer handheld GPS receiver was used to log the position of the vehicle as each access point was detected. Kismet, a popular open-source wireless detection tool, was the software used to log the data. Data included, but was not limited to, the Extended Service Set Identifier (ESSID) or name of the network, Basic Service Set Identifier (BSSID) or MAC address of the WAP, the channel on which the network was operating, the type of encryption used, the date and time the WAP was first and last seen, and GPS latitude and longitude. Of particular interest to this study were the ESSID, BSSID, encryption type, and GPS position. The collection of this data took place over approximately 30 months, from 2006 to 2008, with a smaller collection in 2011-2012 for comparison of rates of encryption adoption. The data was collected in two US communities, one in the South, the other in the Midwest.

After collection, the data for approximately 40,000 WAPs was imported in to Microsoft Excel, and after duplicates were removed, based on the BSSID, about 16,384 WAPs remained. Finally, WAPs falling outside the boundaries of the counties investigated in the study were removed, leaving 13,636 usable WAPs. The data was separated by county, using 2000 Census boundaries to delineate the borders. This resulted in one county with 9583 observed WAPs and the other with 4053.

4.3. Socioeconomic data

Data for the socioeconomic conditions in the counties was obtained from the 2000 Census at the block group level (generally the size of several neighborhood blocks in an urban area). Relevant fields were extracted for all block groups (n=192) lying within the two counties. The variables of interest were household income, age, education level, race, and workforce type. Income categories were patterned after the Pew Internet and American Life project. Income levels used were $0–$24,999; $25,000–$49,999; $50,000–$74,999; $75,000–$99,999; and greater than $100,000. Age breakdowns were 18-24, 25-29, 30-34, 35-39, 40-44, and more than 44 years of age. Education levels were high school, bachelor's degree, or advanced degree. Race categories were taken directly from the census.

Workforce type categorization was carried out using prior research based on the definitions of knowledge workers and whether workers were "blue collar" or "white collar" [1],[4]. The following census categories were classified as "Information Workers" for purposes of this study; information, finance, insurance, real estate, rental and leasing, professional scientific, management, administrative, and waste management services. Although waste management does not really fit with the other information workers in a strict sense, the census groups it with other professional services and no further breakdown is furnished, meaning it cannot be separated, and was thus left in this category. All other major categories were used as-is, and were classified as non-information workers.

The census data and the WAP data were analyzed using ArcGIS 9.3. Using a spatial join, a GIS function that overlays two dataset in order to determine their geographic relationship, each WAP was assigned the socio-economic attributes of the block group in which it lay. Queries were then performed to determine the

number of open or protected (with any one of WEP, WPA or WPA2 encryption) WAPs for each of the census variables. A graphical example of protected vs. unprotected WAPs overlaid onto the census age data is given in Figure 1.

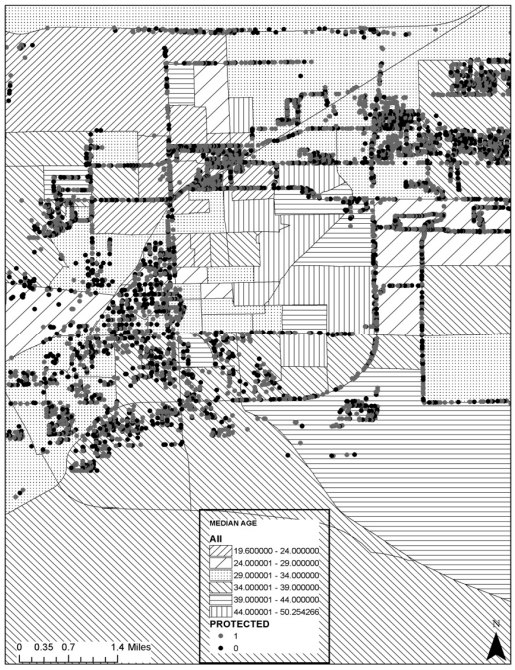

Figure 1. Wireless access points overlaid onto Census block groups by median age

5. Analysis

Bivariate correlations were used because the number of cases (192) was not large enough to use multiple regression, due to the multicollinearity of the predictors introducing high intercorrelations. The Pearson correlations were conducted to determine the relationship between various independent variables such as age and workforce type against the dependent variable of whether or not a WAP used encryption. PASW version 18 was used for this analysis. For each census block group, the percentage of open vs. protected WAPs was found, using the normalized percentages. The descriptive statistics for the variables are presented in Table 1.

