Workshop on Security in Ubiquitous Computing
UBICOMP2002
Goeteborg Sweden, 29th September 2002, 09h00 – 18h30

URL: www.teco.edu/~philip/ubicomp2002ws/

Keywords
Trust Models, Privacy, Identity, Context Awareness, Context Authentication, Location Hiding, Entity Recognition, Content Protection

Introduction

The question may be asked, "why is this the right time to be talking about ubiquitous computing?" The answer to this resides with society, technology, and markets. Firstly, there is sufficient evidence to suggest that the awareness and acceptance of the value of computing is already in a sense ubiquitous and across a wide range of society. For example, email continues to be an important resource for asynchronous communication between people, even when continents apart. Online banking, shopping, video conferencing, and instant messaging are also representative of how technology progressively disappears into everyday life. Furthermore, the mobile phone and computing explosion has transformed the expectations for meeting deadlines and maintaining contact. Secondly, technology is significantly closer to facilitating the visions of ubiquitous computing – the Smart-Its project[1] shows the possibilities for embedding context-sensing networks into the environment; the PersonalServer [12] from Intel Research has managed to harness large-scale computing resources in a small space; the groundwork for developing and deploying programmable matter and smart dust exists today, as presented by keynote speaker Wil Mcarthy[2]; additionally, various projects show how the computer is capable of evaluating location [13], movement [14], and even gestures [15]. Finally, the market shows a trend of decreasing cost, increasing capacity and increasing demand for devices classified as pervasive or ubiquitous computing technologies [16]: consider the current ease of acquisition of mobile phones, PDA's (Personal Digital Assistants), MDA's (Mobile Digital Assistants), Smart Boards or Touch Screens, as compared to say ten years ago.

Consequently, we can also ask: "why is this the right time to be talking about **security** in ubiquitous computing, and furthermore, applying it to active research and development?" The answer to this may also be stated with regards to society-awareness, state of technology, and relevant growth of market. In the same sense that people are actively aware of the benefits of email and mobility, they are still shy and perhaps rightfully paranoid about what details they exchange in the presence of technology. As technology becomes more and more a persistent presence, will society become more and more weary of vulnerability imposed by abuse or malfunction of technology? Will the fear that struck upon the realization that the Internet was not inherently secure be transferred to and exacerbated in UbiComp? On the contrary, can we as technologists circumvent these fears by providing the assurance of security mechanisms compatible with social expectations and legal jurisdiction? A further point to ponder is that if the general public's confidence in the dependability and trustworthiness of Ubicomp systems is not won (that is, benefits sufficiently outweigh risks), the prospects for Ubicomp systems will perhaps not live up to their claims.

This document reports the outcome of analysis, presentations, discussion and summarization of the first workshop on Security in Ubiquitous Computing, held as part of the UBICOMP2002 conference. We also seek to present the compliance of our work in security with other fields in

[1] Smart-Its is part of the EU sponsored Disappearing Computer Project, IST-2000-25428
[2] Wil Mcarthy is an author of science fiction and science periodicals, with work on programmable matter appearing in Nature Magazine and Wired Magazine. He delivered the keynote presentation at UbiComp2002

ubiquitous computing. There were 19 people in attendance, which allowed the discussion to comfortably exceed its intended time.

Deviations from the Old Model

As an introduction to the workshop, we were given a refresher of the state of today's security mechanisms typified by firewalls for access control and policy management, static, hierarchical trust models and the general tendency to be focused at the network layer. This was metaphorically depicted as a castle, where everything unknown is kept out, as well as the current security imbalance in what was coined as the "security trinity" (communications, applications, resources), where the tendency is to concentrate security efforts on communications or the networking layer, as opposed to integrated into the applications and resources[3]. Mention may be made of the WiTness project[4], which focuses on providing libraries, services, architecture and standards for application layer security. Ubicomp related visions and supporting technologies suggest the expansion of the following criteria that change the way we think about security:

(i) Wireless media supporting from personal area to wide area networks; (ii) ad hoc association of devices at the network and session layers; (iii) location and context considerations in policy management; (iv) heterogeneity of content encoding at the transport and application layers, as well as (v) wide-scale variability in the processing and storage capabilities of the representative devices.

This then diminishes the effectiveness of the castle approach, as legitimate interactivity is expected to occur beyond its walls. Furthermore, static policies for access control and trust will either be significant application hindrances or (intentionally or unintentionally) by-passed. Security has to be reflective of the goals of the user and not simply a set of system-centric constraints. Moreover, the availability of richer context information may augment the scope and value of data to be protected, yet may also serve to augment the strategies for protecting these elements of data. We also considered that data is not only of personal value but may be the cornerstone of profitability for many types of businesses as implied by the existence of copyright laws associated with various types of media.

In each of the following sections, we further describe why the current way of doing things is insufficient, suggests the requirements or necessary strategies, and outline the relevant work-in-progress presented during the workshop.

Trust in Ubicomp Environments

Trust was defined as "a means to reason about and accept risk in situations of partial information and assign privileges accordingly [1]" and "qualified reliance on received information. [2]"

As Ubicomp seeks to weave the computer into the fabric of everyday life, most of the issues with today's ways of computing stem from their dissimilarity to the way humans innately operate. This was noted with regards to trust by English et. al, where they stated: "Trusted entities are decided by some central authority, be it the end user or system administrator. This coarse view of trust fails to capture the many intricacies of trust as intuitively viewed by humans." [1] The progression of Ubicomp research shows evidence of increased decentralization, which may lead to situations where devices are disconnected from a centralized trust authority, as well as invocation of services while in a "hostile" environment. Today's trust models neglect or do not facilitate the dynamic aspects of trust. Trust models in Ubicomp will therefore need to facilitate localized

[3] This was a presentation by Joachim Posegga where he summarized the issues facing ubiquitous and pervasive computing.

[4] WiTness is a EU sponsored project entitled "Wireless Trust for Mobile Business" IST-2001-32275. The project is led by SAP AG and includes partners from the mobile device provider, mobile network operator, smart card development, and research fields.

decisions about trust. Furthermore, in our world, trust is not determined from a one-dimensional viewpoint; rather, the validity of trust is based on both identity and context. Context implies that the trust relationship between two entities is a continuum rather than a discrete event-based evaluation. Shankar argued that trust models for Ubicomp would need to embrace both identity and context, capturing the needs of both traditional and ubiquitous computing [2]. The term "Identity" invoked another thread of discussion, which included an analysis of the deficiencies of current authentication schemes in Ubicomp, a comparison of authentication and recognition, and a look at the requirements for entity recognition methodologies. Seigneur et al presented current authentication mechanisms as a subset of recognition - that is, current techniques tend to require some form of preliminary enrolment in a system, requiring centralized administrator presence, whereas recognition may include various forms of negotiation (not excluding legacy techniques), be evaluated on the basis of context-relevant attributes as opposed to static identities, independent of third-party intervention (recognition schemes are evaluated locally), and modified based on the experience of past and present interactions [3].

After considering the constraints (or perceived requirements) of Ubicomp for trust, as described in the previous paragraph, we were presented with work in progress on "Dynamic Trust" [1], "Continuums of Trust" [2], and "Entity Recognition" [3].

The Dynamic Trust model proposed is built on three processes – Formation, Evolution and Exploitation [1]. The aims are to incorporate explicit values for trust, embrace flexibility in the use of these values (equivalent to human intuition), and therefore provide for the determination of an initial level of trust when entities meet for the first time. Trust formation is about a decision to accept a risk by granting certain privileges until there is evidence that shows it is unwise. This gathering of evidence is what is involved in the trust evolution process, where initial levels of trust are progressively modified based on interactive experiences reported from personal observation, recommendation, or by reputation. Exploitation is then the use of trust information to produce compensatory behaviour – this is the notion of adaptive trust management. The attribute vector methodology presented as the foundation for organizing and evaluating trust in a unified model. This therefore may be used to organize and evaluate trust in both traditional (identity-based) or Ubicomp (context-based) environments. Trust levels are determined as an operation on collective continuous attributes as opposed to a one-dimensional token. This may be seen as a candidate model for formation and evolution of trust with reference to the dynamic trust model proposed above. The relation to the entity recognition model could also be stated as a basis for initial trust formation and this also needs the provision of an organized representation of attributes and interactive evidence. Nevertheless, there was an ongoing debate regarding the semantic relationship between recognition and authentication. This was resolved as stating that recognition may be seen as authentication by assertion (assertion of capability, previous activity, or knowledge), while authentication may be considered as a form of recognition where previous enrolment in a central system is necessary.

