Multi-modal Authentication for Ubiquitous Computing Environments*

Taekyoung Kwon, Sang-ho Park, and Sooyeon Shin

Dept. of Computer Engineering
Sejong University, Seoul, 143-747, Korea
tkwon@sejong.ac.kr, {superh1,shinsy}@sju.ac.kr

Abstract. In ubiquitous computing environments, the computer technology will recede into the background of our lives for its ultimate goal, invisibility. For ensuring security and privacy in those environments, both human beings and surrounding devices should be authenticated under the interaction methods that are used for ubiquitous services. However, the invisibility of devices, the adaptiveness of interactions, and the varying performance of devices will make it difficult to achieve it. In this paper, we reconsider authentication for ubiquitous computing environments and propose a conceptual framework for resolving the difficulties.

1 Introduction

Ubiquitous computing will integrate computation into the physical environments under its ultimate goal, invisibility. In other words, the computer technology recedes into the background of our lives. The construction of ubiquitous computing environments means that human beings surrounded by real world objects are actually surrounded by various kinds of (hidden but communicating) electronic devices embedded into those objects, and they are also embodied by such tiny devices. There will be a need to change the way of interacting with computers, services, and the surrounding physical objects into more natural and casual ways. This new computing paradigm is being emphasized as an exciting revolutionary shift that makes us transfer to the next computing era called the age of calm technology [14]. Our living environments will be transformed to the spaces of intelligent and pro-active computing devices such as the so-called ambient devices, where it is unnecessary for us to continually rationalize the use of computing systems or even services. Under the goal of invisibility, we should conduct various kinds of human-computer interactions with such distinct computing devices even at the time we are not aware of using them, on the contrary to the virtual world stuffs, in the real world.

For ubiquitous service availability, we should move around and be identified by those devices very frequently. We should also be authenticated when we need to claim

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2006-C1090-0603-0028).

C. Stephanidis (Ed.): Universal Access in HCI, Part II, HCII 2007, LNCS 4555, pp. 113–121, 2007.

our identity or authority for security of services [3, 4]. However, there are at least three difficulties in achieving it in the ubiquitous computing environments. First, since the devices authenticating us are usually invisible, we should mind the so-called *calm adversaries*[1] around us. There exists the high risk to disclose secret information to the calm adversaries. Second, authentication should be carried out adaptively depending on the user preference as well as the available interaction methods. For example, we may not want to give a password loud when speech recognition is only possible, since we may fear that someone can hear our speech. We should mind other recognition methods and radio devices for privacy reasons likewise. Third, the communicating devices and sensing devices may vary with regard to their performance. Thus, it is feasible that the required authentication level cannot be met again.

In this paper, we reconsider authentication for ubiquitous computing environments and propose a conceptual framework for it. Multi-modality and its relation should be considered more carefully than multi-factor has been done for traditional authentication methods. This result is the main stem of our on-going work, the pro-active authentication considering human-computer interactions. The rest of this paper is organized as follows. In Section 2, we examine the current authentication technologies. In Section 3, we discuss our authentication framework for ubiquitous computing. In Section 4, we conduct a simple experiment corresponding to the pre-processing of multi-modal authentication in our framework and discuss its result. This paper is concluded in Section 5.

2 Authentication Technology

Authentication means the process of proving and verifying the claimed identity, and has been studied and applied for many years in computing environments. For authentication of human beings in those environments, three kinds of factors are usually considered, such as what we know (e.g., passwords, passphrases, or personal identification numbers), what we have (e.g., identification cards, security tokens, or software tokens), and what we are (e.g., fingerprint, retinal patterns, voice patterns, or other biometric identifier). Sometimes a combination of them is used, e.g., a bank card and a PIN, for producing better security in person authentication. This is called multi-factor authentication in the literature.

Specifically in biometric authentication, we use another term, multi-modal authentication, for describing the enhancement to increase the accuracy of authentication systems in five different ways: multiple biometrics, multiple acquisitions of the same biometry, multiple representations for the same biometry, multiple units of the same biometry, and multiple sensors for the same biometry. The multi-modality is accordingly used for describing the multiple treatments of biometric traits associated to a person in the literature [2, 13].

[1] Ubiquitous computing technologies could allow ill-intentioned individuals to deploy secret surveillance networks for spying on unaware victims, subsequently being used in unanticipated and illegal ways, even if they were initially deployed for legitimate purposes. Since the adversaries are invisible and utilize the calm technology, we call them the calm adversaries who can conduct data collection, coordinated analysis, and automated event correlation easily.

