Easy-to-Use Firewall Management for Home Users

Kristiina Karvonen
Helsinki University of Technology
P.O.B 5400 TKK
02015 Finland
+358 9 451 8362
kk@tml.hut.fi

Pauli Vesterinen
Helsinki University of Technology
P.O.B. 5400 TKK
02015 Finland
pauli.vesterinen@tkk.fi

Jukka Manner
Helsinki University of Technology
P.O.B. 5400 TKK
02015 Finland
+358 9 4161
jukka.manner@tml.hut.fi

ABSTRACT
In this paper, we identify usability challenges presented by internetworking multiple homes, with a special focus on home network firewall management. The homes nowadays have an internet connection and multiple computers more and more often. The security of the home network is key to safe and trusting usage of this network. Firewalls have a major role in providing this security, acting as safety guard against network attacks. However, in order to truly provide security for the home network, the management of the firewall needs to be easy to use and to understand. The work at hand presents a graphical user interface (GUI) aimed for home network users for enabling easy-to-use, understandable firewall management.

Categories and Subject Descriptors
H.5.2 [User Interfaces]: Evaluation/methodology; K.6.5 [Security and Protection]: Authentication

General Terms
Management, Design, Security, Human Factors

Keywords
Home networks, security, firewall management, usability

1. INTRODUCTION
Currently, more and more homes have multiple computers and other devices that are connected both to each other and to the network [8] [13]. The security of the home network is key to safe and trusting usage of this network. Firewalls have a major role in providing this security, acting as safety guard for the home network against network attacks, but also protecting the Internet from malicious users. Luckily, as regards the end-users, firewalls seem to belong to the best-understood part of computer security – an area often considered as hard to understand and manage by the average, non-technical users [1][6][17][18]. However, even if users can understand the firewalls main functionality and express the need for it, the current firewall management can still be tricky, and the users may easily end up compromising their security by misunderstandings and due to desire for avoiding any elaborate or repeated security configurations: users tend to see security as a hindrance, not as something of interest *per se* [7].

The work at hand presents a graphical user interface (GUI) aimed for home network users for enabling easy-to-use, understandable firewall management. We will first present a short introduction to home networks, and proceed by presenting the current GUI, and some results of the first usability tests we have run with the GUI.

2. HOME NETWORK
What constitutes a home network in practice is not a simple question [2] [3]. In order to identify the challenges embedded in building internetworking between multiple homes in a secure and easily manageable way, we first need to understand what kind of totality of devices, applications, and information we are to manage. The basic concepts of "home", "network", "internetworking", "user" etc. are ambiguous – in order to proceed we need to build working definitions of the basic concepts we are dealing with.

One of the main advantages of home network is that it allows the creation of totality where different kinds of terminals can be used together for accessing any content and services that are part of the home network. The home network can be used for sharing content: photos, records, or videos can be accessed both within home with own or visiting terminals, or remotely from outside the home, enabling a wider audience of this type of personal content, but with restricted access that enhances the privacy as compared with completely open ways of sharing, as e.g. by using flickr.com or similar services for sharing photographs with others online. Sharing photos – and thus sharing memories and experiences – is one of the key uses that will have core place in the emerging home networks also. For example, in one family in the user study we have reported in [9], a grandson had placed a "home server" in his grandmother's apartment, allowing easy access to the joint digital photo collection of the two for the grandmother.

Home networks also allow mixing of content coming from different sources. A typical example of this could be interactive television. In the home networking scenario, members of the family could share and join experiences by interacting with their personal devices on the TV show, competing against each other or against the others as a team. In the future, it will also become possible to enrich the contents by tagging and marking, enabling the sharing experiences of the content as well. A simple example is music sharing, where it is already possible to add tags to the streams for others to look up as "interesting parts".

