UDC 004.056:004.7

S. O. Kostyshyn

SECURITY AND PRIVACY ISSUES OF UBIQUITOUS COMPUTING IN THE OFFICE SETTING

Ubiquitous computing (ubicomp) has been an area of considerable scientific interest since 1991. An outline of it and related security issues can be found, for example, in [7]. A large number of publications and projects have focused on ubicomp technologies in the home setting. In contrast, this paper overviews its security and privacy implications at the workplace.

There are several security-related features that a modern office ubicomp environment could be reasonably expected to possess as opposed to home and mobile contexts:

1. A network constantly managed by professionals and, to some extent, governed by centralized security policies.
2. Permanent Internet connection and, as a result, availability of trusted third parties for the purposes of authentication.
3. High or critical business value of information stored and, more importantly, transferred.
4. “Guest” people and devices whose identity it may be hard to establish.

Privacy concerns are stronger in the office setting. Traditionally, home and wearable ubicomp devices are assumed to collect a spectrum of private information for purposes ranging from deducing personal preferences to providing medical care. On the other hand, in “weak” ubicomp [8] that is more realistic for modern offices a large part of such information is next to useless and is not supposed to be acquired in the first place. Yet, it could be inferred from routinely gathered data or retrieved secretly.

Traditionally, security of a system is understood as a complex of its three properties: confidentiality, integrity and availability. The nature of pervasive computing has important implications on each of these components, especially the two latter [9]. Ubiquitous computing devices are usually characterized by tighter constraints than conventional personal computers, specifically of computing power, memory size and battery life (if applicable). With regard to encryption these constraints mean that use of “expensive” public key cryptography (in particular encryption and verification operations)

should be minimized in favor of computationally “cheaper” symmetric cryptography [9]. Some authors also argue that “the domination of asymmetric cryptography has, in part, been spurred by the need to implement identity authentication” [2, p. 90], and therefore question its merits in ubicomp where the identity authentication is of low, if any, practical value (see below).

Much debate is evolving around the entities that are to be authenticated. Creese et al. [2] argue that the traditional identity authentication is unsuitable for ubicomp for at least two reasons: interactions take place between devices, for which it might be impossible to establish identities; even if verified, such an identity itself gives no confidence about the device’s future proper behavior. They suggest instead that individual attributes of devices (location, manufacturer, state, history etc.) are authenticated, provided that such attributes are “chosen to achieve assurance about which devices are the subject of interaction, and what those devices will do” [2, p. 85].

The assumption we made about constant availability of trusted third parties in office environment is important here as in that case existing authentication techniques may be used.

Any device that carries some ID or certificate can become a target of attack seeking to extract that information. Small size of ubicomp nodes facilitates their theft and covert replacement. This means that it’s reasonable to make the devices tamper resistant so that the ultimate cost of retrieving information from them becomes disproportionately high.

Regarding availability, ubicomp introduces a type of denial of service attacks aiming to deplete a device’s battery. In the office environment this threat’s severity can be limited, though not eliminated, by powering the devices centrally where possible.

Also one cannot avoid the social implications of ubicomp. By the very nature, it has a potential of an ideal surveillance system [7], “a dream come true for electronic stalkers and "big brothers"” [1, p. 1]. The discussion of privacy issues of ambient intelligence has become commonplace in scientific circles, to the extent that its prevalence has attracted criticism [8, p. 410]. However, it is widely believed that the future of ubicomp market will ultimately depend on its ability to ensure privacy of users.

Gow [4] describes three domains of privacy in ubicomp: technical, regulatory (including legal) and sociological. At present, the problems best developed within the technical domain are those of location privacy and user anonymity. Interesting recent works in this area include [5] introducing an

intuitive concept of “virtual walls”, and [1] describing a hierarchical structure creating a “mist” to hide user identities and/or physical location from other users and the system itself.

From a different perspective, [6] presents a device for aiding in RFID tag management including blocking unwanted reader-tag interactions by means of selective jamming. Being probably an acceptable solution for well-informed individuals, it requires on the person’s part more knowledge than could be expected from a typical ubicomp target user.

Robinson et al. [7] maintain that the technology itself is not enough to ensure privacy, and rely on legislation for protecting it. There is a progress in the area of privacy regulation in different jurisdictions, primarily EU and USA.

Finally, a number of publications treat the problem of privacy from the social perspective. For example, [3] coins such terms as “digital territory” and “virtual residence”. That approach is highly intuitive but lacks a technical foundation. As a result, it remains unclear how (and whether) suggested concepts could be implemented technologically in ubicomp.

Security and privacy of ubicomp are combinations of technological, legal and social challenges. This paper has attempted to highlight a number of such problems as relevant to present-day office environments employing limited implementations of the ubicomp potential.

References

1. Al-Muhtadi J., Campbell R., Kapadia A., Dennis Mickunas M., Yi S. Routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments // International Conference of Distributed Computing Systems (ICDCS 2002). – Vienna, 2002. – P. 65-74. – http://ciae.cs.uiuc.edu/mist/mist.pdf .
2. Creese S., Goldsmith M., Roscoe B., Zakiuddin I. Research Directions for Trust and Security in Human-Centric Computing // Ed. Robinson P., Vogt H., Wagealla W. Privacy, Security and Trust within the Context of Pervasive Computing. – Springer, 2005. – P. 83-91.
3. Daskala B., Maghiros I. D1gital Territ0ries – Towards the protection of public and private space in a digital and Ambient Intelligence environment. – Institute for Prospective Technological Studies (IPTS), 2007. – 122 p. – http://ftp.jrc.es/eur22765en.pdf .
4. Gow G. Privacy and Ubiquitous Network Societies // ITU Workshop on Ubiquitous Network Societies. – ITU, 2005. – 34 p. – http://itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf .
5. Kapadia A., Henderson T., Fielding J. J., Kotz D. Virtual Walls: Protecting Digital Privacy in Pervasive Environments // International Conference on Pervasive Computing. – Springer, 2007. – 18 p. – http://www.ists.dartmouth.edu/library/365.pdf .
6. Rieback M., Gaydadjiev G., Crispo B., Hofman R., Tanenbaum A. A Platform for RFID Security and Privacy Administration. – 2006. – 14 p. – http://www.cs.vu.nl/~melanie/rfid_guardian/papers/lisa.06.pdf .
7. Robinson P., Vogt H., Wagealla W. Some Research Challenges in Pervasive Computing // Ed. Robinson P., Vogt H., Wagealla W. Privacy, Security and Trust within the Context of Pervasive Computing. – Springer, 2005. – P. 1-16.

8. Rogers. Y. Moving on from Weiser's Vision of Calm Computing: Engaging UbiComp Experiences // Ed. Dourish P., Friday A. Ubicomp 2006. – LNCS vol. 4206. – 2006. – P. 404-421. – http://www.slis.indiana.edu/faculty/yrogers/papers/Rogers_Ubicomp06.pdf .
9. Stajano F., Anderson R. J. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks // 7th Security Protocols Workshop. LNCS vol. 1796. – Cambridge, 1999. – http://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf .