Hassle Free Fitness Monitoring

David Jea[1], Jason Liu[1], Thomas Schmid[1], Mani Srivastava[12]
UCLA Electrical Engineering Department[1]
UCLA Computer Science Department[2]
{dcjea, schmid, mbs}@ee.ucla.edu; jasonliu0907@ucla.edu

ABSTRACT

Fitness monitoring is a fundamental service in pervasive healthcare, but finding a balance between usability and privacy is a hard challenge. Integrating biometric technologies such as fingerprint into devices can achieve an invisible interface that enhances usability. However, our survey shows that nearly one third of people are concerned with disclosing sensitive biometrics for non-critical fitness monitoring applications. To lessen users' anxieties in privacy concerns, we propose a new way of identification by only utilizing imprecise biometrics and existing information. Our solution is "hassle free" because it maintains the devices' original user interface without adding additional sensors and sacrificing user privacy. This design achieves usability by preserving familiar interaction for users and is valuable because habits are hard to change. We demonstrate this idea with a fitness monitoring system for the healthy individuals in a workplace. The system uses collected physiological information (weight, blood pressure and heart rate) and context information (computer network activity) to identify a user. Our system is more suitable for home or workplace applications, because of the involved uncertainties. Our experiments show that we can achieve a correct user identification of up to 87%. We believe that our solution can serve as an easy addition to the simple interfaces of current technology by enhancing them with smart algorithms.

1. INTRODUCTION

Fitness monitoring is probably one of the most fundamental functionalities of pervasive healthcare systems. Proactively recording vital signs, such as weight and blood pressure changes over time, enables a caregiver to deliver qualified medical services [21]. We are interested in the fitness monitoring of healthy individuals in workplaces or homes. Since this population has no serious health threats, they lack strong motivation in participation. U*sability* becomes one of the main factors that provoke (or diminish) users' interests in using a device. The interface should be simple and non intrusive. Typing a name into a computer can already be too much hassle in order to just record a weight. In addition, workplaces are semi-public, where *privacy* seems to be another concern for many users. Balancing usability and privacy is one important issue in pervasive healthcare [22].

1.1 Invisibility

Invisibility is one of the key components in pervasive computing [20][27]. We can combine biometric technologies to achieve the invisibility characteristic in the interface. For example, integrating a fingerprint scanner into the 'start' button of a blood pressure monitor or adding cameras to perform facial recognition functions are some viable ways that allow the system to identify a user "silently", without any form of interaction. However, they require additional hardware, which increases the high cost of medical devices. In addition, possible ad hoc setup due to user installation introduces further complexity in processing. Even without these issues, such biometric systems might not be widely acceptable among the device users because of privacy concerns. Users may hesitate to store personal information, such as a fingerprint, in a device accessed by many people.

1.2 Privacy

We conducted a short survey on privacy concerns, and results (see Section 3) show that nearly one third of people are concerned with disclosing sensitive biometrics for non-critical fitness monitoring applications. This is in agreement with other user studies in [12][6] where the authors describe that people worry about the tracking and abusing of the system. In [1], 89.2 percent of the sampled people reported medium or high concerns about privacy. This year (2008), in New York, workers are protesting over using palm print scanners to automate employee tracking. "*The palm print thing really grabs people as a step too far.*" said Ed Ott, executive director of the New York City Central Labor Council of the AFL-CIO [3]. A similar battle has been fought in Pittsburgh in 2006 [13].

1.3 Design Guidelines

To lessen users' anxieties in privacy while maintaining high usability, a device should identify a user with the following design guidelines:

1. *Any data that the system records cannot be used as hard evidence (in court) to pinpoint exactly who the user is. (privacy).*
2. *The system is allowed to use existing information. (feasibility).*
3. *The original interface is maintained such that people of all age groups naturally know how to use it. (usability).*

In this paper, we explore these guidelines. We present survey results to show that there is no straightforward method that can fulfill both usability and privacy requirements at the same time. Current solutions compromise among the two, either sacrificing privacy for usability or vice versa.

