Improving Users' Security Choices on Home Wireless Networks

Justin T. Ho [1], David Dearman [2], Khai N. Truong [2]

[1] Google
Mountain View, CA 94043 USA
me@justinho.com

[2] Department of Computer Science
University of Toronto
Toronto, ON M5S 3G4 Canada
{dearman, khai}@cs.toronto.edu

ABSTRACT

Home networks are common but notoriously difficult to setup and maintain. The difficulty users experience in setting up and maintaining their home network is problematic because of the numerous security threats that can exploit poorly configured and maintained network security. Because there is little empirical data to characterize the usability problems associated with the adoption of wireless network security, we surveyed primary caretakers and users of 20 home networks, examining their perceptions and usage of the security features available to them. We found that users did not understand the difference between access control lists and encryption, and that devices fail to properly notify users of weak security configuration choices. To address these issues, we designed and evaluated a novel wireless router configuration wizard that encouraged strong security choices by improving the network configuration steps. We found that security choices made by users of our wizard resulted in stronger security practices when compared to the wizard from a leading equipment manufacturer.

Categories and Subject Descriptors

H.5.2 **[Information Interfaces and Presentation]:** User Interfaces; D.4.6 **[Software]:** Security and Protection—*Information flow controls*

General Terms

Design, Human Factors, Security

Keywords

Usable security, access control, wireless network, configuration, mental model

1. INTRODUCTION

Networks within the home are increasingly more common. In 2005, nearly 30 million households in the US had a home network [23] and the annual worldwide wireless networking equipment sales are forecast to exceed $4 billion in 2012 [24]. These wireless networks connect an ever-increasing set of devices such as gaming consoles, entertainment centers, PDAs, mobile phones, laptops and desktop computers. However, home networks remain difficult to set up and maintain. Nearly a quarter of wireless access points purchased by consumers in 2006 were returned because users were unable to properly set up and integrate them into their home networks [15]. These statistics are particularly concerning given the number of threats that exist to electronic networks. From problems with freeloading neighbors who steal bandwidth, to internet hackers who compromise home machines for spam attacks and botnets [10], the threat to the average broadband home network is very real and can have lasting legal consequences. For example, home users have been charged with copyright violations [14], and forced to pay additional bandwidth charges [11].

Past research suggests that certain wireless encryption technologies are ineffective [2, 5, 8, 21] and users are either unable or unwilling to exert the effort necessary to secure their networks properly [3, 6]. However, these studies have focused on a relatively technology savvy population (*i.e.*, households with at least one member who is technically proficient). Thus, the challenges with deploying and securing a home network for the broader population remain to be studied.

In this work, we performed a city-wide survey of wireless network signals across a diverse number of dwellings and interviewed the primary caretakers of 20 home networks to understand how their home networks are deployed and secured. This approach allowed us to identify common sources of confusion and problems faced by a broad range of end-users. Our study revealed that:

- the unique user experience supported by the out-of-the-box tools provided by different manufacturers have a significant impact of the use of encryption,
- users commonly use the default settings provided by their router's configuration wizard,
- users rarely install and maintain highly secure encryption keys across their devices,
- users rarely use the additional and advanced configuration features available in a router's setup menus when securing a home network, and
- users do not perceive a difference between encryption and access control lists.

These results suggest that better security practices and home network configuration choices can be designed and implemented directly using a new set of network configuration steps. To this end, we modified an open source router firmware such that it:

- encourages the user to consider plausible configuration choices that are dynamically generated by the system rather than the blank or predefined default option

Symposium On Usable Privacy and Security (SOUPS) 2010, July 14-16, 2010, Redmond, WA, USA.

- generates a random 63-character WPA2 AES encryption key that is automatically transmitted to all the user's network devices via a SSL-encrypted and password secured webpage, and
- automatically identifies and collects the MAC address of authorized devices for MAC address filtering.

We conducted a user study to determine the effectiveness of these changes. We found that participants were able to configure a router using our wizard to employ a greater level of encryption (WPA2) than otherwise.

2. BACKGROUND AND RELATED WORK

Home networks have become increasingly popular and now connect an ever increasing set of devices. Many of the underlying networking protocols used in these networks were originally designed to be set up and managed by professionals, and the complexity associated with setting up, maintaining and troubleshooting a home network are often immense. Calvert, Edwards and Grinter [4] argue that the home network of the future must have an explicit user interface, be self-configuring, self-administering, secure by default, and compatible with existing external TCP/IP-based applications though application independence and support for composition. To meet these requirements, they propose that the home network adopt a "smart middle" design which would eliminate the need to configure IP address settings on each device. This would allow home users to simply "connect and use" their devices as they currently do with telephones and television cable boxes in the home [4, 19].

Shehan and Edwards [19] discuss six models for achieving the above goal, ranging from replacing all existing protocols and standards used on the Internet with new ones that focus on usability and making the Internet accessible to all to building functionality into the gateway that bridges home networks to the public Internet thereby allowing a "fresh start" in the home. Work in improving the usability and security of the home network broadly falls into one or more of these models. For example, Yang and Edwards explored the alignment of the security process on a home wireless network with physical security [25] by using an explicit interface to provision access to the network. The ICEbox also doubled as a centralized network monitoring device. A usability study confirmed that this device reduced the complexity of common tasks, as well as the benefit from tangible and physical affordances to the configuration process, but that additional provisioning techniques should be explored in the future. The infrared transceiver is similar to the project by Balfanz *et al*., [1] which requires that devices are brought into physical range for network access provisioning which is a limitation of this work.

To make networking technologies more accessible to the home user, Stoll *et al.* [20] created a visualization to support the development user perceptions of firewall and security software. They found that their firewall visualization improved security choices and helped users make fewer configuration errors. Raja *et al.* were able to significantly improve the mental model and understanding of the Windows Vista Firewall by including greater context about network location and connections in the interface [17].

The way these technologies are envisioned and understood is critical, but networking technologies must also fit into existing social structures in the home [10]. Additionally, the physical site of the network, the building structure and space plan play important roles in the design of a home network [18]. Some households may wire Ethernet, while others rely on alternatives such as powerline and wireless networking technologies. Home users wrestle with the variety of networking mediums; the physical structure may affect wireless signal reach, and the feasibility of running multiple cables may affect network topology, requiring additional switching or repeater equipment. The presence of other devices in the home may also generate interference affecting network performance and reliability.

On the security front, a lack of understanding of virtual network boundaries created by wireless networks and the access paradox described by Chetty *et al.* has resulted in a gap between users' perceptions and the technical reality that is their home network [6]. Chetty *et al.* describe home networks that were secured merely by distance between the road and the wireless network, or the now deprecated Wired Equivalent Privacy (WEP) encryption method. These choices may suggest usability problems with the technology, although additional empirical data is necessary to quantify the extent to which the problems experienced by the participants of this study can be generalized.

