

USER-CENTERED DESIGN OF A SECURE P2P PERSONAL AND SOCIAL NETWORKING PLATFORM

Zoe Antoniou and Dimitris. N. Kalofonos
Nokia Research Centre Cambridge
3 Cambridge Centre, Cambridge
MA, 02142, USA
{zoe.antoniou, dimitris.kalofonos}@nokia.com

ABSTRACT

Advances in Peer-to-Peer (P2P) and web technologies have recently enabled P2P personal and social networking. The key to the success of such systems is middleware and tools that will allow non-expert consumers to manage their networks and share their resources easily and intuitively. This is the motivation behind MyNet, a P2P platform that enables non-expert users to easily organize their resources and share them in their immediate social neighborhood. In this paper, we present our experience following a user-centered approach in designing the MyNet system: using real-world metaphors in the core system, leveraging NFC-based touch to mirror human behavior models, and involving actual users in the design process. The results of our initial usability evaluation are also presented in detail.

KEY WORDS

P2P networking, security, NFC, usability evaluation

1. Introduction

A number of recent developments are changing the ways we can access and share personal information. First, there is an explosion of personal digital content and services residing on increasingly network-enabled consumer devices (e.g. phones, cameras, music players, DVRs, game consoles). Second, a number of peer-to-peer (P2P) technologies (e.g. UIA [1], JXTA [2]) can offer seamless and pervasive connectivity among users' personal devices and those of others. Finally, "Web 2.0" technologies and services are giving unprecedented access and control of the Internet to non-expert users and are creating a culture of sharing. In theory, it is possible for consumers to use today's technologies to create their own P2P networks and share information with others. In practice, this is out of reach for all but the most technically skilled users.

Even though existing technologies can form the basis of a platform for P2P personal and social networking, they are not enough. We believe that the key to the success of such a platform is, as in web-based social networking, the creation of easy-to-use tools that will enable non-expert consumers to manage their personal and social networks and share their resources. Furthermore, since devices are

personal, the platform must make users confident not only that it offers comprehensive security and privacy protection, but that it offers them the means to make the right security decisions.

MyNet [3] is a secure, P2P personal and social networking platform of middleware and user interaction tools, whose primary goal is to dramatically simplify the deployment, management and use of secure, consumer networks and distributed services. MyNet is optimized for connecting to devices in a user's immediate social neighborhood: the user's own devices and those of one or two social hops away. These devices can be several physical hops apart and they form a web of overlay nodes which can be exploited in two distinct ways: routing purposes and social interaction. The resulting design is a new network navigation model based on social relationships. Global access within a Personal and Social Network become as simple as selecting an icon, while complex configuration for service discovery, network access, and security remain hidden from the end-user.

In this paper, we present our experience following a user-centered approach in designing the MyNet system. First, the core system design is based on intuitive real-world metaphors: routing and trust based on personal and social networks, "ticket"-like authorization credentials called *Passlets*, and presentation based on social relationships. Second, we use intuitive user interaction "touch", based on Near Field Communication (NFC) [4], to mirror human behavior models, e.g. establish trust with what you see and touch, and sharing with a gesture. Finally, we follow an iterative approach involving non-expert users in the design process, by conducting small-scale usability tests and incorporating feedback in the design. The results of our initial usability evaluation are also detailed here.

The rest of this paper is organized as follows: in Section 2 we present related work; in Section 3 we give motivating use cases, while in Section 4 we describe our objectives and approach; in Section 5 we present a system overview from the user's perspective; in Section 6 we present the results of an initial usability evaluation; finally, in Section 7 we present our conclusions and some future directions.

2. Related Work

MyNet's provides a set of functionality that is not typical in today's Social Networking systems [3]. Most popular such systems rely on web-based centralized interfaces (e.g. Facebook [5], Myspace [6], Flickr [7]). In addition, there exist a number of peer-to-peer social data-sharing systems, such as Turtle [8], SPROUT [9], F2F [10] and Tribler [11]. None of the above supports a truly intuitive user interaction with respect to sharing both content and services, as well as, the creation of secure Personal Networks. Likewise, several systems attempt to address the ease of use in configuring firewalls [12], [13]; these systems do not match MyNet's fine-grained access policies as they cannot identify individual users.