1.4 Proposed Solution

We continue by proposing a "hassle free" solution that maintains the original interface without adding additional sensors but utilizes (1) imprecise information and (2) existing information to identify a user. We demonstrate the idea with a fitness monitoring system for the healthy individuals in a workplace. The identity inference consists of a biometric matcher based on a naïve Bayes classifier and a context reasoning component based on reified temporal logic. We deployed the system in a lab and collected 1.5 months of data from 9 participants. Our experiments show that we can achieve a correct user identification of up to 87% (with complete physiological information) and 84% (with partial/complete physiological information plus user presence context reasoning).

2. RELATED WORK

2.1 Identification and Authentication

With the widespread deployment of smart devices, security and privacy become one of the greatest concerns in pervasive computing [10]. Al-Muhtadi [2] described the essential first steps of any security system in the context of ubiquitous computing to be (1) Identification: the process of linking an entity with an identity; and (2) Authentication: verification of the claimed or detected identity of an entity. To authenticate the identity of a user, it requires a proof from him/her. This can be *what s/he knows* (knowledge-based: such as a password), *what s/he possesses* (possession-based: such as an ID card) or *who s/he is* (biometric: such as fingerprints). There are also *context-based* authentication methods where the system uses the context information (such as location) to grant user accesses [4].

2.2 Open Issues

The identification and privacy in pervasive computing are complex. Ranganathan [19] analyzes five barriers and suggests a fundamental re-examination. The first "who am I talking to" problem describes the difficulty in identifying an entity. Other questions such as "will my privacy be safeguarded?" and "can I trust the device I am communicating with" capture widespread society concerns in privacy-sensitive information. There are also regulations. The HIPAA [9] Privacy Rule is the set of national standards in protecting all "*Individually identifiable health information*" that health care providers and health care clearinghouses shall comply with.

Finding the balancing between usability and privacy has no easy solution. Jalal [2] states that "the very same features that make ubiquitous computing environments convenient and powerful make them vulnerable to new security and privacy threats." We can find a similar statement in [7] where Bhaskar uses "paradoxical" to describe a location-based service without revealing identity.

3. PRIVACY CONCERNS

Biometric authentication mechanisms [11] utilize physiological or behavioral signatures to identify a user. Since it is based on the fact of "who s/he is", there is no need to memorize a password or carry a card. Biometric identification therefore enhances the usability of an interface and is promising for ubiquitous applications. However, this form of identification raises considerable privacy issues.

3.1 User Survey

We conducted a scenario-based survey to properly demonstrate the privacy concerns in a workplace. The survey results were collected from the graduate students in UCLA Electrical Engineering and Computer Science departments. The author visited these students individually in their cubicles and labs to ask for a quick survey. Figure 1 shows the design of this questionnaire. To avoid bias, there was no explanation on the research problem that the author is working on. The students made her/his own selection solely based on the information obtained from the questionnaire. To promote users' participation, we design the questionnaire in an extremely simple fashion such that it consists of only one question. We have collected a total of **77** user opinions on this matter.

3.2 Questionnaire Design

As shown in Figure 1, the top part of the questionnaire is a given scenario for a long-term fitness monitoring application in workspaces using sensitive information. The bottom part is the question for users. The three options <A>, <B> and <C> indicate their preferences in privacy and usability.

We hid the following implications in the questionnaire. First, to enhance usability, we limit the interface to biometrics. Second, the office (or lab, cubicle, etc.) is a semi-public space that a limited group of people can access. Some people may feel secured in it while others do not. Third, in most cases, weight and blood pressure measurements are non-critical health information. It is good to know and keep track of, in order to detect a possible illness, but we can also get by without measuring it on a daily basis. Fourth, "fingerprint" and "voice pattern" are unique biometrics that a person possesses. A person can easily change a user ID and password, but it is difficult to change the bio-

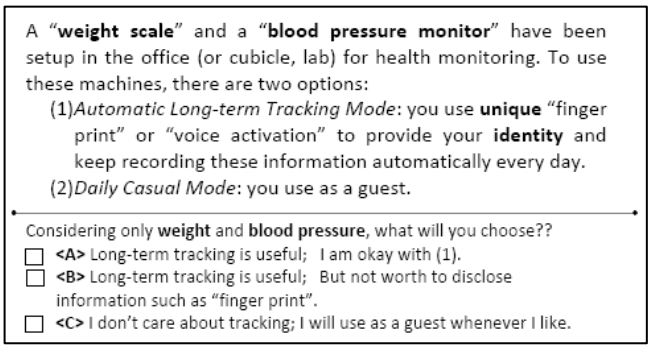

Figure 1. The questionnaire.

metric. In other words, we ask the participants whether they are willing to risk disclosing highly sensitive information for non-critical data collection in a semi-public space.

