AMBIENT INTELLIGENCE ENVIRONMENTS: FOCUS ON A HUMAN

by

ALŽBĚTA KRAUSOVÁ*

For the past few decades people have faced a dramatic technological development. One of the new technologies that are predicted to be massively widespread in the future is Ambient Intelligence. One can imagine Ambient Intelligence as an environment with embedded sensors enabling the environment to anticipate wishes of its users and to adapt itself accordingly. Development and utilization of such environments, however, entail new threats. The aim of this paper is to identify these threats and the dangers resulting from the need to collect and further process all kinds of data in order to provide highly personalized services.

KEYWORDS

Ambient Intelligence, privacy, threats to privacy, data protection

1. INTRODUCTION

Each new technology influences the society and may entail unpredictable impacts. The aim of this article is to describe the technology of Ambient Intelligence (AmI), its principles and practical implementations, and to define threats that this technology may pose to the society. The analysis of AmI environments will be based on the work done in the scope of the SERENITY project,[1] a European project aiming at enhancing security and dependability in AmI environments.

First of all, AmI environments will be introduced in detail. Next, the idea of AmI environments will be challenged with the concept and the importance of privacy. Later, the threats that AmI environments may pose will be identified. Then, the technical solutions representing a means of prevention

* Former legal researcher of ICRI – K.U. Leuven – IBBT. Currently Ph.D. Student at the Faculty of Law, Masaryk University, Brno. E-mail: Betty.Krausova@seznam.cz

[1] For more details about the project see http://www.serenity-project.org/ or http://www.serenity-forum.org/

of some previously mentioned threats will be presented. Finally, the conclusion will outline some ideas for further research.

2. AMBIENT INTELLIGENCE AND ENVIRONMENT

The aim of this section is to introduce AmI environments in detail. AmI represents a human oriented technology. It is based on the convergence of three technologies: Ubiquitous Computing, Ubiquitous Communications, and User Friendly Interfaces.[2] The main task of Ubiquitous Computing is to integrate sensors and other micro devices into everyday objects. The field of Ubiquitous Communication allows communication and interaction of various devices. User Friendly Interfaces then enable "interacting with devices in a human-like way. The main technologies are speech, gesture, emotions, artificial skins, and multimodal interaction".[3] In other words, the AmI technology aims at creating "seamless environment[s] of smart networked devices that [are] aware of the human presence and together with the ever-enhancing data-mining capabilities [give] the possibility for personal data to be invisibly captured, analyzed and exchanged among countless sensors, processors, databases, and devices to provide personalized and contextualized information services".[4]

The vision of AmI foresees environments in which people will "be surrounded by intelligent interfaces supported by computing and networking technology that is embedded in everyday objects such as furniture, clothes, vehicles, roads and smart materials – even particles of decorative substances like paint".[5]

The development of AmI environments is heading to creating systems and services that are characteristic with the following features: they are "networked, mobile, seamless, and scalable, offering the capability to be always best connected any time, anywhere and to anything; […] embedded into the things of everyday life […] intelligent and personalized, and therefore more centred on the user and their needs; […] rich in content and experiences and in visual and multimodal interaction".[6]

---

[2] IST Advisory Group 1999, Orientations for Workprogramme 2000 and beyond, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-99-final.pdf. Accessed 21 August 2008.

[3] IST Advisory Group 2004, Experience and Application Research: Involving Users in the Development of Ambient Intelligence, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/2004_ear_web_en.pdf. Accessed 21 August 2008. p. 17.

[4] Qtd. on pp. 60-61 in Gadzheva, M. 2008, 'Privacy in the Age of Transparency: The New Vulnerability of the Individual', Social Science Computer Review, vol. 26, no. 1, pp. 60-74.

[5] IST Advisory Group 2003, Ambient Intelligence: From Vision to Reality, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-ist2003_consolidated_report.pdf. Accessed 16 July 2008. p. 8.

[6] IST Advisory Group 2006, ISTAG Report on Shaping Europe's Future Through ICT, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-shaping-europe-future-ict-march-2006-en.pdf. Accessed 21 August 2008. p. 2.

The application of AmI systems is presumed to be very wide. The systems and services with the above mentioned features are to be used in the sphere of telecommunications including value added services, in the home environment, in business, health services, e-government, and in the automotive and other industry[7].

One of the interesting applications of AmI systems is in the e-health domain. Currently, there already exist some prototypes of "smart houses" that utilize AmI systems. As particular examples the vision of the SERENITY project Smart Items scenario and the Smart Home in Sherbrook will be introduced.

