2009

58 Percent Secure: Why Do So Many Wireless Networks Not Use Encryption?

Glen Sagers
Illinois State University, gsagers@ilstu.edu

Bryan Hosack
Illinois State University, bhosack@ilstu.edu

58 Percent Secure[1]: Why Do So Many Wireless Networks Not Use Encryption?

Glen Sagers
Illinois State University
gsagers@ilstu.edu

Bryan Hosack
Illinois State University
bhosack@ilstu.edu

ABSTRACT

This research project will analyze a large (n=98,000) dataset of wireless access points in two medium-sized US cities to examine changes in the use of encryption in 802.11 wireless networks over time. Further, changes in the use of encryption in these networks based on the socio-economic status of the network owner, and based on whether the owner is a business or an individual will be investigated. There is currently almost no research investigating the spread of wireless encryption as wireless networks become more prevalent.

This ground-breaking research will establish a baseline for business and personal use of encryption in wireless networks, correlated with socioeconomic status and other census data. This baseline will help future researchers determine whether changes to wireless protocols and changes in methods of setting up wireless equipment increases the use of security protocols, thereby increasing the security of the network.

Keywords: Wireless, 802.11, Wi-Fi security, wardriving, WEP, WPA, WPA2, GPS, Geographical Information Systems (GIS)

[1] The estimate of 58% was taken from wigle.net, and is based on 16,000,000 access points; accessed February, 2009

INTRODUCTION

802.11 wireless networks (also commonly known as WiFi networks or Wireless LANs – WLANs), have been widely deployed over the past decade, starting out as a technology used when running cable to a specific location was cost-prohibitive, to the situation we see today where WiFi is becoming so ubiquitous that many coffee shops, restaurants, hotels, and other establishments offer "free WiFi" as a perk in their advertising. Other establishments sell Internet access by the hour, often using WiFi as the medium for connection. Businesses have deployed wireless networks to allow workers to move away from their desks and still have access to corporate network resources. As the price of laptops, PDAs, phones (such as Apple's iPhone, and several other so-called "smartphones"), and other portable devices with 802.11 capability has decreased, home users have installed these networks to increase mobility and to avoid running wire through the walls of their homes. These networks allow home users to share files between computers, stream media to portable devices, and of course, access the Internet without being tied to a wall jack. As of 2005, approximately 52% of US households had wireless networks, and that number keeps growing (Cai, 2005).

Wireless LANs are a convenient way to allow multiple mobile users to connect to a network, but these networks also have documented security flaws. The original 802.11b standard, released in 1999, had fairly weak security, and while the security protocols built into subsequent versions have improved, often the security features of wireless access points or routers were turned off by default, and users were required to have some technical know-how to turn the security features on. This scenario of off-by-default security, coupled with the fact that wireless routers had a default SSID (service set identifier, which is the name used to identify a particular network, such as Aprils_Network, or John_Wifi) which corresponded to the manufacturer's name, meant that often, networks with the default SSID were left wide-open for anyone to access. This has led some wags to term these routers as members of the "Linksys Global Network" (Arstechnica, 2007). This situation has changed over the last few years; most new small office/home office (SOHO) access points and routers ship with a random SSID, and at least a minimum of security turned on by default. Further, as users have become more educated about the issues surrounding wireless security, more users may be turning on and using the available security features. Yet given that the so-called digital divide tends to divide computer and Internet users along socioeconomic lines (Ching, et al., 2005, Po-An Hsieh et al., 2008), it may be reasonable to expect that a similar situation exists for awareness of wireless security issues, and the ability to address them (Fenu and Piras, 2008). This would mean that many wireless networks owned by those of lower socio-economic status would be using unprotected hardware.

Original 802.11b used WEP (wired equivalent privacy) encryption to provide, as the name implies, a level of security equal to connecting the machine to a wired network. This security standard was quickly shown to have inherent flaws. This encryption method was replaced by WPA (WiFi Protected Access), which subsequently proved to have flaws of its own. WPA was replaced by WPA2 in 2005, which has proven trustworthy to date (as long as complex passphrases or 802.11i encryption is used). Although the older security protocols have been replaced in new equipment, a large install base of older equipment exists, and, in some cases, older equipment is reused or sold second hand. This creates a situation in which wireless security has nominally increased by virtue of improvements in the protocols, but may not have actually improved.