3.3 Survey Results

Table 1 presents the survey results. The application clearly shows its non-critical property where **~70%** of the people would think long-term tracking of weights and blood pressure is useful. At the same time **~30%** of them consider disclosing sensitive information for such applications is not worth it. The results reflect one of the public concerns described in the privacy and biometric framework published by the National Science & Technology Council (NTSC) [17]. In section V.A.1, it states "The concern is that biometric systems collect a lot of unique personal information and use the personal information to make small decisions." and asks the question "Does the individual feel he or she is giving and receiving items of equal value?" From the survey results, we clearly see the grey area for privacy concerns in workplaces.

4. THE PROPOSED DESIGN

User group <C> requires the easiest guest operating mode that all commercial products currently employ. Group <A> trusts that access to information will be controlled at every level of the system. Designing systems for group <A> is feasible, although potentially difficult and costly.

4.1 The Challenge

User group <B> is the most challenging to satisfy. They are concerned in revealing the sensitive biometrics even in their workplaces. Some users also request pseudonym access when taking these personal physiological measurements. Design solutions for user group <B> roll back to knowledge-based or possession-based authentication methods. However, neither method fulfills usability and privacy requirements simultaneously.

Knowledge-based authentication methods require a user to interact with the system, which is obtrusive in usability [5]. To require a user to enter a password every time s/he takes a weight measurement does not seem appealing at all. However, this solution has the advantage of creating pseudonym access (where a user creates a login name and associated password) for privacy-concerned users.

The possession-based authentication methods require a user to use a specific carryon token when accessing the system. The "always carry the token" requirement can be a heavy burden at home, but an acceptable overhead in the office. In addition, it does not provide the pseudonym access capabilities. Common tokens such as a driver license or a student ID card uniquely associate an identity to the token. Other tokens (such as a door card) provide the role of one user but do not distinguish among the same group of users. Stajano discussed the vulnerability of possession-based authentication in [23].

<A> Long-term tracking is useful; I am okay with biometric authentication.	28^{+} (**36.36%**) $^{+}$6 out of 28 people are the author's labmates.
<*B*> Long-term tracking is useful; But not worth to disclose information such as fingerprint.	26 (**33.76%**)
<*C*> I don't care about tracking; I will use as a guest whenever I like.	23 (**29.87%**)

Female	11	Under 25	13
Male	66	25 – 35	56
Total	**77**	35 – 45	7
		Above 45	1

Table 1. Survey results.

As was shown in the survey, the biometric authentication has privacy concerns. The search continues for other options that balance both privacy and usability while satisfying user group <B>.

4.2 Fitness Monitoring System

In fitness monitoring applications, the physiological information of weight, blood pressure and heart rate are the most popular information that people would like to record. Such physiological information has high variances and is not suitable for an exact biometric identification. However, we can ask the question what level of accuracy such a system can achieve in mapping the collected data to a user. Since this is a non-critical application, if the accuracy is sufficiently high, we can then loosen the required sensitive inputs from users.

The core of the system is to infer an anonymous identity based on imprecise physiological data and activity context information. Due to the deficiency of imprecise physiological data, the system also uses context information as assistance to reduce ambiguity. However, the system does not actively query any context information of a user. It is rather a passive process that is limited to the existing information. For example, the system does not request the GPS module on a cell phone to report back Alice's current location; instead, the system uses the fact that Alice has just swiped her door card to infer that she is in the room. It is the security system that records this access information, and this fact will not change with or without the identity inference system.

