IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9729

Ethical Issues in Pervasive Computing Security

Dr. M. Mohamed Ismail

Associate Professor, Department of Computer Science, Mazharul Uloom College, Ambur

Abstract: The importance of awareness with regard information systems (IS) security has been recently acknowledged. This paper studies the applicability of one aspect of the awareness approach, namely ethics and morality, to the context of pervasive computing. This paper presents an overview of ethical theories by discussing descriptivism and universal prescriptivism, the latter of which is then applied to the context of IS security. A model of ethical thinking in organizational context is developed, problem areas and hypotheses are identified and preliminary solutions are presented.

The model is applied to a pervasive computing security scenario where it reveals key problem areas that are ad-dressed with the help of the awareness approach and the preliminary solutions presented.

Keywords: ethics, information systems security, awareness

1 INTRODUCTION

1.1 Security in pervasive computing

Security has been defined as a process of assessing threats, vulnerabilities, and attacks; analyzing the risks; and developing and deploying safeguards and countermeasures to attain the desired risk level and optimal cost-benefit ratio [16].

Technological advances have changed the nature of computing and information security considerably. Three discrete steps in this development have been identified, namely standalone mainframe computing, multi-user computing environment, and personal computers and networks [18]. It can be argued that pervasive (ubiquitous) computing would be the fourth step in this development.

What is new in the world of pervasive computing from the security perspective is that everything computes, communicates and potentially contains private, sensitive information. This means that ensuring security using only technological solutions is going to be more difficult than ever before. Other ways to improve security must be sought.

1.2 Overview of approaches to minimizing user-related faults in IS security

Recent research to minimizing user-related faults in information systems (IS) security can be roughly summarized as follows [11]. First, since ancient times, punishment has been used to discourage 'wrongdoing' [1]. It has been debated whether punishment as deterrence is relevant in the context of contemporary IS security or not. Results that support the economic theories of punishment [17] have been published. However, scholars of the behavioural community have presented much evidence of the negative long-run consequences related to the use of punishment, for instance loss of productivity, increased dissatisfaction, and aggression [14].

Second, the importance of ease of safe use and the related transparency principle have been presented [9]. Similarly, a social approach, named User-centered security (UCS), has been put forward [19]. However, some argue that 'ease of safe use' has not been properly defined [11]. Moreover, some elements of the mentioned approaches are argued to teach users to take security as granted, which may lead to neglecting or misusing forthcoming security mechanisms. Further-more, the aforementioned approaches are criticized for not presenting guidelines to modeling let alone resolving conflicting requirements.

Third, the Organizational psychology and incident analysis (OPIA) approach has argued that human errors can only be overcome by understanding human behaviour [15]. How-ever, According to Siponen, the six theses that constitute OPIA do not stand up to closer psychological scrutiny [11]. For instance, the effects of weakness of will and lack of commitment are not taken into account.

Fourth, the importance of awareness has been underlined [17] since it has been perceived instrumental to the effort of reducing 'human error'. The topic has been approached systematically, and program frameworks have been developed [7]. Extending the analysis, Siponen has presented a conceptual foundation for organizational information security awareness that differentiates between the framework ('hard', structural) and content (informal, interdisciplinary) aspects [10].

 This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9729

1.3 Role of ethics in the awareness approach

Siponen argues that with regard to security guidelines, education should aim at the users internalizing the needs that drive the security guidelines [10]. Thus, it is important that security guidelines are justified as normative claims, i.e., arguments and justifications are given. As a result, users may change their attitude and motivation towards the guidelines in the inteded way, and attain prescriptive awareness of the subject of security, which is central target of the awareness approach.
Persuasive communication, such as argumentation and justification, has been widely studied in the behavioural sciences, the results of which can be applied to the field of information security[18][10]. Siponen constructs a toolbox formation security [18] [10]. Siponen constructs a toolbox of seven approaches that can help in the quest of prescriptive awareness. One of these approaches is Morals and ethics, others include rationality, feeling of security and appealing to emotions.

The rest of this paper is structured as follows. Section 2 provides an introduction to ethics. Section 3 introduces a model of ethical processing in the context of IS security and presents the lessons learnt. Section 4 presents an example of application of the model in educating users in ubiquitous computing security. Section 5 discusses our findings and Section 6 provides a conclusion to this article.

2. OVERVIEW OF ETHICAL THEORIES

Ethical theories can be divided into two categories: the descriptive and the normative (non-descriptive) [12] [5]. We will first discuss descriptivism, for its attractiveness, and then turn to universal prescriptivism an example of normative ethical theories, for its theoretic rigor and applicability in IS security. Covering the whole landscape of ethical theories is outside the scope of this paper.

2.1 Descriptivism

In most societies, people will instinctively frown upon certain actions, such as killing a person for monetary gain. It is only natural to draw conclusions, over time, following empirical tradition, by observing and analysing these instictive reactions. It is also natural to synthesize from this evidence that wrongness is a property of certain kinds of actions. This line of reasoning is called descriptivism: in an effort to study what ought to be, the present given norms and traditions of a society are studied.

Cultural relativism is an example of descriptivism. Cultural relativism holds that the morality of an action depends on culture: what is morally right in one culture, may be morally wrong in another. Moreover, it holds that one culture cannot be held superior to another.

As an example, breaking into information systems is al-lowed in hacker ethics. According to cultural relativism, we are not allowed to hold our prevailing culture, namely that privacy is important and must be protected, superior. Hence, it has been argued that human morality cannot be applied for the protection against security violations [6].

However, descriptivism in general and the case of hacker ethics in particular have been shown to be fallacious [4] [12]. Descriptivism ignores the principle of factual / normative dualism, ’no ought from an is’, thus succumbing to being a naturalistic fallacy [8].

Consequently, descriptive theories cannot be used to construct sustainable ethical standpoints, and thus should be rejected.

2.2 Universal prescriptivism

The theory of universal prescriptivism by R. M. Hare is based on a two-level model of moral processing: intuitions and critical thinking [4]. Intuitions are simple prima facie principles that can be used in daily life, for instance, ’do not steal’ and ’protect the innocent’.

Universal prescriptivism recognizes that intuitions are not applicable to all situations. For example, it should not be immoral to steal the plans of a war criminal in order to prevent him from committing genocide.

Hence, universal prescriptivism holds that when in a situation where intuitions are insufficient, critical thinking should be employed to come up with a universal maxim that one would agree with no matter which role one had in the situation.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9729

2.2.1 Universalization

The process of universalization is a key element in the theory of universal prescriptivism [4]. Roughly summarized, the process is as follows.
First, a crude approximation of the moral instruction should be obtained to be used as candidate maxim in the process. This candidate maxim should then be universalized, i.e. all references to individuals removed, leaving only universal properties of the situation left. The candidate maxim should then be modified so that we would find it agreeable, no matter which position we had in the situation. At this point it is important to reflect the situation from a universal perspective, i.e. understand how the situation affects the preferences of individuals who find themselves playing various roles in the situation. The process ends when the candidate maxim satisfies both of these conditions.

3 ETHICS AND SECURITY MANAGEMENT

Ethics has a big influence on the behaviour of individuals. If we accept Hare's argumentation, and for the purposes of this article we do, even the egoistic amoralist will submit to behaving morally [4]. If individuals (both users and security managers) can be encouraged to engage in ethical thinking in the IS security context, this persuasive power can be utilized in IS security management. This is also the role that ethics has in the awareness approach 1.3.

Ethics has another role in IS security management as well. The cognitive models of ethical theories can be utilized to construct models of ethical thinking. This section establishes a model based on R. M. Hare's two level model of ethical processing. This section also identifies our perception of the problem areas in the context of IS security, and provides preliminary instructions to addressing those problems. This section also sheds light to the importance of organizational culture in this context.

3.1 Model of ethical thinking and problems in contemporary organizations

As discussed in 2.2, according to Hare, there are two levels on which moral processing occurs: the intuitive level and the level of critical thinking, the latter of which should be engaged when the first proves insufficient.

Figure 1 depicts our interpretation of Hare's two-level model [4] in the organizational context. We have identified three memory units (intuitions, specific solutions, and ethi-cal models and frameworks) and eight processes (P0 through P7).

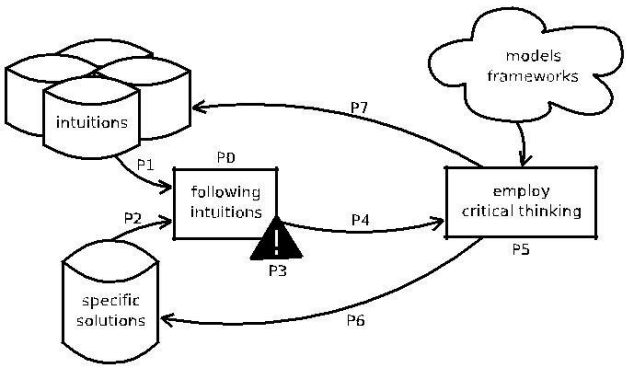

Figure 1 - interpretation of Hare's two-level model

Although the memory units reside within each individual, the extent to which they are socialized varies considerably. First, ethical models and frameworks are individual's interpretations of universal ethical theories. These interpretations should be openly discussed during ethics teaching thereby establishing some common ground of interpretation.

Second, intuitions are learned over years and decades and are commonly transferred through social heritage. Addition-ally, a common set of intuitions is usually established during group formation and groups usually also, more or less, through social controls, enforce the intuitions [2].

Finally, in contrast to the first two, individuals may hesitate to actively communicate any specific solutions they may have resolved to others. This is not because they'd feel ex-posed, but because they may feel, quite correctly, that with-out serious consideration, specific solutions may not be generalizable, which open communication often, incorrectly

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9729

and unfortunately, implies.

The mental processes described by Hare are modeled in Figure 1. In day-to-day business, we operate (P0) by applying our intuitions (P1) to the present situation. If we already have developed a specific solution that can be applied in this particular situation, we use it instead (P2). However, should we notice (P3) that our intuitions are in conflict or perhaps insufficient, we should switch (P4) to critical thinking mode, where we apply (P5) the ethical theories and frameworks we have learned to the situation. Hopefully, a solution to this particular situation will emerge. We will store (P6) this solution to our specific solutions 'database' for further reference (P2).
We will next identify eight hypotheses H1 through H8) on which we will build four sketches for solutions (S1 through S4).

It is our perception that the process of critical thinking is quite expensive in terms of time and mental processing effort (H1), particularly so if the individual is not equipped with the models and frameworks provided by ethical theories. Indeed, it may be that the cost would be infinite, i.e. the problem would be insoluble from the perspective of the individual.

Moreover, if an individual is placed in a situation where most of his intuitions are out of place (H2), as is plausibly the case in the context of contemporary, complex, interconnected, and constantly evolving IS security, the individual would have to trigger critical thinking all the time. If the individual has a prohibitively high critical thinking unit cost, what else can be expected of the individual but frustration and eventual negligence of moral aspects (H3)?

Furthermore, if intuitions are incorrectly formulated and do not capture what is essential (H4), how are individuals supposed to notice (P3) when their intuitions would result in violating that which is essential? For instance, we argue that 'do not kill' could be better formulated as 'preserve human life' because the latter captures the essential point of the maxim better and would forbid one from simply letting someone expire.

Hence, it is our perception that there are two key problem areas: incorrectly formulated intuitions that results in problems in noticing their limitations (H4), and high cost of critical thinking (H1). Moreover, we argue that solving the latter problem will make the transition (P4) easier (H5). This will in turn encourage individuals to be more sensitive to ehtical problems in day-to-day business (H6), hence improving the process of ethical problem spotting (P3) as well.

