Context Sensitive Adaptive Authentication

R.J. Hulsebosch[1], M.S. Bargh[1], G. Lenzini[1], P.W.G. Ebben[1], and S.M. Iacob[2]

[1] Telematica Instituut, PO Box 589, 7500 AN, Enschede, The Netherlands
{Bob.Hulsebosch, Mortaza.Bargh, Gabriele.Lenzini, Peter.Ebben}@telin.nl
[2] Decis Lab, PO Box 90, 2600 AB, Delft, The Netherlands
Sorin.iacob@icis.decis.nl

Abstract. We exploit the ability to sense and use context information to augment or replace the traditional static security measures by making them more adaptable to a given context and thereby less intrusive. We demonstrate that by fusing location information obtained from various sources that are associated to the user and are available over time, the confidence in the identity of the user can be increased considerably. In fact, the level of confidence in the identity of the user is related to the probability that the user is at a certain location. This probability is used as a measure to parameterize the authentication level of the user making it thereby much more adaptive to changing situational circumstances. In this paper we describe the theoretical background for a context-sensitive adaptation of authentication and the design and validation of the system that we have developed to adaptively authenticate a user on the basis of the location of his sensed identity tokens.

Keywords: Authentication; context awareness; adaptive; probability.

1 Introduction

In traditional security systems, security services are pre-configured to a static behavior and cannot be adapted dynamically to new constraints. This limitation is due to two main shortcomings: the adoption of non-adaptive behavior and the inability of considering context information.

To address the first shortcoming, i.e. non-adaptive behavior, security services must be flexible and able to cope with different situations. Adaptive security mechanisms (e.g., [1], [2]) are able to dynamically respond to environmental changes by re-configuring their security functions. Moreover, they support the idea that security can be more effective if variable levels of security are presented to users and to systems. For each security level a certain threshold must be fulfilled, which may be absolute or statistical; thresholds indicate degrees of security with respect to assurance, availability, execution efficiency, etc. Adaptive security solutions are known to ensure a high level of usability (e.g., they avoid absolute identity verification), realism (e.g., their access control mechanisms are fine-grained), sensibility to external constraints (e.g., power limitations may influence the choice of encryption algorithm), and ability to deal with exceptional situations (e.g., emergencies are treated differently).

G. Kortuem et al. (Eds.): EuroSSC 2007, LNCS 4793, pp. 93–109, 2007.

One means of ensuring security adaptation is parameterization [3], [4], [5], [6]. Parameterization of security implies the ability of identifying levels of security. For instance, for each security service such as authentication, authorization, confidentiality, and integrity, levels of security are expressed. Moreover, one should also be able to compute a value corresponding to a security level, i.e. the performance of the security function should be made measurable. Parameterization is one approach to making security adaptive. Another approach would be to adapt the security level by means of structural changes of the system. Being the simplest method, we focus on parameterized adaptation of security services and in particular authentication.

Regarding the second shortcoming, i.e., the inability of considering contextual information, security services require a context-aware infrastructure for the detection and interpretation of context information in order to allow for a controlled security adaptation when needed [7]. Context information can include any sort of data such as human factors (user habits, mental state, social environment, task-related activities), the physical environment (location, network connectivity, battery power), business data (goal-directed activities, trust), and time. What context information is relevant for a certain situation is not fully predictable and depends on the specific application. A security context can be defined as the information collected from the user and his application environment that is relevant to the security infrastructure of both the user and the application [8]. Context information thus forms, besides the traditional security services, an additional important element of the security context. An illustrative example is the use of location and velocity information to infer that a user is a train traveler and therefore is granted access to services offered in the train [9].

In this paper, we propose to combine parameterization and context-awareness to control security adaptation. We call this paradigm *context-sensitive adaptive security*. Its goal is to optimize the security functionality for a given situational context in a non-intrusive way. In fact, we can imagine a system that, by constantly monitoring and analyzing context information, is able to maintain the desired security level and to respond to new security constraints that may arise from changes in the situational context. We believe that systems can achieve a higher trustworthiness, security, usability, and flexibility by adding the ability to automatically adapt their security functionality depending on changes in the situational context.

To support and evaluate this idea, we have set-up an authentication experiment where different sources of location information contribute to evaluating the degree of authentication of a user. In fact, we have devised and prototypically implemented a location-aware component that combines user identity tokens with location information extracted from an arbitrary set of sensors. Different sensed identity tokens (e.g., RFID badge or Bluetooth-enabled mobile phone) are associated to location information and are fused to calculate the probability that the user is at a certain location. This probability is used by an application to determine the user's authentication level: the lower the probability, the lower the authentication level. We show that by fusing various sources of location information that are available over time, the confidence in the identity of the user can be effectively evaluated.

The structure of the paper is as follows. Section 2 introduces and discusses the security features of context-sensitive adaptive authentication. Section 3 discusses the sensor fusing probability algorithm that serves our goal and also provides several simulation results to illustrate and validate the behavior of the algorithm. Section 4

describes the design of our system to support context sensitive adaptive authentication. This is explained by means of an application scenario that we have implemented. Section 5 discusses several essential features of our system. Section 6 compares our approach with related work in the field. Finally, Section 7 presents the conclusions of our work and future outlook.

