# ICEbox: Toward Easy-to-Use Home Networking

Jeonghwa Yang and W. Keith Edwards
Graphics, Visualization and Usability Center
College of Computing
Georgia Institute of Technology
{jeonghwa, keith}@cc.gatech.edu

**Abstract.** Home networking is becoming an essential part of everyday life. However, empirical studies and consumer reports indicate that the complexities of configuring and maintaining the home network impose a high barrier for most householders. In this paper, we explore the sources of the complexity of the home network, and describe a solution we have built to address this complexity. We have developed a prototype network appliance that acts as a centralized point of control for the home network, providing device provisioning and reprovisioning, security, discovery, and monitoring. Our solution provides a simple physical UI for network control, using pointing to introduce new devices onto the network, and a physical lock to secure network access. Results of our user studies indicate that users found this appliance both useful and usable as a network configuration and management tool.

**Keywords:** Home networking, usability, user interface, and ICEbox.

## 1 Introduction

Increasingly, networking technology is finding its way into the home. Recent studies, for example, indicate that 43 million households in the US have broadband access, and many of these have a home network [5]; similar trends exist in much of the industrialized world. However, despite this rapid uptake of networking technologies, there are severe user interface hurdles. Data from consumer research firms and the mainstream press, for example, cite home networking technology as *the most returned item* at "big box" electronics stores [20]; consumers typically cite complexity of installation and configuration as the key impediment to adopting a home network [15]. As recently as this year (2006), roughly a quarter of the people who purchased wireless networks returned them because they were unable to properly configure and install them [16].

The user interface hurdles posed by home networking include not just the initial problems of configuring and installing the network and the devices on it, but also the ongoing monitoring and management of the network, troubleshooting when things break, and — occasionally — reconfiguring the overall network itself (such as when the network topology or service provider changes).

The networking concepts that are exposed to home network users today are fundamentally unchanged from those that were exposed to trained system- and
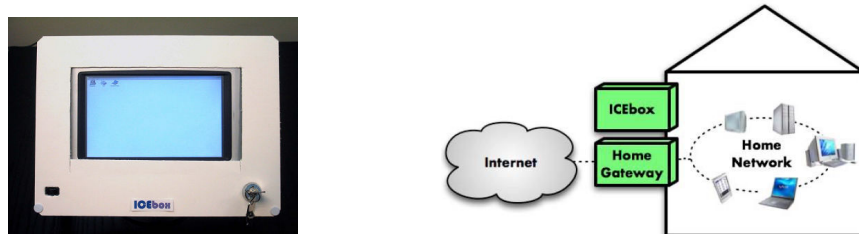
**Fig. 1.** The ICEbox hardware prototype and its location in the home network topology

network-administrators during the mid 1970's when the current Internet protocol suite was developed [3]. In order to effectively install and securely manage a network, users must understand basic network architecture (that a router separates the internal network from the external), terminology (Domain Name Service, IP addresses, ports), security (firewalls, Network Address Translation, port forwarding), and more. And while technologies such as the Dynamic Host Configuration Protocol (DHCP) [6], Zeroconf [4], and others address certain aspects of network usability, they have clearly not solved the problem, as shown by the return rates and user frustration noted above. Thus, we believe there is a need for HCI researchers to focus on new mechanisms and tools that can provide a better user experience for home networking.

Based on earlier empirical work designed to uncover problem areas in home networking, we have created a network appliance designed to reduce the complexity and increase the usability of the home network (Figure 1). This appliance, called the *ICEbox* (for *installation*, *configuration*, and *evolution* box), acts as a logical front door to the home network, serving as a central point of control for the home network, and providing a unified interface for home network management that shields the user from the technical details of the network

The ICEbox addresses common problems with device configuration, network security, and monitoring and troubleshooting. A simple physical pointing interface is used for initial client device configuration; a graphical interface combined with physical controls on the ICEbox provides access to management functions, including network security. The architecture and interface effectively minimize user interaction with client devices in the management of the network.

In the following sections we present an overview of previous work in addressing the usability issues of home networking, and use this work to motivate a discussion of the specific problems that arise in home networking, which the ICEbox addresses. Next, we describe the ICEbox system and its features. We then describe a user study, in which we examined the usability of the key features of the ICEbox. Finally we close with future research directions.

