Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 197 (2008) 105–119
www.elsevier.com/locate/entcs

Trust-enhanced Security in Location-based Adaptive Authentication

Gabriele Lenzini,[1] Mortaza S. Bargh and Bob Hulsebosch

Telematica Instituut
7523XC Enschede, The Netherlands

Abstract

We propose trust to enhance security in adaptive and non-intrusive user authentication in controlled and pervasive environments. In addition to who a user is (e.g., via biometrics) and what a user knows (e.g., a password, a PIN), recent authentication solutions evaluate what a user has. The user's identity is then derived from what detectable accredited items (e.g., badges, RFIDs) and personal devices (e.g., smartphones, PDAs) the user shows when authenticating. The level of security of the access is set consequently. Position information is also considered in authentication; only those users carrying authorised items in proximity of certain places can benefit from available resources at those places. Unfortunately, items such as badges, mobile phones, smart phones, RFID-ed cards can be stolen, forgotten, or lost with a consequent risk of identity theft and intrusion. In controlled environment like buildings, where sensors can detect a wide range of different types of items, the security of authentication can be improved by evaluating the amount of trust that can be reposed on the user standing in the area from where he tries to access a resource. This piece of information can be calculated from the positions of all the items linkable to the requester as sensed along time by the different sensors available. Sensors are seen as recommenders that give opinions on a user being in a requested position depending on what they have perceived in the environment. We apply Subjective Logics to model recommendations that originate from different types of location detectors and to combine them into a trust value. Our solution has been tested to improve authentication in an intelligent coffee corner of our research institute. A user at the coffee corner can see, displayed on a wall screen, the position of his colleagues depending on the level of authentication he obtains. The user authentication level depends on the number and on the quality of tokens he provides when authenticating. We comment how the use of a location-based trust (on the requester standing at the coffee corner) improves the adaptability, the non-intrusiveness, and the security of the authentication process. We validate our proposal with a simulation that shows how location-based trust changes when a user device moves away from the coffee corner.

Keywords: Trust-enhanced Security, Adaptive Authentication, Sensor Fusing, Subjective Logic.

1 Introduction

In the domain of pervasive computing, users make use of their personal devices, for example smart phones, laptops, PDAs *etc*, to benefit from resources or services offered by the environment. The access is usually protected by access control mechanisms that demand users to show authorised credentials before granting a request

[1] Contact author: Gabriele.Lenzini@telin.nl

doi:10.1016/j.entcs.2007.12.020

of use. User credentials have the ultimate goal to authenticate the user, that is to convince the access control engine that the requester has the identity, the role, or the privileges [20, 19] that allows him to use (possibly with some limitation) the resource/service according to an authorisation policy.

Typical authentication solutions consider who a user is (e.g., biometric measurements), what a user knows (e.g., a password, a PIN) and, recently, also what the user has (e.g., badges, RFIDs, smart-phones, PDAs). In this latter case, the user's identity is derived from the detectable accredited items and personal devices the user carries when authenticating.

Particular attention is needed when security is asked to be adaptive and when privacy is asked to be preserved. Adaptivity requires flexible procedures of control being able to react to situational changes in a non-intrusive way. For example, a user trying (with his personal device) to access to a web-service offered by the railway company should be allowed to use the service when he is actually travelling on a train, but he must be deprived of the same rights as soon as he leaves the train [9]. Privacy targets contradict those of a secure authentication that requires revealing private information like a PIN or a credit card number. In fact, while service providers demand for users' personal data to protect their services from misuse, users want to avoid releasing personal information when not strictly necessary.

Indirect information about the user, such as *contextual* data, can be used to reach adaptability while reducing the frequency of the need of confidential information. By processing positional data, the resources available in a certain place can be accessed by users carrying accredited items in proximity of that place. Unfortunately, the analysis of multiple contextual data presents typical difficulties that arise from the management of multiple sources of context information [24]. Some source provides only partial pieces of information about the user (e.g., Bluetooth devices indicate where the device, not the user, is located); others are only partially unreliable (e.g., sensors have a certain probability of false positiveness). Sources can also be contradictory (e.g., the RFID sensor shows that the user is at the first floor, but the GPS indicates he is out of the building): because badges, mobile phones, smart phones, and RFID-ed cards can be stolen, forgotten, or lost, contradictions in the location of those devices may reveal an identity theft and an attempt of intrusion.

To enhance security in adaptive and non-intrusive authentication we propose to associate the authentication process with a *trust evaluation process*. Intuitively, by the analysis of the different kinds of location information related to a requester, we evaluate the trust that can be reposed on a statement about position of the requester. To evaluate the trustworthiness on a user position, we consider the different sources of location information as recommenders giving opinion on the statement "the user, whose identity emerges from the identity tokens provided, is standing in proximity of the place where the request is submitted". Recommendations are merged into a trust value. The (context-independent) authentication is therefore re-evaluated at the light of the trust emerging from the context. In case of low trustworthiness, the user can be asked to provide additional (context-related or context-independent) credentials. We design a theoretical framework based on

Subjective Logic [10,11] and we instantiate it in an intelligent coffee corner scenario we have set up in our research institute. Presently, a user approaching the coffee corner can see, on a wall-screen, the position of his colleagues. Which colleagues will appear on the screen depends upon the level of authentication the user obtains by the number and the quality of identity tokens provided when authenticating.

We propose to enhance the coffee corner's authentication with the use of location-based trust. Location-based trust on "the user standing at the coffee corner" is evaluated from the location of the different items belonging to the user and sensed in the environment. The access control engine can evaluate the trust information together with the level of (context-independent) authentication to decide upon the access. In a simulation, we show how the location-based trust changes when a detectable user device is brought near or moved away the coffee table. We cope with sensors that cover different area and that collect location information at different time frequencies.

Our proposal requires the support of an infrastructure where contextual information and digital identities (anonymous or not) are appropriately managed. We therefore make use of the infrastructure that has been developed in the Dutch Freeband project called AWARENESS [8], to which our study is strictly connected.