2 Authentication with Context

In computer security, authentication is the process of attempting to verify the digital identity of the user. In a ubiquitous context-aware computing environment, users can authenticate themselves using a variety of means with a variable degree of reliability. User authentication means can be classified into the following three classes:

1. *what the user is* (e.g., fingerprint or other unique biometric identifiers);
2. *what the user has* (e.g., ID card, security token, or cell phone);
3. *what the user knows* (e.g., a password, a pass phrase or a PIN).

Most of today's widely available authentication solutions can not guarantee very high quality user identification. For instance, if a user enters the right username/password combination, there is still a certain amount of uncertainty on whether we are really dealing with this user; the combination could have been eavesdropped. Even the use of biometric identification solutions is not 100% accurate; there is always a chance for a false positive or negative. Clearly, the assumption that a user's identity can be verified with absolute certainty is unrealistic in most of the scenarios, but the confidence on the user's identity can increase with the adoption of clever strategies. Generally, the combination of methods such as a bankcard and a PIN (called "two-factor authentication") or the username/password authentication solution with the biometric identification, results in a more reliable user identification. Potentially, the more solutions that can be used to authenticate the user, the stronger the system's confidence in that user's identity will be.

Formally, if A_1, A_2, …, A_n, are the confidence values associated with different authentication methods (e.g., RFID, username/password, Bluetooth, biometrics) then, under the assumption that all authentication methods have yielded a positive outcome, the overall confidence OC associated with the composite authentication solution may, using e.g. probability theory, be calculated with the following formula [10]:

$$OC = 1 - (1 - A_1)(1 - A_2)....(1 - A_n) \quad (1)$$

Here, A_i's are authentication values in the real interval [0, 1], where 1 expresses the highest confidence, and 0 the lowest. Informally, Eq. (1) says that sources with low confidence have a weak impact, while sources with a high confidence bring to a higher OC. For example, if the authentication confidence of an RFID badge is A_{RFID} = 0.80 and that of a Bluetooth (BT) device is A_{BT} = 0.60, the resulting OC is 0.92.

Although Eq. (1) represents a significant improvement with respect to single source authentication, the use of combined identification sources is always reliable as well. For example, what if the RFID badge and the BT device of the same user are almost simultaneously used at two completely different locations? In addition, what if the time interval between two different authentication sources of the same user is

long? Moreover, we also note that the determination of meaningful authentication confidence values for each authentication technique (i.e., the values $A_1,\ldots,A_n$) proves difficult and is strongly application specific [11]. As a solution, we propose to look at the context of the authentication process, specifically, location and time. In our vision, location and time constitute the fourth authentication class, namely "*where the user is, and when*". Thus, in addition to combined identification inputs, the use of sensor information allows the system to reason about the belief in the composite information to come to a higher authentication status.

User authentication information derived from sensors in the environment can result in a significant enhancement of the confidence strength of the identification service. For instance, if a RFID reader at the entrance of the building has identified a user via his RFID badge, and at the same time, a BT dongle at the third floor of the building has identified the BT-enabled Personal Device Assistant (PDA) of the same user, granting the user access to confidential files via his PDA should be restricted. This restriction arises from the contradictory location information of the two identification measures and it results into a lower accuracy of the user identification and therefore into a lower authentication level. On the contrary, if the locations match, the confidence in the identity of the user should be higher. In other words, the overall confidence in the identity of the user is also influenced by the location and time associated with the respective RFID and BT identifiers.

In this paper, we approximate the authentication confidence with the probability of the user being at a given location at a particular time. Thus:

$$OC \approx P_m \tag{2}$$

Here, P_m is the probability of the user being at a certain location based upon the composite location information of different sensed identity tokens that are associated to him. In the case of our RFID and BT example, P_m is the probability that the user is at the location where he has requested access to resources; that probability is based upon the locations of the sensors that have sensed the user's RFID and BT tokens.

3 Location Sensor Fusing

In the following sections we describe and discuss the algorithm used to calculate the probability P_m according to the available location information of that user.

3.1 Theoretical Study

We start with some notation and with the formal statement of the problem.

Sensors and Cells. Our setting is a region T (e.g., a building or a city). The location of a user u who is somewhere in T, can be detected via his personal devices by different sensor sources $S^1,\ldots,S^n$, where indexes *1,…,n* stands for type of sensors. Each sensor type S^X is a set of sensors $S_1^X, S_2^X,\ldots,S_{|X|}^X$ with *non-necessarily disjoint* coverage regions or cells of $C_1^X, C_2^X,\ldots,C_{|X|}^X$, respectively. For example, a S^{RFID}

source can include n sensors $S_1^{RFID}, S_2^{RFID}, ..., S_n^{RFID}$ whose cells are $C_1^{RFID}, C_2^{RFID}, ..., C_n^{RFID}$. The area of any arbitrary region A is denoted by $\|A\|$.

Our first assumption regards the area covered by each sensor source.