In this paper, we view the multi-modality as more concrete sub-categories of the multi-factor for authentication. In other words, not only biometric traits but also the other two factors are classified in more details with regard to the modality, and they could be used together.

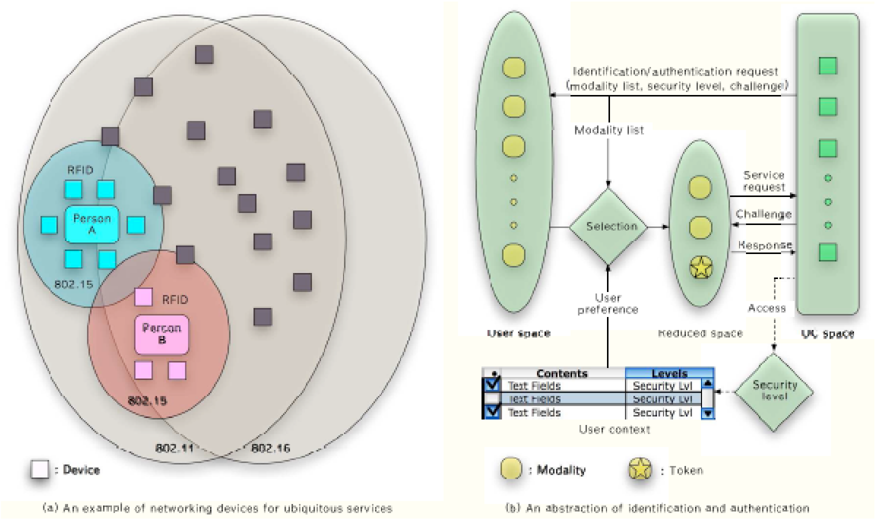
3 Authentication for Ubiquitous Computing

3.1 A Conceptual Framework

In ubiquitous computing environments, authentication (and identification) must be conducted frequently, mostly without user's awareness, between: person-and-person, person-and-device, and device-and-device. A number of authentication events could occur for a person simultaneously whereas the human user is moving around with expecting various seamless services. Those ubiquitous services may have very different authentication requirements and security levels, while users may have their preferred authentication methods and the given devices can be lack of the required authentication methods. Privacy infringement is another major problem for authentication in such environments since physical devices as well as data packets can be captured and the related transactions can be traced easily by adversaries. Thus, it may not be trivial to apply traditional authentication methods without considering these distinct features [7, 10, 12].

We would like to propose a conceptual framework that the existing authentication methods can be used and combined consistently. In ubiquitous computing environments, there must be many surrounding (ambient) devices, e.g., wireless sensor networks (WSNs), around the person, and also many belonging devices of personal area networks (PANs). Thus in many cases, the person authentication could be the authentication of person's belongings as well. Fig. 1-(a) depicts the case that two mobile users having their respective PANs meet each other, and they are also connected to the environment networks, definitely without their awareness. The physical domain can be bound by the radio coverage of devices, but we need more to model an abstract domain that defines an authenticated boundary. We mean by the space such an authenticated domain, whereas the spaces can be layered and overlapped according to different security levels and network connectivity. For example, a user space may be constructed in the PAN layer and also linked to the user's home network layer. In case of Fig. 1-(a), there should be a number of interactions in the overlapped spaces, and their identification and authentication processes can be modeled as shown in Fig. 1-(b). Note that surrounding devices may stand by in the ubiquitous computing (UC) spaces, whereas belonging devices do in user spaces.

From now on, we handle authentication both for identification and authentication since identification is only about distinguishing an entity from the others and can be considered as a part of authentication process. In Fig. 1-(b), when a user space meet a UC space, meaning a user move into a certain environment, several authentication requests (or beacon messages) may be pushed to the user space. Such requests should contain at least available modality lists, required security levels, and random challenges. Note that the modality lists should also reflect available interfaces. These can be constructed efficiently in textual form. Depending on the communication channels that each request are sent over, awareness of corresponding devices and sometimes of the user will be necessary. The user preferences collected contextually in the PAN and sometimes the user's real time decision can then be combined with the given modality lists for constructing the reduced user space that is composed of the real time authentication factors. Fig. 1-(b), a token is rather a general term for a temporary ticket for specific services. Upon the service requests which may contain the prepared modality, specific authentication protocols could be conducted between the reduced space and the UC space. In the UC space, the user context could be fetched very in part from the PAN or through public (global) networks in an authentic manner if a need arises after identification. It is desirable to have three parts such as private, public, and anonimized parts in the user context for privacy reasons, and maintain them according to security levels. Finally, the user space can be merged with the UC space for ubiquitous services through the authenticated channels established from the reduced space. Two different user spaces can be modeled similarly for authentication, for example, simply by substituting for the UC space, respectively.