Many configuration and maintenance problems are caused by the underlying networking protocols. These protocols were originally designed to be set up and managed by professionals, not end users. The need for each device to have a valid IP address, subnet mask and default gateway means that each device must be configured before it can function on the network (unlike other home appliances and electronics such as the telephone). A mis-configured device can also disrupt network function for all other connected devices (*e.g.,* IP conflicts) [4, 19]. Technologies such as DHCP only serve to mitigate the problem and help semi-automate the process, but do not eliminate the problem altogether. These gaps between how network technologies work and users' understanding often result in broken expectations between users and their digital home [3, 16].

The aforementioned works highlight that many of the problems with network technologies are abstract with no discernable mapping to physical objects in the real world. Concepts such as "WEP encryption" and "WPA encryption" are intangible by nature. Whereas the difference between a weaker padlock and a stronger padlock may be physically and visually apparent, the majority of wireless network technologies remain intangible by nature. This places a much larger emphasis on the user interface and its ability to communicate these differences to users. Our work focuses on understanding how networks are used and deployed on a larger scale and with a broader subject pool, specifically focusing on their security practices and configuration choices. In this work, we explore how to improve users' security choices for their home networks. We do so while simultaneously addressing the usability issues identified by Yang *et al*. [25], and lowering the amount of work that is necessary to set up and secure these home networks in general.

3. HOME NETWORKING SECURITY CHOICES & PRACTICES

In this section, we first describe a survey of the wireless network encryption used in various residential neighborhoods and apartment buildings throughout the city of Toronto, Ontario,

Table 1. Wireless network survey area, network density and average income data from 2001 Census [22].

Area ID	*Area Size*	*Description of Area*	*Average Income*
Area-A	~1 sq km	Urban, semi-detached/town homes, 10 minutes from city centre	$69,118
Area –B	~1 sq km	Exclusive urban neighborhood, single detached homes, 20 minutes from city centre	$131,162
Area –C	~1 sq km	Suburban neighborhood, semi-detached/town homes, 30 minutes from city centre	$64,677
Area –D	~1 sq km	Suburban neighborhood, single detached homes, 45 minutes from city centre	$63,238
Area – E	~ 1 sq km	Very exclusive suburban neighborhood, single detached homes, 30 minutes from city centre	$423,226
Building-F1	292 units; 32 floors	High density downtown core residential apartment buildings, > 20 storey	$89,664
Building-F2	300 units; 25 floors		
Building-F3	252 units; 20 floors		
Building-F4	476 units; 26 floors		
Building-F5	170 units; 20 floors		
Building-F6	325 units; 13 floors		

Table 2. The wireless network survey data for each of the five residential neighbourhoods (Area-[A-E]) and six apartment buildings (Building-F[1-6]). Reported for each area is the number of observed access points (APs), the density of the APs, and the proportion of observed APs that are unencrypted.

Area ID	*Access Point Density n/km*	*Access Points n*	*Unencrypted Access Points n (%)*
Area-A	0.139	1456	290 (19.9)
Area-B	0.170	839	193 (23.0)
Area-C	0.104	610	154 (25.2)
Area-D	0.135	760	177 (23.3)
Area-E	0.080	19	9 (47.4)
Area-[A-E]	Average = 0.124	Total = 3684	Total = 823 (22.3)
Building-F1	0.800	133	16 (12.0)
Building-F2	1.02	149	24 (16.1)
Building-F3	0.804	130	21 (16.2)
Building-F4	1.09	219	33 (15.1)
Building-F5	2.13	90	20 (22.2)
Building-F6	1.22	142	13 (9.15)
Building-F[1-6]	Average = 1.17	Total = 863	Total = 127 (14.7)

Canada. The purpose of this survey is to understand how home networks are currently deployed. We then describe an interview study we performed to gain deeper insights about specific security practices and choices used by participants when they set up and maintain their home networks.

3.1 Wireless Signal Survey

To gain a sense of how network encryption is used by the general population in various residential neighborhoods and apartment buildings throughout the city of Toronto, Canada, we developed a custom wireless scanning application that uses the Windows Vista networking API. The application captured all wireless networks that broadcast their Service Set Identifiers (SSIDs), and all networks that did not broadcast their SSID but were currently in use. The application ran on a Fujitsu Lifebook and was functionally equivalent to scanning for available networks in the operating system. We did not use more aggressive scanning techniques to detect all networks, but rather chose to respect the wishes of those who configured their home network to be invisible. We were able to differentiate access points (APs) that have a similar SSID by using the MAC address. The application was configured to query the networking stack for available SSIDs every five seconds, and log newly discovered AP MAC addresses, the wireless channel/frequency and received signal strength. Duplicate observations of access points were not logged. However, separate log files were created for each street of a residential neighborhood and each floor of surveyed apartment buildings. We kept separate log files for each floor and street because it would allow us to observe the density of access point and the propagation of the wireless signals. The scan of an apartment building was conducted by walking the public hallways of each floor—never entering a private residence. The scan of a

Table 3. Encryption use in the apartment buildings and residential neighbourhoods. Reported is the number and percentage of wireless networks that use WEP, WPA and WPA2 encryption.

Area ID	*None*	*Encrypted*	*WEP*	*WPA*	*WPA2*
	n (%)	*n (%)*	*n (%)*	*n (%)*	*n (%)*
Areas [A-E]	823 (22.3)	2861 (77.7)	1863 (50.6)	679 (18.4)	319 (8.66)
Buildings F[1-6]	127 (14.7)	736 (85.3)	460 (53.3)	185 (21.4)	91 (10.5)
All	**950 (20.9)**	**3597 (79.1)**	**2323 (51.1)**	**864 (19.0)**	**410 (9.02)**

residential neighborhood was conducted using a vehicle driving each street at approximately 12km/hr. The size of the areas driven within each neighborhood is approximately one square kilometer.

In total, we surveyed 6 different areas of Toronto (which we refer to as Areas A-F). Five of the residential neighbourhoods that we surveyed (Table 1: identified as Area-[A-E]), include a mixture of both urban and suburban areas comprised of detached and semi-detached homes between 10-45 minutes from the city centre. Neighborhoods Area-B and Area-E are acknowledged as upper class, having a higher level of income than Area-A, Area-C and Area-D. The sixth area (F) was a high density area of the downtown core which consisted primarily of apartment buildings. In Area F, we surveyed six apartment buildings (Table 1: identified as Building-F[1-6]) which were constructed between 1976 and 2007. These apartments include a total of 136 floors and approximately 1800 individual units.

In the remainder of this section, we present our analysis of the survey data, focusing on overall encryption usage, the influence of manufacturer and dwelling type of encryption usage, and the density and configuration of access points. Overall, a total of 4623 unique Access Point (AP) MAC addresses were observed during our wireless scans, 4574 of which we used to create our data set. We removed 76 of the APs from the data set because they are APs owned and operated by local wireless network service providers, and not APs used for a home network. We observed 863 unique APs in the six apartment buildings (863/4574; 18.9% of our overall dataset) and 3684 unique APs in the five residential neighborhoods (3684/4547; 81.0% of our overall dataset; Table 2).