Assumption 1. For each source S^X, cells $C_1^X, C_2^X, ..., C_{|X|}^X$ partition the whole T. With $S_i^X = 1$ we denote the event that user u is detected by sensor S_i^X. This event indicates that the sensor detects the user's corresponding device in cell C_i^X. A consequence of Assumption 1 is that if $S_i^X = 1$, then $S_j^X = 0, \forall j \neq i$. This can be regarded as a quantization of the user location to one cell of the sensor source.

Sensor Error Model. Generally errors are associated with such a quantization process. Three error causes can be identified. The first error depends on the reliability of sensors themselves. For instance, a BT device can be detected within five meters from a dongle 95% of the time. In addition, sensors also have a probability of misidentification, i.e. the sensor incorrectly says the device is in the area or misses the presence of the user. The second error depends on the probability of the user carrying the device corresponding to that sensor source (e.g., RFID reader). All location sensing technologies rely on the user carrying or using a certain device like a RFID badge, BT-enabled PDA or smart phone, WLAN enabled laptop or even a keyboard. So knowing the location of the device implies that the location of the user is known as well. Finally, the third error is introduced by the "freshness" of the sensor information; the older the information the less reliable it is.

Indeed, most product specifications of location sensing technologies give the conditional probability that the device is correctly detected if it is present in its cell. Let's denote this probability by $P(S_i^X = 1 \mid u \in C_i^X) = q_i^X$. The probability of the complement event, i.e., $p'^X_i = P(S_i^X = 0 \mid u \in C_i^X) = 1 - q_i^X$, is called "false negative" probability. In addition, location technologies have a probability of misidentification, that is $P(S_i^X = 1 \mid u \notin C_i^X) = p_i^X$. This probability is called "false positive" probability. The aforementioned three sources of errors are contributors to the false positive and false negative probabilities p'^X_i and p_i^X.

Observation. *Referring to Assumption 1, we can also release that* $C_1^X, C_2^X, ..., C_{|X|}^X$ are mutually disjoint.

In fact, this requirement is a way of obtaining a quantization of the user location to one cell of the sensor source. This quantization is needed to cope with two or more sensors (of the same type) detecting the same user at different locations. We note that quantization can be obtained at the sensor source level as well by selecting just one sensor in case of inter-type conflict. A detailed explanation about how to carry out this quantization is out of our scope here.

Depending on the outcomes of the sensors of a certain type and on the quantization method used, one can derive per sensor type p^X and q^X values from p_i^X and q_i^X values. For example, consider the case where only one sensor gets triggered and the pairs (p_i^X , q_i^X) are the same for $i:1...|X|$. Then, for that sensor type, we have: $q^X = P(S_i^X = 1 | u \in C_i^X) = q_i^X (1-p_i^X)^{|X|-1}$ and $p^X = P(S_i^X = 1 | u \notin C_i^X) = p_i^X (1-q_i^X)(1-p_i^X)^{|X|-2}$.

From this point on we will base our calculation on these p^X and q^X values that are independent of the individual sensors.

Proposition 1. For each $R \subseteq C_i^X$, $P(S_i^X = 1 | u \in R) = q^X$. For each $R \subset \overline{C}_i^X$, where $\overline{C}_i^X$ denotes the complement set of C_i^X in T , $P(S_i^X = 1 | u \in R) = p^X$.

The following assumption regards the typology of source errors that we admit in our setting.

Assumption 2. We consider only false positive errors in our setting. This assumption follows the quantization process imposed by each sensor type. That is our sensor fusion method considers only those sensors types that have detected a user's presence and each sensor type detects a user's presence in only one of their cells.

Our last assumption concerns the independence of sensors. Though strictly speaking sensors are not mutually independent, the following (weaker) conditional independency is reasonable true for most sensors setting.

Assumption 3. Sensors are conditionally independent, that is:

$$If\ P(S_i^X = 1 | u \in C_i^X) = q^X\ then\ \forall j, Y\ \ P(S_i^X = 1 | u \in C_i^X, S_j^Y = 1) = q^X$$

$$If\ P(S_i^X = 1 | u \notin C_i^X) = p^X\ then\ \forall j, Y\ \ P(S_i^X = 1 | u \notin C_i^X, S_j^Y = 1) = p^X$$

Informally, the position of the user inside or outside of a sensor's cell determines the behavior of the sensor. In other words, the behavior of the sensor is independent of whether or not other sensors of different types are triggered.

Fusing Sensor Sources. Fusing n sensor sources concerns the computation of the probability that user u is in a region of interest I , given that n sources $(S_{i_1}^1, ..., S_{i_n}^n) \subseteq S^1 \times ... \times S^n$ have indicated that the user is in their cells $C_{i_1}^1, ..., C_{i_n}^n$, respectively (i.e., $S_{i_1}^1 = 1, ..., S_{i_n}^n = 1$). Thus we are interested in the probability

$$P_m = P(u \in I | S_{i_1}^1 = 1, ..., S_{i_n}^n = 1) = \frac{P(u \in I, S_{i_1}^1 = 1, ..., S_{i_n}^n = 1)}{P(S_{i_1}^1 = 1, ..., S_{i_n}^n = 1)} \quad (3)$$

In the following we derive two relations for the numerator and denominator of Eq. (3). Note that the effect of region I appears only in the numerator relation.