As all costs, this cost too has two components: unit cost and amount purchased, or, equivalently, frequency of purchase.

There are two steps to be taken to drive the high unit cost down. First, individuals should be educated to understand ethical theories and their applications in the organization's field of operations (S1). This educational effort is not trivial and its success is not self-evident, but highly dependent on the organizational culture. Moreover, teaching ethics requires knowledge of ethical theories and persuasive discussion skills; indoctrination must be avoided. Siponen and Vartiainen have presented a framework for an ethics curriculum based on universalization [13] that in our opinion could be quite suitable in the context of the presented model.

Second, some sort of process should be established to tackle the most difficult ethical dilemmas (S2). For instance, a monthly ethics workshop could be arranged.

Means should be sought to minimize the need to resort to critical thinking in resolving the ethical dilemmas of day-to-day business. There are two ways to do this. First, the collective intuitions of the organization can be adjusted to better suit the environment in which they are used (S3). This process is shown in the model (P7). Also, the limitations of new, revised intuitions should be clearer, thus facilitating ethical problem spotting (P3).

Second, individuals could be encouraged to share the specific solutions they have rendered with others (S4). It should be underlined that generalization of the specific solutions must be avoided and that even if some specific solution proves to be unsustainable or downright wrong, the individual who rendered it should not be penalized, even in the slightest way.

3.2 Organization culture

Applicability of ethics to security management depends heavily on the culture of the organization in which it is to be applied. For instance, any double standards quickly undermine any basis for ethical discourse: the business active of the organization must be able to stand up to moral scrutiny.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9729

Also, people tend to avoid disobeying direct orders. If an individual is directly ordered to commit an act which the individual perceives immoral, one of two things will happen. First, ethical aspects may get completely thrown out of the window. Alternatively, a moral conflict may ensue. This will put the individual under substantial stress. The result of such a situation is highly unpredictable. Either way, from an ethical viewpoint, the results are undesirable.

Thus, if ethical thinking, decision-making and behaviour is to be encouraged, individuals should be given the opportunity to exercise their free will and autonomy [3]. Moreover, the organizational culture should foster an open climate for communication and discourse, and employees should feel respected by the employer [12].

4 EXAMPLE OF APPLICATION OF ETHICS TO PERVASIVE COMPUTING SECURITY

4.1 Scenario

Let us set our example in the context of a consultancy agency that stores and processes very sensitive information about its clients. As many consultancy agencies today, our example agency is quite narrowly focused on a very specific field of operations. For most clients, the mere association with the agency would raise inconvenient questions, for example with regard the clients' strategic intentions.

Let us imagine that a conference with a large number of participants is held on some quite general topic, say on net-works and organizations. Let us imagine that the organizers of the conference want to perform an experiment with the conference participants, say they wish to test facial expression recognition software.

Conference organizers have developed an application to make the necessary calculations. Participants are asked to upload the email addresses they have stored in their PDAs and cell phones. To protect the privacy of the participants, the organizers only process hashes of addresses, so that matching addresses can be identified but addresses them-selves cannot. Participants are given an electronic name tag with an RFID chip so that RFID scanners placed in the conference area can tell when two acquaintances are in the same space. Cameras attached to facial expression recognition software are configured to instruct the name tags to play a chime and flash whenever the system recognizes that two acquaintances are close to one another but have not yet recognized one another.

A consultant of our example consultancy agency participates to the conference. When asked to upload his contact information, which he knows contains client information, he refuses, because email addresses of clients have been classified confidential. The organizer convinces him that the email addresses of his clients will be safe because they will only be stored in a mangled form. This assures him that he can upload his contact information and still be in line with the agency policy. He wishes to run into his friends from the days at the academy and thus uploads the information.

Let us imagine that, unbeknownst to the consultant, a client is also taking part to the conference. She too is asked to upload her contact information, she too hesitates, but upon privacy assurances she too agrees to upload.