3.1.1 The Majority of Networks Use Encryption

The majority of home APs (3597/4574; 79.1%) we observed used encryption, a result contradictory to prior research that suggests the majority of wireless network do not use encryption [2]. As presented in Table 3, the type of encryption used varied, with WEP (51.1%) being used significantly more than WPA (19.0%) and WPA2 (9.0%). Subsequent follow-up interviews with network caretakers (discussed in Section 3.2) revealed that WEP is most commonly used because one of more devices on the network does not support WPA/WPA2 and that the higher levels of encryption are not perceived necessary for their home networks.

3.1.2 Apartment Buildings Use Encryption More Frequently than Residential Neighborhoods

There is a significant difference $[\chi^2 (8, N=4574)=101.7, p<0.001]$ in encryption use (Table 3) between apartment buildings and residential neighborhoods. The APs in apartment buildings use encryption more frequently (736/863; 85.3%) than those in the residential neighborhoods (2861/3684; 77.7%). We postulate that the greater use of encryption for APs in apartment buildings is due in part to the higher density of visible networks and people.

The networks in Area-E are a noteworthy exception because of the extremely low density of houses in this area. The number of networks is approximately equivalent to the number of houses. Chetty *et al.* [6] reported that one of their participants did not use encryption because s/he perceived the distance between their house and the road as providing adequate protection. We believe that the extremely low use of encryption (52.6%) in Area-E is due in part to a similar reason—the physical distance between dwellings and access roads affords a perception of security.

3.1.3 Manufacturers' Default Settings Influences Encryption Use

We cross-referenced the collected set of AP MAC addresses with the IEEE OUI registration database [13] to identify the manufacturer of the observed devices. The six most frequently observed AP manufacturers were Cisco-Linksys, D-Link, Apple, 2Wire, Netgear, and Belkin; representing roughly 75% of all networks we observed. The data we gathered showed that the device manufacturer is a strong influence on the use of encryption and the type of encryption used. APs manufactured by 2Wire, Inc. (98.7%) and Apple (89.7%) use encryption more commonly than Cisco-Linksys (76.5%), D-Link (74.7%), Netgear (77.2%) and Belkin (75.2%). Apple base stations also have the highest percentage of WPA2 encryption (48.0%) followed by Belkin (12.5%). Similarly, 2Wire APs have the highest percentage of WEP encryption (89.6%) followed by D-Link (52.5%).

The differences in use of encryption and the type of encryption used suggest that the manufacturers' default setting and out-of-the-box configuration procedure has an impact on how a network is configured. We classified 507 of the 4574 (11.1%) networks as configured using the default, out-of-the-box configuration. Using the MAC addresses, we determined that these networks had vendor specified default SSIDs, and were not using any form of encryption. The default SSIDs and encryption settings were determined using the product manuals publically available on manufacturers' websites. Although there is no way to determine the exact model for each AP using just the MAC address, we examined three or more manuals for each manufacturer to determine the default setting for their devices. For example, we were able to identify: "default", "linksys", "dlink", "SMC", "belkin54g", "NETGEAR" and "TRENDnet" as having no encryption out-of-the-box. We recognize that our classification method is not perfect, as we did not attempt to access each network to determine if MAC filtering or other protection mechanisms were being used. However, we posit that the number of users who would go to the trouble of configuring MAC filtering, yet not configure the SSID and network encryption

would be low. Additionally, we found a number of networks (255/4574; 5.57%) that used an ISP-provided network name. These devices had been configured to use WEP encryption out-of-the-box and the ISP had printed the default WEP key on a sticker on the top of the device. From our data, most of these users (89.6%) had likely continued to use these settings, despite WEP's inherent weaknesses. These results affirm our qualitative studies on users' security needs (discussed in Section 3.2) and their likelihood to use any form of encryption as long as it did not impact on the usability of the network.

3.2 Interviews with Network Caretakers

Equipped with more information about the wireless landscape across the city, we performed an in-depth, semi-structured interview with the caretakers of home networks. To develop an initial understanding of participants' home networks, we developed a paper questionnaire which asked participants to list all the devices that operate on their networks, draw the current configurations of their networks with respect to the devices they listed, describe the ideal configurations of their home networks and rate how difficult each device is to configure. We also provided the participants with a paper questionnaire surveying: their perception of network protection techniques; the importance and effectiveness of each method (5-point Likert scale); and, which protection techniques they currently use. Protection techniques included: firewalls, antivirus software, network encryption (WEP, WPA, *etc.*), MAC address filtering, network access lists, and VPNs (virtual private networks).

Upon completion of the survey, we conducted a semi-structured interview with each person. We used each participant's responses from the survey as the initial points of discussion during the interviews. We asked participants questions that explored planning and network setup; the devices used and their location around the home; the physical and virtual security boundaries they established and justification for their wireless network name. Next, we asked questions about the maintenance and change process, any documentation they maintain, performance issues they experience, sources of interference and other frustrations. Participants were asked to refer back to information they provided in the surveys and encouraged to give examples of their experiences with their home networks. All interviews were recorded and then transcribed with participant consent. At the end of the interview, a disposable camera (to take pictures of their networking equipment) and a prepaid envelope (to return the surveys and camera) were given to participants.

We recruited 18 participants (12 male, 6 female) using advertisements placed in the community (*e.g.*, areas that we had previously scanned) and on social networking sites. Participant age varied from 18 to 65. The 18 participants were active caretakers of 20 home networks. Two of the participants were students and identified two primary residences; their paternal home, and their residence used during the school year. Three people we interviewed also informally set up other people's networks as well as their own. In total, the 20 networks officially serviced approximately 60 people. We compensated interview participants $15 for their time.

Interview participants lived in different dwelling types, ranging from high-rise apartment buildings to single detached homes. These dwellings were in the downtown core of a major Canadian metropolitan area, its midtown, as well as the suburbs. The participants' proficiency with their network varied. Two of the participants were IT professionals, and as such they were proficient in configuring their own network. The participant pool also included those who work as social worker, lawyer, poker player, archivist, music student, *etc.* Seven were network novices who depended on others and IT professionals to configure their network for them. The size and complexity of networks varied from simple three device networks (a wireless router and two laptops) to complex configurations ($\bar{x}$ =6.3 devices, SD=2.24) that consisted of multiple desktops (some wired, some wireless), home media servers, VoIP adapters, USB and networked printers (wired and wireless), gaming consoles (wired and wireless) as well as wireless bridges designed to extend network reach.