The SERENITY Smart Items scenario describes a 56-year-old widowed man, called Bob, who is discharged from hospital after a cardiac arrest. His health, however, still needs to be monitored. Bob joins a special experimental programme and has a sensor network installed in his house. The sensor network monitors information on room temperature, pressure and humidity, lamp status, movements of the inhabitants, etc. Moreover, Bob is supplied with a smart item that regularly collects health information, such as his heart rate, blood pressure and bodily temperature. This information is then conveyed and stored on Bob's e-health mobile terminal, e.g. his PDA that enables him to communicate the data to his doctor. Integration of applications managing the sensor network and the e-health devices is presumed.[8]

The Smart Home located at Université de Sherbrook is an existing prototype of a house which aim is to assist people suffering from dementia, schizophrenia, and other diseases. The house is equipped with the following devices: infra-red presence sensors, electro-magnetic door sensors, sensitive rug / pressure mats, floor pressure mats, interaction centre, interactive touch screen TV, cameras for remote monitoring, speakers, RFID antennas, and an electronic pill dispenser.[9]

The above mentioned prototypes are designed for patients. However, the AmI technology is intended to be implemented in common households as well in order to help to create lives as comfortable as possible. The question is whether the price for such comfort would not be too high. The following section will challenge the idea of AmI environments with the concept of privacy.

---

[7] IST Advisory Group 2002, Software technologies, embedded systems and distributed systems: A European strategy towards an Ambient Intelligent environment, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag_kk4402472encfull.pdf. Accessed 21 August 2008.

[8] SERENITY Project, A7 Deliverable – A7.D1.1 – Scenario Selection and Definition, EU-IST-IP 6th Framework Programme - SERENITY 27587, http://www.serenity-forum.org/IMG/zip/A7_1_.D1.1_scenarios_v1.1_final.zip. Accessed 2 January 2009.

[9] SERENITY Project, Securing Smart Home: How SERENITY Patterns Enforce Security in Remote Healthcare Systems, http://www.serenity-forum.org/IMG/pdf/serenity_leaflet08_web.pdf. Accessed 25 November 2008.

3. PRIVACY IN AMI ENVIRONMENTS

The previous section described some particular functions, features, and possibilities of AmI environments. In order to fulfil their functions, AmI systems must process huge amounts of various kinds of data that, in many cases, are personal data, eventually sensitive personal data. This, of course, gives rise to questions about privacy of an individual living in such environment. Privacy is for the majority of people an ambiguous term which can be interpreted individually. Therefore, the next subsection will describe the notion of privacy in its complexity.

3.1. CONCEPTS OF PRIVACY

Throughout the history various scientists have come up with various definitions of privacy. The most important conceptions of privacy have been clearly classified by Daniel J. Solove in his latest book Understanding Privacy:[10] In 1890, Warren and Brandeis defined privacy simply as the "right to be left alone". Approximately at the same time Godkin came up with the definition of privacy in the terms of "limited access to the self" and emphasized a control an individual has over living together with other people and over dissemination of personal information related to him or her. Posner considers privacy as primarily related to secrecy and thus promotes a right of an individual "to conceal discreditable facts about himself".[11] Westin later redefines privacy purely as a control over personal information when he states that "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[12] Another conception of privacy is based on "the protection of the integrity of personality".[13] Other authors, such as Farber, Gerstein, or Innes, connect privacy with intimacy.

The latest theory of privacy was recently introduced by Solove also in this book.[14] Solove created taxonomy of privacy problems recognized by the society. This taxonomy includes problems related to information collection, information processing, dissemination of information, and invasions into individuals' private affairs.

As the proper functioning of AmI environments is, inter alia, based on continuous monitoring of individuals, the individual's right of privacy defined through the above mentioned concepts could be endangered. This

[10] Solove, D. J. 2008, Understanding Privacy, Harvard University Press, London.
[11] Qtd. on p. 21 in Solove, D. J. 2008, Understanding Privacy, Harvard University Press, London.
[12] Qtd. on p. 24 in Solove, D. J. 2008, Understanding Privacy, Harvard University Press, London.
[13] *supra* note 10
[14] *supra* note 10

is even more significant in case when personal or sensitive personal data are processed. Why the protection of privacy is such a major issue will be explained in the following subsection.