The danger in unprotected wireless networks lies in the fact that by design, wireless equipment broadcasts a radio signal. The signal is usable up to approximately 100 meters, but can be overheard much further, approximately 500 meters in some circumstances. These signals carry data sent by the user, including the addresses and contents of web pages visited, email sent and received, files downloaded, and may even contain passwords sent across the network and other private data. This data may be intercepted by anyone within the several hundred meter radius, using almost any computer with a wireless network card and some easy-to-install and use software. If the access point does not use wireless security, much of the intercepted data will be in clear-text, and can be read by a human or computer application. Any user connected via wireless to this access point is in danger of having their data stolen. Such unprotected networks can also be utilized by unethical individuals to access the Internet, or even mount attacks on other networks (Fairlie, 2008). When security is turned on in the network, at least assuming that the current WPA2 standard is used, and good passphrases or pre-shared keys (PSKs) are utilized, the data cannot be read by others, and unauthorized users cannot connect to the access point. Although older wireless protocols are not as secure as the current WPA2 standard, any degree of encryption used provides some protection against snooping of private data.

This problem is further exacerbated because the exact encryption type used in a given wireless network can be easily determined by simply receiving the signal from the network. These signals, carrying the SSID of the network and what type of encryption is used on the network, can be easily picked up by programs such as Kismet, Netstumbler and Wellenreiter, and correlated with the Global Positioning System (GPS) position of the wireless receiver at the time the signal is detected. This process of mapping GPS positions of the individual or vehicle at the time the signal is picked up is known as wardriving.

The position and security protocol information obtained through wardriving may then be stored in a database and plotted by mapping software. Thus, the degree of use of given security protocols can be determined, and the spread of newer encryption protocols over time and by geographical area is possible. There is little research to date that attempts to determine whether wireless encryption has grown more ubiquitous with time, and correspondingly few studies that attempt to determine why users may not implement wireless security on their networks. The only study so far to investigate this problem used approximately 3000 wireless access points in 59 neighborhoods to determine whether educational levels, population density, or income had any effect on the use of wireless security (Hottel, Carter, Deniszczuk, 2006). The results of this study were inconclusive, but may suggest that there is little advantage due to educational levels or personal income. This study aims to use a much larger dataset, gathered in 2 different US communities in different parts of the country to investigate whether those variables or other drivers are responsible for the decision to use wireless encryption.

PROPOSED MODEL

Based on the literature outlined above, this exploratory study will allow examination of the following propositions, which are discussed in detail below:

1. It is proposed that the digital divide which separates those of lower socioeconomic status from those of higher status will be present or accentuated in wireless encryption.
2. It is proposed that wireless encryption will be more widely used in business environments than home environments.
3. It is proposed that business users will utilize higher-security wireless encryption methods than home networks.
4. It is proposed that for any given socioeconomic status, the use of encryption will have increased over time.
5. It is proposed that the rate of use of wireless encryption will increase faster in areas of higher socioeconomic status.
6. It is proposed that the rate of use of wireless encryption will increase faster in business regions than residential areas.

There are several meanings of the term digital divide. It may refer to lack of equipment, lack of usage opportunities, lack of elementary experience to digital media, or a lack of skills caused by insufficient user-friendliness or inadequate education (Van Dijk, 1999). This final meaning is the one with which we are most concerned in this research, as a lack of skills in setting up wireless access points will lead to unprotected networks. The digital divide exists between countries of lower economic status and more developed nations, but it also exists between socio-economic classes within the United States. Low formal education levels translated to poor general computers skills (Van Dijk & Hacker, 2003). If the digital divide separates individuals in their skill in utilizing computers and applications, it is reasonable to assume that those difficulties will carry over into network setup and configuration, leading to some home networks being left unprotected.

Since businesses typically have funds budgeted to pay for professional setup of their networks and computing equipment, it may be expected that these businesses will utilize wireless encryption to a greater degree than home users, as the professional installers should realize the dangers associated with unencrypted wireless. Experience has shown that not all corporate networks are protected, as evidenced by media reports of successful attacks (Kindervag, 2007). Just as professionals should know that encryption is necessary, they should also understand the differences between types of encryption, and implement the strongest types. Since some networks were likely initially set up during periods where only the weaker WEP or WPA standards were available, and have not been updated since, at least some networks are likely utilizing the older standards. As equipment reaches the end of its useful life and is upgraded, newer protocols will be used. Since business users have a budget for new technology and a periodic cycle of technology refreshes, they will upgrade to newer equipment with corresponding improvements in encryption methods more quickly than home users.