## 2 Related Work

Much of the literature from the HCI community that has explored networking has focused on improving the tools of trained administrators (e.g. [8, 24]). The emphasis on tools for use in managed networks in unsurprising given the prevalence of such networks; however, these tools are typically very technical in nature and are often

designed for "heads down" use—meaning, for use as a management console by a professional whose job it is to monitor the network. These characteristics make such tools a poor fit for home users who have neither the expertise nor the desire to manually manage the minutia of their networks.

While some empirical work has focused on the home, this work has largely focused on home *computing* rather than home *networking*. With a notable early exception [22], most of this work has been conducted in the last few years as home computing adoption has grown (see, e.g. [11, 14]). When the home network appears in these studies it is usually indirectly, through the use of networked applications (such as web browsing and home shopping) rather than the setup, management, and troubleshooting of the network itself. One exception to this categorization [13] does confirm the problematic aspects of home networking, noting that 89% of families in their study needed support from an external help desk during the first year of their Internet use.

Two empirical research studies have focused on the user experience of networking per se. These include an investigation of "early adopter" home network users [9] and an investigation into the user-visible consequences of applications that make use of discovery technology [23]. Both of these have informed the specific approaches taken by the ICEbox, as described in the next section.

In addition to this HCI-driven work, research from the networking community has also focused on new technologies, tools, and protocols to improve the user experience of home networking. PARC's Network-in-a-box (NiaB) system [2] is the work most closely related to ours. NiaB allows users to add laptops to a secure wireless network by walking up to an access point and physically pointing a laptop at it. The functionality of NiaB, however, is restricted only to secure wireless configuration. NiaB uses a short-range communication mechanism to facilitate the exchange of certificates needed for 802.1x wireless security. The goal of the ICEbox, on the other hand, is to deal with other aspects of secure device provisioning, as well as higher-level service and application configuration, and monitoring of the network.

Although NiaB uses a pointing interface based on a short-range communication mechanism similar to ours, the use of such interfaces for device identification was introduced in the GesturePen system [21]. GesturePen allows users to select devices through a pointing gesture using custom tags and a custom stylus, instead of navigating through traditional user interface widgets such as lists.

Sony's FEEL and SyncTab [18, 19] also demonstrate the effectiveness of leveraging short-range communication and direct manipulation for ease of configuration, especially for establishing connections between two devices such as a camera and a printer or a PC and a TV. FEEL uses short-range wireless data transmission to exchange information necessary for setting up a connection; users point one device at another or put two devices in close proximity to create a network connection between them. SyncTab uses synchronous actions for establishing network connections. When users want to establish a connection between two devices, they synchronously press a button on both devices.

Techniques similar to both of these have been adopted in commercial products, such as recent Linksys Access Points that use a technique similar to SyncTab. Other commercial systems have focused on techniques that, while more cumbersome than the physical pointing or button interfaces, can provide a degree of automatic

configuration. For example, Windows Connect Now (WCN) [17] provides an alternative mechanism for home wireless configuration in which users run a Wireless Network Setup Wizard that configures their computer for a new wireless network, and saves the configuration details on a USB key. Users then use the USB key to update the settings of the wireless access point and to set up other computers. While WCN clearly simplifies the process of setting up a wireless network, it only deals with basic SSID and WEP key provisioning for wireless networks. Further, it requires significant interaction (running the Wireless Network Setup Wizard) at each device.

In addition to these systems, there are a number of technologies that try to remove all user interaction from certain aspects of network configuration, including the Dynamic Host Configuration Protocol (DHCP), the Simple Service Discovery Protocol (SSDP) used by UPnP [7], and Zeroconf [4]. While all of these technologies share a similar focus on removing the complexity of configuration, they only deal with a small subset of the overall networking problem. They do not, for example, deal with lower-layer configuration details (such as link layer or physical layer configuration, including WiFi provisioning), trust associations (such as WEP keys, 802.1x certificates), nor higher-layer application defaults (such as printers or file shares). They also do not provide monitoring functionality that may be necessary for users.

We build upon the approach taken by NiaB, FEEL, and GesturePen by also using a short-range pointing technique to bootstrap device associations. In our case, this pointing interface is layered on an extensible introduction protocol amenable to other interaction techniques (such as the USB key mechanism used by WCN). Further, however, we *extend* all of these systems by going beyond initial network-layer configuration to provide a host of functions for link-, service- and application-layer configuration, and ongoing network monitoring.

## 3 Home Networking: What's The Problem?

This section discusses the key usability problems inherent in home networking today. Our description of these problems is based in analysis of earlier empirical studies undertaken by our group [9, 24]; here we report only on the high-level findings from these studies.