Denominator. Cells $C_{i_1}^1,...,C_{i_n}^n$ are like an order-n Venn diagram that includes n simple closed curves in the T plane. These curves partition the T plane into maximum 2^n connected and disjoint regions $R_1,...,R_K$, where $K \le 2^n$, $\sum_{k=1}^{K} \|R_k\| = \|T\|$ or $\bigcup_{k=1}^{K} R_k = T$, $\forall k \ne k'$: $R_k \cap R_{k'} = \phi$; and $R_k \subset C_{i_j}^j$ XOR $R_k \subset \overline{C}_{i_j}^j$ for $j = 1...n$. Term $P(S_{i_1}^1 = 1,...,S_{i_n}^n = 1)$ can be rewritten as follows:

$$\sum_{k=1}^{K} P(u \in R_k) \cdot P(S_{i_1}^1 = 1,..., S_{i_n}^n = 1 | u \in R_k) = \sum_{k=1}^{K} P(u \in R_k) \prod_{j=1}^{n} (q^j)^{\alpha_{kj}} (p^j)^{1-\alpha_{kj}} \quad (4)$$

Here $\alpha_{kj} = 1$ if $R_k \subset C_{i_j}^j$ and $\alpha_{kj} = 0$ if $R_k \subset \overline{C}_{i_j}^j$. In Eq. (4), we used the independency condition of sensors because either $R_k \subset C_{i_j}^j$ or $R_k \subset \overline{C}_{i_j}^j$ for $j = 1...n$. Assuming a uniform distribution for user location in all regions, we have:

$$P(S_{i_1}^1 = 1,..., S_{i_n}^n = 1) = \frac{1}{\|T\|} \sum_{k=1}^{K} \|R_k\| \cdot \prod_{j=1}^{n} (q^j)^{\alpha_{kj}} (p^j)^{1-\alpha_{kj}} \quad (5)$$

The time complexity of Eq. (5) grows exponentially in n; hereto we need to calculate Eq. (4) or (5) for all disjoint regions obtained from intersections of n cells $C_{i_1}^1,...,C_{i_n}^n$.

Numerator. The numerator can be written as:

$$P(u \in I, S_{i_1}^1 = 1,..., S_{i_n}^n = 1) = P(u \in I) P(S_{i_1}^1 = 1,..., S_{i_n}^n = 1 | u \in I) \quad (6)$$

In the second term of Eq. (6) it is given that user $u \in I$. The intersections of cells $C_{i_1}^1,...,C_{i_n}^n$ with region I are like an order-n Venn diagram with n simple closed curves in the I plane. These closed curves partition the plane into maximum 2^n connected and disjoint regions $R_1^I,...,R_{K'}^I$, where $K' \le 2^n$; $\sum_{k=1}^{K'} \|R_k^I\| = \|I\|$ or $\bigcup_{k=1}^{K'} R_k^I = I$, $\forall k \ne k'$: $R_k^I \cap R_k^I = \phi$; and $R_k^I \subset C_{i_j}^j \oplus R_k^I \subset \overline{C}_{i_j}^j$ for $j = 1...n$. Here $\oplus$ denote exclusive disjunction. The term $P(S_{i_1}^1 = 1,...,S_{i_n}^n = 1 | u \in I)$ in Eq. (6) can be rewritten as follows:

$$\sum_{k=1}^{K'} P(u \in R_k^I | u \in I) P(S_{i_1}^1 = 1,...,S_{i_n}^n = 1 | u \in I, u \in R_k^I) = \sum_{k=1}^{K'} P(u \in R_k^I | u \in I) \prod_{j=1}^{n} (q^j)^{\alpha_{kj}} (p^j)^{1-\alpha_{kj}} \quad (7)$$

In which: $\alpha_{kj} = 1$ if $R_k^I \subset C_{i_j}^j$ and $\alpha_{kj} = 0$ if $R_k^I \subset \overline{C}_{i_j}^j$. Eq. (7) uses the independency condition of sensors because either $R_k^I \subset C_{i_j}^j$ or $R_k^I \subset \overline{C}_{i_j}^j$, $j = 1...n$. In

case of uniform distribution for user location in all regions, we have: $P(S_{i_1}^1 = 1,...,S_{i_n}^n = 1 | u \in I) = \frac{1}{\|I\|} \sum_{k=1}^{K} \|R_k^I\| \cdot \prod_{j=1}^{n} (q^j)^{\alpha_{kj}} (p^j)^{1-\alpha_{kj}}$. Thus from Eq. (6):

$$P(u \in I, S_{i_1}^1 = 1,...,S_{i_n}^n = 1) = \frac{1}{\|T\|} \sum_{k=1}^{K} \|R_k^I\| \cdot \prod_{j=1}^{n} (q^j)^{\alpha_{kj}} (p^j)^{1-\alpha_{kj}} \quad (8)$$