(a) An example of networking devices for ubiquitous services

(b) An abstraction of identification and authentication

Fig. 1. Authentication for ubiquitous computing

3.2 A Scenario with Authentication Protocols

We discuss the implementation of our conceptual framework with a simple scenario by exploiting the existing authentication methods. It is assumed that a public key infrastructure (PKI) exists in a distributed manner and can be accessed by the space connected to a global network. It should also be reasonable to presume that basic PAN devices as well as biometric traits are already registered to a user's home network in an authentic manner. The home network should have several layered UC spaces. Finally we assume that a temporary ticket called a token is issued for a user by the authorities in PKIs, and stored in the user's PAN device. Let us omit the technical details in this paper; rather, we describe a single scenario with authentication building blocks only.

A simple scenario is that a human user wakes up in the morning, dresses himself up, and goes out to the office. When he wakes up, the UC spaces of his home network detect it and awake his PAN devices in a pro-active manner, according to his master context stored in the home network. A simple challenge-response protocol might be sufficient for identification requests of devices since they are already registered, but the status such as integrity and consistency of user context in the PAN and the modality of the PAN must be checked explicitly. A kind of digital signature or message authentication codes (MACs) can be used for it.

While he dresses himself up, new devices such as RFIDs of clothes are added (e.g., as a list of carried items) to the PAN. When we consider the PAN that is constructed through a specific communications mechanism such as a Bluetooth standard (IEEE 802.15.1), an RFID reader being capable of reading tags must be connected to the PAN for identifying and registering RFIDs in the PAN. A kind of blocker tags may also be necessary for privacy reasons [6]. Otherwise, the privacy-enhancing RFID authentication protocol that is based on symmetric key cryptography can be used for the purpose [9]. User's awareness is not yet required, but is soon necessary if he requests a specific broadcast service on TV that needs authorization with a password. The authentication request may be pushed by describing the required modality and security levels. Since the user must already been identified, the password can only be entered if a key pad is available around him but otherwise he can choose another input method through ambient devices. For password authentication with a broadcast center, a concrete method of IEEE P1363.2 can be applied [5]. However, if he cannot enter nor speak the password currently or his context explicitly describes that he doesn't want his awareness on this event, a different authentication method can be applied, by letting the password be encrypted by AES, an advanced encryption standard algorithm, at the previous registration phase and the encryption key be split to the PAN devices. Thus, if the user's PAN device accomplishes its authentication with the surrounding UC device as above, the split key can be transferred to the authenticated ambient device for decrypting the password.