The outline of the paper is as follows: Section 2 discusses the idea of strengthening authentication by the use of contextual information and context-aware trust. Section 3 reminds the basics of Subjective Logic, whilst section 4 explains how to calculate trust given a set of location sources. Section 5 describes how to instantiate our framework into a realistic model of sensors. Section 6 comments the results of the simulation we did to validate our location-based trust algorithm. The related work is presented in Section 7 and Section 8 draws the conclusion and points out the future work.

2 Location-based Trust in Authentication

This section gives insight into our idea of using contextual data and location-based trust in the authentication process.

Since the first works about a trust approach to security, (e.g., [5,19,4]) we know that behind any request of access to a resource there is the provision of a set of credentials. The entity that guards the access to the resource validates whether the credentials conform with the local security policy before granting the request. In the pervasive domain that we are addressing, credentials are generally constituted by who the user is and what the user knows, namely biometric measurements and secrets. Because people carry personal devices, recent solutions accept also "what the user has" as a paradigm for identification.

At least at conceptual level, when a requester submits his request and credentials he also submits an *authentication statement*, p, which expresses a claim, for example, saying that the requester possesses certain qualities of which the set of credentials, C, constitutes or contributes to a proof of validity. Here we imagine the requester forwarding the pair (C, p) to the access control agent acting as an oracle: by the

analysis of C the agent checks or builds a proof (cf. [1,2]) for the validity of p and judges whether to allow access or not. Keeping this description as simple as possible, (i.e., without considering obligations and post-conditions [7]), the analysis of (C, p) returns a confidence value, L. If binary, L expresses either an authorisation or a denial; if multivalued, it relates to the level of confidence in the requester identity or role and then to the level of authentication granted. Without loss of generality, we assume that L ranges in the real interval $[0, 1]$. Here, $L = 0$ is the lowest value, meaning access denied, and $L = 1$ is the highest, meaning full access.

When $C = \{c_1, \ldots, c_n\}$ are multiple identity credentials (i.e., password, RFID, Bluetooth, *etc*) the confidence level L can be calculated as $1-(1-L_1)(1-L_2)\ldots(1-L_n)$ [17]. Here, each L_i expresses the measure of confidence in the user's identity that emerges from the analysis of c_i. Informally, sources with low confidence values decrease L, while sources with a high confidence values increase L. The relation above assumes that the credential items are independent, which makes sense if all of them are validated within a given common context. Moreover, L depends only on those credentials that are actually shown by the requester. Generally, however, the context in which each authentication method validates the corresponding credential is not the same for all methods. For example, the RFID attests the location of a user within a circle of 5 meters, while the Bluetooth does it within a circle of 10 meters; or the cells of RFID and of Bluetooth overlap partially with each other or with the area of interest at which the authentication process takes place. Such contextual differences at which various credentials are derived and validated should be taken into account in an advanced authentication framework. In this contribution we propose to model these contextual discrepancies as a measure of trust that applies to the process of merging the credential items. We present an authentication framework with such a trust management component.

Contextual information can be modelled in trust-based security according to what proposed in [15]. In that research, Krukow affirms that a model of security that includes trust management requires, besides the set C of signed credentials, an additional set I of not necessarily accredited information such as, for instance, recommendations. The set I is used to improve the authentication process. In our domain, we assume that I is related with "location" information of the items in C. For example, a mobile phone is both an identity credential (we can check if a mobile phone is Bob's, for example) and a source of location information (it links to the network cell where the mobile phone is detected). Then, I is used to build a set of recommendations about a security-related statement that concerns the position of the user. Recommendations are then merged into a measure of the trustworthiness of that statement. The statement p considered in this paper sounds informally as "the user, whose identity (or role) emerges from C, is standing at the location where the request has been forwarded". Our proposal to enhance the adaptability of security and privacy in authentication is built on the evaluation of a context-driven trust measure, $trust(p)$, in addition to the evaluation of the authentication confidence level L. The validity of p, i.e., the evaluation of L, is derived from intrinsic properties of C whilst the measurement of $trust(p)$ derives from the analysis

of contextual properties in I. Our proposal is conceived for controlled environments, like buildings, shop centres, cities, or generally well defined areas where I can be easily collected.

Example 2.1 Bob requests for a certain service from his registered WiFi-enabled laptop. He stands at a certain location l, so p informally expresses the statement that is Bob standing at location l. Bob also carries a Bluetooth-enabled smart phone, accredited to him, whose presence (thanks to a Bluetooth detector) is considered in the authentication process. An identification with a badge would have been preferred in this case, so the control access agent authenticate Bob at a confidence level 0.88. To the laptop corresponds an authentication level of 0.7, while the presence of a Bob's Bluetooth device determines a 0.6 level of confidence. The overall L is then $1 - 0.3 \times 0.4 = 0.88$. Bob is assumed in proximity of l, but contextual data indicates that Bob's badge has been sensed at the same time in a different location far from l: thus, $trust(p)$ is low. If the authentication process is adaptive, the access control engine can either it can take into account extra contextual information (e.g., other location sources) to enlighten about Bob standing at l, or ask for additional credentials (e.g., Bob's password).

We supports the use of context-aware trust as a back-end stage of a primary validation process, as studied in [22]. Therefore, once $trust(p)$ is evaluated, the overall and context-aware degree of access is $L \odot trust(p)$, where $\odot$ is an appropriate operator. For example, if we also assume that trust values range in the real interval $[0, 1]$ (where 0 means distrust and 1 complete trust) $\odot$ can be the real multiplication. In case of complete trust the authentication result is left untouched, otherwise it is de-amplified at the light of $trust(p)$.

In the following sections, we tailor our study to deal with user's location. We approximate p with $u \in l$ (we write $p(l)$) where u is the requester and l is the location from where the request originated. The basic idea standing behind the solution we are proposing can be applied, with some technical differences, to manage with generic contextual data and authentication statements.