In the remainder of this section, we present the results from our interviews with network caretakers. We use descriptive statistics to present and discuss the quantitative survey data. We tabulated the Likert scale survey data from the 18 interview participants and nine household occupants to analyze how important and effective they perceived different home network protection technologies to be and to determine whether any correlation existed between these perceptions. Three researchers transcribed and analyzed all the interviews and performed qualitative analysis to identify trends in the data.

3.2.1 Network Security and Encryption

A positive correlation between perceived importance and effectiveness was found with Spearman's rank order correlation coefficient (p=0.01) for firewalls. This correlation also existed for antivirus, network encryption and VPNs. Participants gave the highest rating of both importance (=4.48) and effectiveness (=4.05) to antivirus software. This was followed by firewall importance (=4) and effectiveness (=3.95).

A large majority of the participants (16/18) claimed they recognized the importance of securing their network and use some type of encryption. However, a few of these participants also stated that they thought a malicious user would be able to break this encryption:

> *"…it's a cognitive dissonance thing…security, encryption…we should probably do that, but they say people can crack it anyway…"*

Several participants even reported trying simple passwords on neighbors' secured networks, and reported success with using "password", "admin" or "pass" on these networks:

> *"So you learn. 'RTC' has no password… that [another network's SSID]'s password is 'admin'…"*

Despite their own successful attempts to connect to networks they were not authorized to use, some participants believed that a simple encryption key was sufficient and reported using their phone number as an encryption key. A few participants expressed frustration that some devices they owned forced them into using WEP encryption instead of the stronger WPA2 standard, even though they were using unsophisticated or easily guessable encryption keys.

Not surprisingly, it seemed that the convenience of provisioning network access was more important than a strong sense security:

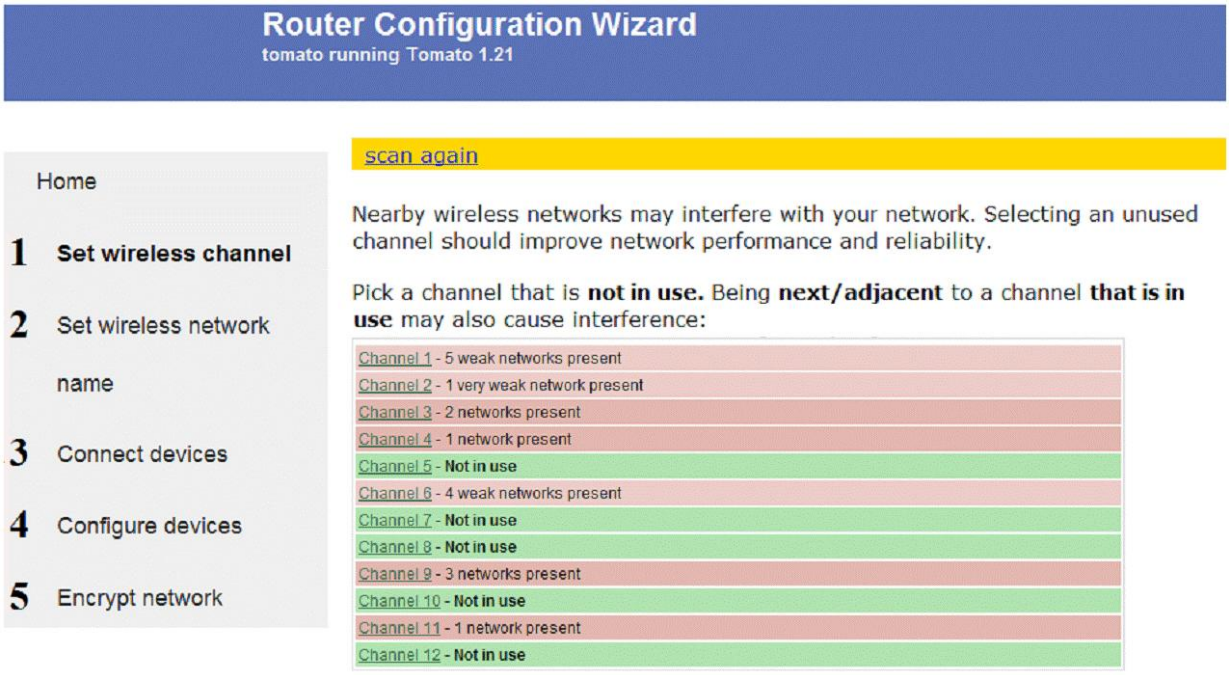

Figure 1. Our prototype wizard, which ran entirely inside a web browser and helped users configure their router securely.

"I just don't want to be the lowest fruit on the tree. If it shows as encrypted, that's good enough for me…"

In contrast, the IT professionals we surveyed (2/18) clearly understood the difference between the two. These participants reported that they used both MAC filtering and WPA2 (AES) encryption with a strong encryption key. They also would remove temporary MAC entries once a guest had left, and one had even gone so far as to purchase a WPA2 capable network bridge for a WPA2-incapable device, so that he would not have to switch his network to WEP.

3.2.2 Network Naming Practices

Similar to previous research which examined how users named their Bluetooth-enabled mobile devices [12], we also learned that people selected names for their network in interesting ways. For example, some participants reported selecting names from popular movies and television shows to separate their network from others, while others used "SmithNet" because "it's mine". In the latter cases, the need to keep their network distinct effectively had turned their network name into a signpost, often including their name. Another participant chose to take this a level further and established additional structure to his network naming scheme: "BC2301-Donald", where BC was an abbreviation of his building name, 2301 was his suite number, and Donald was his last name.

3.2.3 Access Control List vs. Encryption

Some participants appear to perceive access control and encryption as a similar component of security. Only IT savvy participants (2/18) clearly understood the difference between the two. They used both MAC filtering and strong encryption. These two participants also kept frequent guests in the MAC address table, but reported that they removed temporary entries once a guest had left.

The remaining participants did not understand the notion of a MAC address (16/18). They did not use an access control list (ACL) to keep unwanted users off their home network. Instead, participants reported using a "password" (*i.e.*, their encryption key) to protect their network against unauthorized users.

4. A NOVEL ROUTER WIZARD

Few participants reported utilizing all the features of the firmware but instead relied on the out-of-box wizard for the entire process. Most users did not have a clear understanding of advanced features (for example, how encryption and access control mechanisms differed). These functions often were not used in the participant's home network settings because most commercial wizards do not configure such functionalities on these devices; however, these features do exist within their router's set up menus. When the system does not provide users with guidance and recommendations for added security, most networks are set up with only the most basic settings, often using blank or default choices. For example, current encryption key fields are simple text fields that make it difficult for the average user to configure their network securely, even if they were willing to put in additional effort.

