# Exploring the Feasibility of a Spatial User Interface Paradigm for Privacy-Enhancing Technology

Mike Bergmann[1], Martin Rost[2] and John Sören Pettersson[3]

[1] Technical University Dresden, Germany. mb41@inf.tu-dresden.de
[2] Independent Centre for Privacy Privacy Protection (ICPP), Germany. martin.rost@datenschutzzentrum.de
[3] Karlstad University, Sweden. john_soren.pettersson@kau.se

## Introduction

Electronic devices get more and more involved in many of our communication processes for personal and professional activities. Each communication process may implicitly affect our privacy. An example may be the location trace of mobile phones. Experts present identity management systems to preserve the user's[1] privacy [2]. In digital correspondence users should decide about disclosure of personally identifiable information (in the following simply called "data"). However, identity management for Everyman is not yet a commonplace.

To address the whole area of identity management, it is necessary to find an easy to understand model similar to the usage of a phone or a debit card. We suppose that after the shell and command line solutions and the window-based interface, one now has to look for a new paradigm to provide more intuitive handling of the communication process and work flow.

In particular, we have been interested in how to facilitate for users to manage several preference settings, so that different communication partners are treated differently by the user's identity management tool without demanding the user to change settings during ordinary use of his communication devices. We refine the "Virtual City" idea, originally proposed by Andreas Pfitzmann and published in [7], using a town map as a user interface, to manage identity related processes regarding these devices. This interface could potentially allow users with various levels of education to manage their digital identities intuitively by transferring their existing ex-

[1] In the context of this paper, the term "user" describes the person who is using the digital equipment related to the identity management sensitive activities.

*Advances in Information Systems Development: Bridging the Gap between Academia and Industry*. Edited by A.G. Nilsson *et al*., Springer, 2005

periences. We have let ordinary Internet users judge some features of this paradigm to gather results on spatial user interfaces for identity management. These results are presented in this paper together with a discussion on their implications for further elaboration both of the interface paradigm itself as well as of the conditions for user testing such a paradigm.

Immediately below some of the relevant publications in this field are summerized. Then the town map is introduced as a metaphor to visualize identity management related processes. We continue by presenting a test set-up based on animated screen mock-ups as a way to address the question of how to conduct user evaluation in the lack of an implemented town map user interface. We also discuss test results that derive from sessions including 34 test participants. Finally, the paper endeavours an outlook on the place in the 'computer' of user interfaces for privacy protection.

## Related Work

An early work on users' interaction with identity management systems is found in [11] where also the term privacy-enhancing technology (PET) is introduced to refer to the "variety of technologies that safeguard personal privacy by minimizing or eliminating the collection of identifiable data". Identity management is an important part of such technology but beside identity management there are special techniques such as cryptography which are not in themselves related to identity management.

Still, usability issues are not very frequent in PET studies. This is in contrast to the public interest in, on the one hand, privacy in the information society, and, on the other hand, new user interface metaphors (e.g., [10] and [13]).

A statement about the significance of usable interfaces with respect to identity management we find in [1], where Acquisti et al. examine the cost of usability from the economic point of view. They state that "[...] Reducing options can lead to reduced usability, scaring away the users and leaving a useless anonymity system." We will discuss the question how to avoid this.

Wohlgemuth et al. [14], and earlier Gerd tom Markotten and Kaiser [6], develop the thesis about the necessity of a comfortable user interface to enable users to apply identity management. We agree with the authors' statements. Their suggestions are based on conventional window-based control elements such as lists, buttons etc. Also the integration of protection properties into user interfaces, as developed by Wolf and Pfitzmann [15], projects the identity management functionality to common window-based controls. We will extend this approach using a well-known graphical metaphor.

The idea to build a virtual city to manage identities and relations is mentioned by Hansen and Berlich [7]. However, the authors only raise the issue without drawing a concrete scenario. Rost [12] discussed this approach from a sociological point of view. We elaborate this idea further.

It should also be mentioned that leading design experts often bemoan metaphors in user interfaces. Setting out finding a new global metaphor one should consider the criticism launched by Cooper and Reimann against keeping a whole user interface within the confines of a single metaphor ([4], p. 253). They furthermore stress the utility of having controls easily utilized by users. As will be explained further on, we will introduce city districts in a rather metaphoric sense, but only to provide quick and clear access for the user. Indeed, what we will suggest here may not be the only user interface paradigm used within a computer system.