One of the primary sources of complexity concerns correctly **provisioning devices** for the home network. This task involves configuring or adapting devices to the particular circumstances and context of a specific home network, and includes not just network-layer configuration, but also higher-layer details of the home network, such as which printer to use and where file shares reside. Provisioning is especially arduous, as it requires not just knowledge of how to operate the new client device, but also the *particulars* of the home network it is joining (what form of security—if any—is used on this network? What form of addressing? What is the network's topology?). Many of these details are hidden from users, leading to problems with setting up new devices correctly. The difficulty of provisioning suggests that removing as much of this manual work as possible from the user is essential to improving network usability.

In addition to initial setup, another particularly troubling aspect of provisioning is that it is also *fragile*. Any **change to the topological structure** of the network, for instance, adding a new access point for example or change of Internet Service Provider, may necessitate *all existing clients* being reprovisioned to work on the reconfigured network. Likewise, tasks such as swapping out a printer require that the existing machines on the network be reconfigured to know about the new device

The creation and management of **security and trust associations** are likewise problematic. Few networks in our studies had strong security (no 802.1x or MAC access controls, for example). Several participants had no wireless security enabled at all. Of course, with most commercial access points, householders can connect to the Internet without configuring any security at all. This suggests that any secure networking solution must be as easy to use *or easier* than using no security at all. The heavyweight and static nature of most network security technologies also conflicted with users' desires to support visitors or neighbors. Many in our studies expressed a desire to allow network access (perhaps transiently) to visitors or to neighbors. This need suggests that more lightweight security mechanisms are required, especially ones that can grant selective access to network resources, potentially with the ability to revoke access. These mechanisms must again be as easy to use as not, or householders will be unlikely to take advantage of them.

**Ongoing network and device monitoring** is another problematic area for home users. While few users outside of hobbyists *want* to do this work, it is occasionally necessary. Especially since users may have enlisted help from a friend or neighbor to set up their networks, they may not have any clue about how to repair the network if it stops working. The logical and sometimes even physical infrastructure of the home network is often invisible to its users. This invisibility makes it hard to check home network status and is also problematic at the time of troubleshooting. This suggests that we need tools that can support visual monitoring and management of the home network, designed not for constant use, but for occasional use during troubleshooting.

Lastly, even technologies designed to simplify network management may break down in complex networks. For example, current multicast-based **discovery protocols** do not cross link boundaries. This was apparent in a number of our subjects' homes, notably when trying to set up music streaming between wired and wireless machines. Of course, one common alternative to discovery protocols—using a managed directory service—requires human administration in order to populate the directory service. This experience suggests that new approaches are needed for service discovery that can operate at the small scale of the home network, but yet can cope with the potentially complex topology of the home.

## 4 ICEbox Overview

Based on the problems noted above, we have created an architecture designed to eliminate—or at least mitigate—user interface problems with provisioning, evolution, trust management, monitoring, and discovery. Our contribution is on new interfaces for existing network technologies, rather than on new networking or security technology.
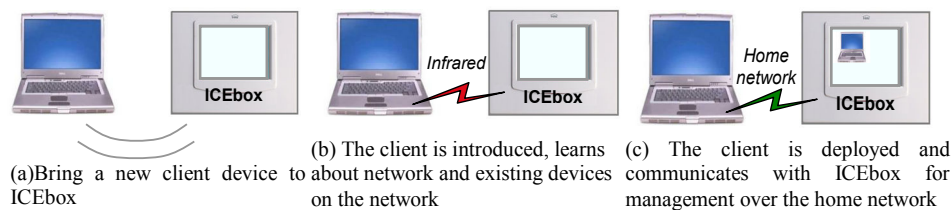
(a) Bring a new client device to ICEbox

(b) The client is introduced, learns about network and existing devices on the network

(c) The client is deployed and communicates with ICEbox for management over the home network

**Fig. 2.** The ICEBox device configuration steps

Our approach is based on simple physical actions by the user (such as pointing and turning a key in a lock), which then drive an architecture in which clients securely delegate configuration tasks to a centralized management node, the ICEbox.

By entrusting the ICEbox—rather than individual clients—with configuration responsibility, we separate those aspects of configuration that *must* be done by a user (because they cannot be intuited by systems, and therefore require human agency) from those that are incidental technical details (and thus can be automated).