A noteworthy observation made by Molva[5] was that the issues covered here in trust are quite similar to those in ad hoc networking security forums. One of the methodologies being explored in the ad hoc network community is the application of Game Theory to evaluation of trust.

User-Centric Security

There is a degree of intolerance for the constraints that some security systems impose on users, causing distractions from their intended tasks. The initial expectation when including this topic in the workshop was that we would have for the most part investigated issues concerning security and usability. However, we found essential overlaps with the next section on context awareness, and most of the discussion promoted in this area was therefore with regards to maintaining social user expectations (or rights) when interacting with a ubiquitous system or environment. The

[5] Refik Molva is an active member in the multicast and ad hoc security communities

expectations that we discussed were mainly those of privacy, integrity, authenticity, and adaptability.

Privacy may be described as the controlled access to data that may reveal exploitable information, which may potentially compromise a person or organization's legal, social or financial identity. Therefore, users of information and context driven systems should be aware of how they are being sensed and what the information is being used for. On the contrary, users should still not be disrupted from enjoying legitimate and desirable services, available to them as a result of personal information being transferred. The fundamental service premise by Wu for such systems was that adaptive security services are required that do not hinder usability/ enjoyment of services, and do not blockade all statistical gathering activities of service providers [4]. That is, the goals of Ubicomp systems are essentially to maximise user experience, maximise service provision, and minimize user and service disruption. Yet privacy is a social right and a legislative directive; should this over-rule the usability initiatives of Ubicomp? P3P (Platform for Privacy Protection)[6] was cited as a possible privacy policy management scheme, but required some extensions to fit the granularity requirements of Ubicomp. Anonymity and Pseudonym provision are also useful mechanisms for protecting at least an entity's legal identity. As seen from the conference proceedings, there is plenty work going on in this direction: Langheinrich presented ideas for incorporating privacy enhancing infrastructure in the ubiquitous computing environment through extensions of P3P [17], while Jiang et al presented a fundamental policy for systems facilitating privacy through the asymmetry of information flowing between data owners, collectors and future users [18]. We also note the workshop on designing privacy enhancing systems that occurred in parallel to this one[7]. It is quite interesting to compare the issues dealt with in these separate forums.

Indeed, a lot of our deliberations were over the question, "so what really is new in Ubicomp for security?" One scenario depicted by Bussard was that interactions with physical artefacts might proceed without any confirmation of ownership, accountability or authenticity [5]. This could lead to seemingly simple user exploitations such as impersonating a genuine artefact through introducing a fake proxy, or what is known in traditional security circles as a *man in the middle attack*. Therefore, in the similar fashion to people being authenticated in traditional environments, physical artefacts also need to be authenticated to avoid users being misled. This authentication could be based on multiple attributes including location, time, and other quantifiable, significant and perceivable attributes. Many of today's authentication methodologies are based on challenge-response protocols, that is, you can prove who you are by being able to correctly counter my challenge. However, response time is always a factor to consider in security, as a lapse in a transaction opens up a window of opportunity for an attacker. Therefore, proximity may evolve to be a useful factor in facilitating trust and assurance of authenticity in Ubicomp environments. Furthermore, touch or physical contact is almost the most definite guarantee for trusting another physical party. This interaction substrate was proposed not only to facilitate physical trust, but for providing a medium for undeniable, speedy transfer of challenge-response data.