The prototypes in [14] and [15] offer a very easy to use UI for sharing. In particular, [14] allows users to create buddies and groups, and specify the visibility and permissions of files without the need for ACLs. Their focus, though, is on file or photo sharing alone, and sharing can take place only in local subnets or through centralized servers. They have no elements of real-world point-and-click interaction and very limited GUI tools for the management of permissions and access control.

3. Example Use Cases

Alice has a Personal Network which consists of her mobile phone, the home PC and a security camera. While at work, she uses her laptop to retrieve the proposal she was working on over the weekend from her home PC. She also uses her mobile phone to check on her new pet cat through the security camera.

James's Personal Network includes his mobile phone and his home media server. While on a trip he meets his old colleague George. Over dinner, James talks about his new baby daughter and wants to share some photos. He TAPs George's phone with his mobile phone to give him access to the baby photos at his home media server. George can now see the photos in his phone but chooses to display them on his big-screen TV so that everyone can watch.

Another meeting is about to start and Chris is getting ready to take notes with his laptop. He has set up a Wiki page for this project on his desktop PC and he wants to give all project members access rights to view and edit it. Using his laptop he sends a Passlet to the entire group. Members of the team have now access to the Wiki page.

4. A User-Centered Design Approach

Our main objective in designing MyNet was to design a system that can be used by everyday users, without requiring any special training or expertise. More specifically, we set the following design goals:

- Build a personal, virtual private network easily and securely. Use any device in your personal network to access any of your resources (devices, services, content) wherever they are connected. Mobility and disconnections are supported and handled gracefully.

- Link personal networks together to create social networks that can be exploited both for routing and for social interaction. Sharing resources and forming groups within your Social Network is as easy as using a device in your Personal Network.
- Use simple techniques to manage the security of your Personal Network and share access with other users in your Social Network. Enable fine-grained access control to all resources while hiding the complexity.
- Create a user experience based on social interaction models, so intuitive that anyone can understand the results of all network and security management.
- Build the system on top of a connectivity and security framework that is purely ad-hoc and peer-to-peer.

The design approach was user-centred, focusing on the end-user's perspective of the system:

- The front-end design takes advantage of metaphors that are based on familiar terms and representations from everyday life and social relationships: (a) users create Personal Networks that consist of their personal devices, (b) Personal Networks can be linked together to form Social Networks, (c) a user can share his/her personal devices or content with another user by granting a Passlet which is the equivalent to an electronic permissions ticket and (d) Passlets give access to users, not devices.
- Rather than requiring new models of behavior, we embrace intuitive human activities, such as pointing and touching, by adopting the "touch" UI paradigm in our system through NFC interfaces in mobile devices. Humans trust objects they can see and touch. An efficient UI design using "touch" can replace multiple manual steps and lengthy configuration processes with simple one-step touch gestures.
- We follow a phased design approach that includes user feedback at crucial decisions. User involvement is incorporated through an iterative cycle of design interchanged with small-scale usability tests.

5. MyNet Overview

This section presents a functional overview of MyNet from the user's perspective; details about the system architecture and protocols can be found in [3].

MyNet leverages existing P2P network overlay technologies and introduces middleware and UI tools that add intuitive personal and social network management, secure resource discovery, service management, and fine-grained security. A wizard-like interface, part of a MyNet UI tool called MyNetBook, first guides the user to imprint his/her identity on a new device. Devices of the same owner are joined to create a Personal Network (PN) using MyNetBook's introduction process, which may be as simple as a TAPing gesture. Personal Networks can then be linked using the same MyNetBook introduction process to create Social Networks. Users can choose to share access to the resources they own with their social contacts through the use of Passlets, real-world metaphors

resembling “passes” or “tickets”, which prescribe a set of user-level permissions that the user grants to the recipient. The security framework recognizes peer devices within a Personal Network and allows unlimited access among them, without requiring any user action. Social contacts, on the other hand, can only discover and use allowed resources, thus empowering the user to a fine-grained access control over his/her Personal Network.