In our model, users bring new devices onto the home network through a simple "introduction" step at the ICEbox (Figure 2). This step is through a physical pointing gesture, leveraging the proximity afforded by short-range communication to bootstrap communication and a trust relationship between the device and the ICEbox (Figure 2-a). This step effectively tells the ICEbox, *"This new device should be considered a part of my home network."* The client at that point delegates all future configuration responsibility to the ICEbox.

During this introduction phase, software on the client provides the ICEbox with details about itself, such as its type, network MAC addresses, what services it may offer, and so forth (Figure 2-b). This information is used by ICEbox to build up a model of client devices that exist on the home network.

Next, the ICEbox provides the new client device with a set of configurations that allow it to operate on the home network (also Figure 2-b). These configurations contain not only information necessary for link- and network-layer operation (SSID, WEP keys, address and router assignments, netmask, and so forth), but also application- and service-layer settings. These latter include, for example, information about printers deployed on the home network and fileshares on the network; for clients such as laptops, this information is used to install necessary printer configuration information as well as shortcuts to fileshares on the desktop. Such application- and service-layer information comes from the ICEbox's model of devices on the network, built up through repeated earlier introductions; this model can be used alongside network monitoring tools to drive a range of interactive monitoring and troubleshooting tools.

After introduction, the ICEbox adds the device to its model of the home network, and then notifies existing devices of the addition of the new one if necessary. For example, introducing a new printer onto the network will cause the ICEbox to communicate information about this new printer to all computers already installed on the home network. This mechanism moves from a model of linear complexity (adding a new device requires manual update of all existing clients on the network) to constant complexity (adding a new device is a single operation, no matter how many clients are already on the network).

Once deployed, the client device and ICEbox communicate using normal TCP/IP-based protocols. The client provides the ICEbox with details about its location in the

network (based on which provisioned address it is using), and communicates status information back to the ICEbox. The ICEbox can use this protocol deliver new configuration information to the client remotely, to reprovision it when new devices appear (Figure 2-c).

This model yields a number of benefits. First, it can better support novice users by reducing the complexity of bringing new devices onto the network correctly. Users need only perform a simple introduction step to associate a device with the ICEbox and thus bring it onto the network, rather than hassling with tedious network configuration parameters; likewise, the addition of new clients can cause *existing* devices on the network to be updated to know about these new clients. Second, this model can support "UI-free" client devices, such as small, single-purpose information appliances that may not have mice, keyboards, or screens. Client devices need no UI in order to communicate with the ICEbox. Third, this model allows us to avoid some of the problems with multicast-based discovery protocols in complex multi-link home networks, by using the ICEbox as a self-populating directory service. Finally, the network model maintained by the ICEbox, coupled with the management protocols it uses for ongoing communication with clients, can drive a range of interactive tools that can support end-users' understanding, monitoring, and troubleshooting of the network. In the following section, we describe these features of the ICEbox in detail.


## 4  ICEbox Features

### 4.1. Physical Form

We investigated a number of physical form factors for the ICEbox, including integrating it into an existing home gateway router and building a software-only version that could execute on arbitrary PCs. While these approaches have the advantage of not requiring an extra "box" in the home, they restrict the UI approaches we could take. Namely, existing home gateway routers have no screen that could be used for the monitoring functions of the ICEbox; and, while we could create an arbitrarily complex UI on a PC platform, we felt it was important to move away from "PC-style" interfaces that require mice and keyboards.

Thus, our initial ICEbox prototype is implemented as a stand-alone mini networked appliance, which has several unique features, one of which is a color LCD touch screen that is used as an input and display device. The ICEbox is equipped with an infrared transceiver and a standard Ethernet port; the infrared transceiver is used for communication between the ICEbox and devices yet not attached to the home network, while the Ethernet port is used for communication between the ICEbox and devices attached to the home network. Another salient feature of the ICEbox is a physical key lock. This is used to restrict the ICEbox's ability to add devices to the network or configure devices on the network, as described below.

This form factor closely resembles a standard home security pad. It is roughly the same size as such a pad, has a small screen and lock, but otherwise no physical controls. Our previous studies indicated that network infrastructure equipment, such as access points and routers, is often hidden from view in users' houses. Such

"invisibility" means that these devices are not positioned to easily notify users of problems—users are unlikely to notice a red light flashing, for example. By making the ICEbox resemble a home security pad, and by making it a vertical device, our goal is to explore placement opportunities that might be more amenable to visibility (such as placing the device on a wall near the security controls or a light switch).

The ICEbox is logically located at the boundary between the home network and the Internet, sitting just behind the home gateway router in our current implementation. In a future implementation the ICEbox will likely subsume the functionality of the router.