Table 1. Descriptive Statistics for All Variables in First Iteration (N=192)

	Mean	Std. Dev.
% protected access points	.515	.231
Education (Bachelor's)	.312	.208
Median Age	33.667	8.165
Median Income ($)	44,017.810	24,672.110
% Information workers	.254	.102
% White population	.785	.216

A case can be made for the existence of a security gap in wireless access points. The only variable that correlates significantly with percentage of protected wireless access points is the percentage of white population ($r = .190$; $p = .008$). While none of the other demographic variables correlate with percent protected, all correlate with percentage of white population. Due to the collinearity of race with such factors as education and income levels, it is not a stretch to say that richer, more highly educated whites are more likely to have their WiFi networks protected. Table 2 shows the variable correlations.

Adding the information profession tells mostly the same story, except that the percentage in information worker professions does not correlate with either percent white or with percentage of protected access points. This is likely do the fact that the Census data includes several categories that are only loosely knowledge workers, and also waste management, which does not fit well. There may be a relationship between information workers, especially in IT and related fields, and the ability to securely configure a wireless access point, but the data available is not granular enough to evaluate this relationship.

A smaller set of data was collected in 2011-2012, and the rates of encryption use were compared to the 2006-2008 dataset. The results confirm that the counties studied mathc the statistics published by wigle.net, showing an increase in encryption use from about 44% in January 2007 to about 59% in January 2012. These data were only used to show increases in encryption use over time.

Table 2. Correlations

		% Prot.	Income	White %	Age	Advanced Ed.
% Prot.	Pearson Correlation	1				
	Sig. (2-tailed)					
Income	Pearson Correlation	.096	1			
	Sig. (2-tailed)	.184				
White %	Pearson Correlation	.190**	.486**	1		
	Sig. (2-tailed)	.008	.000			
Age	Pearson Correlation	.072	.663**	.352**	1	
	Sig. (2-tailed)	.318	.000	.000		
Advanced Ed.	Pearson Correlation	.037	.647**	.322**	.553**	1
	Sig. (2-tailed)	.611	.000	.000	.000	

** Correlation significant at the 0.01 level (2-tailed).

Table 3 Correlations, including information professions

		% Prot.	Income	White %	Age	Advanced Ed.	Info Worker
% Prot.	Pearson Correlation	1					
	Sig. (2-tailed)						
Income	Pearson Correlation	.096	1				
	Sig. (2-tailed)	.184					
White %	Pearson Correlation	.190**	.486**	1			
	Sig. (2-tailed)	.008	.000				
Age	Pearson Correlation	.072	.663**	.352**	1		
	Sig. (2-tailed)	.318	.000	.000			
AdvanceEd.	Pearson Correlation	.037	.647**	.322**	.553**	1	
	Sig. (2-tailed)	.611	.000	.000	.000		
Info Worker	Pearson Correlation	.141	.220**	.049	.035	-.016	1
	Sig. (2-tailed)	.051	.002	.503	.632	.823	

** Correlation significant at the 0.01 level (2-tailed).

6. Discussion

The findings indicate that some socioeconomic factors do inform us of the adoption of wireless protection. The results for education are a classic case of the digital divide, and follow the pattern seen in terms of access to computers or Internet use [1], [14].

By using data at the aggregate census block level, it is difficult to draw conclusions about individuals. Since individual level data is not likely to be able readily available—for this research team or any other – the only conclusions that can be drawn are at the aggregated level. In this case, the conclusion is that:

Census blocks with a higher percentage of whites—which are also more likely to have higher mean incomes, ages, and advanced education levels—are more likely to have a higher percentage of protection of their WiFi networks.

It can be generalized that higher-income white individuals, who likely have advanced education are probably more likely to be protected. This ecological generalization is merely likely; to find true correlations would require gathering of individual-level data, a difficult and potentially invasive proposition.

Minority races typically have less access to and lower knowledge of technology, a pattern reflected in our analysis [17]. The white population was apparently more aware of and was more likely to use WAP encryption. Could this disparity be avoided by targeted campaigns to certain ethnic groups explaining the need for wireless encryption?

Few previous studies have examined workforce type in terms of the classical digital divide and found that information workers have more access to technology [1]. This pattern was not shown in this study, but it is possible that this could be found if Census workforce data could be further subdivided.

Income had no significant effect on the use of encryption. This is somewhat surprising, as logic would dictate that those who have the most to lose might be the most likely to protect their assets, but no evidence of this was found.