During the conference, the consultant and the client meet by coincidence. Upon their mutual agreement of not revealing their business relationship, they ignore one another. However, the facial expression recognition algorithm recognizes that two acquaintances are within each other's vicinity but have not recognized one another and thus, has the name tags chime and flash. Embarrassment, rumors, media frenzy, and breach of contract lawsuits ensue.

4.2 Analysis

How could ethical considerations have helped in the context of the above scenario? Upon first glance, it can be argued the consultant was not acting unethically. He was instructed to keep client email addresses confidential, that is, not expose them for others to see. He can argue that this is exactly what he did; the email addresses were hashed on his PDA using a well-known high-grade hashing algorithm before uploading them to the organizer's database. The email addresses cannot be obtained by studying the information he uploaded.

The above argument is true on the factual level. However, the issue isn't that the email addresses of clients were ex-posed. Instead, the issue is that the relationship with a client has been exposed.

Again, how is this related to ethics? The short answer is that it isn't, not directly. The long answer is that the consultant wasn't sufficiently aware of what was required of him and that we will be in a much better position to fix this lack of

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9729

awareness if we submit ourselves to thinking critically about what exactly is it that is wrong or right. Moreover, we can identify problems in the consultant's thinking by applying the two-level model presented in 3.1.

If we formulate the problem with the consultant in terms of the two-level model, we will quickly discover that the consultant did apply his intuitions (P1): he first refused to disclose classified information, and upon meeting a client, acted as if they were strangers. We won't be able to tell if he tried to apply any specific solutions prior to uploading (P2), but this is likely irrelevant because the situation was completely new to him.

Thus, we have identified three intuitions:

- if one meets a client in a public situation, one must pre-tend that you are complete strangers
- one must keep client information confidential (including names, email addresses, telephone numbers, ...)
- cryptographic hash of confidential information is not confidential (because the confidential information can-not be deduced from the hash and hence, confidentiality is preserved)

The first two intuitions are practical approximations of a higher-level maxim, 'do not reveal our clients'. The third in-tuition is derived from the cryptographic properties of hash algorithms. All of these are defendable and 'true', as intuitions go.

There is a loophole, however. Cryptographic hashes can be used to identify matches. In other words, information about client identity is leaked.

The root cau**se of the problem is that the consultant failed to notice** (P3) that critical thinking would have been needed. Two reasons for this can be identified. First, the consultant may have been insufficiently motivated to engage in critical thinking, either because altogether low awareness towards ethical issues, or perceived high unit cost of critical thinking. Second, the unfortunate formulation of the intuitions may have contributed to their limitations going unnoticed.

4.3 Solution

The following approaches should have been taken in the agency to prevent the problem from manifesting.First, the security awareness of the individuals in the agency should have been raised. A framework and methods to achieve this have been presented by Siponen [10]. It should be noted that one of the methods presented by Siponen is the application of ethics. For instance, we could apply the process of universalization to the situation of revealing a sensitive business relationship.

Second, the collective intuitions should have been adjusted (S3, P7). The second intuition identified above, namely 'keep client information confidential', fails to capture the essence of the higher-level maxim; email addresses and telephone numbers are not the sensitive part, the association with the agency is. In other words, all relations (agency, client) are confidential regardless of what information is used as identifier. We believe this mismatch between intuitions and what is truly meant could have been noticed had the agency engaged in collective critical thinking (S2).

5. DISCUSSIONS

This paper identified two roles that ethics has in pervasive computing security.
First, the role of ethics as one aspect in the awareness approach in information systems (IS) security was explored by the means of a literary review in Section 1. It was discovered that ethical theories can be very useful in formulating, arguing and defending security policies sustainably, which is necessary to reach prescriptive awareness of security issues. This is, in turn, necessary to change the attitude and motivation of individuals towards the guidelines of the security policy in the inteded way [10].