3 Theoretical Background

This section reminds the basics of belief theory and the Subjective Logic. All the definitions reported here are taken from [11, 13].

Definition 3.1 [Frame of Discernment] A finite set Θ is called a *frame of discernment*, or simply a *frame*, when its elements are interpreted as possible answers to a certain question and when we know or belief that exactly one of these answers is correct. A *state* is an non-empty subset of elements in Θ.

A frame is an epistemic object; its elements are correct relative to our knowledge.

Definition 3.2 [Belief Mass Assignment] Given a frame of discernment Θ, a *belief mass assignment* is a function $m_\Theta : 2^\Theta \to [0, 1]$ such that for each subset $x \in 2^\Theta$, $m_\Theta(x) \leq 1$, $m_\Theta(\emptyset) = 0$, and $\sum_{x \in 2^\Theta} m_\Theta(x) = 1$. Here, 2^Θ is the power-set of Θ.

Given a state A, $m_\Theta(A)$ expresses the belief assigned to A. It does not express any belief in sub-states of A in particular. Given a belief mass assignment we can calculate an *opinion* on a state to be true.

Definition 3.3 [Opinion] Given a frame of discernment Θ and a belief mass assignment m_Θ, an *opinion* on a state $A \in 2^\Theta$ is a triple $(b(A), d(A), u(A))$ in $[0,1]^3$ such that $b(A) + d(A) + u(A) = 1$. An opinion expresses the belief, the disbelief, and the uncertainty about A to be true. It is calculated as follows (x ranges over 2^Θ):

$$b(A) = \sum_{x \subseteq A} m_\Theta(x) \qquad d(A) = \sum_{x \cap A = \emptyset} m_\Theta(x) \qquad u(A) = \sum_{x \cap A \neq \emptyset, x \not\subseteq A} m_\Theta(x)$$

From $(b(A), d(A), u(A))$ it is possible to calculate the *probability of expectation* of A being true, $E(A) = \sum_{x \subseteq 2^\Theta} m_\Theta(x) a(A/x)$. Here $a(A/x)$, called *relative atomicity* of A to x, stands for $|A \cap x|/|x|$, where $|A|$ is the cardinality of A.

We propose to use $E(\_)$ to be the context-aware function i.e., the *trust*$(\_)$ we introduced in Section 2. Before showing how to define a frame of discernment in our framework and how to assign a belief mass assignment on it, let us remind how opinions can be combined. The Subjective Logic theory provides many operators for combining opinions, but it requires opinions being built from a *binary frame*, i.e., a frame that contains only two atomic states, A and its complement $\neg A$. Given a (non-binary) frame, a binary frame can be build by "focusing" on a specific state.

Definition 3.4 [Frame with focus on A] Let Θ be a frame of discernment, m_Θ a belief mass assignment, and $(b(A), d(A), u(A))$ the belief, disbelief and uncertainty on a state $A \in 2^\Theta$. Then $\tilde{\Theta} = \{A, \neg A\}$ is the binary *frame with focus on* A whose $m_{\tilde{\Theta}}$ is defined as follows:$m_{\tilde{\Theta}}(A) = b(A)$, $m_{\tilde{\Theta}}(\neg A) = d(A)$, and $m_{\tilde{\Theta}}(\tilde{\Theta}) = u(A)$.

It can be proved that belief, disbelief, and uncertainty functions are identical in 2^Θ and $2^{\tilde{\Theta}}$. $a_{\tilde{\Theta}}(A)$ can be calculated consequently. In our framework we use the commutative and associative operator $\oplus$, called *Bayesian consensus*, used to "merge" opinions with the same focus. If $\omega_A^s = (b^s(A), d^s(A), u^s(A))$ and $\omega_A^{s'} = (b^{s'}(A), d^{s'}(A), u^{s'}(A))$ are two opinions on A in the subjective viewpoint of entities s and s', resp., and with relative atomicity $a^s(A)$ and $a^{s'}(A)$, resp., then the $\omega_A^s \oplus \omega_A^{s'}$ is the opinion $\omega_A^{[s,s']}$ of the imaginary entity $[s, s']$. The opinion $\omega_A^{[s,s']}$ reflects the opinions of s and s' both in a fair and equal way. It is calculated in the following way:

$$b^{[s,s']}(A) = (b^s(A)u^{s'}(A) + b^{s'}(A)u^s(A))/\kappa)$$
$$d^{[s,s']}(A) = (d^s(A)u^{s'}(A) + d^{s'}(A)u^s(A))/\kappa)$$
$$u^{[s,s']}(A) = (u^s(A)u^{s'}(A))/\kappa$$
$$a^{[s,s']}(A) = \frac{(a^{s'}(A)u^s(A) + a^s(A)u^{s'}(A) - (a^s(A) + a^{s'}(A))u^s(A)u^{s'}(A))}{u^s(A) + u^{s'}(A) - 2u^s(A)u^{s'}(A)}$$

Here $\kappa = u^s(A) + u^{s'}(A) - u^s(A)u^{s'}(A)$, and $a^{[s,s']}(A) = (a^s(A) + a^{s'}(A))/2$ when $u^s(A) = u^{s'}(A) = 1$. More operators of the Subjective Logic are described in [11].

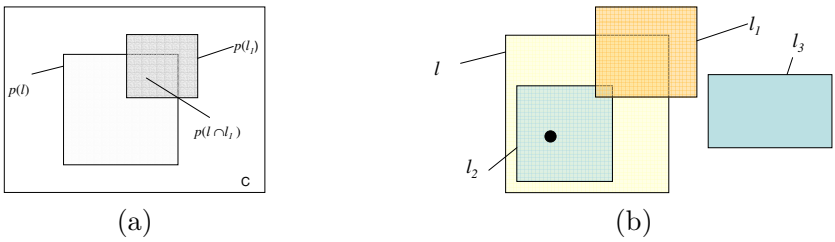


Fig. 1. (a) The frame we propose in our setting. (b) The situation referred by Example 4.1. The black spot indicates where the user's device is. l is the location where the user forwards his request. l_1, l_2, l_3 are the locations controlled by sensors s_1, s_2 and s_3 respectively.

4 How to Calculate the Location-based Trust

This section discusses how to calculate $trust(p(l))$ i.e., the location-based trust in the user staying in location l, the place from where the user forwards its authentication request.

We indicate with $\mathcal{L}$ the space of all locations. The portions of $\mathcal{L}$ where user devices can be detected are called *cells*. Because each device is also an identification item for the user, with a little abuse of terminology, we talk about user's device position and user position interchangeably. We let l, $l_1, l_2 \ldots$ range over the set of all possible cells. We assume a set $\{s_1, \ldots, s_n\}$ of independent location sensor sources; each s_i is responsible for the coverage of the correspondent cell l_i. Cells $l_1, \ldots, l_k$ are not necessarily disjoint. The exact location of a user device within a cell is unknown; it can occupy any position inside the cell with the same probability. Sensors are also subjected both to false positive and false negative errors, so when they trigger (resp., they do not trigger) the presence (resp., absence) of the user in their cell is known only with a certain probability.When the sensor s_i detects the presence of the user's device (written $s_i = 1$) we know that the user u stays within cell l_i (i.e., $u \in l_i$) with probability $P(u \in l_i \,|\, s_i = 1)$. Because each s_i is expected to scan its cell at known intervals of time, it is also known if a sensor has not triggered (written $s_i = 0$). If it is the case, we know that the user stays outside the cell l_i (i.e., $u \notin l_i$) with a probability $P(u \notin l_i \,|\, s_i = 0)$.

We associate a frame $\Theta_i = \{p(l_i \cap l), p(l_i \setminus l), p(l \setminus l_i), p(\mathcal{L} \setminus (l_i \cup l))\}$ to each sensors s_i. The frame Θ_i contains the (mutually disjoint) propositions about the location of the user with respect to the zones that are intercepted, in $\mathcal{L}$, by cell l_i and l (cf. Figure 1 (a)). We associate the belief masses to Θ_i depending whether the sensor has triggered or has not. In the following definitions we give the specification of the

belief mass m_{Θ_i} in the two cases, written $m_{\Theta_i}^{s_i=1}(x)$ and $m_{\Theta_i}^{s_i=0}(x)$, respectively:

$$m_{\Theta_i}^{s_i=1}(x)=\begin{cases} P(u \in l_i \,|\, s_i = 1), \\ \text{if } x = \{p(l_i \backslash l), p(l_i \cap l)\} \\ 1 - P(u \in l_i \,|\, s_i = 1), \\ \text{if } x = \{p(l \backslash l_i), p(\mathcal{L} \backslash (l_i \cup l))\} \\ 0, \quad \text{otherwise} \end{cases} \qquad m_{\Theta_i}^{s_i=0}(x)=\begin{cases} 1 - P(u \notin l_i \,|\, s_i = 0), \\ \text{if } x = \{p(l_i \backslash l), p(l_i \cap l)\} \\ P(u \notin l_i \,|\, s_i = 0), \\ \text{if } x = \{p(l \backslash l_i), p(\mathcal{L} \backslash (l_i \cup l))\} \\ 0, \quad \text{otherwise} \end{cases}$$

We now calculate the trust that a sensor s_i has in the proposition $p(l)$ by applying Definition 3.3. Once assigned the belief, disbelief and uncertainty we build a binary frame $\tilde{\Theta}_i = \{p(l), \neg p(l)\}$ *with focus on* $p(l)$, whose belief mass is set according to Definition 3.4, that is $m_{\tilde{\Theta}_i}(p(l)) = b(p(l))$, $m_{\tilde{\Theta}_i}(\neg p(l)) = d(p(l))$, and $m_{\tilde{\Theta}_i}(\tilde{\Theta}_i) = u(p(l))$. Then, we calculate $\omega_{u \in l}^{s_i}$ for each sensor s_i. The overall trust is the Bayesian consensus among the sensors opinions, that is $\omega_{u \in l} = \oplus_i(\omega_{u \in l}^{s_i})$.

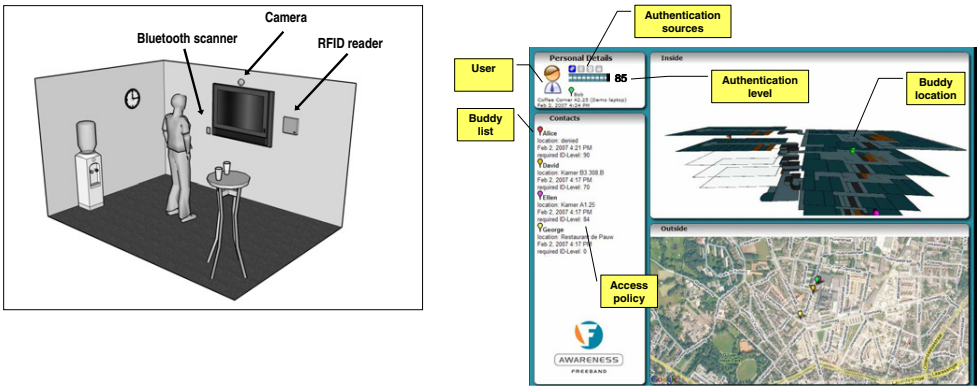
Example 4.1 Let assume $\{l, l_1, l_2, l_3\}$, and three sensor sources s_1, s_2, and s_3 controlling the respective cells. The geometrical characteristic of the cells are as in Figure 1 (b). Associated with our area of reference, $\mathcal{L}$ (a square including all the cell, omitted in Figure) we have the following three different frames of discernment: $\Theta_i = \{p(l \setminus l_i), p(l_i \setminus l), p(l \cap l_i), p(\mathcal{L} \setminus (l \cup l_i))\}$ for $i = 1, 2, 3$. We assume to have $P(u \in l_1 \mid s_1 = 1) = 0.99$, $P(u \in l_2 \mid s_2 = 1) = 0.97$, and $P(u \notin l_3 \mid s_3 = 0) = 0.96$. These probabilities are used to define the belief mass assignment, as explained in the text. If a device is located in l_2 as indicated by the black spot in Figure 1(b) the sensors' opinions about the device being in l are, resp., $\omega_{u \in l}^{s_1} = (0.0, 0.0, 1.0)$ with $a^{s_1}(u \in l) = 0.75$, $\omega_{u \in l}^{s_2} = (0.0, 0.0, 1.0)$ with $a^{s_2}(u \in l) = 0.98$, and $\omega_{u \in l}^{s_3} = (0.0, 0.0, 1.0)$ with $a^{s_3}(u \in l) = 0.75$. The consensus opinion is $\omega_{u \in l}^{s_1:s_2:s_3} = (0.0, 0.0, 1.0)$ with $a = 0.78$ and the probability of expectation of belief, i.e., our *trust*$(p(l))$, is 0.78.