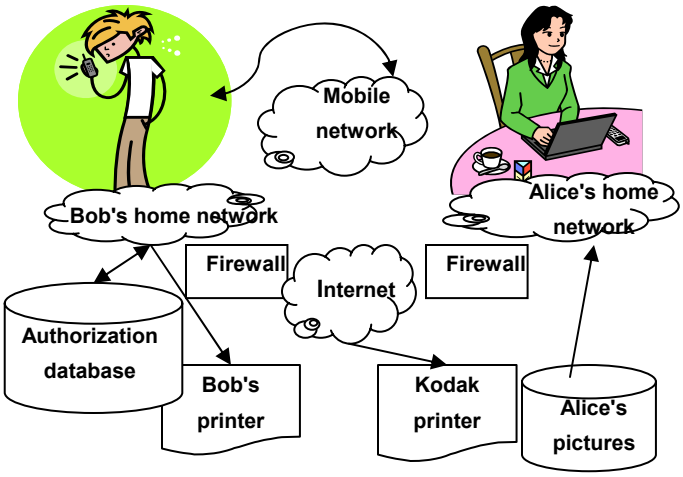

Figure 1. An example of access points between two home networks

Of course, a fully-fledged home network could also be utilised for surveillance-related purposes. For example, the parents might want to check if their kids already arrived home from school and how they are doing while still at work. One more possibility is to control the home devices when away. A good example of a remote control users need is in the paper by Gross et al. [6], who report on the users' expressed wish to "take care of the home" remotely in their study.

The above scenarios illustrate some cases of how the home wireless network can be used. To realize these visions, further development is required on several technology areas. For example, novel circuit and radio technologies are required for the implementation of the network itself. In addition, terminals must be able to work in heterogeneous networks, which must be made secure too. Finally, the applications and the content have to be interchangeable between the different devices. On basis of these observations, we have defined the home network in the following way: Home network is a constantly changing totality of devices – computer, A/V systems, mobile devices, etc. – that can be connected to each other, together with the internet and broadband connections, and that is used by a non-technical user group, typically a family, for personal needs.

3. MANAGING THE HOME NETWORK

It seems to be commonplace that in the homes, one household member tends to have the major responsibility over managing the network, and the other household members do not need to be as knowledgeable about the network [4] [9]. Grinter et al [3] have identified three themes potentially causing trouble in home network maintenance. These are: 1) the myriad of networks that exist in households, 2) the household tensions that emerge due to different personalities and individual needs 3) the collective challenges met with in network administration and troubleshooting. They identify also the invisibility and (in)comprehensibility of the networks as problematic issues in home network management.

In regard to the special needs of different household members of varying ages and capabilities, the paper by Grinter et al. [5] presents a good report on the current level of understanding of the behaviour of the teenage members of the families. The authors also present nicely the current state of existing home network usage practices, the telephone still dominating home communications. Yet, they report on increasing awareness of households on Internet technologies, and the family becoming a source of recreational computing. This increased usage of computers at home has also been the source of research studies, especially email and the World Wide Web (WWW) (e.g., [11], [15], and [16]). They further report on the findings of Kraut et al. [10] on how households tended to prefer communication activities over information activities. According to the authors, this ability to use the computer as a communication appliance may require not only personal access but also that members of our social circle have this, as well. Edwards and Grinter [3] have presented seven challenges that home environment presents to ubiquitous computing technology. These include the deployment of such technologies; technical questions in interoperability, manageability and reliability; social issues in adoption of domestic technologies, as well as design issues.

3.1 Firewall Management

Firewalls are a widely deployed security mechanism, aimed for protection of data and assets behind the firewall. Firewalls act by screening the network traffic in one way or the other, filtering out unwanted traffic. There exists a plethora of different approaches to how the firewall can be implemented: Firewalls can exist on varying levels of the Internet protocol stack, they can be implemented as stand-alone or integrated elements, and their functionalities may differ from each other to a great extent.

In a home network, a firewall can be set up to protect traffic to and from the home network. Luckily, even non-technical users tend to recognize and express the need for firewalls, probably due to the concreteness of the concept. However, implementing, configuring, and managing the firewall falls outside the scope of many users, who would prefer to buy this service from a vendor or rather do without [3][4]. Even when users are willing to manage the firewall protecting their home network, they may run into trouble by making unwise choices for allowing and denying access to their network via the firewall.

A typical home network firewall today has a pre-defined set of rules, which work for most users and applications. However, many of these rules are not needed, or are too simple and flexible, and are always enabled, making the home network nodes vulnerable to a variety of attacks. Moreover, these firewalls typically do not restrict outgoing connections. By restricting also outgoing connections, the firewall protects other nodes on the Internet from viruses and worms spreading, and many sorts of attacks, e.g., distributed denial-of-service, initiated by home network computers taken over by an attacker.

3.2 Firewall Management GUI

Our approach has been to keep the home network always closed as default option – whenever the user wishes to access the outside network, the firewall management GUI will prompt the user for opening the connection for the given application. Thus, only connections specifically indicated by a real person are allowed. The signaling mechanism used in our work is the NAT/Firewall NSIS Signaling Layer protocol [14] defined by the IETF Next Steps In Signaling (NSIS) working group [12].