### 4.2 Interfaces for Device Introduction

As noted in the related work section, a number of earlier projects have demonstrated the benefits of short-range communication techniques for device association. Such mechanisms allow two devices to communicate in an ad-hoc, secure manner with no pre-configuration required. Thus, they serve as an ideal "bootstrapping" mechanism, since they can operate without explicit human involvement in configuration. Second, by limiting the range of such techniques, they provide an implicit interaction boundary, making them amenable to physical gestures such as pointing or touching two devices together.

However, pointing can also be problematic. One would not wish, for example, to have to point an Internet-enabled refrigerator at the ICEbox in order to provision it for the home network. Also, such mechanisms require the client device to be powered on in order to communicate; while this may not be an issue with laptops, it complicates the use of pointing techniques for devices such as desktops and printers (we will return to this issue in the Concluding Remarks section).

To support a range of introduction techniques—including pointing, as well as others—we have defined an abstract introduction protocol that can be carried over a number of different transports. In our current implementation, however, we carry this protocol over infrared (and thus use a short-range pointing interface) as our sole introduction mechanism. Our goal at this stage of our research is to refine the introduction protocol sufficiently that it can work for a range of devices, and then later to explore how this protocol can be manifested in a variety of specific interaction techniques. Thus,other short-range mechanisms could also be used, as long as they support the ability to transfer data bi-directionally and to detect packet loss. For example, this might include digital over-the-air audio, short-range RF, and inductive communication. Further, the introduction protocol could be layered over an existing TCP/IP protocol, or even "sneakernet" mechanisms (such as shuttling a USB key back and forth between devices).

### 4.3 A Physical Lock for Securing the Home Network

Protecting the network from unwanted access is another source of complexity for home users. It requires that users understand the security syntax and semantics of their specific home network. By automating the provisioning step—including passing WEP keys and SSIDs—the ICEbox hides basic security configuration, requiring no

knowledge on the part of users about security. Since security configuration happens automatically at the time of introduction, we obviate the possibility that users might neglect to set up security.

But this model introduces new factors into the security equation. By requiring physical access to the ICEbox in order to add to or change the network, this approach transforms the problem of network security to one of physical security—as long as physical access to the ICEbox itself is restricted, then interlopers cannot easily add an unauthorized device to the home network. For some users, in some circumstances, this level of security may be sufficient. However, for more security-conscious users, there are times when even physical security might be insufficient. For example, home visitors (neighborhood teenagers for example) might have access to the ICEbox while they are in the home. Therefore, we provide an additional layer of security to optionally restrict access to the ICEbox functions.

There are many potential ways to add this extra security layer. One is to require users to enter a password (on either the device or the ICEbox) in order to complete the introduction step. While such a solution is simple to implement, it has all the problems of traditional password solutions [1]: it requires that users remember the password, requires that they perform an extra step at each introduction, and requires that we provide extra UI mechanisms to enter, change, and manage the password.

Instead, the ICEbox provides a hardware-based solution that maps to existing practices and metaphors. As mentioned before, our metaphor is that the ICEbox is a logical door to the home network. Thus, like a physical door, the ICEbox appliance is equipped with a physical lock that enables access to its introduction and management features. A homeowner uses a key to unlock the ICEbox when he or she wants to attach a new device to the home network, and can also unlock the ICEbox when a visitor appears with a device the owner wishes to provision onto the network. In much the same way that users may leave a copy of a physical key with trusted friends, users may also leave the key to the network with associates. Likewise, users who are not concerned with additional security can simply leave the device unlocked.

This door lock metaphor can provide a greater degree of security to prevent unauthorized devices or users from joining the home network. The physical lock allows users to restrict access in a natural way while not requiring any network- or system-level security knowledge from users, nor requiring the use of mechanisms such as passwords or access control lists.