5.1 Personal and Social Networks

A MyNet device is a routable and authenticatable overlay network endpoint, which hosts the user’s services and content. MyNet devices can be physical devices or virtual devices hosted in physical devices (e.g. internet hosts providing MyNet virtual devices as a service to users). Each MyNet device exposes information and content by running one or more user-services, e.g. printing, file sharing. The user can express his/her intent on how to define permissions for these services. Each user-service may be implemented by more underlying distributed system-services, about which the user is oblivious.

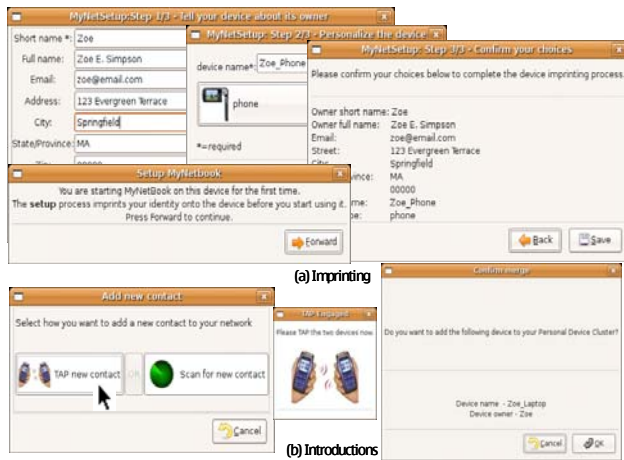


Figure 1: Example of imprinting and introduction UI.

A new device becomes a MyNet device belonging to a specific user/owner using the MyNet *imprinting* process. During the imprinting process, the device is imprinted with the new owner’s identity and profile, and an owner secret (e.g. a PIN, password, user RFID key, fingerprint) [16]. The owner secret is used to authenticate the owner before critical actions to provide additional protection against misuse in the case a personal device is lost. The user is able to set preferences about which actions will be protected by this secret. An example of our prototype UI for imprinting is shown in Figure 1(a). The user is guided through a wizard-like UI to enter (a) a name for the PN, (b) profile information that can be used in the context of social networking, and (c) the owner secret (e.g. PIN).

After a device is imprinted, the user will have the option to merge it with other devices he/she may own to create a PN, the basic cell of a MyNet network, through the MyNet *introduction* process. Once merged, the two devices become part of the same PN. A user can follow the same MyNet introduction process to link his/her PN to

the PN of another user. The result is the mutual addition of a social contact (or buddy) to both users’ MyNetBooks. Both merging and linking requires mutual consent from both sides and they are reversible. An example of the MyNet introduction UI for adding new devices and social contacts is shown in Figure 1(b). The TAP button allows the user to discover another device by “touching” its NFC [4] interface, while the SCAN button achieves this by a conventional “network search”, e.g. Bonjour [17].

5.2 A Touch is worth a Thousand Clicks

In an effort to make the user interaction model truly intuitive, MyNet borrows from social behavior paradigms. Humans tend to trust objects they can see and touch. Pointing to an object is a very familiar gesture both in real life and in traditional user interfaces. Such gestures can express a user’s intent to interact with objects in the immediate physical vicinity. As a result, physical space becomes an extension to the traditional 2-D GUI display.

Low proximity wireless communication technologies, such as NFC [4], provide a means for realizing this interaction model. A one-step action from the user, such as select-and-touch or point-and-click ([18], [19]) is sufficient to complete a MyNet interaction, such as adding a new device in the PN, adding a new social contact, or giving a Passlet. As an alternative, for devices not featuring NFC interfaces, MyNet uses local area multicast (e.g. Bonjour [17]) to provide similar functionality, at the cost of more manual involvement and a less intuitive experience.

5.3 Usable Security by Design

Today, managing pervasive access to personal devices is almost impossible for non-expert users, and just improving the UI to existing security infrastructure is not enough. For example, assume Zoe meets Sacha in a café and would like to give him temporary access to the public photos in her home PC. Assuming Zoe subscribes to some dynamic DNS service to enable global addressing, she would have to login remotely to her router/firewall and open a hole to expose her PC’s web-server, which would make it accessible to everyone, not only Sacha. She would then have to enable security on her web-server (e.g. creating certificates, etc.), password-protect her photos directory, edit the web-server Access Control List (ACL) to add Sacha as a user and give him access to her public photos directory. Revoking his access would imply repeating the process in reverse order.