5 Instance of our framework

This section explains how our framework can be realised in a realistic sensors network.

In section 4 we have assumed being able to calculate $P(u \in l_i \mid s_i = 1)$ and $P(u \notin l_i \,|\, s_i = 0)$ for all i. Indeed, most product specifications of location sensors give the conditional probability that the device is correctly detected when and where it is present in its cell, that is $P(s_i = 1 \,|\, u \in l_i) = q_i$. The probability of the complement event i.e., $P(s_i = 0 \,|\, u \in l_i) = 1 - q_i$ is called false negative probability. In addition, location technologies provide the probability of a misidentification, that is the false positive probability $P(s_i = 1 \,|\, u \notin l_i) = p_i$. Thus $P(s_i = 0 \,|\, u \notin l_i) = 1 - p_i$. We work under the following assumption:

Assumption 1 *Sensors are conditionally independent, that is,* $\forall j, i$ $P(s_i = 1 \mid u \in l_i) = P(s_i = 1 \,|\, u \in l_i, s_j = 1)$ *and* $P(s_i = 1 \,|\, u \notin l_i) = P(s_i = 1 \,|\, u \notin l_i, s_j = 1)$.



(a) (b)

Fig. 2. (a) The intelligent coffee corner scenario. Different sensors accept different identity tokens to authenticate user. (b) A screen-shot from the screen of the coffee corner scenario. Depending on the authentication level of the user, the position of of a list of colleagues of his is displayed on the screen. The authentication level is driven by the number of identity tokens that are shown at the coffee corner

Assumption 1 says that the position of a user device inside or outside a sensor's cell determines the behaviour of the sensor. Concerning this behaviour, each sensor is independent on whether or not the other sensors of different types are triggered.

Lemma 5.1 *Under Assumption 1 we have* $P(u \in l_i \,|\, s_i = 1) = \frac{q_i P(u \in l_i)}{P(u \in l_i)(q_i - p_i) + p_i}$ *and* $P(u \notin l_i \,|\, s_i = 0) = \frac{(1-p_i)P(u \notin l_i)}{P(u \in l_i)(p_i - q_i) + (1-p_i)}$

Proof. It follows form the Bayesian theorem. □

Under the maximum entropy approach [3], the distribution of users in the grid is uniform and $P(u \in l_i) = \frac{|l_i|}{|\mathcal{L}|}$ and $P(u \notin l_i) = 1 - \frac{|l_i|}{|\mathcal{L}|}$. Thus, the expressions in Lemma 5.1 become $P(u \in l_i \mid s_i = 1) = \frac{q_i |l_i|}{|l_i|(q_i - p_i) + p_i |\mathcal{L}|}$ and $P(u \notin l_i \mid s_i = 0) = \frac{(1-p_i)(|\mathcal{L}| - |l_i|)}{|l_i|(p_i - q_i) + (1-p_i)|\mathcal{L}|}$.

6 Validation and experimental results

This section describes and comments the simulation that validates our theoretical framework.

The simulation refers to an intelligent coffee corner that has been arranged in our research institute (Figure 2 (a)). A user approaching the coffee corner identifies himself by showing different identity tokens, in fact, mobile items that are RFID, Bluetooth, GPS, WiFi enabled. On a wall screen he can see the position of his colleagues (see Figure 2 (b)), but this information is available only if the colleagues have expressed, in terms of a policy, their approval be watched by that user. They also request that their position is visible only if the identification level of that user is above a certain value. We assume that the user identifies himself at the coffee corner and that he obtains an authentication level L. This is what our coffee corner is actually doing at the present implementation. The simulation shows how trust

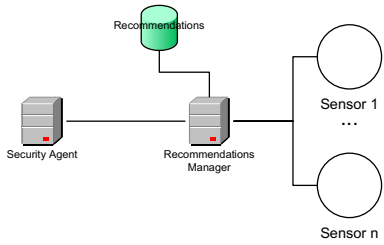


Fig. 3. The architecture of our trust-enhanced authentication solution. The security agent, i.e., the access control engine, is supported by a recommendations manager that collects sensors data and recommendations on security agent request.

changes when a user's device moves away from the coffee corner. A number of sensors for that device are disposed in the environment as in Figure 4. They scan their cells at different time rate so in the simulation we extend our theoretical framework to cope with sensors whose outputs change with time.

We calculate $trust(p(l))$ depending on the position of the user's mobile device. Here l is the coffee corner location. Thus, the overall context-aware authentication level, $L \odot trust(p(l))$, is studied indirectly by following the trend of $trust(p(l))$.

Figure 3 depicts the three essential elements of our model of trust-enhanced authentication architecture, which consists of the following subjects: a security agent, a recommendations manager, and the set of sensors $\{s_1, \ldots, s_n\}$. The security agent evaluates the authentication level considering the credentials (cf. Section 2) shown at the request. The recommendations manager collects opinions from the sensors and calculates $trust(p(l))$. For keeping the explanation easier, we assume a centralised implementation of the recommendations manager (a distributed implementation is also possible). For the same reason, all the sensors detect the same type of mobile token, let say Bluetooth enable-devices. Our simulation uses a discrete and linear time structure. The recommendations manager knows the sensors' technical features, namely their false positive and false negative parameters, and the geometry of the cells they control. It also knows the sensors' scanning time rate, k_i. Thus, a sensor scans l_i every $n \cdot k_i$ intervals of time, with n ranging over naturals. For example, a sensor with scanning rate $k = 5$ scans its cell at time $0, 5, 10$ and so forth. With $s_i(nk_i) = 1$ (resp., $s_i(nk_i) = 0$) we indicate that s_i has detected (resp. has not detected) the user's device in l_i at time interval $t = nk_i$. By collecting the sensors' outputs along time, the recommendations manager has a complete knowledge of what happens in $\mathcal{L}$.

Let assume, for a moment, that all the sensors have a unit scanning rate (i.e., $\forall i, k_i = 1$). At a certain time t, when the security agent demands for the evaluation of $trust(p(l))$, the recommendations manager checks the data it has received from the sensors, calculates their opinions $\omega^{s_i}_{u \in l}(t)$ knowing what s_i has detected at time t, and composes the overall trust as described in Section 4 and Section 5.

What does it happen when we release the assumption that all the sensors have the same unit scanning rate? It may happen that $s_i(t) = \perp$ where $\perp$ means that the sensor input is undefined. It has not performed any scan at time t and no data, for that time, are available to the manager. For what has been said so far, the recommendations manager is able to calculate $\omega^{s_i}_{u \in l}(t)$ for a sensor s_i only if it has

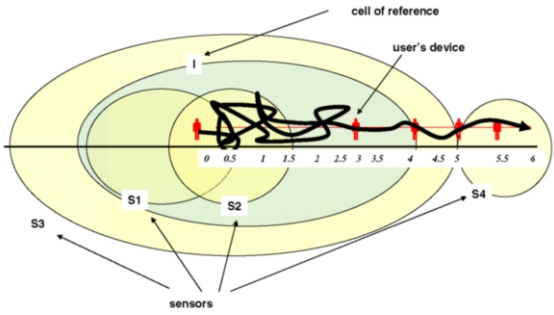


Fig. 4. How the user device moves in our simulation. First, the device is close to location l, then it moves away as intuitively depicted by the bold line. The unit of movement is 0.5. The exact device's movement is given by the following vector of positions: [0; 0; 0; 0.5; 0.5; 0.5; 1; 1; 0.5; 0.5; 0.5; 1; 1; 1.5; 1.5; 2; 2; 2.5; 2.5; 2; 2; 1.5; 1.5; 1; 1; 1; 1.5; 1.5; 2; 2; 2.5; 2.5; 3; 3; 3.5; 3.5; 4; 4; 4.5; 4.5; 5; 5; 5.5; 5.5; 6]. For all i, $q_i = P(u \in l_i \mid s_i = 1) = 0.99$ and $p = P(u \notin l_i \mid s_i = 0) = 0.01$. The scanning rates of the sensors are: $k_2 = k_4 = 2$, $k_1 = 1$, and $k_3 = 5$ unit of time.

a fresh datum from it.

In the simulation we estimate $\omega^{s_i}_{u\in l}(t)$ from $s_i(t')$, where t' is the $\max\{nk_i : nk_i < t, s_i(nk_i) \neq \perp\}$ i.e., the latest interval of time where a datum is received from the sensor. Thus, $\omega^{s_i}_{u\in l}(t)$ is the opinion that emerges by considering an augmented cell $l_i(t) = l_i + \delta_i(t - nk_i)$, where $\delta_i(t - nk_i)$ is the additional space that the device detectable by s_i (and linked to the user) might have run in the while. Generally speaking, the calculation of $\delta_i(t - nk_i)$ depends upon the following factors: (1) the value of $s_i(t')$ (i.e., the information the sensor has detected the last time) and (2) the structure of $\mathcal{L}$ (i.e., its walls, the disposition of corridors, entrances, exits etc., and how users move into it).

The dependence from (1) has a conceptual motivation. If $s_i(nk_i) = 1$ this means that at time nk_i there was evidence that the user was in l_i. If the user has moved, he will be probably in $l_i + \delta_i(t - nk_i)$. To approximate $\omega^{s_i}_{u\in l}(t)$ we reshape the frame by considering the new cell $l_i + \delta_i(t - nk_i)$. Anyhow, when assigning the belief mass to this new frame of discernment, we use $P(u \in l_i \mid s_i = 1)$ (*vs.* $P(u \in l_i + \delta_i(t - nk_i) \mid s_i = 1)$). Accordingly to the Subjective Logic theory, because there are no new evidences (but only deductions) there is no justification for incrementing the belief. We use the previous amount of belief but "spread" over a larger area. If $s_i(nk_i) = 0$, instead, this means that the sensor had evidence at time nk_i that the user was not in l_i (if the user is somewhere in $\mathcal{L}$, then the sensor had evidence that $u \in \mathcal{L} \setminus l_i$). In this case there is no justification in using an augmented cell, and $\delta_i(t - nk_i) = 0$. Indeed, we could consider a negative $\delta_i(t - nk_i)$, which means to assume that the user has moved within l_i, but it is unsecure to deduce in favour of the user being close to the authentication location if no clear evidence supports it. Then $\delta_i(t - nk_i) = 0$ is a conservative and secure attitude.