Ubicomp technologies are positioned to enhance the adaptability of computational systems as well as to computationally augment physical environments. This implies a desired progression towards a harmonization of the physical and virtual environments. Kreutzer et al presented ideas from the perspective of identity; they suggest that devices should behave in similar manner to the users that they impersonate/ represent in a given situation. This is the notion of Identity Management [6]; that is, a user's behaviour changes per situation, such that they select the representative data to be presented in a particular situation; this behaviour should be translated to the device such that compliance with the user's policy is ideally implicit. Perhaps totally implicit is not always attainable, but the best we can aim for is minimisation of distractive user

[6] P3P is a standard supported by the W3 consortium; URL: www.w3.org/P3P/

[7] The workshop on designing privacy enhancing systems may be found under the list of workshops at www.ubicomp2002.org

intervention. Furthermore, identity management should be a localized activity, and not reliant on third party services or infrastructure. One comprehensive way of talking about adaptive behaviour is the user interface presented by the device. That is, as a user moves from environment to environment the device should be auto-configure itself to respond appropriately to the services of that environment, including what it presents to the user as well as the services, based on the context sensed. The next section goes on to describe some of the relationships between security and context-awareness that came out of the discussion.

Security and Context-Awareness

There is ongoing research and discussion about the exact definition and representation of “context” with respect to Ubicomp. It is settled that it is not just location but constituted of many elements, attributes and activities. There are quite a few models being researched from ontological bases, which seek to capture human activity, environmental behaviour, and correct interpretation of situations [19]. There are therefore complementary concepts of Ubicomp and security presented by these initiatives. On one hand we can consider security implications because of imminent delocalisation of context information, but on the other, the potential for context richness to facilitate more proactive and usable security mechanisms. One other interesting goal for Ubicomp presented during the conference was coined as “0^3 (zero “cubed”) Computing” [20]. That is, can ubiquitous environments achieve such a thing as zero configuration, maintenance and downtime? We extended this question to security as well.

Shankar et al promoted automation of setting up and initialising security mechanisms and sessions [7]. That is, security management is one of the more burdensome activities associated with security mechanisms overall. It is also often said that many of the breaches in security systems are resultant from administrative oversight. Therefore, is it likely that if the management processes are automated, reducing the administrative error factor, that a system is rendered more secure? The methodology proposed was based on evaluating the context in such a manner that users experiencing the same context would result in compatible security decisions, for example, securely exchanging confidential information within a contextually-defined group. The applicability of such a scheme is clear when considering ad hoc group communication. As suggested in the previous paragraph, it is inconceivable and impractical to perceive context in its entirety without establishing bounds. The idea of “Context Views” was offered as a way of expressing context based on the interest of an application. Therefore, through receiving context view information from services providing the relevant views to subscribers, localized security-relevant decisions may be made compatible with a set sharing the same context. The outstanding questions surround the authenticity of perceived context upon which cooperative security decisions are made.

It is clear that malicious usage of context information is a potentially daunting fear of Ubicomp. Context awareness as a facility for remote distribution and coordination was the perspective taken by Kato, as he described the use of context information to organize distributed objects working together towards the same objective [8]. Application scenarios can therefore be derived within the home, office and community. The example discussed during this session was a Town Management System, where the public places and utilities of a town are enriched through UbiComp technology to provide better customer, visitor and collaborative services. These services are based on the principle that resources should act more in a role of servitude, detect people’s needs and respond appropriately [8]. Systems without such facilities in place require that people explicitly search for required information, sometimes resulting in extensive efforts. Nevertheless, providing a high-degree of information accessibility and flexibility may introduce higher risks of denial of service attacks and integrity degradation. Furthermore, by the systems being capable of pushing information towards patrons, there may be occasions where the bounds of privacy are by-passed. One approach proposed was the ability for services to transfer operation privileges based on the situation. Operation privileges are abstracted in the form of a remote control object/ token, which can be granted or taken away based on the user’s treatment of the privileges.

Issues concerning privacy in UbiComp systems are often associated with privacy of location. Determination, representation and appropriate use of location information are fundamental to many applications based on UbiComp technology, including visitor guides, transportation, office management systems, and dispatch of emergency and medical services. Nevertheless, location related to a person or critical entity remains a sensitive piece of information, as it may be used for malicious purposes surrounding tracking of identities. Hergartner presented their use of “location-protecting policies”, showing how the specification, management and probable conflicts of such policies differ based on the environment and situation [9]. Policies may be specified for “rooms” or for actual users. This takes into consideration that the definition of a room is constrained to the granularity of location sensing available to the system. In any event, there may arise conflicts in the policies specified per user and per room. For example, a person X does not want to be located by a person Y, but the room policy for room R in which X resides allows Y to view all people currently in that room. This shows the need for resolving conflicts through prioritisation (avoid the conflict), intersection (detect and capture the conflict), and synchronization (resolve the conflict) of policies. The overall management of these policies may be either centralized or distributed, based on the nature and activity of the associated business or organization.