## 4.4 Visual Interface for Device Monitoring

The model of the home network created by the ICEbox is used to drive a graphical display of the network. The touchscreen display on the ICEbox displays the devices on the home network and lets users monitor them. Each device that has been introduced to the network is represented by an icon on the display. Touching a device icon brings up details of that device, including device and service descriptions and real-time connectivity status (whether the device is reachable or not) for all devices on the home network. To determine device connectivity, the ICEbox uses a simple monitoring protocol, sending out periodic connectivity status check messages to all devices and updates their connectivity in its model and on the display (Figure 3).
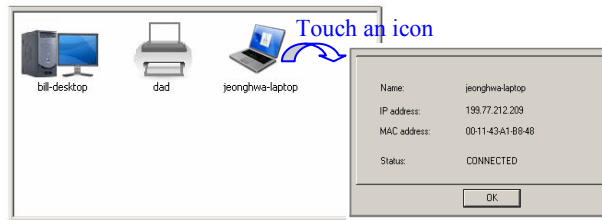
**Fig. 3.** Touch screen visual interface for device monitoring

### 4.5 Directory and Discovery Features

As noted earlier, typical multicast based discovery protocols such as mDNS used by Zeroconf [4], and SSDP used by UPnP [12], suffer from problems when used in complex network topologies. Because these protocols generally work only on a single network segment (given their multicast time-to-live radius), users find that devices that should automatically discover each other sometimes do not. Correcting such problems requires an understanding of physical layer network topology.

The typical solution to multi-segment discovery involves the deployment of a directory service (such as is used by the Service Location Protocol, SLP [10]). In the home setting, however, such approaches are untenable because they require explicit administration to deploy, configure, populate and maintain the contents of the service as devices come and go.

In contrast, a key advantage of the centralized network model of the ICEbox is that it can provide a robust mechanism for device and service discovery without the administrative hassles of a managed directory service. Since the ICEbox maintains a list of all devices currently on the network, it acts as a *self-populating* directory service; clients use a simple lookup protocol to query it for devices that match specified types. This approach mitigates many of the scoping problems seen with multicast-based discovery protocols without adding additional administrative burden.

## 5 User Experience

We performed an evaluation to investigate the usability and utility of the three key features of the ICEbox user interface: introducing devices to the home network, securing the home network, and monitoring the home network. Our goal with this study was to get a sense of the overall usability and utility of our approach, rather than to perform an in-depth usability analysis and task metrics. The first task compared ICEbox device introduction with a common method for manual setup of devices on the home network. The second task examined securing the home network. The third explored the usability and utility of the visual interface and monitoring features the ICEbox.

We built a networked home environment in our laboratory, instrumented with a Netgear 54WRG614 wireless access point, an ICEbox appliance, a networked printer, and several wireless laptops. Participants were invited to our laboratory to participate

in the study. While there are limits to studying home networking in a lab, controlled conditions give us repeatability that would be unobtainable on a real network, which is essential in studying usability rather than the network technology itself.

Ten users, 3 males and 7 females, aged 20-35 years old, participated in our study, all of whom have a network at home. Half of the participants described themselves as novices who had never set up networked devices before (their roommate, friend, or spouse had configured their networks for them). The other half had previous experience setting up networked devices in their homes. Their knowledge varied, with some users describing themselves as "familiar" with network setup, while other "beginners" still had experience installing and configuring network devices at home.

## 5.1. Device Configuration

The configuration task consisted of two sub-tasks: adding a new laptop to an existing secure home network, and then configuring the laptop to use a new networked printer. We used a WEP-enabled secure network for our tests since we believe users do desire security on their networks at home if it can be provided easily. We chose a wireless laptop and a printer to test both network-level and application-level configuration, respectively, since these are common in many networked households.

We used a within-subjects design in which each participant performed trials using the ICEbox and the existing manual methods. For each trial, each participant was first asked to add an unconfigured wireless laptop to the home network; then, the laptop correctly configured, he or she was then asked to configure access to the printer from the laptop. For the manual trials these tasks involved using the existing tools provided by the OS and access point, and the "Add Printer" Wizard, respectively. We gave a brief verbal overview of both systems and provided participants the instructions that come with the Netgear access point and with an ICEbox instruction sheet; participants were told that they could refer to either as necessary.

Participants were asked to think out loud during the study, and we recorded audio from these trials. Trials ended when the participant claimed to have finished or gave up.

Experienced users succeeded in configuring the laptop and the printer for both the manual setup and the ICEbox setup, with the ICEbox allowing faster configuration. Novice users, however, showed a more noticeable difference between the two methods. Four of five novice participants gave up configuration in the manual task. Some of them referred to the instruction manual for assistance; however, despite this, they eventually gave up since they could not understand the manual. Meanwhile, all novice participants succeeded in configuration with the ICEbox. After the study, we administered a post-study questionnaire to gain insight into participants' subjective impressions of each method and overall method preference. Participants were very positive about using the ICEbox as a configuration tool. Nine of the ten participants preferred using the ICEbox to the manual set up method, and eight of these strongly preferred using the ICEbox. One experienced user still preferred the manual setup because it was more familiar to her. All participants agreed that the ICEbox was an easier way to configure devices.