4.1 High-Level Design Goals

We modified a router firmware to include a wizard that exposes functionality and attempts to automate the configuration process, leveraging all available security techniques currently available, while keeping the entire process simple and accessible to our users (Figure 1). The goals were to design a set of steps which provided the user with not only clear explanations of the various security functionalities to allow a user to make informed decisions but also seed the system with sample configuration settings that are secure. For example, any text fields that require user input (SSID, encryption key, *etc*.) should encourage secure settings and

Figure 2. Our prototype wizard displayed a list of connected computers and allowed users to grant access to the network via MAC address filtering. The MAC address was automatically collected from connected devices and did not require users to type this information manually.

make the process of securing the network as easy as possible (*i.e.*, by offering to randomly generate encryption keys). Specifically, our design:

- Encourages users to set network names and encryption keys that do not contain personally identifying information such as their name, address or telephone number. Instead, the system auto-generates plausible network names by coupling randomly selected dictionary words, and encourages the use of randomly generated encryption keys. This design specifically addresses cases where the user often uses personally identifiable information (and furthermore derivable information) in both the network name and the encryption key.
- Automates the process of transferring a long encryption key to devices. The system minimizes any tedious work that may arise as a result of strong security settings such as manually retyping a long encryption key.
- Encourages the use of MAC address filtering (Figure 2) which allows users to consciously choose which devices they want to have access to their network.

4.2 Implementation Detail

We based our wizard on Tomato 1.21 (polarcloud.com/tomato) and the open-source Linksys firmware for the Linksys wireless router, model WRT54GL. This is a standards compliant IEEE 802.11 b/g wireless router with 4-port 10/100 switch. Our prototype wizard was completely web-based and encourages random network name selection (returns a random dictionary word each time), strong encryption settings (WPA2 with AES) using a strong encryption key (randomly generated key 63-characters in length) and provides a mechanism for users to capture and explicitly authorize MAC addresses of devices they recognize and wanted to permit on the network.

Although most HTML frames and CGI-powered wizards typically used in routers cause a loss of context between wizard steps, we used AJAX based calls to the router, eliminating the need to reload pages, even between steps that required a router reboot. This ability to maintain user state in the browser made our wizard much more predictable and allowed users to navigate back and forth between steps without worry. This web-based wizard also meant that there would not be a CD that would need to be found again when configuration changes needed to be made.

Our wizard supports a new method for configuring the home network. Specifically, this new method is comprised of the following steps:

1. Channel selection

The router automatically scans for nearby wireless networks and displayed a list of networks that it detected, and instructs the user to select a channel that was not already in use (Figure 1). This step was designed to minimize the amount of interference and hopefully improve network reliability.

2. Network naming/SSID

The wizard encourages the naming of the network (Service Set Identifier or SSID) with impersonal information. The wizard displays names of nearby wireless networks, four random dictionary words, and a suggested network name that combines two randomly selected words from a dictionary. A sample network name might be, "Cereal bowl". By randomly selecting words from the dictionary instead of providing a default such as "linksys" or "dlink" we wanted to encourage the user to select a name that was unique, yet did not personally identify them[1]. As the passphrases in WPA/WPA2 are hashed using the SSID as one component, crackers have pre-computed billions of dictionary-based keys for typical default SSIDs such as "linksys" and selecting a non-standard network name dramatically increases the security of a wireless network [7].

3. MAC address collection

We designed the wizard to allow users to explicitly permit devices onto their network–a process which captured the physical MAC address of all connected devices, and allowed the user to either permit or deny a specific device from accessing the network (Figure 2). With the SSID configured in the previous step and the network still unencrypted, the system then instructs the user to search for and connect to the network they created. Once devices are connected, the wizard displays a list of connected devices showing the computer/device name, IP address and MAC address. The user checks "allow" next to each device they recognize and want to permit onto the wireless network.

4. Enable MAC filtering

The user then enables MAC filtering so only devices selected in the previous step would be connected to the network.

[1] In our proof-of-concept implementation, a simple dictionary of ten words was put into the wizard, from which four random words were selected each time and used as suggestions for the network name. A full implementation would need to increase the dictionary size to several thousand words at a minimum to ensure a reasonable amount of randomness and prevent collisions. SSIDs can also be augmented with other tokens, such as MAC addresses to maintain uniqueness.

5. Encryption selection

Next, the wizard asks the user to select the encryption method and to specify an encryption key. The wizard encourages the use of strong security by being secure by default. The wizard offers WEP 64 bit, WEP 128 bit, WPA with AES and WPA2 with AES as possible options. The wizard strongly recommended WPA2 by listing it as the default setting. If the user has compatibility issues with using WPA2 on all her devices, the system then suggests WPA. The system tells the user to avoid using WEP because "it is easily compromised". Additionally, a randomly generated key of maximum length is automatically generated but the user is given the option to manually type in an encryption key as well, if they so choose.

6. Transfer encryption key to devices

Although long encryption keys are typically avoided by users because of the overhead incurred in manually transferring the key to their devices, we designed the wizard such that devices can easily employ the strongest encryption by publishing the key on a secure webpage. Before encryption is enabled the user is instructed to load the secure webpage on all the devices they want to connect to the network. When the user loads the website and authenticates the encryption method and key are displayed, and instructions are provided for how to copy the key into the clipboard of the device they were using. This eliminates the need for a manual key transfer.

7. Enable network encryption and reconnect devices

The router then enables encryption. The wizard then instructs the user to search for available networks, and reconnect them to the wireless network. This time, the network would appear as secured. When a device tries to connect with the network, the user would be asked to paste in the encryption key from the previous step. We believe that the brief exposure of the encryption key to the network is an acceptable risk, given the increase in security that is achieved in return. We argue that the combination of MAC filtering (permitting only authorized devices onto the network,) SSL encryption and the webpage authentication requirement (using the router administration username and password) is sufficient protection of the network encryption key. The brief period of time during which this information is published allows users to quickly transfer this information without having to resort to out-of-band methods (*i.e.*, saving the key to a text file on a USB key). Unlike with a USB key, this webpage publishing method exposes the key for only a certain amount of time as the page is disabled after the process. For future maintenance purposes, the page can again be quickly re-enabled to facilitate the transfer of the information to new devices.

Although the randomly generated key may not be memorable we are able to achieve higher network security, with a minimal increase in the difficulty of transferring the key. As the router assists the user in the key transfer process, it is not necessary to store the encryption key and network settings anywhere – the maintenance wizard can aid in the addition of devices in the future. Some commercial products typically recommend WPA for compatibility reasons. The prevalence of devices which do not support the latest encryption standard is outside of the scope of this paper, however, we looked at which encryption method users preferred, when given the choice.

To add new devices, the user simply needs to restart the wizard from step 3 onwards. The router saves the list of previously permitted MAC addresses and encryption settings. However, it disconnects all devices that are permitted (and currently connected) and blocks access to the secure webpage publishing the encryption key. The user then needs to specify which new devices are allowed to access the network before re-enabling MAC filtering. The router then reapplies the previous encryption settings in step 5.