Second, a cognitive model for ethical thinking in the con-text of IS security was developed using Hare's two-level model as basis. Several potential problem areas were identified in the model and hypotheses were formulated. Also, several preliminary sketches for solutions were developed.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9729

5.1 Limitations and open questions

This study has two major weaknesses that must be addressed before the results of this study are applied to practice. First, in section 3.1, our hypotheses (H1 through H6) are not backed by empirical research but are, for the moment, based on mere intuitions. Second, a cost-benefit analysis needs to be performed. This is a nontrivial problem because estimating the indirect costs associated with unethical business conducts is difficult. Moreover, the solutions offered in 3.1 (S1 through S4) involve high risks due to uncertainties of organizational learning.

Additionally, the practical applications of this study are limited to individuals within an organization and perhaps in directly connected (partner) organizations. While this approach seeks to help individuals defend their information systems in hostile environments as well (through advocating secure ways of working), there is little hope that the motives of a determined outside intruder can be affected using applications of this study. Hence, it is paramount to understand that application of ethics is merely one tool in the toolbox of IS security management.

6. CONCLUSIONS

This article introduced two ways to apply ethics to pervasive computing security. The article first briefly described the context of pervasive computing and what approaches have been explored to minimizing user-related faults in information systems (IS) security. The awareness approach was selected for use in the article, and the role of ethics in it was described.
Section 2 provided a brief introduction to the ethical theories of descriptivism and universal prescriptivism, the latter of which was selected for use in Section 3.
Section 3 introduced a model of ethical thinking and identified in it probable problem areas in the context of IS security in contemporary organizations. Preliminary solutions to address those problems were provided.
The model was applied to a pervasive computing security issue in Section 4. Using the model, the root cause of the problem was identified and a way to correct the situation was developed. The awareness approach was also applied.
Section 5 discussed our findings with regard applying ethics to security in the context of pervasive computing and discussed limitations of our findings and open questions.

REFERENCES

[1] J. C. Ball. The deterrence concept in criminology and law. The Journal of Criminal Law, Criminology and Police Science, 46:347, 1955.
[2] D. Buchanan and A. Huczynski. Organizational Be-haviour: An Introductory Text. Prentice Hall, 4th edi-tion, 2004.
[3] R. M. Hare. Autonomy as an educational ideal, 1975.
[4] R. M. Hare. Moral Thinking: its levels, method and point. Oxford University Press, 1981.
[5] R. M. Hare. A taxonomy of ethical theories. In Sorting out Ethics. Oxford University Press, 1997.
[6] J. Leiwo and S. Heikkuri. An analysis of ethics as foundation of information security in distributed systems Proceedings of the 31st Hawaiian International conference on System Sciences (HICSS-31), 1998.
[7] NIST. Information technology security training requirements: A role-and performance-based model.Technical Report SP 800-16, NIST, March 1998.
[8] K. Popper. What can Logic do for Philosophy?, volume Supplementary Vol. XXII. Aristotelian Society, 1948.
[9] J. H. Saltzer and M. D. Schroeder. The protection ofinformation in computer systems. Proceedings of the IEEE, 63(1), September 1975.
[10] M. T. Siponen. A conceptional foundation for organizational information security awareness. Information Resources Management Journal, 8(1):31–41, 2000.
[11] M. T. Siponen. Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. Information Resources Management Journal, 8(5):197–209, 2000.
[12] M. T. Siponen. On the role of human morality in information system security: From the problems of descriptivism to non-descriptive foundations. Information Resources Management Journal, 14(4):15–23, Oct. 2001.
[13] M. T. Siponen and T. Vartiainen. End-user ethics teaching: Issues and a solution based on universalization. Proceedings of the 34th Hawaii International Conference on System Sciences, 2001.
[14] B. F. Skinner. Science and Human Behaviour. Macmillan, New YorK, NY, 1953.
[15] M. E. M. Spruit. Competing against human failing.15th IFIP World Computer Congress, 1998.
[16] F. Stajano. Security for Ubiquitous Computing. John Wiley & Sons, February 2002.