### 5.2. Securing the Home Network

We ran a pre-study session in which participants were asked to secure the home network using the existing Netgear wireless security setup method. Only two out of ten participants succeeded in securing the wireless home network. They used the wireless network wizard or the Netgear access point web interface for this task. The other eight participants were unable to complete the task, despite having the product manuals available. On the other hand, all participants understood and were able to use the ICEbox key lock interface. Based on our interviews with them, most users understood the lock as a way to "keep outsiders out" of the network. Qualitatively, all of our participants preferred the key lock interface to the manual security set up method; users noted the physicality of the interface as being important in making is the functionality both apparent and intuitive.

### 5.3. Monitoring the Home Network

We were interested in gaining a qualitative sense of the utility as well as the usability of the monitoring features of the ICEbox. Overall, most network-experienced users and some novice users expressed their interest in this functionality, with several providing suggestions for refining the feature set. Meanwhile, three novice users reported that they did not need this feature since they had no need for network monitoring.

Other users, more familiar with network configuration and troubleshooting tasks, expressed interest in having an easily available depiction of network status, and an interest in having an icon for the entire network in addition to the individual devices on it (for controlling network and firewall parameters, for instance). A number of suggestions revolved around desires to add functionality behind network configuration and monitoring, such as remote control of devices in the home.

### 5.4. Study Summary

Although we view our study as a high-level exploration of the usability and utility of centralized network management in the home, we do believe that it points to the promise of this model. For the majority of our users, the ICEbox significantly reduced the complexity of certain home networking tasks. We found that even novice users were able to configure wireless devices easily, secure the network, and monitor devices' connection status without deep knowledge of networking. We believe that these experiences highlight the utility of *removing* as much interaction as possible from the network setup process.

We also noted during our study that, although few participants referred to manuals (as might be expected), none of the ICEbox users referred to the instruction sheet in order to accomplish tasks. We believe that this demonstrates the utility of a simple set of physical interactions for network configuration, and especially the value of having tangible, physical affordances to functionality that is often hidden (such as security configuration).

There were, however, several features that our participants did not like. Many of these concerned the difficulty of infrared communications: finding and facing infrared ports on two devices was not familiar to most users, which suggests that further work on introduction protocols is necessary. Likewise, some users advocated for a "mini ICEbox" in the form of a cellphone or other device, which would allow them to bring the ICEbox to the device, rather than the device to the ICEbox. Finally, although users were generally positive about the key mechanism for network security, a number of participants worried about the possibility of loss of the key. At the same time, these users expressed a desire to incorporate other functions into the lock, such as parental access controls for the network.

## 6 Concluding Remarks

In this paper, we analyzed why home networking is difficult for users and then introduced a novel type of network appliance, called the ICEbox, designed to reduce the complexity and increase the usability of home networking. The ICEbox simplifies device configuration through a pointing interface based on a short-range communication; it provides easy-to-use security through a door lock metaphor. Visual monitoring capabilities provide a graphical display of the devices on the network and their current status for easy monitoring of the network.

There are a number of open questions regarding the physical form of the ICEbox, as well as the mechanism used for the introduction protocol; these two issues interrelate with one another. For example, one approach may be to detach part of the ICEbox (a "provisioning wand") that you touch to client devices. Another approach—reminiscent of WCN—is to use a USB memory key. Some of these mechanisms are restrictive from a systems perspective, because they make multi-round communication between the ICEbox and client difficult (you'd have to walk back and forth with your USB key to perform the multi-round introduction protocol, for example). Balancing the systems benefits of two-way communication against users' effort is necessary to find the "sweet spot" of low-overhead, automated introduction.

In parallel with this, we are planning a series of studies to inform other future goals of the project. For example, one issue that the current ICEbox implementation does not deal with is easy revocation of access to the home network, especially for "transient" devices such as those of visitors. Many users now provide access to their home networks to visitors or neighbors. While the current ICEbox implementation allows easy access to the network for these users, we have no easy way to close the network to them after they leave. What are the most flexible (and socially appropriate) ways to allow such transient access? The interface challenge here is in providing easy access without overburdening the introduction step with a checklist of possible rights and time periods for which access is granted, nor with requiring that users remember to revoke visitor access once they leave.

Finally, our current protocols work best when the ICEbox is the first entity deployed onto the network. This allows it to build up its network model as new devices are introduced to it. We plan to explore techniques to allow post hoc introduction of the ICEbox onto the network.