Further, differentiation between standard user and administrative user was implemented, where only the administrative user, after logging in with username and password, can configure which applications are allowed network access. The standard user can only open and close the network access for the applications the administrative user has added to the GUI. In the administrative view, user can add or remove applications from the GUI, as well as configure their properties. **Figure 2** shows the firewall management GUI in administrative view.

The GUI is divided into several areas. Uppermost is the Information field, where user is shown information on the latest connection opened or closed (1). Furthest on the left are the connection buttons, which can be added or removed, and enabled or disabled in the administrative view (4). In the middle is shown current status of each connection. When the greyed arrow image next to the connection name is turned blue, this indicates that the connection is currently open (2). Furthest right are placed buttons for closing the application and for hiding/opening the GUI in advanced view. In the lowest part of the GUI, there are buttons for adding new connection buttons, changing the settings of the connections, and removing connection buttons (3).

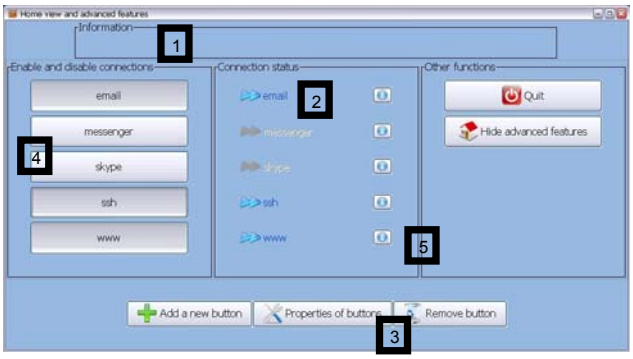

Figure 2. The Firewall management GUI

4. USABILITY TESTING OF THE GUI

We have run a usability test with 9 users in order to test the basic understandability of the concept of managing the network access with the firewall management GUI. Even though the initial results show that users were, in general, able to proceed through the test, succeeding in the test tasks, it became clear that the users did not fully understand the functionalities presented by the GUI. The test setting was quite limited in that the GUI was used separately, not in connection with the applications it was supposed to give network access to. Further, the test group was rather small and the test participants were students in a technical university. The understandability of how to operate with the GUI will probably be much less with users with less technical background, and when used in a more rich environment, i.e., in connection with the applications.

Enhancements to our GUI based on the usability testing include at least the following (numbers refer to items in **Fig.2**):

1. Clearer Information field: the information field showed information on the latest connection opened only for five seconds, after which it disappeared and the field was left empty. On basis of the usability tests, we will redesign this space as a log, showing all connection changes during one session to enable easy keeping in track with current connection history.
2. Simpler configuration of the data flow direction: originally, we differentiated between outgoing and inbound connections on the UI level. However, as most connections are outgoing, and the average home user has difficulties in differentiating between the two, we decided it not to be wise to show the difference to user at all, only showing if a connection is open or not with these indicators in the "Connection status" part of the UI.
3. Renaming of buttons: Some of the buttons in the UI were badly named, e.g. the "Properties of buttons", which seemed to refer to the design or layout of the UI, whereas in reality it was intended for changing the "Connectivity settings". All the UI buttons in this area should rather talk about "connections" than the buttons themselves.
4. Allowing for personalization: Currently, the UI was quite rigid, e.g. the connection buttons appeared in alphabetical order in the UI. Free reorganizing of connection buttons according to e.g. most frequently used first, and so on, were properties users expressed a wish for in the usability tests.
5. Even less technical jargon: from the info button placed next to each connection, the user could gain a pop-up telling about the connection type. However, this information was not understandable to all users, who would have preferred to have more informative text with full sentences to be presented in the pop-up message.

Further redesign items on basis of the usability testing include improving the understandability of changing the properties of buttons to be easier as it currently was according to the outcomes of the usability testing.

5. CONCLUSIONS

As already described, in our first version of the GUI the user could configure the firewall rules based on the direction of the service. The aim was to allow users to set up rules for various services, both on the Internet and offered from the home network to others. In practice, the vast majority of the users do not host services themselves. Therefore, having a field in the setup windows about the direction of the data was somewhat misleading. The new version of the GUI sets up by default rules for outbound services. Rules for incoming services hosted within the home network are set up separately.