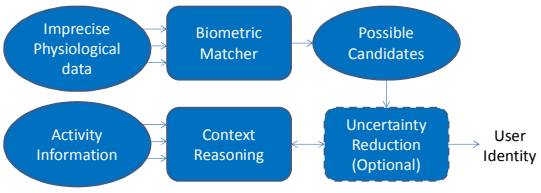

Figure 2. The components of the identity inference engine

The identity inference engine consists of two main components as illustrated in Figure 2. The Biometric matcher takes physiological data input and generates a pool of possible candidates. Context reasoning takes user activity information gathered by other systems to infer a user's physi-

cal presence. The result is then passed through the optional uncertainty reduction component to adjust the possibility of each possible candidate based on their context information.

4.3 Target Audience

With the possible inaccurate inferences on the identity of a user, this design is especially feasible in the home or workplace scenario for the following reasons. (1) *Diverseness in physicality*. In the 2006 survey [8], the average size of an American family was 3.13. Because of age and gender, it is highly possible that the components of an American family naturally have diverse physicality. Therefore, the system can easily infer the identity correctly even if the characteristic of a biometric is not unique. (2) *Fluidity of identity*. The possible users at home or office are usually fixed; they do not change frequently. The limited candidate pool size increases the probability of making correct identification. (3) *Requirement of Usability*. We observe that a user has various degrees of usability expectation for different places. In the home scenario, a user expects high usability. When in a public place, such as a coffee shop, a user tends to be more cautious and aware of security. The usability in a workplace is a grey region that falls somewhere in between. (4) *Activity patterns*. Users in an office employ consistent activities and users at home are more likely to perform more varied activities. There are no fixed activity patterns for the public scenario. We compare the intrinsic properties of these places in Figure 3.

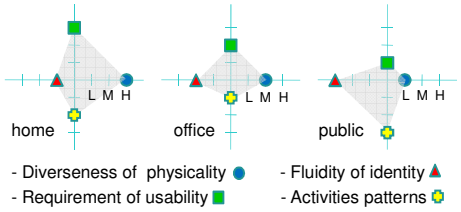

Figure 3. The caparison among home, office and public.

5. IMPLEMENTATION

We present a prototype system that performs fitness monitoring (weight, blood pressure, heart rate) for healthy individuals in workplaces. To test the feasibility of the proposed idea, we designed and deployed a system in our lab. The system consists of a weight scale (A&D Medical UC-321PL) and a blood pressure monitor (A&D Medical UA-767PC). Both devices communicate with a laptop via their RS-232C ports. A data collection program written in C++ runs on the laptop to continuously record and timestamp the weight and blood pressure readings. There are text input and speech recognition interfaces for a user to input the name. This step is required to establish ground truth for the experiment. The network activity information is used to infer the presence context of a user. The firewall server runs a monitoring program that continuously logs networking traffic from each computer. We specifically take traffic information of port 80 (the HTTP port). The assumption is that most graduate students browse the internet (access email, etc.) occasionally when they are at work. We use this assumption to infer their presence in the lab.

5.1 Biometric Matcher

We implement a naive Bayes classifier [16] that combines multiple sensor observations for the purpose of inferring the identity of a subject. The naïve Bayes classifier assumes that each observation is independent of every other observation, and in practice it often competes well against more sophisticated classifiers [18]. By applying Bayes' Theorem and independence assumptions, the probabilistic classifier is described as,

$$p(I \mid O_1,\ldots,O_n) = p(I)\prod_{i=1}^{n} p(O_i \mid I) \Big/ p(O_1,\ldots,O_n),$$

where the class variable I is the identity of users and O is the set of sensor observations.

5.1.1 The Model of Weight, Blood Pressure, and Heart Rate

We establish simple Gaussian models for weight, blood pressure, and heart rate in a Bayes classifier. After the first five measurements, the mean is updated through an exponential moving average, $M_t = \alpha \cdot W_{t-1} + (1-\alpha) \cdot M_{t-1}$. We set α to 0.2 for this study, which gives more importance to recent observations. The system only updates the mean if the confidence to the user's identity is greater than 65%. We set the standard deviation of weights to 3lbs, considering the amount of food intake, difference in clothing, and typical daily weight variation. The standard deviation of the systolic blood pressure and diastolic blood pressure are set to 15 mmHg and 13mmHg respectively according to [15]. The standard deviation of the heart rate is set to 20bpm considering that this monitoring station is set in a workplace environment rather than an exercising place.