The dependence from (2) requires a knowledge of $\mathcal{L}$ and a model of movement of users in it. $\delta_i(x)$ is then defined accordingly to that specific movement model. In our simulation, we adopted a very simple solution: the user moves everywhere with equal probability. Thus, when $\delta_i(t - nk_i) \neq 0$ because of (1), $l_i + \delta_i(t - nk_i)$ is a

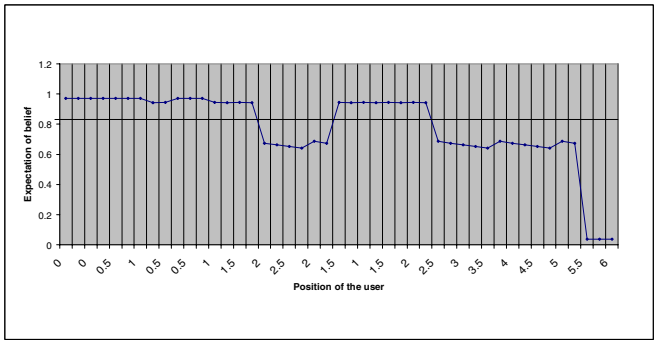


Fig. 5. Graphic showing the change in $trust(p(l))$ in our simulation. The movement of the device is described in Figure 4.

cell c_i' with a larger radius than l_i. In our simulation we set a radius's increment of 10% of $t - nk_i$.

Figure 5 reports the values we obtained for $trust(p(l))$ when the device moves from l as explain in Figure 4. Looking at Figure 5, it is evident how trust stays high when the device in within l; the three opinions converge on the belief that user is in l. Trust starts decreasing as the device moves away from l. Interesting are the little peaks in position, 2, 4 and 5. They are due to fresh data while the conservative estimation of trust from the manager was decreasing trust. Finally, trust drops down when the device comes into the range of sensor s_4, and evidences against the user being in l are communicated to the manager.

7 Related Work

The problem of distributed authentication has been widely studied for long time (cf. [2]). To survey the efforts and the contributions in this area would be too ambitious. Our work addresses the authentication procedures and methods only in suggesting the use of context and context-based trust as a subsidiary information to improve the result from traditional authentication process.

From this point of view, Bhatti *et al.* [18] have already underlined the importance of contextual information in access control and designed an access control scheme –an extension of their XML Role Based Access Control (X-RBAC) framework– to incorporate trust domains and (temporal and non-temporal) contextual condition into access control policies. Montanari *et al.* [16] recognised context as an important factor in guiding both policy specification and enforcement in the specification of dynamic and adaptable security policies in ubiquitous environments (see also [23]). Our work does not focus on policy specification and enforcement based on context information, but instead it underlines the importance of contextual information as a mean for trustworthiness evaluation. Moreover, we address the theories of belief as a mean to cope with contextual information.

Bohn and Vogt discuss a probabilistic sensor fusion algorithm to predict an user's

position within a building [6]. The fusion algorithm runs over a map of the building, which constitutes the grid over which probabilities are combined and updated along time. This work describes a complementary approach to ours. We think that an approach based on belief theory is more appropriate than one based probability theory for developing a general-purpose sensor fusion algorithm. In fact, our proposal is easily scalable with the number of sensors and, although our approach is instantiated with location based information, it can easily be be extended towards other context types.

The use of belief theories in sensor fusing has been studied by Wu *et al.*, who used Dempster-Shafer Belief theory to fuse data coming from independent sensors monitoring a user's focus of attention during a round-table meeting [25, 24]. Subjective Logic has been used by Svesson and Jøsang in intrusion detection to fuse alerts coming from multiple detectors [21]. Alerts on different anomalies are "conjuncted" to calculate the belief if an attack, which is based on those anomalies, is occurred. Alerts coming from not completely trusted sensors are discounted before being processed. Subjective Logic has been also proposed and applied in a variety of application domains concerning trust (cf. [10, 12]). The benefits of using Subjective Logic with respect the Dempster's Rule in sensor fusion are studied in [14]. Our work confirms the flexibility and applicability of Subjective Logic where the need of algebraically combining trust values is critical. To our knowledge, we are the first in applying Subjective Logic in the domain of context-aware trust combined with traditional authentication methods.

8 Conclusion and Future Work

The amount of trust in an authentication procedure guarding the access to services offered in a pervasive and controlled environment like a building, depends not only on the strength of the procedure but also on the context in which the authentication takes place. For example, when the authentication accepts as identification tokens "what the user has", identity tokens lost, stolen, or forgotten can be used by someone else to impersonate maliciously the user's identity. We proposed and described an evaluation method for enhancing the authentication procedure by the use of contextual information, like location. Whilst the authentication procedure determines the level of authentication considering the quality and number of the identification items shown by a user at the moment of the request, the trustworthiness of the authentication combines the location of the multiple user-associated identity tokens that are detected by means of a sensor network.

We use Subjective Logic to assign a trust value to the statement "the user, whose identity emerges from the identity tokens provided, is standing at the location where the request has been forwarded". The trust value is then combined with the (context-independent) authentication status of that user into a new (context-aware) authentication status. The use of trust also allows less intrusive and more private solutions for authentication: user's confidential credentials, like a PIN, can be asked only in case of low trustworthiness on his position. Moreover, the context-dependent

authentication status of the user can be used for optimising the security adaptation of the access control process.

Because our simulations confirm the theoretical expectation on the trend of trust, we are currently implementing our algorithm in a office application that allows the user to view, on a wall screen, the location of his buddy colleagues depending on his authentication level. The authentication procedure we have now is based on the recognition of personal devices assumed to belong to the user (i.e., PDA, badge, laptop, Bluetooth devices, RFID). Here, we want to avoid unauthorised use of the service, for example by someone else using a badge of that user, or sitting at his desk, while the user is temporarily away.

Furthermore, there is a desire to extend our study towards solutions for the establishment of contextual-trust maintenance. For this purpose we are going to clarify how contextual information can concur to the management of the context-aware trustworthiness of a certain trustee, and how contextual information affects the traditional trust establishment and management process.

Acknowledgement

This research has been supported by the Dutch Freeband Communication Research Program (AWARENESS project) under contract BSIK 03025.

References

[1] Appel, A. W. and E. W. Felten, *Proof-carrying authentication*, in: *Proc. of the 6th ACM conference on Computer and communications security (CCS'99), 1-4 November 1999, Singapore* (1999), pp. 52–62.