As a major step in improving the previous scenario, MyNet uses *Passlets* [20], which are based on the real-world metaphor of “passes” or “tickets”, whereby a user grants a Passlet to prescribe a set of high-level permissions he/she wants to grant the recipient (Figure 2). MyNet translates the user-level permissions carried in Passlets to the appropriate system-level settings and takes care of secure remote connectivity and addressing, without exposing complex security concepts such as ACL, encryption keys or certificates to the end-users.

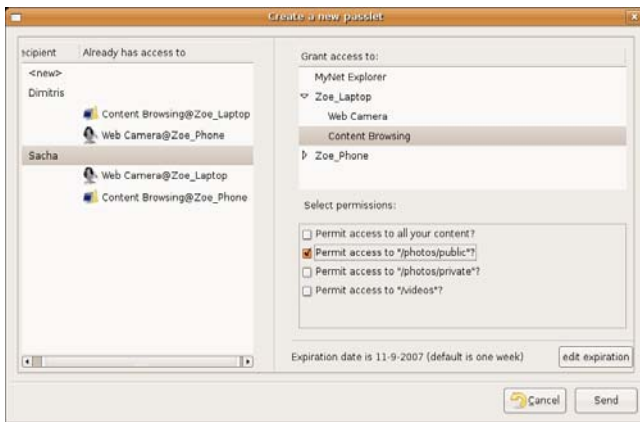


Figure 2: An example of the Passlet Manager UI.

A user can use the MyNetBook Passlet Manager on any PN device to create Passlets that will allow the recipient to access any target resource in the Personal Network. The Passlet recipient can be any person or group that can be named by MyNetBook, or any recipient that is determined through a “touch” with the NFC interface. Similarly, a user can use a Passlet he/she has received to access the prescribed resources from any device in the PN. In the above example, after Sacha receives the Passlet shown in Figure 2, he can use his home TV to view Zoe’s public pictures, provided it is not expired or revoked.

5.4 Creating the User Experience with MyNetBook

MyNetBook is the front-end MyNet application that allows the end-user to interact with MyNet. In our prototype, the main GUI widget is a notebook with two tabs, a toolbar at the top and a status bar at the bottom (Figure 3). By selecting the first tab the user can browse and manage his/her Personal Network. By selecting the second one, the user can manage Passlets and access rights. Interactive tasks that require the user’s attention such as setting up MyNet, adding personal devices and contacts, sharing and error notifications are displayed in popup windows. The toolbar buttons are “Build your Net” for adding personal devices to the PN, “Add contact” for adding social contacts to the PN, and “Share” for creating Passlets. The status bar displays status messages.

In the current implementation, MyNetBook visualizes the resources in a hierarchical tree structure. All the devices owned by a user are logically grouped together. Likewise, all services hosted by a device are logically grouped together. Devices are shown as the children of the user and services are the children of devices. MyNetBook presents all the devices, services and contacts in the Personal Network on any PN device. For example, in Figure 3, Zoe owns a Personal Network with two devices, a laptop and a mobile phone, and has two contacts Sacha and Dimitris. She can browse her laptop’s services from the MyNetBook application running on her mobile phone. The user can launch a service (his or that of a contact who has given him a Passlet) simply by double-clicking on the service icon, e.g. Sacha would just have to double-click on Content Browsing to access Zoe’s public photos.