Age was not a statistically significant predictor of use of encryption. Contrary to what one would expect for younger individuals, who are often characterized as more technically savvy would be the most likely to secure their access points, this was not the case. It may be that maturity indicates to individuals that they should protect their networks, and they seek a way to do so.

Finally, education levels did not affect encryption use significantly. Logic would dictate that more educated users might have more experience either with use of secured access points in a university setting, or actual education highlighting the need to secure the WAP, due to awareness campaigns on campus, this was not the case.

7. Limitations and future work

The results of this study indicate that problems exist which prevent the universal use of wireless encryption, despite the fact that protocols have been engineered into products for over a decade. The study, however, has some limitations. First, the WAP data was collected via wardriving in 2006-2008, but the census data available at the block group level at the time of the analysis was from 2000, thus the 2000 Census was used. Even after the 2010 Census data became available, the data available at the block-group level have changed, meaning the data should not be analyzed against that dataset.

Additional collection of wardriving data may show stronger correlations with the factors studied. Further, assuming that additional data collection is in one of the same communities, it may be possible to track individual WAPs (by BSSID/MAC address) to determine whether encryption has been enabled in the interim, possibly indicating greater awareness of the need for encryption.

It would also be useful to know what types of encryption different manufacturers use as the default. The original dataset does not contain this information, but newer wardriving tools capture this information, which may help indicate whether increases in protected WAPs are due to more awareness of the problem at the consumer level, or whether the overall increase in encryption use is mostly due to manufacturers shipping WAPs in a default secure configuration.

This research did not study whether the flawed WPS protocol was in use in WiFi networks, as it pre-dates the release of that security measure. However, new tools were introduced in early 2012 to track whether a network is using WPS. These tools could be used in future studies to determine how many networks which use the otherwise-secure WPA2 security mechanism are vulnerable to this class of attack, and whether that correlates with certain manufacturers.

Finally, the communities studied may not be representative of all communities. Both communities have a fairly high student population, as each has two universities and a community college. The communities also have a high proportion of knowledge workers, due to the aforementioned institutions, and the industries located nearby. Thus, the towns have few concentrations of very low income, very high minority concentrations, or high levels of blue-collar workers in the block groups studied. Targeted wardriving, using the Census 2010 data, could be

performed within block groups fitting all levels of all variables, to further clarify relationships.

8. Conclusion

This study is the first to spatially correlate socioeconomic factors with the use of wireless encryption. Although the results do not show that every factor considered is an indication of the digital divide related to wireless encryption, there are preliminary indications of a similar phenomenon. Those of non-white races appear less likely to properly secure their WAPs. The fact that worldwide only 65% of WAPs are encrypted points to a lack of understanding on the part of users of the need for encryption [10].

In fact, in today's environment, no good reason exists for not using encryption. Even in the case of publicly open hotspots, encryption can and should be used. A "Public WiFi" WAP can be secured via WPA2, and the passphrase posted prominently for customers or similar authorized users. One possible scheme to allow easy access while enabling protection would be to set the WPA2 passphrase to the same value as the SSID, or even broadcast the password as part of the SSID, making it easy for a user to remember. This practice would secure the communications on the network, thanks to WPA2's use of unique, per-user session keys, but still allow easy access.

Manufacturers seem to have realized, at least partially, that WAPs should be secure out-of-the-box. Many companies are shipping consumer-level WAPs with security already enabled. Such WAPs usually have the passphrase printed on a sticker attached to the device. Some of these passphrases, unfortunately, are short, programmatically derived from the MAC address or SSID, or easily found via WPS brute-forcing. These have been shown to be vulnerable to attackers, who simply re-compute the default passphrase by applying the algorithm to public information such as a portion of the SSID and MAC address [7]. To be truly secure, the passphrase must be long, random, and not based on any information related to the WAP.

Frankly, both standards bodies and manufacturers have made strides in default security, but more work needs to be done. From the results of this study, it would appear that beyond simply shipping secure-by-default hardware, education of at least some classes of users is important. This might take the form of manuals in different languages, simplified manuals, or simplified setup routines. Perhaps some of the burden of education should fall on the manufacturer to help users understand that good passphrases are in their own best interest, and educate users on how to select good passphrases.

As Internet use becomes more widespread, especially in terms of financial transactions, it becomes increasingly important to ensure that information exchange is protected. While most online shopping and banking is protected via Transport Layer Security (TLS), recent vulnerabilities in that protocol highlight the need for multiple layers of security. Additionally, there are certainly many messages, such as email, IM, and other content, which aren't protected by other encryption but should be protected from prying eyes. The ease with which sniffing tools can be employed in an environment using a bus topology makes WiFi especially vulnerable.