5. EVALUATION METHOD

We recruited 18 participants to configure a wireless router three times, each time using a different configuration method. For the configuration process, a desktop computer running Windows was hardwired into the router, and the respective router wizard or UI was used each time. Once the router was configured, we asked participants to configure a Lenovo S10 Netbook running Windows, an Apple MacBook Pro running Mac OS, and a WiFi-capable Nokia N95 cellphone onto the network. We included the Nokia N95 because we recognize that not all mobile devices support copy and pasting and wanted to examine the impact this might have on security choices.

Participants were first acquainted with each of the devices, shown how to connect to a wireless network, as well as how to open a web browser to test internet connectivity. Participants also had the option to use an external USB mouse if they felt uncomfortable with the touchpad available on the two notebooks.

The three router configuration methods were as follows, with the presentation order counterbalanced across participants:

A. Linksys Router Web Interface – this baseline condition was used to provide some measure of a participant's technical competency as it provides no wizard to assist the user in configuration. Instead, all the configuration settings are provided in a variety of tabs (Figure 3). This interface is suitable for expert use, but beginners may find it daunting and confusing.

B. Linksys Router Configuration CD – Linksys provides an in-box CD which contains a wizard (Figure 4) that directs users on how to connect networking cables, change the default router password, and configure a network name, encryption type and encryption key. We did not compare against the Cisco Valet (which uses a USB dongle to configure network settings) because the Valet line of products was released after our study. It is important to note that although the USB dongle included with the Valet can assist in configuring desktops and laptops, it cannot assist configuring mobile or embedded devices.

C. Prototype Wizard – Our prototype wizard was modeled after the Linksys wizard, but allows the user to explicitly provision access for particular devices, encouraged the selection of a network name that was a random dictionary word, and pre-generated a random encryption key. This wizard helped users transfer this randomly generated key to all their devices by instructing them to copy and paste the key from an SSL and password secured webpage.

Figure 3. The Linksys router Web interface exposes all of the routers functionality but provides very little in terms of assistance or guidance. This interface is designed for expert users.

We asked participants to configure the router as if it was for their home. In doing so, we were able to understand if a secure configuration is a goal of the users and when our system resulted in a more secure configuration than the two other methods. Because we were interested primarily in a qualitative understanding of the steps that participants would perform to configure their network, we did not record quantitative metrics such as task completion time and click count.

6. EVALUATION RESULTS

Two of the 18 participants were unable to configure the router successfully for all three router conditions. These two participants are excluded from the analysis.

Carryover effects were seen with network naming practices, encryption method as well as the network encryption key selection. We also observed users who attempted to implement MAC address filtering on their own, but were unable to accomplish this using the Linksys Web interface.

6.1.1 Network Naming Practices

With the Linksys Web firmware or Linksys CD wizard, users typically did not change the default "Linksys" network name (14/16 and 7/16, respectively; see Table 4). In contrast, the prototype wizard randomly generated a wireless network name from a local dictionary by combining two dictionary words. For users who opted to specify their own name, the prototype wizard suggested that the name should be unique yet not personally identifiable. This resulted in a network name that was unique (and thus instantly recognizable to users) while still providing stronger security, when compared to names such as "linksys". In situations where the prototype wizard was used first, 3/6 users chose the same name in the subsequent Linksys Web wizard. None of the participants attempted to hide the SSID.

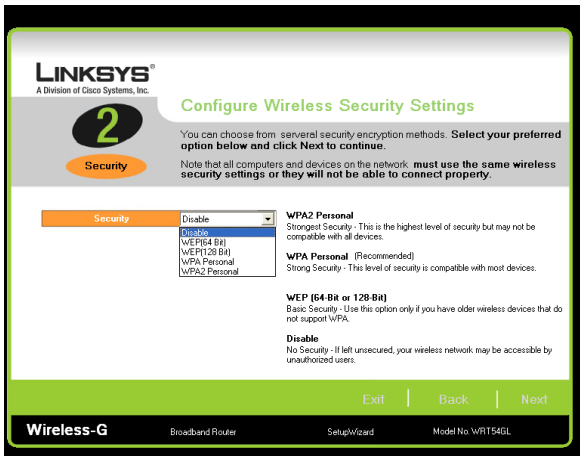

Figure 4. Designed for the novice user, the Linksys wizard runs off a CD and is designed to ensure a user configures all the necessary settings on their router, including: changing the router password; setting the network name; selecting an encryption type; and selecting an encryption key.

6.1.2 Encryption Method

With the prototype wizard (C), all but one participants used WPA2 (15/16). The one participant who selected WEP confirmed that he did this because he felt that this was the most secure.

> *"[WEP]… I use [this] at home… it's the most secure."*

When using the Linksys CD wizard, the majority of users (10/16) selected the recommended WPA encryption method and 5/16 selected the stronger WPA2. All of these five had previously seen our wizard in the study, and subsequent interview questions confirmed that in all cases, these participants had selected WPA2 since the stronger method had been previously recommended by our wizard. This indicates the effect of the default settings and recommendations made by a router interface.

A few users mentioned the lack of information (5/16) about the effectiveness of encryption methods when using these wizards.

> *"It would have been nice to have a glossary of these terms…"*

We believe that with further education users will improve their network security practices. Two participants (2/16) chose WEP because it is the type of encryption used in their workplace. This is a particular concern because it shows that users will mimic the security they perceive implemented by the IT professionals that manage their at work network without fully understanding the possible other measures implemented but not visible. In addition, it highlights the need for these networks to use strong and effective technologies that are openly disclosed to their proper users:

> *"I trust what the professionals do… I will do my banking at work where the network is definitely secure…"*

Table 4. Configured network names for each condition. The Dictionary Word was technically a default setting, but this randomly selected word improved security when compared to static router defaults, or routers which augment network names with device MAC addresses.

Condition	*Router Default (i.e., linksys) n (%)*	*Dictionary Word n (%)*	*User Specified n (%)*
Linksys Web	**14 (87.5)**	0 **(00.0)**	2 (12.5)
Linksys CD	7 (43.8)	0 (00.0)	**9 (56.3)**
Prototype Wizard	0 (00.0)	**9 (56.2)**	7 (43.8)

Table 5. Configured network encryption methods under each condition.

Condition	*Unsecured n (%)*	*WEP n (%)*	*WPA n (%)*	*WPA2 n (%)*
Linksys Web	**14 (87.5)**	0 (00.0)	1 (06.3)	1 **(06.3)**
Linksys CD	0 (00.0)	1 (06.3)	**10 (62.5)**	5 (31.3)
Prototype Wizard	0 (00.0)	1 (06.3)	0 (00.0)	**15 (93.7)**

Table 6. Configured network encryption keys under each condition.