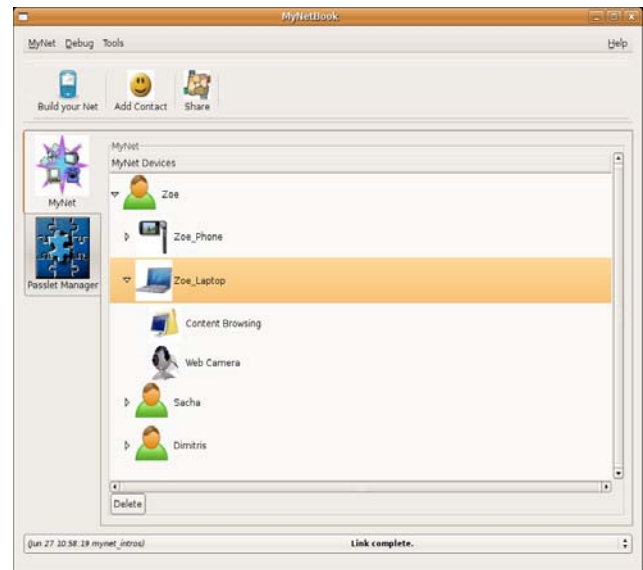


Figure 3: An example of the MyNetBook UI.

6. Usability Evaluation

6.1 Objectives

A pilot usability study was conducted in May 2007 with sub-optimal GUI tools (Figure 4). The study was focused primarily on the users’ perception of MyNet concepts:

- Do users understand the concepts of a Personal Network, Social Network, introductions and Passlets?
- Do users have security and privacy concerns with respect to the integrity of a PN, and the introduction and sharing mechanisms?
- Do users find use for MyNet in their daily activities?
- Are the GUI tools and interaction models usable, learnable and likable (browsing/using PN resources, managing Passlets, adding contacts/ devices)?
- Is it easy and intuitive to complete MyNet tasks?
- Do users find TAPing easy, intuitive and safe?
- Do users feel confident to use the system successfully and do they trust the system to perform as expected?

6.2 Methodology

Participants: There were 13 participants, ages 18-60+, 7 males and 6 females. Most participants (85%) had a literature, music, marketing, finance, business or psychology background. The remaining participants (15%) were engineers. All were familiar with basic e-mail, internet browsing, and use of mobile phone for phone calls. Most had basic computer skills (e.g. MS office, Excel) and approximately 50% had some experience with messaging and sharing applications (e.g. Skype, IM, on-line presence) and wireless proximity technologies (Bluetooth, WLAN, IrDA).

Procedure: The test was an in-lab, one hour session. First the participants filled in a pre-test questionnaire. Then, they were given a short verbal introduction to MyNet and were asked to perform a series of tasks (Table 1). At the end of the experiment, they were debriefed. The test was conducted with one moderator and one silent observer.



Figure 4: MyNet pilot test prototype.

Test Tasks: The participants were asked to complete a series of tasks which highlight the key functionality of MyNet (Table 1). For all the tasks, key assessment measures were ease-of-use of the tools associated with each task, clarity of the end-result after task completion and user understanding of the MyNet concepts.

Task	Testing objective
Setup MyNetBook on your mobile phone	Assess the imprinting process
Add a laptop to your PN using Scanning	Assess the user's understanding of introductions for personal devices
Use the laptop web camera from your phone	Assess the user's understanding of the PN concept and its GUI depiction
Use the phone to share the public photos stored on your laptop with a friend who runs MyNetBook on his/her PDA using TAPing	Assess (a) the introduction and sharing concepts for MyNet contacts, (b) the TAPing introduction process, (c) the user's understanding of the Passlet concept and Passlet creator, (d) prompt the user to express privacy concerns
Access the photos from the PDA	Assess the user's perception of the social network concept and its GUI depiction
Use the phone to share private photos from laptop	Assess the Passlet creator tool as a Passlet editor
Use the phone to revoke access to the photos	Assess the Passlet Manager tool and the user's perception of Passlet revocation

Table 1: Task scenario summary.

6.3 Results

Measurements consisted of observational measures and participant responses to interview items.

Task Completion: Overall, task completion rates were high (Figure 5). Most participants were able to complete all tasks successfully. There were some exceptions in the cases of deducing the concept of a Passlet prior to using it for the first time and editing a previously granted Passlet in order to change its permissions.