This research only begins to answer the question of "Why is encryption not used more widely?" and future studies must continue to ask this question. If user education is to blame, then increased efforts to educate the general public on the need to enable encryption should be undertaken. If, on the other hand, it turns out that the reason for low use of encryption is that it remains too difficult for some users to enable, then simplified setup routines and increased "secure by default" configurations are in order. In short, the problem of lack of WiFi encryption represents an open challenge to the computing community. As WiFi use increases, even current levels of encryption use leave large amounts of personal information vulnerable.

9. References

[1] D.L. Autor, L.F. Katz, and A.B. Krueger, "Computing inequality: have computers changed the labor market?" Quarterly Journal of Economics, vol. 113, 1998, pp. 1169-1213.

[2] Beck, M. Enhanced TKIP Michael Attacks. Dresden, Germany, 2010; http://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf

[3] Berg, G. G., Freeman, M. S., Schneider, K. N. Analyzing the TJ Maxx Data Security Fiasco, New York, NY, 2008; http://www.nysscpa.org/cpajournal/2008/808/essentials/p34.htm.

[4] Davenport .T.H. Thinking for a living: how to get better performance and results from knowledge workers, Harvard Business Press, Boston, MA, 2005.

[5] R.S. Done, "Internet Voting: Bringing Elections to the Desktop", In M.A. Abramson, and M.L. Therese, E-government, Lanham, MD, 2003, pp. 237-238.

[6] S. Fluhrer, I. Mantin, and A. Shamir, A, "Weaknesses in the key scheduling algorithm of RC4", Revised papers from

the 8th Annual International Workshop on Selected Areas in Cryptography, Toronto, Ontario, Canada, 2001, pp. 1-24.

[7] GNU Citizen. Default key algorithm in Thomson and BT Home Hub routers. 2008; http://www.gnucitizen.org/blog/default-key-algorithm-in-thomson-and-bt-home-hub-routers/.

[8] P.G. Harwood, and W.V. McIntosh, "Virtual distance and America's changing sense of community", In P.M. Shane, Democracy online: the prospects for political renewal through the Internet, 209-224, Routledge, New York, NY, 2004.

[9] D.L. Hoffman, T.P. Novak, and A.E. Schlosser, "The evolution of the digital divide: How gaps in internet access may impact electronic commerce", Journal of Computer-Mediated Communication vol. 5, 2000, np.

[10] M. Hottell, D. Carter, and M. Deniszczuk "Predictors of home-based wireless security", in Fifth Workshop on the Economics of Information Security, University of Cambridge, England, 2006, np.

[11] C. Hurley, The World Wide War Drive 4. Las Vegas, NV, 2004; http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-hurley.pdf.

[12] Margolis, J., and A. Fisher, Unlocking the Clubhouse: Women in Computing, MIT Press, Cambridge, MA, 2002.

[13] Mossberger, K., Tolbert, C. J., and Stansbury, M. Virtual inequality: Beyond the digital divide. Georgetown University Press, Washington, D.C., (2003).

[14] Pew internet and american life Project, home broadband adoption, Washington, D.C., 2009 http://www.pewinternet.org/Reports/2009/Home-Broadband-Adoption-2009. aspx.

[15] J. Pick, and R. Azari, "Worldwide digital divide: influences of education, workforce, economic, and policy factors on information technology", in Proceedings of SIGMIS CPR St. Louis, MO, 2007 pp. 78-86.

[16] M.G. Quibria, "Digital divide: eeterminants and policies with special reference to asia." Asian Development Bank, Manila, Philippines, 2002.

[17] G. Seckin, "Digital diversity or digital divide: an exploratory research on age, gender, race and income characteristics of online health information users", International Journal of Diversity in Organisations, Communities & Nations, vol. 10, 2010, pp. 99-116.

[18] J.C. Thomas, and G. Streib, "The new face of government: citizen-initiated contacts in the era of e-government", Journal of Public Administration Research and Theory, vol. 13, 2003, pp. 83–102.

[19] Wigle. WiGLE - Wireless Geographic Logging Engine - Stats. 2011; http://wigle.net/gps/gps/main/stats/

[20] G. Youngs, "Closing the gaps: women, communications and technology", Development, vol. 45, 2002, pp. 23–28.