A suitable user interface should be comfortable for clueless and advanced users alike and should cover the complexity of the identity management in an appropriate manner. An identity management application should help the user to enforce his rights of informational self-determination in a complex digital environment [2]. Different studies document that users worry about their privacy [9]. Moreover, the very special security and privacy related terms regarding PET are difficult to understand for normal users. This incomprehensibility often brings negative effects to privacy and/or security, as outlined in [8] and [5].

Furthermore, in everyday life it is not acceptable for the user to have an explicit learning process to become familiar with the PET.

The wide spread desktop metaphor is not sufficient to make identity-related functions accessible. Communication is at the core of using computers nowadays, and privacy protection should thereby also be in the centre. We see the need to sketch a user interface "beyond the desktop".

## Introducing the Town Map

As already mentioned, the core concept of the town map idea is to describe socially relevant communication relations using the topological information of the communication partners.

Two of the most significant benefits of the town map paradigm are first the richness of possible structure in the map to be applicable for most of the existing and further kinds of communication and second the intuitive perceptions across different cultures.

The town map as a spatial metaphor offers easily approachable hierarchies, e.g. using areal representation it is possible to visualize different environments (private, public, restricted, etc). With less distance it is possible to use the building analogy and inside the building the room analogy. Even in an office, we may have the “classical desk”, a bank safe, etc. At the beginning the town map looks empty, there are symbols and signs, but no personal places.

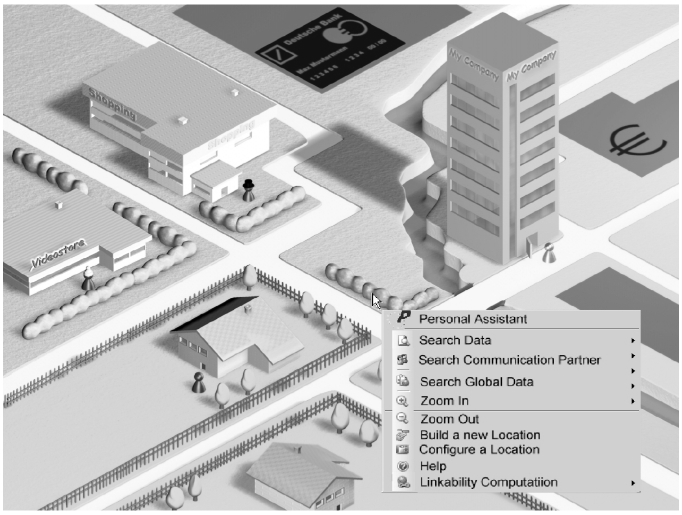


**Fig. 1.** A town map with some attributes and a simple drop-down menu

In particular, it provides an opportunity to deal with one user interface criterion not easily dealt within any program, namely the simultaneous use of several preference settings; in the present context it is the user’s privacy preference settings that are in focus. While font size might be a thing that a user sets once and for all in his Internet browser, it is not that convenient to have only one privacy preference setting active in the browser. How anonymous one prefers to be varies very much according to what service provider one is in contact with or even for what kind of service one is up to. Some standard settings can be defined by (or for) the user, but explicitly switching between settings may be felt as an unnecessary burden for people who are used to browse the web by simply clicking links or entering addresses.

Because privacy protection is a secondary activity in digitally-based communication the identity management functions must not demand extra clicks and key-presses from the user. The question is how to integrate the town map paradigm for user interfaces with the primary activities. In the mock-up we demonstrated in the user test, we catered for three cases:

For the simple case of starting a privacy related application (like email, browser, etc.) and connecting to a communication partner, the town map is very suitable. The map will not emphasize the applications in contrast to the desktop of current PC systems but the communication partners; the corresponding policy settings are implied by location in the map. (In the user test we compromised this global design for a PC system by including the town map as a start page for the browser – it thus functioned as an elaborated bookmark list such as the 'Favorites' in Internet Explorer.)

A quite different case is when the user already is in contact with one service provider, but needs some side issue to be dealt with, such as paying via a pay-service company. Then our PET should be aware of this in order to check credentials for the partner in question. This also means that our PET can show the user what is going on, and we displayed this by a tilted town map introduced in the ordinary browser (cf. explanation to Figure 4).