Augmenting a Security-Minded World

The goal for this segment of the workshop was to take a look at security in ubiquitous computing from the perspective of applying UbiComp technologies (devices, applications, and tools) to sectors where security consciousness and mechanisms pre-exist. Firstly, we noted that security is necessary for the survival of most businesses, and may even be the core of the services offered. This was evident during the e-Business boom of the 1990’s, where failure to consider security risks and integrate the necessary mechanisms into the business plan resulted in massive loss of profit and credibility. Wald presented one business case with high dependability on security, namely PayTV [10]. The broadcast industry is therefore an example where the business model may drive the necessity for security, yet the security model represents a service offered by the organization. The business model of PayTV is centred on secure distribution of copyright content. However, with the wide spread proliferation of devices and content-capturing capabilities, there has occurred an almost viral spread of copyright content beyond legitimate boundaries. This could result in financial losses to the creators, owners and distributors of intellectual content. Therefore, included in the business goals are content protection, end system trust evaluation, and delivery of payment entitled. Businesses like PayTV therefore require an infrastructure that facilitates an online centre with a report-back mechanism and mandatory reconnection for credit renewal. Development and delivery of UbiComp technology and infrastructure should therefore give consideration to the business models, seeking to understand the security implications and motivations for the security mechanisms present.

A complete analysis of security implications may entail an understanding of the factors imposed by society, economics, environmental conditions, the applications in use and the nature (structure, format, volume) of the content being accessed. The interpretation of these varies based on the constraints of the context in which they are applicable. The process of augmentation may be described as (i) collection of both analogue and digital data from the environment, (ii) storage and evaluation of data collected, and (iii) presentation of data or triggering of events relevant and customized for target system users. Therefore, the security risks in UbiComp may be separated into these three phases. A security risk is pending when an attacker can form logical links between contexts, objects, users, and objectives, which can be referred to as “evidence”. Consequently, augmenting an environment may heighten security risks as the production and exchange of evidence between systems and the environment is necessarily increased. Consider an object such as a simple string of numbers (490765432145); it has no value until we link it with the context “is a credit card number”, the user “John X”, and the objective “to make purchases not more than €2000”. Our interpretation of this was that protection goals might also be separated among the augmentation phases identified, translated into relevant policies, and hence associated with mechanisms that protect against unauthorized formation of the links of evidence. Current security policy models are too rigid to appropriately balance both protection and augmentation goals. Coincidently, the integrity of any policy defined must also be protected – this too represents ongoing work [11].

Summary

The important themes revisited and identified during the workshop may be summarized as new models for verifying trust, user-controlled privacy and content protection. We cannot assume priori trust in UbiComp environments, as evidenced by developments in ad hoc networking. Basic credential-based authentication and verification is not sufficient for both security and ubiquitous computing goals to be fulfilled. Research therefore continues in areas such as entity recognition, as well as dynamic and cumulative trust models. The work in these trust models can also be contributed to ongoing work in privacy for UbiComp, where goals include adaptive, user-based and integrated infrastructures for privacy management. These usability, protection and security management goals may then stand to benefit from further research into use of context-awareness technologies. This includes context authentication, application of implicit interaction to security mechanisms, and provision of more finely grained factors for trust models.

Future Agenda

Based on the participation, outcome and discussion following, it was clear that there are needs to continue such forums as afforded by this workshop. There is also the need to document and formally publicize results. These are summarized in the points below:

- Formation of active working group with emphasis on “Security in Ubiquitous Computing”
- Ongoing feedback to UBICOMP through annual workshop on topic: “Security in UbiComp”
- Presence in other security and mobility conferences
- Formation of collaborative efforts leading to publications and projects
- Support for growing privacy frameworks and infrastructures
- Integration of knowledge in other UbiComp sub-communities

Acknowledgements

This workshop may be labelled a success, in terms of achieving the goals of bringing together experts in the field, generating sufficient discussion that led to identification of real issues, and exchanging ideas on research and direction. Therefore, all the participants that took part are to be acknowledged for their contributions of papers, presentations, questions and answers. We also wish to thank the UbiComp 2002 committee for allowing this workshop to be included in the program, and for providing the appropriate resources with which to comfortably conduct it. Finally, special thanks to those who expressed interest in the outcome of the workshop and gave comments and suggestions regarding future forums.