Further considerations we need to take into account with redesign include the following:

- How to integrate the firewall management GUI to the general flow of managing home network access?
- Is there a need for allowing personification of the GUI?
- Is there a need to differentiate between administrative and non-administrative users, or could the firewall

management be made so easy and understandable that all users – except perhaps children of the family - could have the same rights?

- What is the right approach for easy-to-use network access management at homes – is it via the firewall management, or something else altogether?
- How to conduct usability testing for the home network access management in a way that best takes into account the richness of home context and its inhabitants?

One more issue that still needs further investigation is mixing automatic and user-driven firewall control. Our GUI is designed from the expectation that users open all firewall rules manually as needed, and close them also when not needed anymore. Yet, it would be quite trivial to automate this process, e.g., firewall rules for web surfing or email could be signaled automatically when the related applications are started and closed. There are good and bad sides to such an approach and we need to look into this more in the future.

6. REFERENCES

[1] Adams, A and Sasse, M.A. Users Are Not the Enemy. Communications of the ACM, Vol. 42, No. 12, December 1999, pp. 41-46, (1999)

[2] Dourish, P., Grinter, R. E., Delgado de la Flor, J.Joseph, M. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. Journal of Personal and Ubiquitous Computing. 8(6) (2004) 391-401

[3] Edwards, W.K., Grinter, R.E. At Home with Ubiquitous Computing: Seven Challenges. In Proceedings of UbiComp 01, (LNCS 2201). Atlanta, Georgia. September 30 - October 2. 256-272.

[4] Grinter, R. E., Edwards, W. K., Newman, M. W., Ducheneaut, N. The Work to Make the Home Network Work. In Proceedings of the 9th European Conference on Computer Supported Cooperative Work (ECSCW '05). Paris, France, Sept 18-22. (2005) 469-488

[5] Grinter, R. E., Palen, L., and Eldridge, M. 2006. Chatting with teenagers: Considering the place of chat technologies in teen life. ACM Trans. Comput.-Hum. Interact. 13, 4 (Dec. 2006), 423-447.

[6] Gross, J. B. and Rosson, M. B. 2007. Looking for trouble: understanding end-user security management. In *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology* (Cambridge, Massachusetts, March 30 - 31, 2007). CHIMIT '07. ACM Press, New York, NY

[7] Herzog, A. and Shahmehri, N. 2007. User help techniques for usable security. In *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology* (Cambridge, Massachusetts, March 30 - 31, 2007). CHIMIT '07. ACM Press, New York, NY

[8] Horrigan, J., Rainie, L: The Broadband Difference: How online Americans' behavior changes with high-speed Internet connections at home. The Pew Internet Project, www.pewinternet.org/pdfs/PIP_Broadband_trends2006.pdf

[9] Kostiainen, K., Rantapuska, O., Moloney, S., Roto, V. Holmström, U., Karvonen, K.: Usable Access Control inside Home Networks, unpublished manuscript, accepted for IEEE TSPUC (2007)

[10] Kraut, R., Mukhopadhyay, T., Szczypula, J., Kiesler, S., Scherlis, W: Information and communication: Alternative uses of the internet in households. Inf. Syst. Res. 10, 4, (1999) 287– 303

[11] Livinsgstone, S. Young People and New Media: Childhood and the Changing Media Environment. Sage Press, London (2002)

[12] Next Steps In Signaling, IETF. WWW: <http://www.ietf.org/html.charters/nsis-charter.html>

[13] Spinellis, D. 2003. The information furnace: consolidated home control. *Personal Ubiquitous Comput.* 7, 1 (May. 2003), 53-69

[14] Stiemerling, M. Tschofenig, H. Aoun, C. Davies, E. NAT/Firewall NSIS Signaling Layer Protocol (NSLP), March 2007

[15] Turow, J., Kavanaugh, A. L. (eds). The Wired Homestead: An MIT Press Sourcebook on the Internet and the Family. The MIT Press, Cambridge, MA. (2003)

[16] Wellman, B., Haythornthwaite, C. (eds). The Internet in Everyday Life. Blackwell Press, Oxford, UK (2002)

[17] Whitten, A, Tygar, J.D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium, August 1999

[18] Yee, K-P. Guidelines and Strategies for Secure Interaction Design, in Cranor, L.F & Garfinkel, S (Eds.): Security and Usability: Designing secure systems that people can use. O'Reilly Books (2005) 247-274