Thirdly, when a user connects to a communication partner unfamiliar to his PET system (for instance, by clicking on a link on a web page or entering an address in the address field of his browser), then the identity management system should start with maximum privacy settings. If the user wants to bookmark the new site, the system asks for the concomitant policy settings by inviting the user to indicate an appropriate place in the map.

## Living in the Town Map

The typical map contains different areas, districts and buildings, similar to residential areas, city center, business district, recreational parks, etc. These areas represent *different roles* the user can act on. Possibly, avatars at the bounding area of the map will represent corresponding *pseudonyms.*

Areas may be separated by topological borders like rivers and streets. At least four main areas should be defined. The *Public area* represents the anonymous part of the town and incorporates the different social organizations, the shopping area, the entertainment and wellness area etc. The *Business related area* represents the working zone with areas for the company, office, customers and competitors. The "*My Home" area* represents the personal part of the environment and is incorporated in the *Private area* with the different personal social contact partners like houses of friends, family and neighbours, and trusted e-serivces. An example of a town map with some predefined action places is shown in Figure 1.

The topological borders will demarcate different areas with different policies for communication, with different data sets, with different privacy rules and different levels of privacy protection. Entering these areas will change the privacy settings like “do not disclose e-mail address for marketing purpose”, “do not disclose any payment information”, “allow access to nick name” or “enforce unconditional unlinkability” for instance.

Imagine that the default predefined policy for communication in the public area is very restrictive with the lowest level of data disclosure, but around the community area, anonymous communication is not desired, because everybody knows each other. In comparison to this, the working area is characterized by a strong asymmetry between counterparts; the employer knows a lot of details about the employee – clients or customers in comparison know much less (hopefully).

Virtually walking through the town with the mouse pointer, the user’s data policy changes automatically to the predefined set of privacy settings. Connectors between these areas, such as bridges, doors, gates, elevators etc., act as inspection points regarding the communication and privacy settings for the areas. These transition points can allow users to inspect or change the settings. Further domains, with special identity management requirements, could easily be defined. Buildings may contain rooms and areas with dedicated identity management functionality, or simply menu lists with such functions for users who prefer less graphics.

As mentioned above, the main areas include buildings, clustered by the similarity[2] of their privacy policies. In the public area, for instance, there are groups of buildings addressing the shopping context (supermarket, cinema, dry cleaning services), groups addressing the administration context (bank, assurance, e-government), groups for the education context (libraries, universities, school) and the religion context. The distance vs. closeness of the groups to each other could be visualized using different kinds of streets (small alleys, broad roads, avenues, motorways, or similar).

It might be sufficient to have a few predefined places with specific privacy attributes as foreseen in our town map, i.e. the public area, the private area, and the work area. Of course there is a need to offer the possibility to define other places within the map, but predefined places are in all likelihood needed to support novice users.

## Attributes in the Town Map

Attributes are privacy-related policies and properties related to communication partners. Configuration of these attributes may be really complex

[2] It has to be defined how to use slightly different settings in one area and how to visualize the differences without loosing usability and comfortability.

and overburden the normal user. To project these properties intuitively into the town map metaphor we propose the usage of the distances between objects to describe their properties and to group these locations with the topmost level of provision[3] and place them around the other locations with respect to the closeness to other districts. It seems feasible to quarter the whole area into the districts mentioned in the previous section. If a user decides to go inside such a location (e.g., simply by clicking on it) the system may switch to a more detailed presentation, preserving the quartering with respect to the overall privacy settings. Here it opens up new possibilities to introduce associations to special places or direction of movements, similar to joystick-based mobile phone interfaces. The access is granted depending on the access policy of the object and the contingently existing reputation of the user.

## Test Results

How people understand and feel about the town map was tested within the PRIME project (see Acknowledgement) by preference ranking of colour pictures shown in combination with animated user interface video clips.

