FamilyNet: A Tangible Interface for Managing Intimate Social Networks

Wendy E. Mackay & Michel Beaudouin-Lafon
inlsitul : INRIA Futurs & LRI
Université Paris-Sud, Bâtiment 490, 91405 Orsay Cedex, France

ABSTRACT
InterLiving, a longitudinal participatory design project with multi-household families, identified the need for *communication appliances* and a corresponding need for managing small-scale, secure networks, and associated media archives. We describe *FamilyNet*, our solution to the latter problem, which uses public key encryption and a tangible interface simple enough for even children to use, yet extensible to cover a variety of use scenarios.

INTRODUCTION
The interLiving project established long-term relationships with six multi-household families and engaged in a wide variety of participatory design activities. The families repeatedly expressed a desire to stay in touch with each other, in pairs or as small groups of family and friends. In addition to phone and email, they also sought peripheral connections via sound, images, text and touch. They wanted to share personal information and leave traces of themselves using notes, voice, snapshots or video.

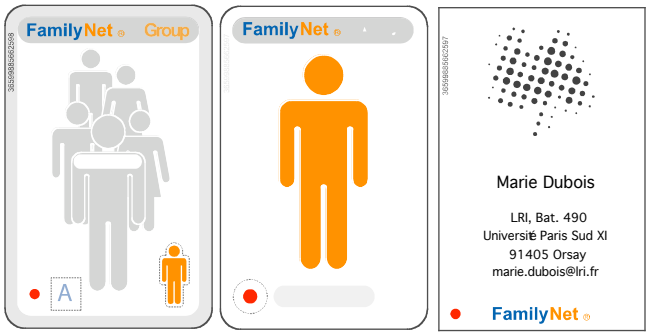
This led us to define a new class of devices to help people stay in touch: *Communication appliances* are simple-to-use, single-function devices that let people communicate, passively or actively, via some medium, with one or more remotely-located friends or family. Hutchinson et al. (2003) and Mackay (2004) describe several devices we created and tested in families' homes, to exchange messages, images, sound and video. Despite increasing research in this area, e.g., Strong & Gaver (1996) and Hindus (2001), few systems have made it to the market.

We argue that the key missing element is lack of an easy method to manage network communication. Just *how* do people hook up communication appliances? One solution is to attach each device to a computer, but this defeats the elegance of a communication appliance and is beyond the capabilities of the families we studied. Another solution is for each device to have its own method of specifying network connections. This, however, requires more development time and cost while increasing complexity for users and raising compatibility issues.

We suggest a third solution: separating communication appliances from network configuration. Providing a single interface to a wide range of communication appliances simplifies establishment and maintenance of small networks, ensures compatibility and provides several levels of control, depending upon users' needs and abilities. The two key challenges are to create a user interface that is powerful yet simple to use and to develop an underlying technology that is robust enough to work in home settings.

We developed *FamilyNet*, a small, networked device with a tangible interface that enables people to specify members of an intimate social network and control access to their communication appliances. We imposed a strong design constraint: A six-year-old child and his 80-year-old grandmother, neither of whom have ever touched a computer, should be able to specify that they want to talk to each other via any communication appliance. We took advantage of the fact that each person deals with a small number of groups, ranging from 2-10, and membership is mostly stable, with occasional needs to add or remove someone. These constraints make it feasible to design a tangible interface, using physical cards to both represent groups and to act as the interface to the network.

FAMILYNET TANGIBLE INTERFACE
Each communication appliance has a *FamilyNet* module that reads RFID-tagged cards (fig. 1). The simplest case uses only pre-configured *group cards* that link to each other: Placing a group card on a communication appliance establishes a secure link with any other appliance on the network with a card from the same group.



Group card Personal card Public card

Fig.1: The three types of *FamilyNet* cards

For an added level of security, group cards can be set to require authentication: first, group members are defined using their *public cards* (see below), then the small figure in the lower right corner is punched out. Placing a group member's *personal card* together with the group card is now required to establish a link. Personal cards should be kept safe, like credit cards, whereas public cards can be distributed freely, like business cards. New public cards are created by placing a personal card and one or more blank public cards on the communication appliance. Similarly,

placing a group card and a public card on the appliance adds that member to the group.

The red dot in the lower left corner of each card represents the right to make a physical copy of the card, and, when punched out, makes the card uncopiable. Typically, one would keep one copiable card in a safe place and use only non-copiable ones on a day-to-day basis. The *A* symbol on the group card represents the right to add and remove group members. When punched out, the card can no longer administer group members. Since copy, authentication and administer rights are physically punched out, changing them is irreversible. Our user studies have demonstrated that this combination of cards and access rights handles a variety of non-trivial situations while remaining easy to understand and use.

