Please reference this paper as
Garzonis, S., O'Neill, E., Kostakos, V., Kaenampornpan, M., and Warr, A. (2004).
A Novel Approach for Identification and Authentication of Users in a Pervasive Environment.
2nd UK-UbiNet Workshop, 5-7th May 2004, University of Cambridge, UK.

A Novel Approach for Identification and Authentication of Users in a Pervasive Environment

Stavros Garzonis, Eamonn O'Neill, Vassilis Kostakos, Manasawee Kaenampornpan, Andy Warr

HCI Group

Department of Computer Science

University of Bath

stagarz@yahoo.com, {vk, eamonn, cspmk, cspaw}@cs.bath.ac.uk

Pervasive computing is a relatively new area of interest within computer science. Most of the challenges faced so far have been technical, as much of the research has been on implementation and the integration of various technologies in the pervasive environment [2]. Although such issues are important and should continue to be studied, they do not address vitally important issues of truly pervasive computing: security and privacy. As computing is moving away from our homes and offices and into our streets, current privacy and security issues are obsolete and need to be modified for our new environment: our pervasive computing world.

Security is an issue which is not often addressed by the HCI community. However, there is a direct, if inverse, relationship between security and usability. In general the more stringent the security, the more it interferes with the user's experience causing a decrease in the usability of the system. The most common impact of security on user interaction is the identification and authentication process: entering usernames and passwords. Considering the desktop paradigm, a user may log on to a computer using a username and password, and never be bothered again by the identification and authentication process while they are logged on. However, when we move into the pervasive environment, this identification and authentication process will intrude more upon the user's interaction as we are exposed to more devices and external networks. The sheer number of usernames and passwords that must be remembered would become a problem [1]. This is considered a major usability problem, with password problems representing 30% of helpdesk calls[1] and up to 90% of users reporting they cannot cope with remembering and using passwords [1].

User identification and authentication can only become worse as we move to a pervasive computing environment, where users have access to a large range of devices and networks. For example, it would be deeply frustrating for users to have to keep entering passwords as they change devices or use different networks, especially when in a pervasive computing world, in which computing resources are intended to become 'invisible' [3].

Current main network security models use IP addressing identification and authentication, which are really of the device and not the user. This model works reasonably well for the traditional deskbound PC user, who typically works at a specific machine with an associated IP-address. Since, in a pervasive computing environment, the user will use different devices and different networks, it would be more beneficial to adopt a new way of identifying the user rather than the device.

Our proposed solution is a network with humans, rather than computing devices. The 'Human Network' is achieved through a combination of embedded biometrics and the use of IPv6 header extensions. This scheme should create a more secure and usable identification procedure and also personalise interaction according to user preferences and the properties of the device being used at the time.

[1] Giga Information Group. http://networking.earthweb.com/netsp/article.php/1444871

Timeouts and password pop-ups impair usability. Embedded biometric systems could perform re-authentication without user intervention. Our proposal is that biometric technologies such as fingerprint, voice authentication and retinal scanners could be placed where the user naturally touches, specks and looks respectively. For example, at a drinks vending machine the user could press the button for a cola. The button could have an embedded fingerprint scanner, allowing the button to dispense the chosen drink and processes the user's information (i.e. perform a transaction with the users back action). As a backup, the system may need to prompt the user to touch a finger scanner or look at the retinal scanner, if the user is not doing so in order to re-authenticate. However, this should be rare, and less intrusive than re-entering a password.

Currently, when a user logs on to a device, they are associated with that device until they log off. However, this can be deceptive in a pervasive computing environment, where devices are publicly available in busy situations, with the risk of a user not logging off. Furthermore, users who have logged into a machine tend to be responsible for operating this machine, and even are responsible for it. These traditional assumptions just do not hold in an environment where potentially hundreds or thousands of devices could be present, each serving the requests of many people for various tasks. A repeated authentication model using biometrics, as described above, could overcome these issues, by integrating user information into each data packet leaving the device. We can achieve this by taking advantage of header extensions available in IPv6, also known as the option mechanism.

IPv6 includes an improved option mechanism over the existing internet protocol, IPv4. IPv6 options are placed in separate extension headers that are located between the IPv6 header and the transport-layer header in a packet. Most IPv6 extension headers are not examined or processed by any router along a packet's delivery path until it arrives at its final destination. This facilitates a major improvement in router performance for packets containing options. In IPv4 the presence of any options requires the router to examine all options. Unlike IPv4 options, IPv6 extension headers can be of arbitrary length and the total amount of options carried in a packet is not limited to 40 bytes. This feature plus the manner in which they are processed, permits IPv6 options to be used for functions which were not practical in IPv4. A good example of this is the inclusion of biometric authentication information to associate information with users.

The same mechanism could also provide a level of support for context awareness by carrying information about the device being used (such as its display size and resolution, connection speed, processing power etc.), the location characteristics of the user and even the activity at hand. This information will remove the need for contextual information to be transmitted separately, and changes to the context would be updated dynamically and transparently through this network protocol.

The concepts of embedded biometric sensors for identification and authentication, and the IPv6 extension headers represent a way of reducing the inverse relationship between security and usability. Combining these will allow users to securely perform tasks in a pervasive computing world without it affecting the users experience or having detrimental effects on their privacy, allowing research visions of "invisible" computing resources to be conceived.

References

[1] Adams, A. and Sasse, M.A., (1999). *Users Are Not The Enemy.* Communications of the ACM. **42**(12): p. 40-47.

[2] Hightower, J. and Borriello, G., (2001). *Location Systems for Ubiquitous Computing.* Computer. **34**(8): p. 57-66.

[3] Weiser, M., (1999). *The computer for the 21st century.* ACM SIGMOBILE Mobile Computing and Communications Review. **3**(3): p. 3-11.