Assuming that $(I \subset C_{i_j}^j) \oplus (I \subset \overline{C}_{i_j}^j)$, $j = 1...n$ (i.e., the area of interest does not overlap with both areas of each cell) then from Eq. (6) and the independency condition of sensors we can directly derive:

$$\begin{aligned} P(u \in I, S_{i_1}^1 = 1,..., S_{i_n}^n = 1) &= P(u \in I) \prod_{j=1}^{n} P(S_{i_j}^j = 1 | u \in I, S_{i_1}^1 = 1,..., S_{i_{j-1}}^{j-1} = 1) \\ = P(u \in I) \prod_{j=1}^{n} P(S_{i_j}^j = 1 | (u \in C_{i_j}^j) \oplus (u \in \overline{C}_{i_j}^j)) &= P(u \in I) \prod_{j=1}^{n} (q^j)^{\alpha_j} (p^j)^{1-\alpha_j} \end{aligned} \quad (9)$$

Here $\alpha_j = 1$ if $I \subset C_{i_j}^j$ and $\alpha_j = 0$ if $I \subset \overline{C}_{i_j}^j$. The time complexity of Eq. (8) grows exponential in n, but with the simplification we used in Eq. (9), it becomes linear in n.

3.2 Simulations

To illustrate the principle of location sensitive adaptive authentication we simulated two extreme situations: overlapping and non-overlapping location sensor information. The first situation assumes a BT device that is sensed in an area that is completely covering the area of interest I. Additionally, there is a second identity token, an RFID badge, that starts with zero coverage and slowly starts overlapping with I. The second situation deals with a BT device that is detected in an area completely outside I whereas the RFID badge slowly starts overlapping with I.

For the simulations the following input data was used: T = 5000 m^2, I = 16 m^2, BT's cell (C_1) is a circle with a fixed radius of 8 m, p = 0.01 and q = 0.95, and RFID's

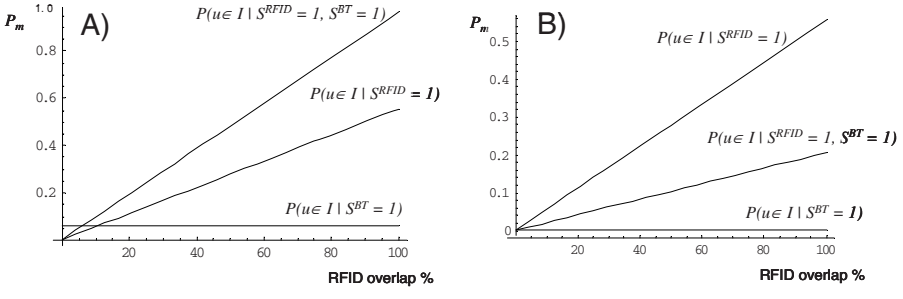

Fig. 1. Individual and fused RFID and BT identity probability as a function of the RFID cell area overlap with the area of interest I. For Fig. 1A the BT identity token has a cell area that is constantly overlapping with I; for Fig. 1B the BT identity token cell area has no overlap with I.

cell (C_2) is a circle with a fixed radius of 1 m, and the relative p = 0.0005 and q = 0.99. Fig. 1A shows the outcome of P_m for the overlapping situation. Clearly observable is the strong increase of P_m in the case that the RFID and BT location sensor information agree with each other. In case of maximal overlap, the individual BT or RFID identification probabilities of 7% or 55%, respectively, sum up to a 'fused' probability of 98%. In case of a conflicting BT identity token, the fused RFID and BT probability drops considerably to less than 25% (Fig. 1B).

4 Design

This section describes the design of a system that uses location information to determine and dynamically adapt the authentication level of a user. The goal of our implementation is to demonstrate and validate the context-sensitive adaptive authentication scheme. The location information from multiple different location sensors is used to calculate P_m, i.e., the probability of the user being in a certain location of interest I, which is supposed to be the location from where the user forwards his access request. The result is used to determine the authentication level of the user and to modify his authorization level accordingly.

For obtaining sensor location information we used the Context Management Framework (CMF) described in [12]. The CMF enables processing and exchange of heterogeneous context information collected from various sensors, is distributed over multiple administrative domains, and stems from different protocol layers. Examples of context information supplied by the CMF include location coordinates via GPS receivers, WLAN access points associations, RFID reader data, BT scan measurements, desktop keyboard typing, and Outlook Calendar meetings.

4.1 Message Flow

For calculating the probability values we implemented the User Location Probability Calculator (ULPC). The ULPC is a context aware component that collects and

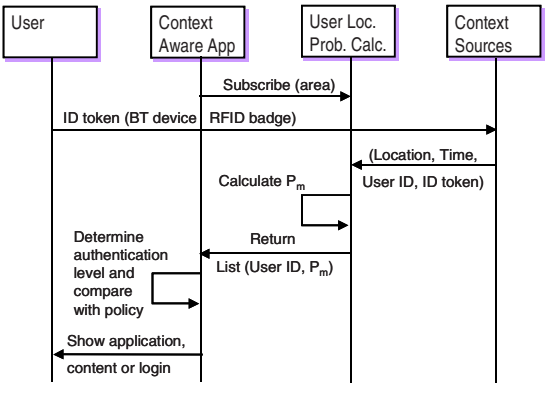

Fig. 2. Message flow for location probability based adaptive authentication

reasons about context information of users obtained from the CMF. Fig. 2 shows the message flow for application service access that relies on a location probability based authentication method.