5.2 Context Reasoning

We build the context reasoning component [26] based upon reified temporal logic [24]. Context reasoning provides the high-level contexts about a user's state and surrounding. Reified temporal logic allows us to express *when* things are true. We adopt the two meta-predicates described in [14]. The notation HOLDS(T, *pro*) expresses that *pro* holds true over time T. Another notation HOLDS_IN(T, *pro*) asserts that *pro* holds true over some time during T. In our prototype, a user's context (such as in the lab at a specific time) is determined through these predicates of the network activity information.

$$HOLDS(T, pro) \Leftrightarrow \forall t.\, in(t,T) \Rightarrow HOLDS(t, pro)$$
$$HOLDS\_IN(T, pro) \Leftrightarrow \exists t'.\, in(t',T) \Rightarrow HOLDS(t', pro)$$

5.2.1 The Model of Presence Context

We use network activities to infer a user's presence in the lab. It is based on network activity information because

most individuals have at least one personal device connecting to the network. Additionally, it is economically efficient to collect information from a single device (router). Figure 4 illustrates these rules. When a fitness monitoring measurement is taken, T_p is set to include the 20 minutes before and after the associated timestamp. The system then infers a user's presence during that period based on following rules. We describe these rules:

1. A user is present during the time period T_p if there is Internet browsing activity on the user's PCs.
   - *PRESENCE* :- HOLDS_IN(T_p, exists(*ACTIVITY*))
2. A user is browsing the Internet during T_{min}, if there is network traffic for more than $\theta_{activity}$ times.
   - *ACTIVITY* :- HOLDS(T_{min}, count(*TRAFFIC*) > $\theta_{activity}$)
3. The network has traffic during $T_{10\text{-}sec}$, if the amount of packets is more than $\theta_{traffic}$.
   - *TRAFFIC* :- HOLDS($T_{10\text{-}sec}$, count(*PACKETS*) > $\theta_{traffic}$)

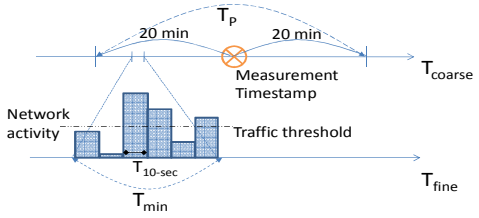

Figure 4. Context Reasoning based on Networking Traffic

6. EXPERIMENTAL RESULTS

We have deployed the system in our lab since mid Feb, and the data points used for this paper are from Feb. 14, 2008 to Mar. 28, 2008. A total of 355 data sets were collected including 185 weight data points and 170 blood pressure /heart rate data points. The total measurement count is 222 times (most participants took measurements on both devices, but sometimes only one device was used). We have a 30-day network monitoring log spread within the period (it does not cover full span of the period due to technical issues). Users are free to take weight and/or blood pressure measurements (heartbeat rate comes with blood pressure measurement) at any time. Therefore, the user usage is in a totally casual fashion to approach reality. The operating interfaces of these devices are maintained as the original ones: one kick to start the weight scale and one button to start the blood pressure monitor. To establish ground truths, we require users to input their name before using the devices. To facilitate this process, we added a small voice recognition system based on CMU Sphinx-4 [25]. This allows users to input by saying instead of typing their name. A total of **9** users have participated, and 6 of them regularly work in lab (thus have network activities).

Table **2** illustrates the challenge of identifying a user based on imprecise physiological information and their usage contexts. With just 9 people, we can easily find 3 groups that have very close weights. Additionally, the blood pressure and heart rate vary considerably depending on the circumstance of the user when taking the measurement. Table **3** shows the classifier results if it uses only one physiological information source. As shown later, combining the four sources of information (weight, systolic and diastolic blood pressure, and heart rate) can significantly enhance the accuracy in identifying a user. However, another challenge is that not all users use both devices each time. Some have a strong tendency in taking only their blood pressure or weight. This is counter to what a good classifier needs, and thus its performance degrades considerably.