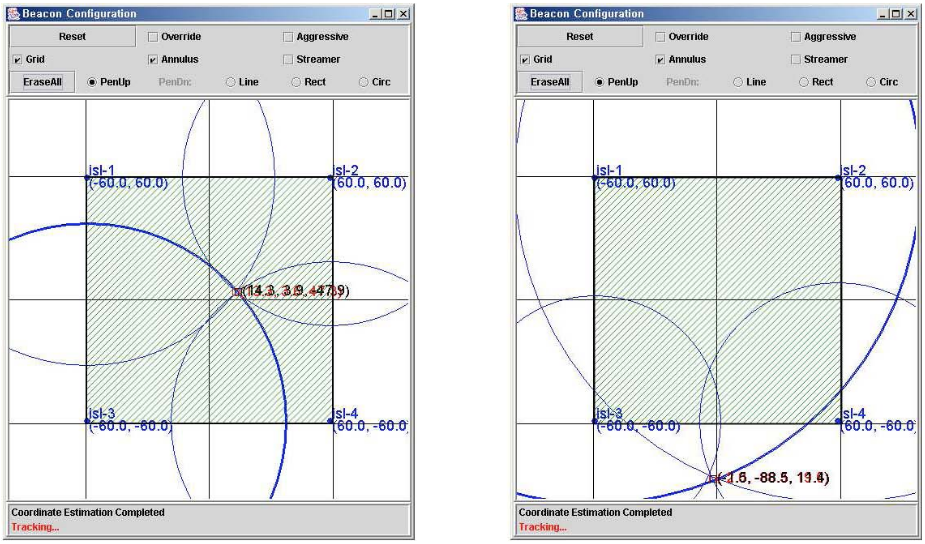
When the user leaves for the office, he may go out trough the main gate of his house. At this time, his master context is set as roaming status for strengthening the privacy controlling security levels. It must be up to his choice to register his destination at this stage as well. While going to the office, if the user wants the same broadcast service on his PDA-like device having a fingerprint sensor, the fingerprint might be better than entering the password in a public space [8]. The fingerprint can be utilized to increase the security level: The PDA-like device captures the user's fingerprint and send its encryption along with the device authentication data to the UC device in his home network through a wider networking device such as a 3/4G cellular phone. The home device can decrypt the password of the roaming user with more authentication data in the reduced space than the above case that the user was home. For reducing the computation and network channel requirements, we can utilize a slight different method for the same goal. When encrypting the password in the home network, the super encryption of it with a key embedded into a biometric template is also prepared and stored in the home network. There are several methods to embed a cryptographic key into biometric templates and restore it using biometric samples. The key instead of the biometric sample itself then can be encrypted and transferred after capturing the user's fingerprint above. The scenario described in this subsection can be implemented with the existing authentication methods in our conceptual framework.

4 Authentication Experiment

We conduct a simple authentication experiment corresponding to the pre-processing of multi-modal authentication in our framework by considering the authentication scenario discussed in Section 3.2. More specifically, we consider the case that a human user is mobile and actually moves around both secure and insecure UC spaces, while the same security level of authentication is necessary in both spaces. For the purpose, we need a privacy-preserving location decision method. The secure UC space means that all ambient devices are authenticated and bound mutually, and the corresponding user space (concentrated on the user PAN) is secure from eavesdropping, while the insecure UC space may be insecure from those perspectives. We assume that an authorized device can only access the sensitive user context including a shared key with regard to the given security levels in the UC space.

In our experiment, we set up the UC space with ambient devices by deploying ultrasonic sensor nodes called Crickets and ZigBee sensor nodes called Berkeley Mica-Z motes. Those devices are bound by themselves through their base stations that are connected respectively in the secure UC space such as a home. We assume that a human user carries a PAN gateway that can communicate with both ZigBee devices and Crickets. Thus, we emulate the PAN gateway by connecting a Mica-Z mote with a Cricket on respective MIB-510 programming boards connected to a portable PC for the user. The list of current items, a number of pseudonyms PN_x, authentication factors, and a unique key K are stored in the Mica-Z mote, while those are made as an encrypted user profile that can be accessed by an authorized device only. We then let the user move with the emulated PAN gateway in our UC space.

As depicted in Fig. 2, four ambient ultrasonic devices named isl-1to 4 are positioned in respective coordinates such as (−60.0, 60.0), (60.0, 60.0), (−60.0, −60.0), and (60.0, −60.0). The inside of the square is assumed as the secure UC space, while the outside is not. When the user moves from the coordinate (14.3, 3.9, 47.9) to (−1.5, −88.5, 11.4), (s)he may listen to the environment where a beacon message including a random challenge R comes from. The user's Cricket estimates its location from those beacon messages but cannot decide the security level of the environment. Thus, we need a query to the environment. Note that, unless the user's Cricket transmits at all, a small degree of location privacy can be provided [11]. In other words, the environment cannot track the user yet, whereas the user's cricket estimates its location. For deciding the location, rather we can devise a privacy-preserving query protocol conducted over a distinct channel by porting our implementation to the Mica-Z mote. In that sense, the user device can query securely whether the user is in the secure UC space or not. The query can be made to an authorized device by encrypting the estimated location under K. The concrete protocol for this query is conducted over a ZigBee channel, and is depicted in Fig. 3.



☐ Override ☐ Aggressive
☑ Grid ☑ Annulus ☐ Streamer
● PenUp ○ Line ○ Rect ○ Circ

Coordinate Estimation Completed
Tracking...