[2] B. W. Lampson, M. B., M. Abadi and E. Wobber, *Authentication in distributed systems: Theory and practise*, ACM Transaction on Computer Systems **4** (1992), pp. 265–310.

[3] Berger, A. L., S. D. Pietra and V. J. D. Pietra, *A maximum entropy approach to natural language processing*, Computational Linguistics **22** (1996), pp. 39–71.

[4] Blaze, M., J. Feigenbaum and A. D. Keromytis, *Keynote: Trust management for public-key infrastructures (position paper)*, in: B. Christianson, B.Crispo, W. S. Harbison and M. Roe, editors, *Proc. of the 6th International Security Protocols Workshop, Cambridge, UK, April 15-17, 1998*, LNCS **1550** (1999), pp. 59–63.

[5] Blaze, M., J. Feigenbaum and J. Lacy, *Decentralized trust management*, in: *Proc. of the 1996 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 6-8 May 1996* (1996), pp. 164–173.

[6] Bohn, J. and H. Vogt, *Robust probabilistic positioning based on high-level sensor-fusion and map knowledge*, Technical Report 421, Institute for Pervasive Computing, Dept. of Computer Science, ETH Zurich, Switzerland (2003).

[7] Cederquist, J. G., R. Corin, M. A. C. Dekker, S. Etalle, J. I. den Hartog and G. Lenzini, *Audit-based compliance control*, International Journal of Information Security, Special Issue Paper **6** (2007), pp. 133–151.

[8] http://www.freeband.nl.

[9] Hulsebosch, R. J., A. H. Salden, M. S. Bargh, P. W. G. Ebben and J. Reitsma, *Context sensitive access control*, in: E. Ferrari and G.-J. Ahn, editors, *Proc. of the 10th ACM symposium on Access control models and technologies (SACMAT05), 1-3 June, 2005, Stockholm, Sweden* (2005), pp. 111–119.

[10] Jøsang, A., *A subjective metric of authentication*, in: J.-J. Quisquater, Y. Deswarte, C. Meadows and D. Gollmann, editors, *Proc. of the 5th European European Symposium on Research in Computer Security (ESORICS 98), Louvain-la-Neuve, Belgium, September 16-18, 1998, Proceedings*, LNCS **1485** (1998), pp. 329–344.

[11] Jøsang, A., *A logic for uncertain probabilities*, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **9** (2001), pp. 279–312.

[12] Jøsang, A., R. Hayward and S. Pope, *Trust network analysis with subjective logic*, in: *Proc. of the 29th Australasian Computer Science Conference (ACSC 2006), January 16–19, 2006, Australia*, ACM International Conference Proceeding Series **48** (2006), pp. 85–94.

[13] Jøsang, A. and S. Pope, *Semantic constraints for trust transitivity*, in: S. Hartmann and M. Stumptner, editors, *Proc. of the 2nd Asia-Pacific Conference on Conceptual Modelling (APCCM2005), Newcastle Australia, 30 January - 4 February 2005*, CRPIT **43** (2005), pp. 59–68.

[14] Jøsang, A., S. Pope, J. Diaz and B. Bouchon-Meunier, *Dempster's rule as seen by little coloured balls* (2005), manuscript, submitted to Information Fusion Journal.

[15] Krukow, K., "Towards a Theory of Trust for the Global Ubiquitous Computer," Ph.D. thesis, Dep. of Computer Science, Univ. of Aarhus, Denmark (2006).

[16] Montanari, R., A. Toninelli and J. M. Bradshaw, *Context-based security management for multi-agent systems*, in: *Proc. of the 2nd IEEE Symposium on Multi-Agent Security and Survivability (MAS&S 2005), Philadelphia, USA, Aug. 30-31* (2005), pp. 75–84.

[17] Ranganathan, A., J. Al-Muhtadi and R. Campbell, *Reasoning about uncertain contexts in pervasive computing environment*, IEEE Pervasive Computing **3** (2004), pp. 62–70.

[18] R.Bhatti, E. Bertino and A. Ghafoor, *A trust-based context-aware access control model for web-services*, Distributed and Parallel Databases **18** (2005), pp. 83–105.

[19] Sandhu, R. S., E. J. Coyne, H. L. Feinstein and C. E. Youman, *Role-based access control models*, IEEE Computer **29** (1996).

[20] Sandhu, R. S. and P. Samarati, *Access control: principles and practise*, IEEE Communications Magazine **9** (1994).

[21] Svensson, H. and A. Jøsang, *Correlation of Intrusion Alarms with Subjective Logic*, Technical Report IMM-TR-2001-14, Informatics and Mathematical Modelling, Technical University of Denmark, DTU (2001).

[22] Toivonen, S., G. Lenzini and I. Uusitalo, *Context-aware trust evaluation functions for dynamic reconfigurable systems*, in: *Proc. of the Models of Trust for the Web workshop (MTW'06), held with the 15th International World Wide Web Conference (WWW2006) May 22, 2006, Edinburgh, Scotland*, CEUR Workshop Proceedings (2006).

[23] Toninelli, A., R. Montanari, L. Kagal and O. Lassila, *A semantic context-aware access control framework for secure collaborations in pervasive computing environments*, in: *Proc. of the Fifth International Semantic Web Conference (ISWC), Athens, GA, Nov. 5-9 2006*, LNCS **4273**, Springer-Verlag, 2006 pp. 473–486.

[24] Wu, H., M. Siegel and S. Ablay, *Sensor Fusion using Dempster-Shafer Theory ii: Static Weighting and Kalman Filter-like Dynamic Weighting*, in: *Proc. of 20th IEEE Instrumentation and Measurement Technology Conference (IMTC 2003), 20-22 May, 2003, Vail, CO, USA* (2003), pp. 907–912.

[25] Wu, H., M. Siegel, R. Stiefelhagen and J. Yang, *Sensor fusion using dempster-shafer theory*, in: *Proc. of the 19th IEEE Instrumentation and Measurement Technology Conference (IMTC 2002), 21-23 May 2002, AK, USA* (2002), pp. 7–12.