User	Similarity in Physiological Information	Seat in Lab	Usage Habit		
			Weight Scale	BP Monitor	Both
A	Light		V	V	
B	They have similar weights. The differences in mean (of all their data points) are less than 1.9 lbs.	V		V	V
C		V			V
D		V	V		
E	Their difference in average weight is 2 lbs.	V			V
F					V
G	Their difference in average weight is 1.1 lbs.	V	V		
H		V			V
I	Heavy		V		

Table 2. Participants of the experiment.

Physiological Data for Classifier	Positive Match	False Match
Weights	57.23%	45.77%
Systolic Blood Pressure	22.02%	77.98%
Diastolic Blood Pressure	43.90%	56.10%
Heartbeat Rate	25%	75%

Table 3. The classifier results for one physiological information source

The biometric matcher using the naïve Bayes classifier to combine all 4 sources of physiological information improves the identification accuracy to ~78%. As we mentioned earlier, due to users' uncertain usages, some of these inputs consist of only one data point (weight) or three data points (systolic and diastolic blood pressure, and heart rate). If the user classification is only based on complete measurements (a total of 134 measurements that have all 4 data points), the accuracy of the classifier improves to 87.3%. This result is shown in Table **4**.

Biometric matcher that combines all 4 physiological sources.	Positive Match	False Match
Classification Results for partial or complete data points.	77.9%	22.1%
Classification Results for complete data points only.	87.3%	12.7%

Table 4. The classifier results based on multiple sources.

Table **5** shows the context reasoning component based on network traffic. We use the fact that a user has to be in the lab to take a measurement to establish ground truths. The positive rate (a user is in the lab and the context reasoning agrees) is 89.47% and the false positive rate (a user is in the

lab and the context reasoning shows the negative answer) is 10.53%. The results are analyzed based on the 114 measurement timestamps from the computers of the 6 regular lab users.

Context Reasoning Component	Positive	False Positive
The presence of a user based on network activity	89.47%	10.53%

Table 5. The accuracy of the context reasoning component.

The system only uses the context reasoning component when it is unsure about the results from the biometric matcher. We set the criteria of context reasoning to the confidence difference between the largest and the second largest of user candidates. If the difference is less than 15%, then the system triggers the context reasoning for these two users. Within the 30-day period where we have networking log (142 measurements), the performance of biometric matcher increases by 5.63% when combined with context reasoning (see Table **6**).

	Biometric Matcher only	Biometric Matcher and Context Reasoning
Accuracy	78.16%	83.80%

Table 6. Combining the biometric matcher with the context reasoning.

7. Discussions

In this study, we have not yet explored the possibility of integrating users' usage habits. We can achieve nearly **100%** accuracy by imposing three rules: (1) User B sometimes measures blood pressure only; (2) User D and G often uses the weight scale only; (3) User E uses the weight scale before the blood pressure monitor and User F uses the two devices in reverse. But how to learn these usage habits remains questionable. Unlike the training data sets for physiological data, properly capturing a habit requires a long-term observation. And with the uncertainty involved in the system, this learning process is difficult to realize.

We estimate that systems like this can identify 8 to 15 people. This is sufficient for family usages., and in workplaces, the proposed design can be integrated with other interfaces. Integration of multiple interfaces empowers users the "control" ability. People with less privacy concerns can use high-accuracy biometrics to perform identification. Highly-privacy-concerned or careless users can use the system as a guest to perform anonymous access. Others may choose the solution proposed in this work. This satisfies most users with the ability to choose the interaction they are comfortable with.

8. CONCLUSIONS

In this paper, we proposed a hassle free design for fitness monitoring. To preserve privacy, the system identifies a user based on imprecise physiological information and existing activity context. The system maintains its original interface for users, in order to provide the same ease of usability. We believe that our design can serve as a bridging solution between present and future pervasive computing.

9. REFERENCES

[1] A. Acquisti, J. Grossklags, "Privacy and Rationality in Individual Decision Making", IEEE Security and Privacy 3, 1 (2005), 26–33.