Finally, a number of widely publicized break-ins and instances of mis-use of wireless access points belonging to others have generated increased public awareness of the need for wireless security (Phifer and Piscitello, 2007). This awareness induces users, whether business or personal, to inspect their wireless networks and upgrade the networks as needed. Further, education, in the form of better documentation included with wireless devices and articles appearing in popular press and computer trade magazines highlighting the need to turn on encryption serve to help users realize the dangers present in mis-configured networks (Bell, 2006). As awareness increases, at least some fraction of users will turn on security or upgrade to newer equipment and security methods. These factors, coupled with the fact that most SOHO routers manufactured in the last few years come with a sane set of security defaults, means that the overall rate of encryption use will increase, as has been shown Wigle.net, 2009). As with many of the factors contributing to the digital divide, it is likely that users of lower

socioeconomic status will not be as well educated in the need for wireless security. Together, these factors lead to a situation in which the use of wireless security protocols should increase over time, but at accelerated rates in business settings, and at faster rates among home users of higher socioeconomic status.

One possible regression model which could result from the data analysis is shown below. In this model, wireless encryption use increases over time; an effect shown to exist (Wigle.net, 2009). The rate at which wireless encryption use increases is moderated by whether the wireless network is owned by a business, and if the network is owned by an individual, the rate of increase is moderated by the owner's socioeconomic status. Business networks are expected to utilize wireless encryption more, and use is expected to increase at a higher rate. For home users, those with increased socioeconomic will utilize wireless encryption more, and the use among those of higher status will increase at a faster rate.

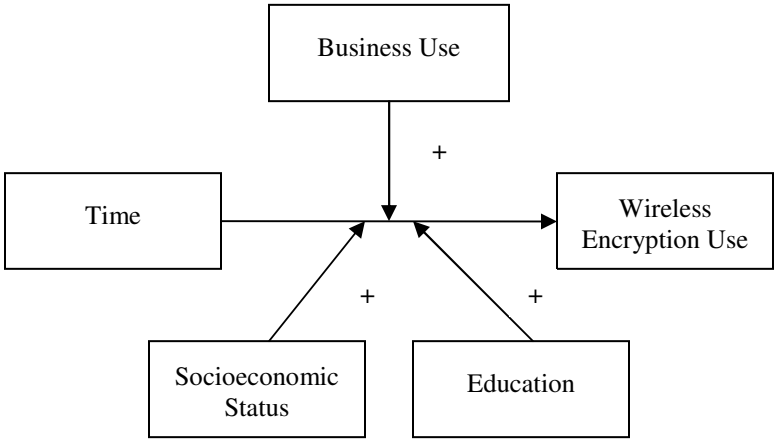

Figure 1: Proposed Model

PROPOSED METHODOLOGY

As users have become more security-conscious, and the security features of routers and access points have improved, there has been some overall increase in the use of encryption (Wigle.net, 2009). However, what remains to be determined is who is utilizing encryption. By overlaying the GPS position of a large (n=98,000) dataset of wireless access points with socioeconomic and land-use data from the US Census and other sources in a geographic information program such as ArcGIS, trends in the spread of wireless security over time and by different regions will be analyzed. This will help determine whether wireless security use is low among certain population segments, and paves the way for research to determine why that may be the case, and what additional steps must be taken to increase the spread of wireless security.

Data for the project consists of a database containing the names and positions of approximately 98,000 access points. The data, gathered over approximately six years, also includes the date mapped and encryption type used. This six year period (2002-2008) represents a portion of the lifecycle of 802.11 wireless networks during which the technology had matured to the point that many individuals and businesses implemented these networks. During this time, all three common encryption methods (WEP, WPA, and WPA2) were or became available, and awareness of the need for encryption likely grew during this period. This data covers two medium-sized US cities (population 125,000 to 175,000), one in the Midwest and one in the South. This data will be combined with publicly-available data on land use and socioeconomic status, such as, but not limited to, county or city plat data and US census data, and the socio-economic status (SES) composite index, an accepted measure in human services research which consists of parents' education, family income, father's occupation, and the presence of certain items in the household (Sawicki & Flynn, 1996). This will allow analysis of use of wireless encryption by various socioeconomic status indicators, whether an area is business or residential, and similar factors. After the data has been incorporated into ArcGIS, maps and statistical tables will be generated showing the density of wireless access points in a given area, and how many of those access points use security protocols. This data will be plotted by year to show changes in the use of wireless access points, and these plots analyzed to determine whether the utilization of encryption has increased during that time. A regression model will be developed to determine the impact of these factors on wireless security and to test the propositions provided above.