Application service access is provided by the ULPC in collaboration with the Context Provider (i.e. CMF). The application subscribes itself to the ULPC for obtaining probability measures of users in a certain area of interest. When a user is detected by location sources of the Context Provider, this information is sent to the ULPC together with a timestamp indicating the time the user has been detected. The ULPC caches this information for all sensor types (e.g. RFID, BT, WLAN, keyboard, etc.) and uses equations (5) and (9) to determine the probability a user is in the area of interest for each new input it receives. The outcome of the calculation is communicated to the application that uses it to determine the actual level of authentication. If other persons are in the area of interest as well, their probability will be communicated as well to the application. If the level of authentication is not sufficiently high the application may ask the user to provide stronger identification information by e.g. presenting a username/password window or by asking for performing an iris scan. In case of multiple persons, the confidentiality of the information shown may be harmed and therefore, the information will be removed from the screen. This is an example of context-aware adaptive confidentiality.

4.2 Buddy Spotter Application

To demonstrate the concept of location sensitive adaptive authentication we build a 'Buddy Spotter' application that allows users to locate their buddies or colleagues. A screen dump of the application's user interface is shown in Fig. 3.

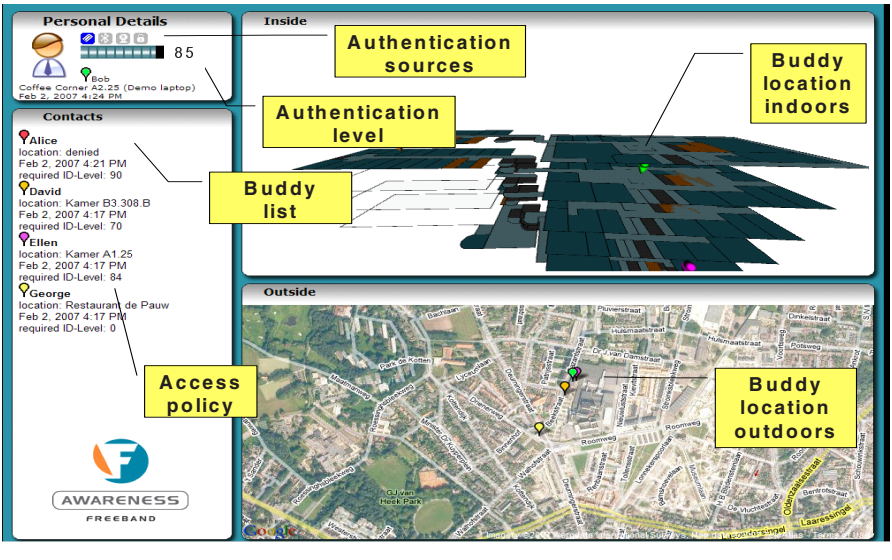

Fig. 3. Screen dump of the Buddy Spotter application

The right-hand panels provide information regarding the user's buddy locations in- and outside the office building. The upper left-hand panel shows the authentication level of the user by means of an "ID-level" display. The ID-level display informs the user about the confidence the application has in his identity and also what sensor information was used to come to this (e.g. by means of BT, RFID, etc.). The lower left-hand panel shows the buddy list of the user. The buddies can specify an ID-level that is required prior to getting access to their location information. If the user's ID-level is not sufficiently high, the location of the buddy shall not be shown. This functionality allows the buddies to preserve their privacy to a certain extend.

5 Discussion

Our location sensitive adaptive security solution may raise questions regarding time dependency, trustworthiness and usability. This section discusses them.

5.1 Dynamicity of Authentication Level

Due to the time-dependent character of location information, the ULPC component calculates the location probability regularly, i.e. every time it gets new location information events from the Context Provider. For instance, a BT device is sensed every five seconds when it is in the neighborhood of a BT dongle. This results in an update of the location probability of the user. However, the RFID authentication method in particular is much more time-sensitive as it has a very accurate location quality and requires an explicit act of the user, i.e., swiping his RFID badge in front of the reader. This means that the RFID location probability drops very rapidly in time or, in other words, the coverage area of the RFID sensor becomes larger depending on the mobility of the user (this is illustrated in Fig. 4).

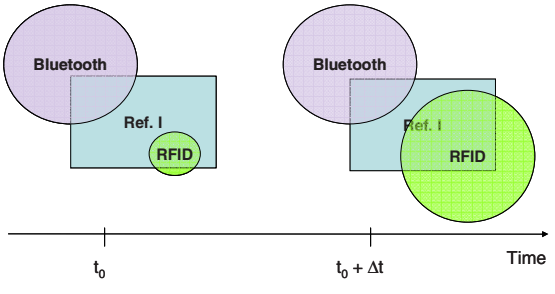

Fig. 4. Changing of RFID cell area in time

With the dropping probability, the level of authentication will drop in time as well, and subsequently the user will automatically lose authorization to resources that require a higher level of authentication than is. The application may then ask the user to upgrade his level of authentication by for instance swiping his RFID badge again.