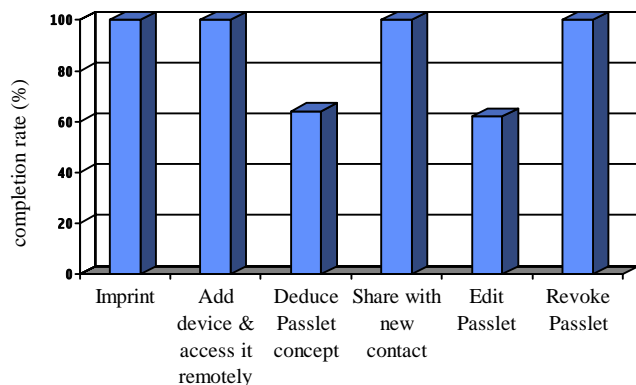


Figure 5: Successful completion rate of key tasks.

After Task Questionnaire (ATQ): The ATQ is a validated 3-item, 3-point scale that measures the users' understanding and satisfaction of the task just completed. For each task, users provided answers to the following:

I understand the end result of task just completed.

What is the end result?

Task completion was easy without major usability flaws.

The answer to the second item was rated based on whether it described the system state with full/partial/no accuracy. There were additional task-specific questions that were rated based on the same scale. Table 2 summarises the key ATQ aspects and their ratings.

ISSUE	YES	IN PART	NO
MyNetBook imprinting			
Users understand the end result of imprinting	77%	15%	8%
Imprinting is a easy to complete	100%	-	-
Users can create, navigate and access a PDC	100%	-	-
Add personal device & access it remotely			
Easy to complete & end result is clear to the user	100%	-	-
Personal network tree-based depiction is clear & easy to navigate and use	85%	15%	-
Sharing with a new contact			
Users want to first add new contact then share as opposed to using the sharing tool directly	54%	-	46%
Adding contacts & sharing raises privacy issues	75%	25%	-
Passlet management			
Users deduce the Passlet concept (before use)	64%	-	36%
Users can issue and revoke Passlets successfully	100%	-	-
Users can edit Passlets successfully	62%	38%	-
Introduction mechanisms			
Users are familiar with WLAN Scanning	30%	-	70%
Users are familiar with NFC TAPing	7%	-	93%
Introduction process based on Scanning is easy	100%	-	-
Introduction process based on TAPing is easy	100%	-	-
Users prefer TAPing over other wireless proximity modalities for portable devices	78%	7%	15%

Table 2: ATQ major ratings.

The ATQ process gave insight into the participants' understanding of MyNet concepts and indicated various ways in which the GUI can aid users in learning and using MyNet functionality. More specifically:

- The imprinting process was easy to complete and 77% of the users correctly deduced that the resulting state was a personal network with one device.
- Creating and managing a PN was a very popular feature, especially in the context of remote access to home devices. All testers were able to add devices with little or no difficulty and found the tree-based visualization easy to follow.
- Sharing with a new contact revealed that participants considered both (a) separating the task of adding a new contact from the task of sharing and (b) adding a new contact only when sharing is intended.

- Though users were not familiar with Passlets, 64% deduced that they are a type of electronic document containing permissions. All users were able to issue and revoke Passlets successfully, while 62% edited one. Overall, Passlets were perceived as a helpful and easy to manage security tool, especially after having completed the process once.
- Participants were not very familiar with Bonjour or NFC technologies and required help (e.g. GUI tooltips or verbal explanation) as to the expected system behaviour. They found both approaches easy to follow and learnable. TAPing for adding devices, contacts and sharing was found particularly intuitive, novel and fun. It was rated as preferable over other proximity wireless technologies by 78% of the participants.

Post-Scenario Qualitative Interview: We interviewed the participants on issues ranging from GUI design patterns to user interaction metaphors to MyNet system concepts. Overall the results were encouraging, indicating that participants found MyNet easy to learn and use despite the prototype quality front-end tools. In addition, participants felt they could trust the system to perform as expected. Passlet revocation was a particularly popular feature as it gave users the assurance that mistakes made during sharing can be reversed.

Adding contacts and sharing prompted most participants to express security and privacy concerns. They wanted to know the exact implication of their actions while adding new contacts and sharing Passlets, e.g. the type of information exchanged, whether received Passlets can be forwarded to third parties, the system vulnerability to hacking and so on. A few participants suggested that educating the user upfront of the system's security features would be very effective. In this context, the fact that adding a contact results in no default sharing unless a Passlet is granted was a very well received feature.

