Security Challenges and Selected Legal Aspects for Wearable Computing

John Lindström, Luleå University of Technology, Sweden

Claas Hanken, Nemetschek Bausoftware GmbH, Germany

ABSTRACT

This paper discusses information security challenges encountered during the wearIT@work project and selected legal aspects of wearable computing. Wearable computing will offer interesting opportunities to improve and reengineer work processes in organizations, but can at the same introduce alignment problems as users in organizations may adopt the new technology before organizations are prepared. In addition, needed supportive legal frameworks have not yet fully addressed the new wearable computing technology. Different alignment concepts for how such challenges can be managed are discussed in the paper.

Keywords: *Alignment Problems, Legal Aspects, Pervasive Computing, Security Challenges, Wearable Computing*

INTRODUCTION

This paper, which is to a large extent based on experiences gained during the wearIT@work[1] project, addresses how organizations can approach security challenges and legal aspects while introducing wearable computing in their organizations. If no well considered approach is used, relying on for instance ad hoc principles, there is a risk that instead of rendering business value, the introduction and use of wearable computing can cause the opposite by usage and user behaviour not aligned with the organization's set of rules and beliefs (Davis, 2002; Lindström, 2009). Looking to the future, there is a need for organizations to find ways to improve work productivity, quality and safety. To reengineer work processes in areas where process innovation has been hard without the proper (wearable) supportive tools, there is a need for new and better technology supporting improved performance and productivity (Davis, 2002; Stanford, 2002a; Pasher, Popper, Raz, & Lawo, 2010). Many lines of work do not allow workers to use a computer, e.g., a laptop or PDA, in the workplace due to the nature of their work, for instance where free or clean hands are required. For those groups, there is a large potential in using wearable computers and systems.

The *wearable computing* paradigm has evolved around three factors: smaller, more

DOI: 10.4018/jitr.2012010104

powerful computers, greater personal mobility and increasing personalization of devices. Closely related to each other are *ubiquitous computing*, which is introduced by Weiser (1991), and *pervasive computing,* which refers to the vision where computers are integrated in the environment and the usage is completely transparent to the user. Wearable computing may thus fall under the category of pervasive computing. Lyytinen and Yoo (2002) argue that pervasive computing services require more effort regarding design and maintenance compared to ubiquitous ones, making the availability and usefulness of pervasive computing services limited. However, we think that the recent advances within context awareness-, localization-, and cloud services make this previous gap small today. Wearable computing is also introduced by the wearIT@work project[2] as follows:

"Wearable mobile computing can empower professionals to higher levels of productivity by providing more seamless and effective forms of access to knowledge at the point of work, collaboration and communication. The new technology of wearable mobile computing will meet the need of many individual professionals for acting more flexibly, effectively and efficiently in the increasingly complicated and challenging European work environment. It can be used to enhance jobs in industry and services to make them both more rewarding and effective and re-elevate the role of the professional at work…"

As wearable computers and systems for different business mature, they can be used in a lot of work areas where there is at present very little or no IT-support. Wearable computers will most likely be used more and more, not only at work but also during leisure time. This is due to the fact that wearables, being very small, integrated into clothing and able to interact intelligently with the surrounding environment as well as detect other computing devices (Lyytinen & Yoo, 2002), will be brought almost everywhere. This exposure to a variety of unsecure or hostile network environments will require a higher level of information security to protect personal integrity and privacy, confidential information and communications. At the same time, the legal frameworks need to adapt to the use of wearables, as they put new requirements on the protection of personal integrity and privacy as well as information security. However, one of the problems with legal frameworks and IT is that the pace of development of IT is so fast that the adaption and development of the legal frameworks is almost always a couple of years or more behind, often forcing the frameworks to be very general.

Related Work

Security issues for wearable and pervasive computing have been evolving during the last two decades as the technologies have matured and come into professional use. Dagon, Martin, and Starner (2004) warn early of viruses as well as theft-of-service and denial-of-service attacks, and Stanford (2002b) adds that use within the healthcare sector requires a balance between usability and privacy, and that there is a need to develop security guidelines regarding, for instance, security administration, network security, data security and strong user authentication, and that a layered approach for wireless security can be a good idea. Mann, Nolan, and Wellman (2003) highlight the risk for social surveillance if privacy is not safeguarded. In addition, looking at fundamental challenges to secure pervasive computing, Thomas and Sandhu (2004) mean that there is a need to integrate a socio-technical perspective and that the classical perimeter security breaks down, requiring support for dynamic trust relationships. Further, they add a need for balance in between non-intrusiveness and security strength, support for context awareness and increased mobility, dynamism and adaptability, as well as resource-constrained operations due to limited computing power.

In the recent security research for wearable and pervasive computing, Stajano (2010) states that the main security problems are, particularly