References

[1] Colin English, Paddy Nixon, Sotirios Terzis, Andrew McGettrick, Helen Lowe, "Dynamic Trust Models for Ubiquitous Computing Environments", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[2] Narendar Shankar, William A. Arbaugh, "On Trust for Ubiquitous Computing", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[3] Jean-Marc Seigneur, Stephen Farrell, Christian Damsgaard Jensen, "Secure Ubiquitous Computing based on Entity Recognition", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[4] Maomao Wu, Adrian Friday, "Integrating Privacy Enhancing Services in Ubiquitous Computing Environments", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[5] Laurent Bussard, Yves Roudier, "Authentication in Ubiquitous Computing", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[6] Uwe Jendricke, Michael Kreutzer, Alf Zugenmaier, “Pervasive Privacy with Identity Management”, Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[7] Narendar Shankar, Dirk Balfanz, "Enabling Secure Ad-hoc Communication using Context-Aware Security Services", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[8] Hiromitsu Kato “Context Aware and Yet Another Service AYA", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[9] Urs Hengartner, Peter Steenkiste, "Protecting People Location Information", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[10] Stephanie Wald, "Secure Media Consumption in a a Ubicomp World", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[11] Håkan Kvarnström, Hans Hedbom, Erland Jonsson, "A Protection Scheme For Security Policies In Ubiquitous Environments Using One-Way Functions", Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002

[12] Roy Want, Trevor Pering, Gunner Danneels, Mutha Kumar, Murali Sundar, John Light, “Personal Server: Changing the Way We Think about Ubiquitous Computing”, UbiComp 2002, Springer LNCS 2498, pp 194 - 209

[13] David Garlan, Dan Siewiorek, Asim Smailagic, and Peter Steenkiste, “Project Aura: Towards Distraction-Free Pervasive Computing”, IEEE Pervasive Computing, special issue on "Integrated Pervasive Computing Environments", Volume 1, Number 2, April-June 2002, pp 22-31

[14] Albrecht Schmidt, Martin Strohbach, Kristof van Laerhoven, Adrian Friday, Hans-Werner Gellersen, “Context Acquisition Based on Load Sensing”, UbiComp 2002, Springer LNCS 2498, pp 333 – 350

[15] Trevor Darrell, Konrad Tollmar, Frank Bentley, Neal Checka, Louis-Phillipe Morency, Ali Rahimi, Alice Oh, “Face-Responsive Interfaces: From Direct Manipulation to Perceptive Presence”, UbiComp 2002, Springer LNCS 2498, pp 135-151

[16] Deborah Estrin, David Culler, Kris Pister, Gaurav Sukhatme, “Connecting the Physical World with Pervasive Networks”, IEEE Pervasive Computing Jan – Mar 2002, pp 59 – 69

[17] Marc Langheinrich, “A Privacy Awareness System for Ubiquitous Computing Environments”, UbiComp 2002, Springer LNCS 2498, pp 237-245

[18] Xiaodong Jiang, Jason I. Hong, James A. Landay, “Socially-Based Modeling of Privacy in Ubiquitous Computing”, UbiComp 2002, Springer LNCS 2498, pp 176-193

[19] James L. Crowley, Joëlle Coutaz, Gaeten Rey, Patrick Reignier, “Perceptual Components for Context Aware Computing”, UbiComp 2002, Springer LNCS 2498, pp 117 - 134

[20] Anthony LaMarca, Waylon Brunette, David Koizumi, Matthew Lease, Stefan B. Sigurdsson, Kevin Sikorski, Dieter Fox, Gaetano Borriello, “PlantCare: An Investigation in Practical Ubiquitous Systems”, UbiComp 2002, Springer LNCS 2498, pp 316-332