(a) A user in the secure UC space

(b) A user in the insecure UC space

Fig. 2. Location detection of a mobile user

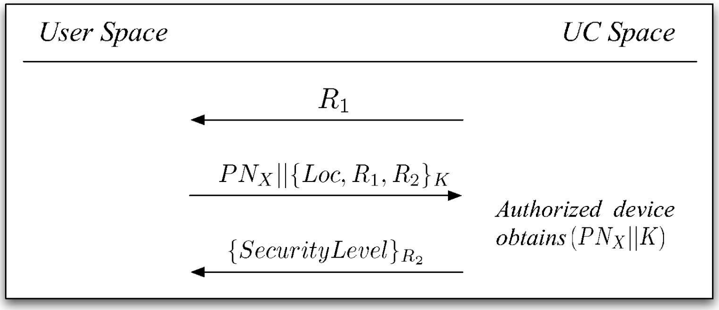
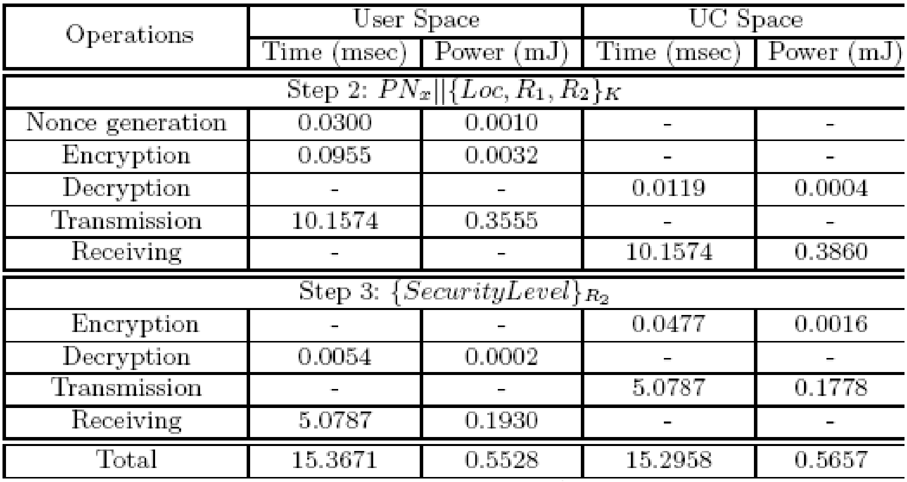

User Space
UC Space
R_1
$PN_X||\{Loc, R_1, R_2\}_K$
Authorized device obtains $(PN_X||K)$
$\{SecurityLevel\}_{R_2}$

Fig. 3. A simple location query protocol

A pseudonym PN_x is used for identification and the random challenge R_1 is encrypted along with the estimated location and another random value R_2, called a nonce. Such a query message can only be processed by the authorized device which can access the user's encrypted context. After examining the queried location, the authorized device can respond with the security level of the corresponding environment by using the nonce R2 as an encryption key. For further authentication and desired application services, the user space can choose and agree on its preferred authentication modality by utilizing this critical information. Implementing and experimenting the further multi-modal authentication is our on-going work. Another on-going work is to enhance the location privacy in our authentication framework [1]. The performance of the simple location query protocol is summarized in Table 1, using the performance matrix of Atmel ATmege128L and that of CC2420 chip [15, 16]. Since the random challenge R is relayed through the Cricket in the user space, we omit the costs required for it in the Table. The protocol running time and its energy costs are very negligible from the efficiency perspectives. We expect the concrete details of the multi-modal authentication experiment in our future work.

Table 1. Performance of location query protocol (Note: 29 byte data packet and 8 byte block cipher are used for $|PN_x|$ =8, |Loc| =3, $|R_x|$ =8, |SecurityLevel| = 1.)



Operations	User Space		UC Space	
	Time (msec)	Power (mJ)	Time (msec)	Power (mJ)
Step 2: $PN_x \| \{Loc, R_1, R_2\}_K$				
Nonce generation	0.0300	0.0010	-	-
Encryption	0.0955	0.0032	-	-
Decryption	-	-	0.0119	0.0004
Transmission	10.1574	0.3555	-	-
Receiving	-	-	10.1574	0.3860
Step 3: $\{SecurityLevel\}_{R_2}$				
Encryption	-	-	0.0477	0.0016
Decryption	0.0054	0.0002	-	-
Transmission	-	-	5.0787	0.1778
Receiving	5.0787	0.1930	-	-
Total	15.3671	0.5528	15.2958	0.5657