CONCLUSION

As noted, there is currently limited research concerning whether the use of encryption in wireless networks is more widespread today than in previous years. Further, although socioeconomic status and educational levels have been correlated with general technical knowledge, there has been little research to date to determine whether this knowledge translates to awareness and use of encryption in wireless networks. Although some sources have empirically shown a moderate increase in the use of encryption over time (Wigle.net, 2009), this is based on a very large sample, and has not been correlated with any other data regarding causes for the increase in wireless security implementation.

This research is cutting edge and will form the first comprehensive research on this topic. As such, it will be a valuable benchmark for researchers trying to determine whether encryption usage has increased and where it could be implemented further. Future studies could attempt to survey wireless users to discover what factors may impact their decision to implement wireless security features. Factors such as satisfaction with user interfaces and intention to use may offer some insight into how wireless users respond to this technology.

REFERENCES

Arstechnica. (2007) The ethics of "stealing" a WiFi connection, Arstechnica forums, available at: http://episteme.arstechnica.com/eve/forums/a/tpc/f/174096756/m/753003659831/p/1, last accessed 1/18/2009.

Bell, M. (2006) Got Wireless Security?, *PCWorld Magazine* (Online Edition), March 13, available at http://www.pcworld.com/article/125040/got_wireless_security.html, last accessed 2/10/09.

Cai, Y. (2005) Public Hot Spots: Moving Beyond Road Warriors, Parks Associates whitepaper, available at: http://www.parksassociates.com/research/reports/tocs/hotspots1.htm, last accessed 1/20/2009.

Ching, C. C., Basham, J. D., Jang, E. (2005) The Legacy of The Digital Divide, *Urban* Education, 40, 4, 394-411.

Fairlie, R. (2008) 14% of US consumers "borrow" free WiFi, ZD net blog, April 22nd, available at: http://blogs.zdnet.com/soho-networking/?p=199, last accessed 1/15/2009.

Fenu, G., and Piras, L. (2008) A Portable Wireless-Based Architecture for Solving Minimum Digital Divide Problems, in Leon Resnick, (Ed.), The Fourth International Conference on Wireless and Mobile Communications, July 27 – Aug 1, Athens, Greece.

Hottell, M., Carter, D., and Deniszczuk, M. (2006) Predictors of Home-Based Wireless Security, in Ross Anderson (Ed.) *Proceedings of The Fifth Workshop on the Economics of Information Security (WEIS 2006),* June 26-28, Robinson College, University of Cambridge, Cambridge, England.

Kindervag, J. (2007) (Mis)Understanding Wireless Security, *Business Communications Review*, 37, 10, 50-53.

Po-An Hsieh, J. J., Rai, A., Keil, M. (2008) Understanding Digital Inequality: Comparing Continued Use Behavioral Models Of The Socio-Economically Advantaged And Disadvantaged, *Management Information Systems Quarterly,* 32, 1, 97-126

Phifer, L., and Piscitello, D. (2007) The Sad and Increasingly Deplorable State of Internet Security, Revisited, *Business Communications Review*, 37, 6, 14-18.

Sawicki, D.S. and Flynn, P. (1996) Neighborhood Indicators, *Journal of the American Planning Association*, 62, 2, 165-184.

van Dijk, J. (1999) *The Network Society, Social Aspects of a New Media,* Sage, Thousand Oaks, CA.

van Dijk, J., and Hacker, K. (2003) The Digital Divide as a Complex and Dynamic Phenomenon, *The Information Society,* 19, 4, 315-326.

Wigle.net. (2009). General Stats, available at: http://wigle.net/gps/gps/main/stats/, last accessed 1/20/2009.