IGI PUBLISHING

ITJ 4919

701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Information Systems for Crisis Response and Management, Volume 1, Issue 2
edited by **Murray E. Jennex and Bartel Van de Walle © 2009, IGI Global**

When and How (Not) to Trust It?

Supporting Virtual Emergency Teamwork

Monika Büscher, Lancaster University, Denmark

Preben Holst Mogensen, University of Aarhus, Denmark

Margit Kristensen, The Alexandra Institute Ltd., Denmark

ABSTRACT

In this article we use the formative evaluation of a prototype 'assembly' of pervasive computing technologies to specify design implications for emergency virtual teamwork tools. The prototype assembly, called "Overview", was implemented in collaboration with police, fire and medical emergency services as part of the real life event management during the Tall Ships' Races 2007 in Denmark. We describe how the emergency teams used the technologies for collaboration between distributed colleagues, to produce shared situation awareness, to manage efforts and resources and respond to minor emergencies. Trust in technology is a key need virtual teams identify in their endeavours to dovetail innovative technologies into emergency work. We show how practices of working up trust are supported by the PalCom open architecture (which was used to build Overview), and delineate design guidelines to enable the productive integration of pervasive computing. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: Palpable Computing; Participatory Design; Trust in Technology; Virtual Teams

INTRODUCTION

Pervasive computing technologies have great potential to augment the work of distributed 'virtual' emergency teams. Experimental R&D shows that interactive maps, mobile and wearable devices, sensor-networks, location tracking, and ambient technologies (e.g. CCTV) could support en route sense-making (Landgren, 2005), risk assessment, resource allocation and communication (Jiang, Hong, Takayama & Landay, 2004), reasoning about conditions on the ground (Betts, Mah, Papasin, del Mundo, McIntosh & Jorgensen, 2005), reconnaissance and navigation (Denef, Ramirez, Dyrks, Stevens 2008), and in-field patient triage and tracking (Lorincz, Malan, Fulford-Jones, Nawoj, Clavel, Shnayder, Mainland, Welsh & Moulton, 2004). However, in practice, the potential of pervasive computing is hard to unlock. Erika Frischknecht Christensen, Medical Director of Pre-hospital care, Central Denmark Region, pinpoints why:

... everybody talks about wireless monitoring, but I haven't seen it work so far. I think one of the things is ... how do I identify the patients, am I sure that what I see on the screen is actually that patient and not that patient? (Discussion, December 2007)

Frischknecht identifies a key need virtual teams encounter in dovetailing innovative technologies into safe emergency work practices: People must be able to trust their technologies.

This is a 'Catch 22' challenge. Trust in technology is 'accepted dependability' (Avizienis, Laprie, Randell & Landwehr, 2004). It grows as technologies become more dependable and familiar, but to become dependable and familiar technologies must be tested in use when they cannot (yet) be trusted. This is particularly difficult in emergency work, where only controlled leaps of faith, combining 'graceful augmentation' (Jul, 2007) with safe levels of redundancy in experimental but realistic use of new technologies will allow innovations to be adopted. This strategy is currently ill supported by many pervasive computing technologies.

In his pioneering vision for 'ubiquitous' computing, it was Mark Weiser's 'highest ideal to make a computer so imbedded, so fitting, so natural, that we use it without even thinking about it." (http://www.ubiq.com/ubicomp/). Weiser's call to make the computer 'invisible' has been enthusiastically interpreted, most often literally. For all the right reasons – e.g. to protect responders from additional work and complexity overload – designers seek to hide computing by embedding it in devices, environments (Lorincz et al, 2004), even clothing (Rantanen, Impiö, Karinsalo, Malmivaara, Reho, Tasanen &Vanhala, 2002), by making it 'autonomous' (Fiedrich, 2000), self-healing, and context-aware (Lorincz et al, 2004). While we value the power of these approaches, we also believe that they can – paradoxically – hamper what they seek to support. This is because Weiser's main concern was not invisibility *per se*, but 'invisibility-in-use', synonymous with the phenomenological notion of 'ready-to-hand', meaning that users are able to focus on their work rather than on their technologies. In this process, trust is not a state of mind, or once-and-for-all accepted dependability, but an ongoing practical achievement. Just as people come to trust other people because they continuously (often precognitively) observe and probe their behaviour in different situations (Boden & Molotch, 1994), people work up trust in technologies through ongoing practical engagement with them (Clarke, Hardstone, Rouncefield & Sommerville, 2006). However, if the technologies are designed to hide their states and processes, people have no basis on which to build their trust. In a conceptual framework for 'palpable computing' we argue that in order to understand and trust technologies people must be able to sense what these technologies are doing or could do for them (Kyng, 2007). To this aim, we have developed an open software architecture and prototype technologies that support people in making computing palpable (Andersen, 2007).