The decay function that might be applied to the position probability depends amongst others on the mechanism that is used to determine the location of the user

and the mobility of the user: the bigger the coverage area of the sensor, the less fast will the user move to another coverage area and thus the slower the authentication level will drop. In order to be able to fuse location information from different sensors the ULPC has to determine, based on timestamps, the time intervals between the most recent location update of a sensor and the locations cached from previous sensors and recalculate their coverage area based upon the mobility of the user. Though we assumed in our model the user to be moving with an average speed of 5 km/hour in the office building (see Fig. 5), this mobility pattern might be sensor and application dependent. In our calculations we assumed the following simple model to describe the mobility of the user:

$$v_{average} * p_{mobility} = v_{effective} \tag{10}$$

With $v_{average}$ representing the average velocity of the user (i.e. 5 km/hour), $p_{mobility}$ the chance that the user will walk away (e.g. 4%) and $v_{effective}$ the effective velocity of the user (i.e. 5.6 cm/second). $p_{mobility}$ strongly depends on the type of sensor and its location. As this is just a simple approach, obviously more research needs to be done here to determine a correct mobility pattern for each sensor type (see also [13]).

The increment of P_m in Fig. 5 is explained by the increase of overlap of the RFID cell with the area of interest I. After the turning point, the expanding RFID cell will have relatively less overlap with I.

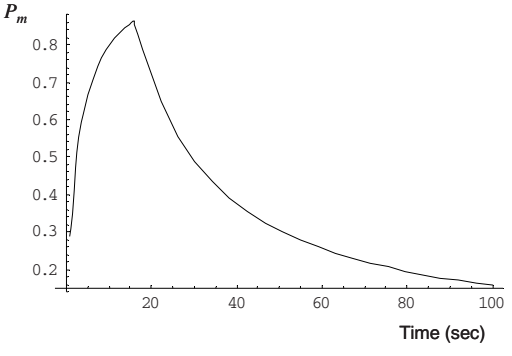

Fig. 5. Dropping of the RFID probability level in time assuming a user velocity of 5 km/hour. All other parameters were similar to those used for Fig. 1.

During application interaction more location information from new sensors may be obtained. This will result in a new level of authentication and subsequent access rights. The ID-level display of the Buddy Spotter application thus changes dynamically in time and so do the access rights the user has.

5.2 Trustworthiness

Trust plays an important role during the exchange of context information. We assume that the users trust the CMF; they have given consent to the CMF to collect their context information. Regarding the privacy of the user towards the application there is

no difference compared to the potential loss of privacy when using traditional authentication services as username/password or security token. The application only obtains a probability value that the user is at a certain location. Furthermore, buddies are allowed to specify their privacy policies in an easy and efficient manner: they only have to set the proper required ID-level. Allowing users to control their personal information is an active area of research. Though many solutions have been proposed, most of them fail in offering user friendliness (e.g. [14]). We belief our parameterized approach offers the user a usable approach to control access to personal information.

5.3 Usability

Usability of security is an extremely important element of IT-security. Direct user involvement is often required in a security service. Two forms of involvement can be distinguished: action and conclusion [14]. An action involves the user to explicitly enter his username/password or swipe his RFID-badge. A security conclusion allows the users to observe some relevant security evidence regarding the security state of the system. For instance, the closed padlock at the bottom of the browser is a security conclusion. Usability principles related to security actions and conclusions are typically expressed in terms of user understanding, knowledge, mental and physical load, and willingness [14]. Our location based authentication approach fulfils several of these principles. Regarding authentication actions we strive to minimize user involvement as much as possible since that is the basic starting point of our approach. In our case the user only has to swipe his RFID badge in front of the reader to nevertheless obtain a relatively high level of authentication after fusing the information with other sources in a transparent manner. Moreover, authentication is also possible without the use of RFID. If for instance BT and WLAN are used, the user is authenticated without having to perform an explicit act.

The ID-level display informs the user about his authentication level and also shows the means by which this level has been achieved (e.g. BT, RFID, WLAN). Our first experiences indicate that users appreciate this information. In particular the benefit of being authenticated in a minimal-intrusive way is appealing. Further tests however are needed to optimize the user experience.

One could argue about the meaningfulness of the ID-level: what does an authentication level of 75% mean? The actual point of discussion here is about parameterizing security and how useful this is. “If you can not measure it, you can not improve it” (1883) ─ one of Lord Kelvin’s famous quotations that may be very applicable to our adaptive security approach. In order to be able to measure the strength of security functions one must first parameterize them. We already mentioned that this is not easy because it involves making the performance of the security function measurable. However, a standardized reference framework that is required for this purpose is lacking. Objective and subjective notions regarding security levels are often mixed making it hard to come to such a reference framework.

We don’t claim that our solution is better than other, existing solutions that have proven their usefulness already in practice for many years. Location sensitive authentication may prove useful in situations that require minimal intrusive and flexible authentication. Such situations are for instance in a hospital where medical personnel frequently has to enter credentials in order to access medical information

[15], emergency situations where access to medical information may be needed on an ad-hoc basis, or ubiquitous computing environments. In other situations, the use of context information can be very well used as an additional parameter to enhance the level of traditional authentication measures, for instance, by combining username/ password with location or calendar information prior to granting access.

6 Related Work

A key element of our work consists of making security adaptive. Though several adaptive approaches for security have been described [1], [2]), the use of context information as a security adaptation parameter hasn't been considered.