5 Conclusion

We study authentication for ubiquitous computing environments in the context of a conceptual framework considering multi-modality for resolving possible difficulties such as the invisibility of devices, the adaptiveness of interactions, and the varying performance of devices. This is the main stem of our on-going work, the pro-active authentication considering human-computer interactions. In this paper, first we construct the conceptual authentication framework in which the user's modality (including authentication factors) is abstracted in a set, called the user space, and is reduced to the so-called runtime reduced space based on the user context and the environmental estimation, whereas the environment is also abstracted in a set, called the UC space. There are interactions between the user space and the UC space for pre-processing of the environmental estimation and modality selection, and for authentication that is required for application services. We also illustrate a ubiquitous authentication scenario in our framework, and discuss that the presented scenario can be implemented with the current technologies in our framework. As for the environmental estimation, we present and experiment to conduct a practical protocol that queries a security level of the environment without leaking both identity and location of a user to unauthorized parties. In the simple experiment, we could observe that such a protocol can be executed in less than 50 msec under the resource-limited 8-bit processor ambient devices. It should take only several hundreds of msec even if we consider the possible transmission delay and processing delay of the encrypted user context by the authorized device, in such a resource-limited computing environment, and we could expect much more improvement from augmenting computing resources. It means that the protocol runs practically with regard to the varying performance of devices. In our future study, we will investigate more concrete details of both frameworks and mechanisms.

References

1. Beresford, A., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Computing, pp. 46–55, (January-March 2003)
2. Bign, J., Duc, B., Smeraldi, F., Fischer, S., Makarov, A.: Multi-modal person authentication. In: Proc. of Face Recognition: From Theory to Applications (NATO-ASI Workshop) (1997)
3. Buennemeyer, T.K., Marchany, R.C., Tront, J.G.: Ubiquitous Security: Privacy versus Protection. In: Proc. of the 2006 International Conf. on Pervasive Systems and Computing, pp. 71–77, (June 2006)
4. Bussard, L., Roudier, Y.: Authentication in Ubiquitous Computing (Extended Abstract)., http://citeseer.ist.psu.edu/547343.html
5. IEEE P1363-2, Standard specifications for password-based public key cryptographic techniques (December 2002), available from http://grouper.ieee.org/groups/1363/
6. Juels, A., Rivest, R., Szyldo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In: Proc. of ACM Conference on Computer and Communications Security, pp. 103–111 (2003)
7. Kagal, L., Finin, T., Joshi, A.: Moving from Security to Distributed Trust in Ubiquitous Computing Environments. IEEE Computer (December 2001)
8. Koreman, J., Morris, A.C., Jassim, S., Sellahewa, H., Chollet, G., Aversano, G., Salicetti, S., Allano, L.: Multi-modal biometric authentication on the SecurePhone PDA. In: Proc. of MMUA workshop on Mult-Modal User Authentication, (May 2006)
9. Lim, C., Kwon, T.: Strong and robust RFID authentication enabling perfect ownership transfer, Information and Communications Security. In: Gorrieri, R., Wehrheim, H. (eds.) FMOODS 2006. LNCS, vol. 4037, pp. 1–20. Springer, Heidelberg (2006)
10. Matsumoto, M., Takagi, Y.: Mutual Authentication Method for Ubiquitous Service Environments. In: Proc. of IEEE Global Telecommunications Conf (GLOBECOM ’03), vol. 3, pp. 1389–1393 (December 2003)
11. Priyantha, N., Chakraborty, A., Balakrishnan, H.: The Cricket location-support system. Mobile Computing and Networking, pp. 32–43 (2000)
12. Stajano, F., Anderson, R.: The Resurrecting Duckling: Security Issues for Ubiquitous Computing. IEEE Computer 35(4) Part Supplementary, 22–26 (2002)
13. Thian, N., Bengio, S.: Why Do Multi-Stream, Multi-Band and Multi-Modal Approaches Work on Biometric User Authentication Tasks? IDIAP research report. In: Proceeding of 2004 Internation Conf. on Acoustics, Speech, and Signal Processing (ICASSP 2004), vol. 5, pp. 893–896, (May 2004)
14. Weiser, M.: Some Computer Science Issues in Ubiquitous Computing. ACM SIGMOBILE Mobile Computing and Communications Review 3(3), 12–21 (July 1999)
15. Crossbow technology, Inc. http://www.xbow.com
16. ZigBee Specification Ver. 1.0 (2005), http://www.zigbee.org