[2] Jalal F. Al-Muhtadi, "An Intelligent Authentication Infrastructure for Ubiquitous Computing Environments," Ph.D. Dissertation, Univ. of Illinois at Urbana-Champaign, 2005.

[3] "Fingerprint Scans Replace Clocking In", The Associated Press, March 26, 2008

[4] J.E. Bardram, R.E. Kjær and M.Ø. Pedersen, "Context-Aware User Authentication - Supporting Proximity-Based Login in Pervasive Computing". In *Proceedings of UbiComp 2003*, Oct 2003

[5] J.E. Bardram, "The Trouble with Login - On Usability and Computer Security in Ubiquitous Computing." *Personal and Ubiquitous Computing*, 9(6):357-367, 2005.

[6] L. Barkhuus and A. Dey. "Location-based services for mobile telephony: a study of users' privacy concerns." In Proceedings of INTERACT 2003, 9th IFIP TC13 International Conference on Human-Computer Interaction. 2003.

[7] P. Bhaskar and S.I. Ahamed, "Privacy in Pervasive Computing and Open Issues," Proceedings of The Second IEEE International Conference on Availability, Reliability and Security (ARES 07), 2007.

[8] Families by Size and Presence of Children: 1990 to 2006, The 2008 Statistical Abstract, U.S. Census Bureau

[9] The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, http://www.hhs.gov/ocr/hipaa/

[10] J. Hong, M. Satyanarayanan, G. Cybenko, "Guest Editors' Introduction: Security & Privacy," Pervasive Computing, IEEE, Volume 6, Issue 4, Oct.-Dec. 2007 Page(s):15 – 17

[11] A.K. Jain, A. Ross and S. Prabhakar, An introduction to biometric recognition, IEEE Trans. Circuits Systems Video Technol. 14 (2004) (1), pp. 4–20

[12] E. Kaasinen, User Needs for Location-aware Mobile Services. Personal and Ubiquitous Computing 2003. 7(1): p.70-79.

[13] R. Lord, "High-tech time clock could be stopped - City plan to scan fingerprints runs into controversy", Pittsburgh Post-Gazette, July 22, 2006

[14] J. Ma and B. Knight, "A Reified Temporal Logic", *The Computer Journal* 1996 39(9):800-807

[15] B.T. Marczak, A. Paprocki, "Blood pressure variability on the basis of 24-hour ambulatory blood pressure monitoring in a group of healthy persons", Przegl Lek. 2001;58(7-8):762-6.

[16] Richard E. Neapolitan, "*Learning Bayesian Networks*", Prentice Hall, 2004.

[17] National Science and Technology Council, "Privacy & Biometrics: Building a Conceptual Foundation", Sep. 2006

[18] I. Rish, "An empirical study of the naive Bayes classifier". IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence, 2001.

[19] K. Ranganathan, "Trustworthy Pervasive Computing: The Hard Security Problems", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004

[20] D. Saha, A. Mukherjee, Pervasive Computing: A Paradigm for the 21st Century, *IEEE Computer*, pp. 25-31, March 2003.

[21] V. Stanford, "Using pervasive computing to deliver elder care", *IEEE Pervasive Computing* , 2002

[22] V. Stanford, "Pervasive health care applications face tough security challenges", IEEE Pervasive Computing, April-June 2002

[23] F. Stajano, "Security For Whom? The Shifting Security Assumptions Of Pervasive Computing", Proc. of International Security Symp., 2002

[24] L. Vila, "A Survey on temporal Reasoning in Articial Intelligence." *Articial Intelligence* 7 (1994) 4-28

[25] W. Walker, P. Lamere, P. Kwok, B. Raj, R. Singh, E. Gouvea, P. Wolf, J. Woelfel, Sphinx-4: A flexible open source framework for speech recognition, Tech. Rep., Sun Microsystems Inc., 2004.

[26] X. Wang, J. S. Dong, C. Y. Chin, S. R. Hettiarachchi, and D. Zhang, "Semantic Space: an infrastructure for smart spaces," IEEE Pervasive Computing, vol. 3, no. 3, pp. 32–39, July–Sep. 2004.

[27] M. Weiser, "The Computer for the 21st Century," *Scientific Am.*, Sept., 1991, pp. 94-104