3.2. IMPORTANCE OF PRIVACY

Although one can encounter sceptics doubting about the importance of privacy, the majority of scientists agree that privacy has a number of substantial functions. First of all, privacy has been recognized as "an important human need. It enables people to manage both personal activities and social interactions. Privacy relates to effective individual and group functioning […]. Failure to meet privacy needs has been shown to be related to antisocial behaviors and aggression".[15] This statement suggests that privacy has psychological functions. In accordance with Pedersen,[16] these functions include contemplation, rejuvenation, confiding, creativity, disapproved consumptions, recovery, catharsis, autonomy, and concealment. The mentioned functions are interconnected with functions defined by Westin: personal autonomy, emotional release, self-evaluation, and limited and protected communication.[17]

In my opinion, privacy has one major function which is superordinate to all previously mentioned functions. This function consists in enabling an individual to regulate the level of own vulnerability. An individual can regulate this level for instance with the selection of personal information to be disseminated or people to spend their time with. Each person has different weaknesses and privacy helps the individual to deal with them without being intimidated by other people.

4. THREATS POSED BY AMI ENVIRONMENTS

In the previous text it was concluded that the very nature of AmI environments can threaten the right of privacy of individuals living in such environments, i.e. their users. The main function of privacy is to enable an individual to regulate the level of own vulnerability. Therefore, the main threat posed by AmI consists in increased vulnerability of a user. Among the causes of this increased vulnerability there belong cases when AmI environment providers act contrary to law or try to evade law. Another cause of increased vulnerability is represented by technical failures in AmI systems. The following sections will illustrate these causes with some examples.

---

[15] Qtd. on p. 147 in Pedersen, D. M. 1997, 'Psychological Functions of Privacy', Journal of Environmental Psychology, vol. 17, no. 2, pp. 147-156.

[16] Pedersen, D. M. 1997, 'Psychological Functions of Privacy', Journal of Environmental Psychology, vol. 17, no. 2, pp. 147-156.

[17] *supra* note 16

4.1. ACTING CONTRARY TO LAW

Although AmI is not a concept specifically regulated by law, there exist rules of processing personal data set out in European and national legislations. The main European directives regulating AmI environments in general are the Data Protection Directive,[18] the Directive on Privacy and Electronic Communications,[19] and the Data Retention Directive.[20] These directives set out many requirements on the data processing. Except of these directives there also exist national criminal codes prohibiting certain acts that result in harming individuals. Acting contrary to law can be performed in an endless number of forms, so only few examples will be mentioned.

Among unlawful acts of AmI environment providers there belongs for instance adoption of weak security measures. Such practice may lead to unintended disclosure of data, and facilitates attacks on network operation (such as eavesdropping, traffic analysis, the insertion of false data, changes to routing behaviour, or physical attacks on sensors).[21] Other examples of unlawful behaviour are breach of confidentiality of personal data or misuse of such data. These may lead to discrimination practices, abusive marketing, blackmailing, or unlawful disclosure.

4.2. EVADING LAW

Evading law consists in twisting the meaning of a particular legal clause. Examples of such practice are extensive interpretation of legitimate grounds for processing of personal data[22] or sale of personal data based on data subject's consent with a wide formulation of data controller's rights. This particular practice is not explicitly prohibited but at the same time it evades law as such practice does not contribute to the well-being of individuals.[23]

---

[18] The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[19] The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection on privacy in the electronic communications sector.

[20] The Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[21] Such attacks should be considered as crimes in accordance with relevant national legislations. The majority of these acts correspond to offences defined by the Council of Europe's Convention on Cybercrime (offences against the confidentiality, integrity and availability of computer data and systems). The examples of the attacks on network operation were taken from Gruetser, M., Schelle, G., Jain, A., Han, R. & Grunwald, D. 2003, Privacy-Aware Location Sensor Networks. http://systems.cs.colorado.edu/Papers/Generated/2003Privacy-AwareSensors.pdf. Accessed 5 August 2008.

[22] Article 7 and Article 8, par. 2 of the Data Protection Directive

[23] Recital 2 of the Data Protection Directive

4.3. TECHNICAL FAILURE

A technical failure in an AmI environment can cause a serious harm to its users. For example power supply shortage, opening door to a stranger, disclosure of (sensitive) personal data or an error of medical device can have dangerous impact on health, security, and dignity of people living in such environment.

5. PREVENTION OF THREADS: TECHNICAL SOLUTIONS

The previous section briefly illustrated some possible threads posed by AmI. In order to minimize these threads, the designers of AmI environments need to find ways how to prevent them. The aim of this section is to explain the technical solution adopted in the SERENITY project.

The SERENITY approach is based on so called Security and Dependability Patterns (S&D Patterns). These S&D Patterns capture the best practices for ensuring security, dependability, privacy, and legal compliance. They actually provide solutions for identified problems in the machine-readable form and thus can be automatically applied in a system. Patterns capturing legal requirements and solutions for legal problems are simply called legal patterns. Initially, legal patterns are written in a natural language.[24] Later, they are formalized by their translation and creation of a model,[25] which is validated by checking its correspondence to the legislation. Finally, the validated pattern is coded and can be applied. The structure of a legal pattern contains description of the Context, identification of the Problem and the Property to be provided,[26] the Solution, and the Monitoring Rules. Translated and coded legal patterns are applied in a system at run-time. This ensures automated enforcement of captured legal requirements.