Condition	*None n (%)*	*Randomly Generated n (%)*	*User Specified n (%)*
Linksys Web	**14 (87.5)**	0 (00.0)	2 (12.5)
Linksys CD	0 (00.0)	0 (00.0)	**16 (100.0)**
Prototype Wizard	0 (00.0)	**12 (75.5)**	4 (25.0)

6.1.3 Encryption Key Selection

The prototype wizard included a function to "generate [a] random key" as well as the ability to transfer the encryption key to other devices on the network via a password protected webpage—eliminating the need to manually type the encryption key on all devices. The majority of participants (12/16) generated a random key and commented that they liked this automatic function:

> *"I liked the random key… [because it] made it seem more secure. A hacker would never guess that…"*

The remaining participants (4/16) chose passwords that they already used on their home network, or passwords they used elsewhere:

> *"I can remember this password since I use it elsewhere"*

A minority of participants (5/16) used an encryption key that is a variation on their name. Of these, only one participant (1/5) had previously seen our prototype wizard. This suggests that users who had been exposed to the random password generator were less likely to use their name as the encryption key even with other router firmware.

Finally, with our prototype wizard, two participants (2/16) experienced difficulty transferring the encryption key to the devices using the secure webpage. In these cases, the participants manually typed the encryption key into the devices and the follow-up interview confirmed that while this was more work, the added level of security was worthwhile to them:

> *"I don't mind typing the long password… only have to do it once…"*

6.1.4 MAC Address Filtering and Device Provisioning

Using the prototype wizard, all of the participants (16/16) successfully enabled and configured MAC address filtering. Several participants explicitly mentioned the process of permitting a particular device access to the network as "very logical". In contrast, MAC address filtering was not enabled and configured by any of the participants (0/16) using the Linksys interfaces. However, three participants (3/6) who used the prototype wizard prior to another wizard attempted to enable MAC address filtering using the Linksys Web interface. These users explored the "Access Restrictions" page heavily, but were unable to successfully locate the correct page in the UI to configure the MAC address filtering.

We recognize that MAC addresses are easily spoofed, but we believe the added feedback (to confirm that the device was successfully connected to the router) encouraged participants by reassuring them that they were completing the steps successfully. More importantly, participants reported that the ability to permit only specific computers onto the network was something they valued, especially when they saw an unknown computer in the list:

> *"Oh, that must be a bad computer, because it's not one of these ones here…"*

While not currently implemented in the prototype wizard, additional functionality can be added to permit the maintenance of devices on the network, which would facilitate the process of adding and removing devices from the network.

6.1.5 Difficulties with Terminology

Participants (7/16) experienced difficulties with the network terminology used by their devices as well as the wireless router wizards. Terms such as "WEP password", "WPA password" (Mac OS), "encryption passphrase" and "encryption pre-shared key" (Linksys CD) are used interchangeable across different devices, leading to confusion. As a result, some participants entered the

router web administration password (3/16), the network name (2/16) or their router's MAC address (1/16) which was printed on the bottom of the router when asked for a "WPA password":

"Network name? Maybe that's the stuff written on the bottom (referring to MAC address)"

"WPA password? Is that the router password? I have a pre-shared key and a router password, so which one is it?"

6.1.6 Router Preference

The majority of participants (10/16) preferred the Linksys configuration—six preferred our prototype wizard. Despite the greater level of security provided by the prototype wizard, the wizard required more steps to configure successfully and the participants cited this as their reason for choosing the Linksys wizard. For example, although the resulting network configured by the stock Linksys firmware was not secure enough for one participant, she liked the fact that it came pre-configured and that no settings needed to be changed on the router before the internet was accessible on the devices. Given the participants' choice it is evident that further work is needed to improve our firmware wizard. Nevertheless, all 16 participants who successfully configured the router using the Linksys CD wizard were also successful at configuring the router using the prototype wizard.

6.1.7 Summary

Almost all (16/18) of the participants were successful in configuring the network using all three methods. The two that failed were unable to configure the router using the two Linksys interface or the prototype wizard.

Of the 16 who were successful, users of the prototype wizard had either selected a random dictionary word or manually specified an SSID. In contrast, nearly half (7/16) of the Linksys CD wizard users used the default SSID of "linksys" which has been shown to reduce network security.

MAC filtering was used successfully by all participants when using the prototype wizard (16/16). The users who were exposed to the prototype wizard prior to either existing router wizards were seen to attempt to find the same functionality in the Linksys Web interface, albeit unsuccessfully.

Nearly all (15/16) of the participants used the stronger WPA2 encryption with the prototype wizard, compared to only five (5/16) with the Linksys CD wizard. All 5 of these participants had previously seen the prototype wizard, showing the impact that the prototype firmware had on users.

The majority of participants (12/16) used a randomly generated encryption key, which dramatically increases the effectiveness of WPA2 encryption. This also illustrates the amount of effort that users are willing to exert to secure their property and users recognized that the additional effort was worthwhile. Finally, we observed confusion around the terms and phrases used across the devices and routers, which we believe is a problem that needs to be addressed.

7. CONCLUSIONS & FUTURE WORK

Wireless networks are common in the modern day home. Our study on the practices of home network caretakers has shown that although the majority of home networks employ encryption, participants often default to using the most basic settings supported by the router's configuration wizard. Rarely, do users maintain and install highly secure encryption keys across their devices. Furthermore, few perceive a difference between encryption and access control lists and few modify the access control lists to prevent unwanted devices from accessing their home network. Because we noticed that equipment from certain manufacturers have a significant impact on the likelihood of encryption usage than equipment from others, we believe that strong network security choices and practices can be encouraged by improving the configuration steps that users must perform when they set up their devices.

In this work, we designed and evaluated a modified router firmware which supports a new set of steps for configuring the home network. The prototype router wizard provided the user with recommended configuration choices that are dynamically generated by the system rather than a blank or predefined default option. An auto-generated 63-character WPA2 AES encryption key is transmitted automatically via a SSL-encrypted and password secured webpage to all the networked devices that are to be configured. In addition, the Mac addresses of these devices is recorded and automatically applied to the address filtering rules.

The majority of participants we studied were able to successfully configure the test network using all three methods. Our prototype wizard encouraged participants to select a random dictionary word or manually specify an SSID, whereas nearly half of the participants used the default "Linksys" SSID when using the Linksys CD wizard. Furthermore, with the prototype wizard, participants used the stronger WPA2 encryption when configuring the network. Additionally, participants successfully incorporated MAC filtering when using the prototype wizard, but had difficulty configuring this feature with the other interfaces. When not presented with the prototype interface prior to the Linksys interfaces, often this feature was not attempted at all; indicating that participants did not consider the need to secure their network in this way. Overall, the results suggest that the modified set of steps used in the prototype wizard made users more aware of the different security features available to them and furthermore lead to stronger security choices and practices.

A wizard that permits users to perform regular maintenance tasks was not included in our study. This prevented us from examining the full impact of the prototype wizard as we did not examine situations where users had to add a device to the network, or troubleshoot problems with their existing wireless network. In addition, we performed this study in a controlled laboratory environment and therefore did not capture the true experience of configuring a network in the home. Physical distances between devices, as well as potential interactions with other home users were not considered. Future work might consider this "whole picture" to improve the home wireless network experience.