# References

1. Adams, A., Sasse, M., Lunt, P.: Making Passwords Secure and Usable. Proc. HCI'97 (1997)
2. Balfanz, D., Durfee, G., Grinter, R., Smetters, D., Stewart, P.: Network-in-a-Box: How to Set Up a Secure Wireless Network in Under a Minute. USENIX Security Symposium (2004)
3. Blumenthal, M. S., Clark, D. D.: Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world. ACM Transactions on Internet Technology, 1:1, 2001
4. Cheshire, S., Steinberg, D.: Zero Configuration Networking: The Definitive Guide. O'Reilly Associates, ISBN 0596101007, (December, 2005)
5. Consumer Electronics Association, Broadband and the Home of Tomorrow, Mar. 30, 2006
6. Droms, R.: Dynamic Host Configuration Protocol, Internet Engineering Task Force Request for Comment (RFC) 2131 (1997)
7. Goland, Y., Cai, T., Leach, P. Gu, Y., Albright, S.: Simple Service Discovery Protocol/1.0: Operating Without an Arbiter. Internet Engineering Task Force Draft, October 28 (1999)
8. Goodall, J. R., Lutters, W. G., Komlodi, A.: I Know My Network: Collaboration and Expertise in Intrusion Detection, In Proc. ACM CSCW (2004) 342 – 345
9. Grinter, R.E., Edwards, W. K.: The Work to Make a Home Network Work, Proc. European Conference on Computer-Supported Cooperative Work (ECSCW'05), (September, 2005).
10. Guttman, E., Perkins, C., Veizades, J., Day, M.: Service Location Protocol, Version 2. Internet Engineering Task Force Request for Comments (RFC) 2608 (1999)
11. Jackson, L. A., Von Eye, A., Barbatsis, G., Biocca, F., Fitzgerald, H.E., Zhao, Y.: The Impact of Internet Use on the Other Size of the Digital Divide. Communications of the ACM, Vol. 47, No. 7 (2004) 43 – 47.
12. Jeronimo, M., Weast, J.: UPnP Design by Example: A Software Developer's Guide to Universal Plug and Play. Intel Press, ISBN 0971786199 (2003)
13. Kiesler, S., Zdaniuk, B., Lundmark, V., Kraut, R.: Troubles With the Internet: The Dynamics of Help at Home. Human Computer Interaction (2000) 323 – 351
14. Kraut, R., Scherlis, W., Mukhopadhyay, T., Manning, J., Kiesler, S.: HomeNet: A Field Trial of Residential Internet Services. In Proc. CHI'96 (1996) 284 – 291
15. Laszlo, J.: Home Networking: Seizing Near-Term Opportunities to Extend Connectivity to Every Room. Jupiter Research (BRB02-V01) (2002)
16. MacMillan, R.: Plugged In: Wireless Networking Baffles Some Customers. Reuters news report, March 10 (2006)
17. Microsoft Corp. Windows Connect Now Architecture whitepaper. April 11 (2005) http://www.microsoft.com/whdc/device/netattach/WCN.mspx
18. Rekimoti, J., Ayatsuka, Y. and Kohno, M. SyncTab: An Interaction Technique for Mobile Networking. In Proc. Mobile CHI (2003) 104 - 115
19. Rekimoto, J., Ayatsuka, Y, Kohno, M., Oba, H.: Proximal Interactions: A Direct Manipulation Technique for Wireless Networking. In Proc. INTERACT2003, 511 – 518
20. Scherf, K.: Parks Associate Panel on Home Networking, in Proceedings of Consumer Electronics Association Conference (2002)
21. Swindells, C., Inkpen, K.M., Dill, J.C., Tory, M.: That one there! Pointing to establish device identity. In Proc. ACM UIST (2002) 151 – 160
22. Vitalari, N. P., Venkatesh, A., Gronhaug, K.: Computing in the Home: Shifts in the Time Allocation Patterns of Households. Communications of the ACM, Vol. 28, No. 5 (1985)
23. Voida, A., Grinter, R. E, Ducheneaut, N., Edwards, W. K., and Newman, M. W.,: Listening In: Practices Surrounding iTunes Music Sharing, In Proc. CHI2005 (2005).
24. Whittaker, S. and Amento, B. Seeing: what you are hearing: Co-ordinating responses to trouble reports in network troubleshooting. In Proc. ECSCW'01, Kluwer Academic Publishers (2003) 219 – 283