Besides the introduced S&D Patterns also a proactive run-time support is created in the scope of the SERENITY approach. Its aim is to adapt an attacked system or an application. This support[27] is also able to identify weaknesses in order to later amend existing S&D Patterns.

---

[24] A good illustration of what kind of a problem a legal pattern can capture is for instance the pattern called 'Ensuring that the Patient Always Has the Right to Access and Request the Correction of his Personal Information'. For more details see SERENITY Project, A1 Deliverable – A1.D3.1 – Initial Set of Security and Privacy Patterns at Organizational Level, EU-IST-IP 6th Framework Programme - SERENITY 27587, http://www.serenity-forum.org/IMG/pdf/A1.D3.1_patterns_at_organizational_level_v1.3_final.pdf.

[25] In the SERENITY project legal patterns were translated with the help of the SI* modelling language and Secure Tropos requirements methodology.

[26] Property refers to a certain quality that should be ensured by application of a particular pattern. Legal patterns generally provide properties of legal compliance or legal certainty.

[27] This support is called SERENITY Runtime Framework.

The presented SERENITY approach shows how the prevention or at least minimization of threads and their harmful consequences can be technically ensured.

6. CONCLUSION

The aim of this article was to describe the technology of AmI and to identify possible threads posed by this technology. It is obvious that AmI entails many threads of which a lot is related to privacy of users of AmI systems. The endeavour to minimize these threads is apparent as well. However, although the designers of AmI systems spend great effort to create them as safe as possible and compliant with law, it is at the same time necessary to question the existing legislation. During the time of its adoption the advent of AmI systems was not presumed. As the very idea of AmI demands processing and integration of huge amounts of data and personal data, there might appear legal lacunae enabling to harm interests of AmI users. In my opinion, further research should be carried out in order to determine whether in the future it will be necessary to adopt special legislation regulating AmI. Apart from the possibility of existence of legal lacunae, it should be also taken in account that private subjects (providers of AmI systems and applications) will sometimes possess nearly complete information on users' private lives. Such research and possible changes in legislation should be carried out before AmI starts to be massively used by public. The reason is the necessity to ensure trust of people in AmI systems in order not to waste already spent investments in the research and development of these systems.

ACKNOWLEDGMENTS

This work was partially funded by the EU Commission through the project IST-FP6-IP-SERENITY.

REFERENCES

[1] Aggarwal, G., Bawa, M., Ganesan, P., Garcia-Molina, H., Kenthapadi, K., Mishra, N., Motwani, R., Srivastava, U., Thomas, D., Widom, J. & Xu, Y. 2004, 'Vision Paper: Enabling Privacy for the Paranoids', VLDB Endowment Inc., http://www.vldb.org/conf/2004/RS19P1.PDF. Accessed 5 August 2008.

[2] Augusto, J. C. & McGullagh, P. 2007, 'Ambient Intelligence: Concepts and Applications', Int'l J. Computer Science and Information Systems, vol. 4, no. 1, pp. 1-28.

[3] Avižienis, A., Laprie, J. C., Randell, B. & Landwehr, C. 2004, 'Basic Concepts and Taxonomy of Dependable and Secure Computing', IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33.

[4] Bygrave, L. A. 2002, Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer Law International, Hague.

[5] Cai, Y. (ed) 2005, Ambient Intelligence for Scientific Discovery: Foundations, Theories, and Systems, Springer-Verlag, Berlin, Heidelberg.

[6] zompagna, L., El Khoury, P., Krausová, A., Massacci, F. & Zannone, N. 2008, 'How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns', Artificial Intelligence and Law, doi: 10.1007/s10506-008-9067-3

[7] Compagna, L., El Khoury, P., Massacci, F., Thomas, R. & Zannone, N. 2007, 'How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach', The Eleventh International Conference on Artificial Intelligence and Law (Proceedings of the Conference, Stanford CA, USA, June 4-8, 2007), pp. 149-153.

[8] Escuredo-Pascual, A. & Hosein, I. 2004, 'Questioning Lawful Access to Traffic Data', Communications of the ACM, vol. 47, no. 3, pp. 77-82.