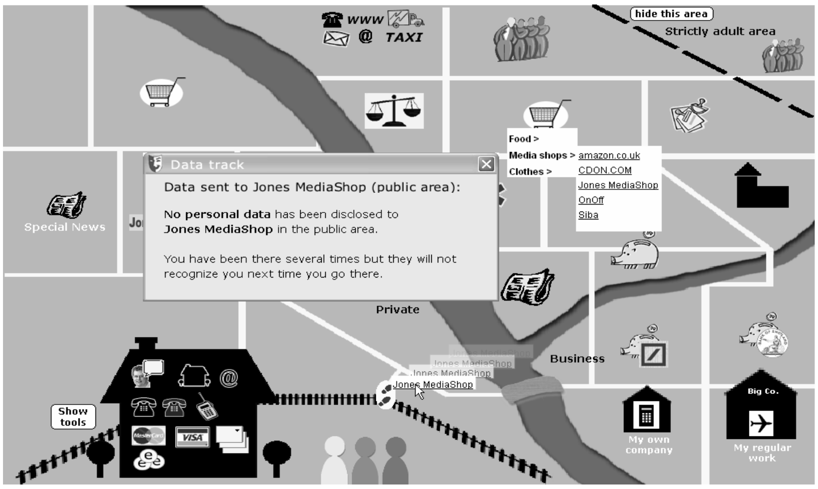
### Aims and Construction of the Test

The town map paradigm was compared to a traditionally styled browser enhanced with roles. In fact, in addition to the Figure 2 TownMap also the CrossRoad of Figure 3 was shown, which is a very simplified town map with the potential to be fitted in small displays. The traditionally styled browser and the more realistic TownMap were animated with a guiding native (= Swedish) voice explaining the actions of the 'user'. Before the test, participants were given a one-page English introduction to identity management and privacy protection. This written introduction also explained two icons appearing in the animations, viz. icons used to symbolise two pre-defined roles. Test sessions were held in lecture halls, allowing multiples of participants in each session.

The goal was not to see if a town map was better than a traditionally styled browser, because most test participants would probably prefer the

[3] From the sociological point of view the groups may be based on the classical four big systems: Economics, Law, Politics, Science. But the organizations are not differentiable by these criteria as far as they implement various connections and communication channels.

browser that looked as they expected, especially since the privacy-enhancement with its specific goals might not be fully comprehended. It must be remembered that people may have varying degrees of understanding of the purpose of identity management and therefore not readily understand the individual steps taken by the ‘user’ in the animations. Considering this, it would be only natural if they prefer a familiar user interface.


Data track

Data sent to Jones MediaShop (public area):

**No personal data** has been disclosed to **Jones MediaShop** in the public area.

You have been there several times but they will not recognize you next time you go there.

**Fig. 2.** User drags a shop’s name to a track icon to get transmission history

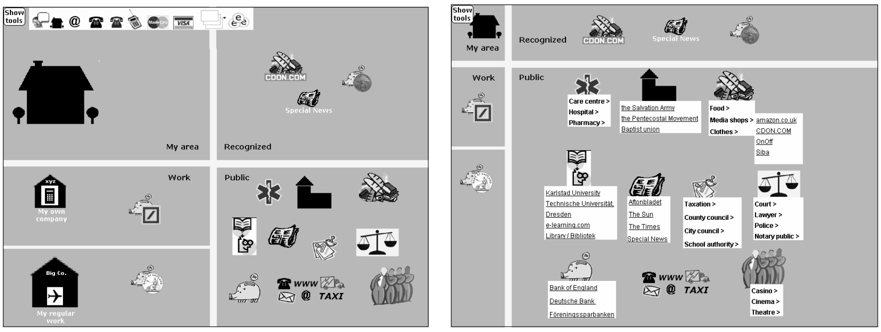
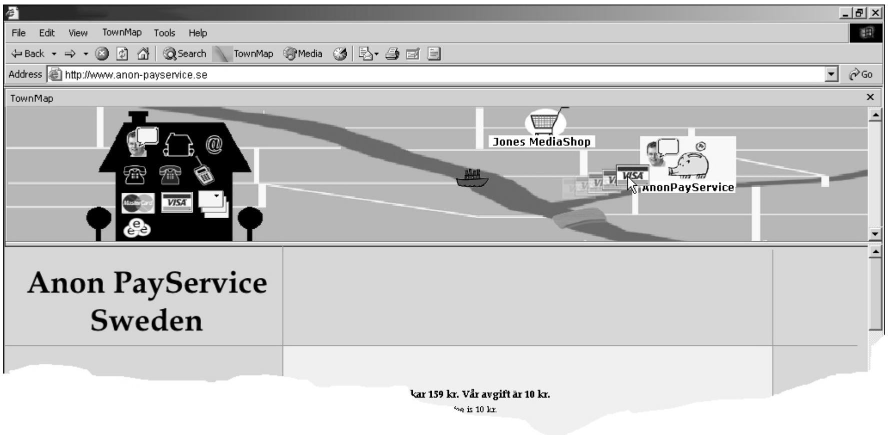


**Fig. 3.** Cross Road consists of four areas; to the right the Public area is enlarged

Thus, the goal was not to see if a town map was better than a traditionally styled browser. Instead, the purpose was to get a basis for discussions within the PRIME project, and of course with interested parties in the rest of the research community, about the semiotic dimension one should venture to play on in more costly prototyping. Especially, since the town map easily allows for demonstrations of data transactions between parties, this feature was included in the animation of the town map (only one of the maps was animated). The user dragged a name icon and a credit card icon to a pay service; his own house and two icons representing the relevant service providers were visible in a tilted town map shown in Figure 4. Later the user also inquired about who had received his name by dropping his name icon on a symbol for his data transactions database (Figure 2).



Anon PayService
Sweden

kar 159 kr. Vår avgift är 10 kr.
ee is 10 kr.

**Fig. 4.** The tested tilted town map (upper half of browser window)

## Results

Thirty-four university students aged 20 and above, some being older than 45, participated in the preference test; all had used Internet Explorer and only some had used other browsers in addition. Our traditionally styled alternative was based on an Internet Explorer mock-up. As expected, the traditional-styled browser got in general a positive response. More than half of the answers gave positive descriptions of it. The maps, on the other hand, were considered by many to be messy.

On the question about their impression of the display of data and money transaction, 19 answered that it facilitates while 11 regarded it as superfluous. Nine of these eleven persons also thought that it looked childish; fifteen thought it looked OK.

When ranking the alternatives, 24 persons put the traditional browser as their primary choice; they also seemed to prefer the simple CrossRoad as a secondary choice. Seven preferred the realistic TownMap and three preferred the simplified CrossRoad, but there was no tendency for the secondary choice.

Two fifths of the participants answered that they would like to be able to switch between designs.

After this paper was submitted this test has been replicated in the USA with 27 university students: the results were in the main similar to the test conducted in Sweden, although a majority of the American subjects wanted to be able to toggle between designs. (The comparison between US and EU users concerned several tests and will be reported in the future.)

## Discussion

In conclusion, even if the map designs were less favoured, there was some interest in this user interface paradigm. This in itself can motivate a further elaboration of this concept. As Allan Cooper explained about targeting a product to a receptive user group: "80% of people in focus groups hated the new Dodge Ram pickup. [Chrysler] went ahead with production, and made it into a bestseller because the other 20% *loved* it. Having people love your product, even if it is only a minority, is how you succeed." ([3] p. 125) But there are further topics of this test that can be discussed.

One should note that the TownMap demonstration film as well as the colour pictures showed maps that were already populated. This fact might have made them appear messier than if users had been introduced with empty maps (corresponding to an empty menu of bookmarks). The bookmarks menu in the Internet Explorer mock-up, on the other hand, contained only six items. In this case it made sense to have only a few items, because the menu did not look sparsely populated as there were simply no empty town districts to fill. The menu was of course short and there were no unmotivated empty spaces. This will have to be remembered for future tests of more elaborate TownMaps or similar user interfaces.

Obviously, there is a conflict between showing first-timers the working of a product and in the same time make him identify himself with the user of that product. In gauging the value of this test one must consider the difficulties of the alternative approach, i.e. of letting test subjects populate the map themselves. Such a test design would be time consuming for two reasons: (1) If participants are to work with the system they would have to do this one-by-one since it is only a mock-up; alternatively, one would have to spend time on producing a working prototype to be able to run it in a computer hall in order to have several participants in each session. (2) Each session takes longer time – to compare, before the preference test real usability tests had in fact been conducted with the traditionally styled mock-up, but these tests often took more than an hour and then it was only one paradigm that was tested. Thus, our preference test was quite cost-efficient even if we might have a “messiness” bias.

One should further note that more than half of the participants answered that animation of transactions “facilitates”. This makes it meaningful to use town map-like formats also in traditionally styled browsers for informing the user of transactions going on. Moreover, it may indicate the utility of using such formats for getting input from the user on data releases. (As explained earlier, in the TownMap demonstration film used in this test some of the animations of transactions were done by the ‘user’.)