FAMILYNET ARCHITECTURE

The *FamilyNet* architecture (fig. 2) relies on *FamilyNet servers* at each location, typically one per household. Each server communicates with the *FamilyNet readers* present in each communication appliance and with *FamilyNet* servers at other locations. Each server also holds local storage for media (sound, image, video, text, gestures, touch or other data) shared by the groups, and a user interface to create and copy cards and to add or remove members. The architecture also includes a public key server and a domain-name server.

FamilyNet requires secure network communication. Public-key cryptography provides the foundation for representing groups and group membership and for ensuring secure communication. Each group and person is represented by a private key-public key pair whose fingerprint is the ID of the group or person. The private key is stored on the group or personal card (on an RFID tag) while the public key is stored on the public-key server. Group membership is represented by the mutual signature of keys: the group key signs the member's key and the member's key signs the group key. This ensures that only someone holding both a group card and a registered group member's personal card can create a link to that group.

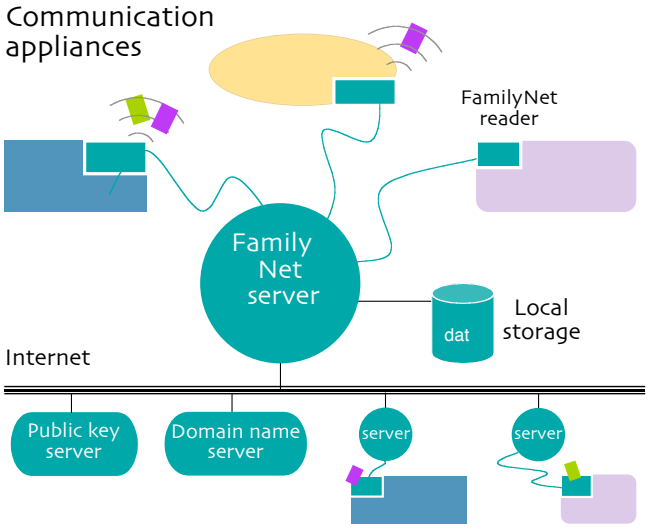


Fig.2: *FamilyNet* architecture

When the first card in a group is placed on a communication appliance and authenticated, a new group multicast address is created and stored on the domain name server, using the group's key fingerprint as ID. This multicast address is then used to communicate within that group. Communications are encrypted with the group's private key and are thus secure. Private keys stay secure by ensuring that they never leak out of the *FamilyNet* reader. Finally, public keys contain only the key fingerprint of the corresponding private card, which is enough to control group membership.

Since group membership and data shared by groups reside in the *FamilyNet* servers, communication appliances can be very lightweight. Replicating data among the *FamilyNet* servers improves robustness, e.g. in case of a crash. Data stored on *FamilyNet* servers is stamped by the group owning it and the time it was created. This allows *FamilyNet* to control all access to data by each communication appliance and to provide services such as filtering or automatic expiration (and deletion) of data.

CONCLUSION

We propose a solution to the problem of interconnecting *communication appliances* that allows the exchange of a variety of personal data among small groups of family and friends. We propose a common interface for managing network configuration of small groups, which can be added as a module to any communication appliance. The simplest version uses pre-configured group cards with RFID tags to create a secure peer-to-peer network using public-key cryptography. The next level of security uses three types of cards with rights to control copying and administration of group membership. We are also working on an on-line version, called Circa, which provides these same services, plus additional features, when controlling access to communication appliances via a computer. *FamilyNet* provides a simple, secure and easy-to-understand user interface for managing small network configuration and thus makes possible a wide range of easy-to-use communication appliances.

REFERENCES

Hindus, D., Mainwaring, S., Hagstrom, A., Leduc, N. & Bayley, L. (2001) Casablanca: Designing Social Communication Devices for the Home. In *Proc. CHI '01 Human Factors in Computing Systems*. ACM Press, pp. 325-332.

Hutchinson, H., Mackay, W., Westerlund, B., Bederson, B., Druin, A., Plaisant, C., Beaudouin-Lafon, M., Conversy, S., Evans, H., Hansen, H., Roussel, N., Eiderbäck, B, Lindquist, S., & Sundblad, Y. (2003) Technology Probes: Inspiring Design for and with Families In *Proc. CHI'03 Human Factors in Computing Systems*, ACM Press, pp. 17-24.

Mackay, W. (2004) The Interactive Thread: Exploring Methods for Multi-Disciplinary Design. In *Proc. DIS'04: Designing Interactive Systems*, ACM Press, pp. 103-112.

Strong, R. & Gaver, W. (1996) Feather, scent and shaker: Supporting simple intimacy. In *CHI'96 Extended Abstracts,*Boston, MA, ACM Press, pp. 444.