Pers Ubiquit Comput (2014) 18:115–116
DOI 10.1007/s00779-012-0630-2

EDITORIAL

Security and trust in context-aware applications

René Mayrhofer · Hedda R. Schmidtke ·
Stephan Sigg

Published online: 27 November 2012

Context-aware appliances are maturing to enter the market place. The sum of smart phones and tablets sold begins to outnumber the number of desktop PCs sold. The number of sensors built into these systems and the processing power also has increased. However, most importantly, context-aware applications platforms are entering the market, making use of sensory information to provide users with advanced functionality as well as novel means of access to information in their environment. As context-aware systems are leaving the laboratories and enter the life of a growing portion of the population, it becomes increasingly important to ensure that crucial features of security and privacy are added to foster and maintain the trust of users. This transition from applications in the laboratory to marketable apps has been a focus of recent research, at conferences such as the Context conference, whose 2011 edition focused on the challenges of commercializing context. This theme issue came out of the increasing demand for making context-aware applications secure and trustworthy.

R. Mayrhofer
School of Informatics/Communications/Media,
University of Applied Sciences Upper Austria,
FH OÖ, Studienbetriebs GmbH, Softwarepark 11,
4232 Hagenberg, Austria
e-mail: rene.mayrhofer@fh-hagenberg.at

H. R. Schmidtke (✉)
Carnegie Mellon University, Boulevard de l'Umuganda,
Kacyiru-Kigali, Rwanda
e-mail: schmidtke@cmu.edu

S. Sigg
National Institute of Informatics (NII),
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan
e-mail: sigg@nii.ac.jp

Conventional techniques cannot fully cover the breadth of new challenges of context-aware applications. Knowledge about the context of users allows an application to support them better, and it also provides valuable information not only to advertising companies but can also—if not adequately protected—be used for malicious purposes: Location information about a user is as valuable to his friends as it is to a burglar. Moreover, information that is made accessible to friends and family members and information to be provided, for instance, to advertisers or employers need to be separated.

The articles collected in this theme issue address challenges and solutions on several levels of a context-aware system, its design, and usage. Hoffmann and Söllner discuss how software engineering methods can be adapted using a concept of trust from the behavioral sciences. Acknowledging that it is better to present users with a trustworthy application from the start, they present a strategy for including evaluations of several parameters of trust into a conventional interview-based user study.

A major challenge in context-aware systems is their dependence on the physical and social world. Location-aware systems act within the personal spaces of an individual and need to be aware of the non-spatial aspects of a location, so as not to be considered invasive by a user. The article by Toch addresses the acquisition of such hard to formalize knowledge by means of crowd-sourcing: The author reasons that, although powerful privacy controls are required, they are difficult in their use and not always accurate. By collecting and analyzing the opinion of a large number of users, his system can inform the mobile device whether to allow or deny access to location information in a specific context.

As mobile devices become personal companions of their owners, containing not only sensitive communication data but acting increasingly also as tools for financial transactions, fast detection of theft of a mobile device is becoming a vital concern for users. Two statistical profiling approaches that could make it possible to detect theft of a mobile device from anomalies in spatio-temporal context are proposed by Yazji et al. They compare two models of spatio-temporal behaviors: a model based on cumulative probability of a trajectory and a model representing trajectories by Markov models.

The increasing value of context information itself is the target of location privacy attacks. Wernke et al. outline a chart of this field assuming a widened, more context-centered perspective. The article analyzes location privacy as being not only a question of protecting location information. Attack scenarios usually involve at least two other parameters of context: time and user identity.

Increasingly, instrumented environments using NFC-enabled smart phones as RFID readers are employed to obtain and process context information by tagging objects and environments. The question arises how this approach can securely scale as massive amounts of RFID tags identify environments, objects, and users. Rahman and Ahamed propose a batch authentication protocol enabling detection of an intrusion of larger numbers of counterfeit tags, a technique that is not only valuable for future smart environments but already today in applications such as medical product authentication.

A major aspect of research on context is its interdisciplinary nature. Context-awareness always regard the context of a human being, thus having cognitive, linguistic, social, legal, and physical dimensions. Research on security and privacy of context-aware systems has to regard all these dimensions. The articles compiled in this theme issue lay out new paths into this wide and new terrain.