In fact, a user may very well benefit from the graphical demonstration of different data disclosures and their effects if third party processors come into play. Possible side-channel attacks might also be easier to visualize than to explain in a text. Thus, the question of visualizing with a town map may not only be thought of as replacing the old desktop but may be introduced via the back door of tutorials and other help functions to become a familiar concept for future communication technology.

## Outlook

This paper raises the question about the feasibility of a new approach to privacy friendly digital environments. It can be argued that by using well-known illustrations from the real world some important issues may be resolved. Currently, the above described system would typically be based on an existing conventional operating systems like Linux, MacOS or Windows. However, it seems conceivable that there is not only a need to create new classes of applications to address the need for managing and administrating the whole communication process with respect to privacy. Instead, this kind of functionality should be directly related to the operating system, or even better should be integrated into the operating system user interface. This guarantees a high level of security, connecting the system to trusted platforms.

## Acknowledgment

We thank all our colleagues for helpful comments, especially Marit Hansen from ICPP, Andreas Pfitzmann, Rainer Böhme from TU Dresden. We thank Simone Fischer-Hübner and Ninni Danielsson, Karlstad University, and Rainer Groh, Katrin Borcea, TU Dresden, and all others for very helpful discussions. Special thanks to Jenny Nilsson, Karlstad University, and Kenneth Ray, TU Dresden, for graphical support. – The work reported in this paper was supported by the PRIME project which receives research funding from the European Community's Sixth Framework Program and the Swiss Federal Office for Education and Science.

## References

[1] Acquisti A, Dingledine R, Syverson P (2003) On the Economics of Anonymity. Proc of Financial Cryptography (FC '03) LNCS 2742. http://freehaven.net/doc/fc03/ econymics.pdf

[2] Clauß S, Köhntopp M (2001) Identity Management and its Support of Multilateral Security. Computer Networks, no 37, pp 205-219

[3] Cooper A (1999) The Inmates are Running the Asylum. SAMS

[4] Cooper A, Reimann R (2003) About Face 2.0 The Essentials of Interaction Design. Wiley Publishing USA

[5] Gerd tom Markotten D (2003) Benutzbare Sicherheit für informationstechnische Systeme. Dissertation an der Albert-Ludwigs-Universität Freiburg

[6] Gerd tom Markotten D, Kaiser J (2000) Benutzbare Sicherheit – Herausforderungen und Modell für E-Commerce-Systeme. Wirtschaftsinformatik, vol 42, no 6, pp 531-538

[7] Hansen M, Berlich P (2003) Identity Management Systems: Gateway and Guardian for Virtual Residences. EMTEL Conference New Media, Technology and Everyday Life in Europe Conference London

[8] Pettersson JS, Fischer-Hübner S (eds) (2004) PRIME Deliverable D6.1.b Evaluation of Early Prototypes. www.prime-project.eu.org/public/prime_products/deliverables/

[9] Leenes R, Lips M (2004) Social Evaluation of Early Prototypes. In: Pettersson JS, Fischer-Hübner S (eds) PRIME Deliverable D6.1.b; see [8].

[10] NN (2004) Metaphorically Speaking. The Economist 373 (8399) Survey of Information Technology. Oct. 28, pp 16-17

[11] van Rossum H, Gardeniers H, Borking J et al (1995) Privacy-Enhancing Technologies: The Path to Anonymity. Registrierkamer The Netherlands, and Information & Privacy Commissioner/Ontario Canada

[12] Rost M (2004) Leben mit der Landkarte – Make Identity-Management Easy. www.maroki.de/pub/privacy/tm.html

[13] Hillenbrand, Th (2004) Melindas Mutantenzoo. Spiegel Online. www.spiegel.de/netzwelt/netzkultur/0,1518,329307,00.html

[14] Wohlgemuth S, Jendricke U, Gerd tom Markotten D, Dorner F, Müller G (2003) Sicherheit und Benutzbarkeit durch Identitätsmanagement. Proc of Aktuelle Trends in der Softwareforschung – Tagungsband zum doITForschungstag 2003 IRB Verlag Stuttgart

[15] Wolf G, Pfitzmann A (2000) Properties of Protection Goals and their Integration into a User Interface. Computer Networks, no 32, pp 685-699