[9] FP7 ICT Advisory Group 2008, 'Working Group Report on ICT and Sustainability (including Energy and Environment)'. ISTweb. ftp://ftp.cordis.europa.eu/pub/ist/docs/sustainability-istag_en.pdf. Accessed 21 August 2008

[10] Gadzheva, M. 2008, 'Privacy in the Age of Transparency: The New Vulnerability of the Individual', Social Science Computer Review, vol. 26, no. 1, pp. 60-74.

[11] Gruetser, M., Schelle, G., Jain, A., Han, R. & Grunwald, D. 2003, Privacy-Aware Location Sensor Networks. http://systems.cs.colorado.edu/Papers/Generated/2003PrivacyAwareSensors.pdf. Accessed 5 August 2008.

[12] Hoofnagle, C. J. 2005, 'Privacy Self Regulation: A Decade of Disappointment', SSRN Electronic Library, http://ssrn.com/abstract=650804. Accessed 18 July 2008.

[13] IST Advisory Group 1999, Orientations for Workprogramme 2000 and beyond, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-99-final.pdf. Accessed 21 August 2008.

[14] IST Advisory Group 2002, Software technologies, embedded systems and distributed systems: A European strategy towards an Ambient Intelligent environment, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag_kk4402472encfull.pdf. Accessed 21 August 2008.

[15] IST Advisory Group 2002, Trust, dependability, security and privacy for IST in FP6, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag_kk4402464encfull.pdf. Accessed 21 August 2008.

[16] IST Advisory Group 2003, Ambient Intelligence: From Vision to Reality, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-ist2003_consolidated_report.pdf. Accessed 16 July 2008.

[17] IST Advisory Group 2004, Experience and Application Research: Involving Users in the Development of Ambient Intelligence, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/2004_ear_web_en.pdf. Accessed 21 August 2008.

[18] IST Advisory Group 2006, ISTAG Report on Shaping Europe's Future Through ICT, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-shaping-europe-future-ict-march-2006-en.pdf. Accessed 21 August 2008.

[19] IST Advisory Group 2006, ISTAG Report on Orientations for Work Programme in FP7, ISTweb, ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-wp-wg-report-ver-final_en.pdf. Accessed 21 August 2008.

[20] Pedersen, D. M. 1997, 'Psychological Functions of Privacy', Journal of Environmental Psychology, vol. 17, no. 2, pp. 147-156.

[21] Perrig, A., Stankovic, J. & Wagner, D. 2004, 'Security in Wireless Sensor Networks', Communications of the ACM, vol. 47, no. 6, pp. 53-57.

[22] Saraogi, M. 2005, Security in Wireless Sensor Networks, http://www.cs.utk.edu/~saraogi/594paper.pdf. Accessed 5 August 2008

[23] SERENITY Project, A1 Deliverable – A1.D3.1 – Initial Set of Security and Privacy Patterns at Organizational Level, EU-IST-IP 6th Framework Programme - SERENITY 27587, http://www.serenity-forum.org/IMG/pdf/A1.D3.1_patterns_at_organizational_level_v1.3_final.pdf. Accessed 2 January 2009.

[24] SERENITY Project, A7 Deliverable – A7.D1.1 – Scenario Selection and Definition, EU-IST-IP 6th Framework Programme - SERENITY 27587, http://www.serenity-forum.org/IMG/zip/A7_1_.D1.1_scenarios_v1.1_final.zip. Accessed 2 January 2009.

[25] SERENITY Project, Securing Smart Home: How SERENITY Patterns Enforce Security in Remote Healthcare Systems, http://www.serenity-forum.org/IMG/pdf/serenity_leaflet08_web.pdf. Accessed 25 November 2008.

[26] Solove, D. J. 2005, 'The New Vulnerability: Data Security and Personal Information', SSRN Electronic Library, http://ssrn.com/abstract=583483. Accessed 15 May 2008.

[27] Solove, D. J. 2008, Understanding Privacy, Harvard University Press, London.

[28] Spiekermann, S. 2005, 'Perceived Control: Scales for Privacy in Ubiquitous Computing', SSRN Electronic Library, http://ssrn.com/abstract=761109. Accessed 15 May 2008.

[29] Stankovic, J. A., Cao, Q., Doan, T., Fang, L., He, Z., Kiran, R., Lin, S., Son, S., Stoleru, R. & Wood, A. 2005, Wireless Sensor Networks for In-Home Healthcare: Potential and Challenges, http://faculty.cs.tamu.edu/stoleru/papers/stankovic05wsn.pdf. Accessed 5 August 2008.

[30] Wahlgren, P. 1992, Automation of Legal Reasoning: A Study on Artificial Intelligence, Kluwer Law and Taxation Publishers, Deventer.