Other privacy concerns arose with respect to lost or stolen devices, user authentication and the privacy of the PN from the operators. Transitive visibility through Friends-of-Friends was another strong concern among half the testers. They felt that the social networking aspect of MyNet should protect the user's contact information from being forwarded without his/her expressed consent.

Finally, participants perceived MyNet as a useful tool for both mobile and fixed devices and saw the potential to utilise it in several daily activities. Among the listed applications were remote access to home devices, sharing content (photos, video, music) with friends, family and group members, as well as, sharing documents and business cards with co-workers, clients and classmates.

7. Conclusions and Future directions

Through this preliminary usability test we gained valuable insight into the users' needs, their perception of MyNet concepts and how to improve the UI tools in order to facilitate a more intuitive user experience. Based on the results, several enhancements have been added into the

design. Users are able to initiate the sharing process either directly or through the introduction of a new contact. The TAPing feature has been reinforced with the addition of *1-Touch Share*; this allows users to simply select a PN resource (content, service) and share it with a single touch gesture. User authentication (e.g. PIN) now protects critical operations such as adding a new personal device. Overall, the GUI tools have been enhanced to provide better guidance and feedback.

MyNet's prototype is currently under preparation for a second usability test with a larger pool of non-expert participants. A major usability challenge is redesigning the GUI to fit the form-factor and software requirements of mobile handsets (Nokia N800 & S60 phones). Small screen real estate, different UI paradigms, mobility and user interaction with one or two hands while maintaining a consistent user experience in all platforms raises several issues which will be addressed in an upcoming paper.

Acknowledgements

The authors wish to thank Aino Ahtinen, the members of the MyNet and UIA projects and the study participants.

References

- [1] B. Ford et al., "Persistent Personal Names for Globally Connected Mobile Devices", in *Proc. OSDI'06*.
- [2] JXTA Community Projects, <https://jxta.dev.java.net/>
- [3] D.N. Kalofonos, Z. Antoniou et al., "MyNet: a Platform for Secure P2P Personal & Social Networking Services", to appear in PerCom 2008.
- [4] NFC Forum, www.nfc-forum.com
- [5] "Facebook," <http://www.facebook.com/>.
- [6] "Myspace," <http://www.myspace.com/>.
- [7] "Flickr", <http://www.flickr.com/>.
- [8] B. Popescu, et al., "Safe and private data sharing with Turtle: Friends Team-Up and Beat the System," *12th SPW*, 2004.
- [9] S. Marti, P. Ganesan, and H. Garcia-Molina, "SPROUT: P2P routing with social networks," in *P2P&DB*, 2004.
- [10] J. Li and F. Dabek, "F2F: Reliable storage in open networks," in *5th IPTPS*, Santa Barbara, CA, Feb. 2006.
- [11] J. Pouwelse et al., "Tribler: A social-based peer-to-peer system," in *5th IPTPS*, Feb. 2006.
- [12] "Firewall builder," <http://www.fwbuilder.org>.
- [13] S. Mizuno et al., "A new remote configurable firewall system for home use gateways," in *Proc. CCNC*, 2005.
- [14] S. Voida et al, "Share and Share Alike: Exploring the User Interface Affordances of File Sharing", in *Proc. CHI*, 2006.
- [15] S. Counts & E. Fellheimer, "Supporting Social Presence through Lightweight Photo Sharing On and Off the Desktop", *Proc. CHI*, 2004.
- [16] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks". *SPW*, 1999.
- [17] Apple Computer, Inc., "Bonjour," <http://developer.apple.com/networking/bonjour/>
- [18] Z. Antoniou & D.N. Kalofonos, "NFC-based Mobile Middleware for Intuitive User Interaction with Security in Smart Homes". In *Proc. of IASTED CSN'06*, 2006.
- [19] Z. Antoniou, & S. Varadan, "Intuitive Mobile User Interaction in Smart Spaces via NFC-enhanced devices", *Proc. IEEE ICCGI*, 2007.
- [20] D.N. Kalofonos & S. Shakhshir, "IntuiSec: a Framework for Intuitive User Interaction with Smart Home Security Using Mobile Devices". In *Proc. IEEE PIMRC'07*, 2007.