From this work, we see a need to make network security a more tangible process by providing users with more relevant feedback about the effectiveness of their security choices. Additionally, we see a need to unify the terms and phrases used across home wireless network equipment vendors, and that networking equipment needs to provide meaningful guidance to users. Finally, we recognize that MAC address filtering is currently a non-effective protection technique against trespassers. However, we believe that the difficulty in determining a permitted MAC

address and ‘spoofing’ a valid MAC address is a deterrent for trespassers. In addition, further modifications to IP standards may help make station-based control methods appropriate in the future.

8. ACKNOWLEDGEMENTS

We thank Gillian Hayes for her feedback on earlier versions of this paper. This study was covered under the University of Toronto’s Ethics Review Office Protocol #22130.

9. REFERENCES

1. Balfanz, D., Durfee, G., Grinter, R. E., Smetters, D. K., and Stewart, P. 2004. Network-in-a-box: how to set up a secure wireless network in under a minute. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13* (San Diego, CA, August 09 - 13, 2004). USENIX Security Symposium. USENIX Association, Berkeley, CA, 207-221.
2. Berghel, H. 2004. Wireless infidelity I: war driving. *Commun. ACM* 47, 9 (Sep. 2004), 21-26.
3. Bly, S., Schilit, B., McDonald, D. W., Rosario, B., and Saint-Hilaire, Y. 2006. Broken expectations in the digital home. In *CHI '06 Extended Abstracts on Human Factors in Computing Systems* (Montréal, Québec, Canada, April 22 - 27, 2006). CHI '06. ACM, New York, NY, 568-573.
4. Calvert, K., Edwards, W. and Grinter, R. 2007. Moving toward the middle: the case against the end-to-end argument in home networking. In *Proceedings of the 6th ACM Conference on Hot Topics in Networks* (Atlanta, GA, November 14-15, 2007). HotNets-VI. ACM, New York, NY.
5. Cam-Winget, N., Housley, R., Wagner, D., and Walker, J. 2003. Security flaws in 802.11 data link protocols. *Commun. ACM* 46, 5 (May. 2003), 35-39.
6. Chetty, M., Sung, J., and Grinter, R. E. 2007. How smart homes learn: the evolution of the networked home and household. In *Proceedings of the 9th international Conference on Ubiquitous Computing* (Innsbruck, Austria, September 16 - 19, 2007). Ubicomp '07. Springer-Verlag, Berlin, Heidelberg, 127-144.
7. Fleishman, G. 2008. GPU-based WPA/WPA2 crack struggles with good passwords. Retrieved June 9, 2010 from Ars Technica: http://arstechnica.com/news.ars/post/20081201-gpu-based-wpawpa2-crack-struggles-with-good-passwords.html
8. Fluhrer, S. R., Mantin, I., and Shamir, A. 2001. Weaknesses in the Key Scheduling Algorithm of RC4. In *Revised Papers From the 8th Annual international Workshop on Selected Areas in Cryptography*. Springer-Verlag, London, 1-24.
9. Geer, D. 2005. Malicious Bots Threaten Network Security. *Computer* 38, 1 (Jan. 2005), 18-20.
10. Grinter, R. E., Edwards, W. K., Newman, M. W., and Ducheneaut, N. 2005. The work to make a home network work. In *Proceedings of the Ninth Conference on European Conference on Computer Supported Cooperative Work* (Paris, France, September 18 - 22, 2005). H. Gellersen, K. Schmidt, M. Beaudouin-Lafon, and W. Mackay, Eds. ECSCW. Springer-Verlag New York, New York, NY, 469-488.
11. Hartley, M. 2008. Heavy web downloaders face broadband fees. Retrieved June 9, 2010 from The Globe and Mail: http://www.theglobeandmail.com/news/technology/article675666.ece
12. Kindberg, T. and Jones, T. 2007. "Merolyn the phone": a study of Bluetooth naming practices. In *Proceedings of the 9th international Conference on Ubiquitous Computing* (Innsbruck, Austria, September 16 - 19, 2007). Ubicomp '07. Springer-Verlag, Berlin, Heidelberg, 318-335.
13. IEEE OUI and Company_id Assignments. 2008. Retrieved June 9, 2010 from the IEEE Standards Association: http://standards.ieee.org/regauth/oui/index.shtml
14. Kravets, D. 2008. MPAA Says No Proof Needed in P2P Copyright Infringement Lawsuits. Retrieved June 9, 2010 from Wired: http://www.wired.com/threatlevel/2008/06/mpaa-says-no-pr/
15. R. MacMillan. 2006. Plugged in: Wireless Networking Baffles Some Customers. Reuters News (2006, March).
16. Poole, E. S., Chetty, M., Grinter, R. E., and Edwards, W. K. 2008. More than meets the eye: transforming the user experience of home network management. In *Proceedings of the 7th ACM Conference on Designing interactive Systems*. DIS '08. ACM, New York, NY, 455-464.
17. Raja, F., Hawkey, K., and Beznosov, K. 2009. Revealing hidden context: improving mental models of personal firewall users. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. SOUPS '09. ACM, New York, NY, 1-12.
18. Rodden, T. and Benford, S. 2003. The evolution of buildings and implications for the design of ubiquitous domestic environments. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA, April 05 - 10, 2003). CHI '03. ACM, New York, NY, 9-16.
19. Shehan, E. and Edwards, W. K. 2007. Home networking and HCI: what hath god wrought? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (San Jose, California, USA, April 28 - May 03, 2007). CHI '07. ACM, New York, NY, 547-556.
20. Stoll, J., Tashman, C. S., Edwards, W., and Spafford, K. 2008. Sesame: informing user security decisions with system visualization. In *Proceeding of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy, April 05 - 10, 2008). CHI '08. ACM, New York, NY, 1045-1054.
21. Stubblefield, A., Ioannidis, J., and Rubin, A. D. 2004. A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). *ACM Trans. Inf. Syst. Secur.* 7, 2 (May. 2004), 319-332.
22. City of Toronto Demographics Information. 2008. Retrieved June 9, 2010 from The City of Toronto: http://www.toronto.ca/demographics/
23. Wang, H. 2006. Networks in the Home: Connected Consumer Electronics. *Parks Associates* (June 2006).
24. Wireless Infonetics Research, Inc. 2008. Driven by 802.11n Technology, Worldwide Wireless LAN Semiconductor Market Will Experience Double-Digit Growth Through 2012, IDC Predicts.
25. Yang, J. and Edwards, W. K. 2007. ICEbox: toward easy-to-use home networking. In Proceedings of the 11th International Conference on Human-Computer Interaction (Rio de Janerio, Brasil, September 10-14, 2007). INTERACT '07. Springer-Verlag, Berlin, Heidelberg. 197-210.