To realize adaptation, we parameterize authentication. We do that on the basis of the probability that the user is at a certain location. Similarly, Ganger proposed the concept of authentication confidences as another approach to parameterize security [3]. Authentication confidences refine the current yes-or-no authentication decisions, allowing systems to cleanly provide partial access rights to authenticated users whose identities are suspect. The proposed solution direction exists of a combination of different authentication technologies. In a similar context, Noble and Corner propose a transient authentication model. In this model, a user wears a small hardware token that constantly authenticates the user to other devices over a short-range wireless link [4]. Covington et al. describe how to parameterize the authentication function [5]. Levin et al. proposed a Quality of Security Service mechanism for modulating and provisioning of predictable security service levels to users [6]. We observe that in most cases the levels of security are relatively static and pre-defined and that there is no relationship with the situational context as a means to determine the actual level of security in a dynamic and flexible manner.

The use of context information for security purposes is not new. In 2003, Leo Marcus introduced and described the logical foundations of the adaptive security infrastructure concept that also takes the environment into account [7]. Our work builds upon these foundations. Similarly, Kouadri et al. proposed a conceptual model for context-based authorizations tuning. This model offers a fine-grained control over access to a protected resource, based on a set of user's and environment state and information [8]. In [9], location and velocity information is used as a means to allow train travelers access to services offered in the train. Hager investigated methods to determine appropriate security protocols for specific wireless network applications [16]. The specific problem being addressed was that there are tradeoffs between security, performance and efficiency among current and proposed security protocols and that these tradeoffs are influenced by the constrained network capacity and limited mobile nodes (i.e. the context). Yee and Korba propose a context-aware security policy agent that is responsible for selecting security services and mechanisms for mobile Internet services according to the user's preferences, power of the mobile device and location [17]. Furthermore, security policy negotiation between the service provider and consumer is described by Yee and Korba as well [18]. An approach to building security services for context-aware environments with a strong focus on the design of security services that incorporate the use of security-relevant "context" to provide flexible access control and policy enforcement is described in

[19]. This approach is based on the concept of context-dependent roles. The related work on context aware security focuses in general on using context information for authorization purposes while we focus on context-aware user authentication.

We determine the probability that the user is in a certain area of interest. Our probability approach resembles that of [13] that describes a middleware approach for probabilistic location determination in general. There are other probability approaches for sensor data fusion but they often have a different goal. Abowd et al. describe in a Location Service that fuses sensor information using a fairly straightforward temporal and heuristic algorithm for the purpose of customized communication [20]. Bohn and Vogt [21] use a probabilistic positioning service that employs an available ubiquitous computing infrastructure for the localization of mobile devices. Data from these sources are transformed independently of each other into an abstract representation of location estimates. By means of a probabilistic fusion process, these estimates are then combined into a single position value.

7 Conclusions

The transparent nature of pervasive and ubiquitous computing environments where context information is used to enhance service experience motivates the need for security functionality that will be transparent, customized, and non-intrusive. The context sensitive adaptive security paradigm allows for adaptation of the security depending on a set of relevant information collected from the dynamic environment and the preferences and capabilities of the interacting entities, i.e. the context. As the environment evolves, the context changes and so should security in order to dynamically cope with new requirements. We argue that security services, like authentication and access control, can be made less intrusive, more intelligent, and able to adapt to the rapidly changing contexts of the environment. To validate this argument we show that by fusing various sources of location information that are available over time, the confidence in the user identity associated to the sensed devices can be increased considerably. The outcome of the location fusion and reasoning process is a value that expresses the probability that the user is at a certain location. This probability is used as a measure not only to authenticate the user based on location information but to parameterize the authentication level as well making it thereby much more adaptive to changing situational circumstances. In particular the heterogeneity of the sensed personal devices strongly contributes to the enhancement and robustness of the location-based authentication. A user is less likely to lose two or more personal devices at the same time. Furthermore, face recognition technology and calendar information could be used as additional, independent measures that help to identify the user based upon his location. For instance a web cam can identify a user at a certain location and Outlook Calendar may tell the ULPC that the user is out of office or in a certain meeting room. Future work will focus on such extensions as well as improvements in the algorithms used and user experience validation.

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

References

1. Schneck, P.A., Schwan, K.: Dynamic Authentication for High-Performance Networked Applications. In: Proc. of the 6th International Workshop on Quality of Service (IWQoS 1998) Napa, California, USA, pp. 127–136 (1998)
2. Ryutov, T., Zhou, R., Neumann, C., Leithead, T., Seamons, K.E.: Adaptive Trust Negotiation and Access Control. In: SACMAT 2005. Proc. of the ACM Symposium on Access Control Models and Technologies, Stockholm, Sweden, pp. 139–146. ACM Press, New York (2005)
3. Ganger, G.B.: Authentication Confidences. In: Proc. of the Eighth Workshop on Hot Topics in Operating Systems (HotOS-VII 2001), Elmau/Oberbayern, Germany, p. 169 (2001)
4. Noble, B.D., Corner, M.D.: The Case for Transient Authentication. In: Proc. of the 10th ACM SIGOPS European Workshop, Saint-Emilion, France, pp. 24–29. ACM Press, New York (2002)
5. Covington, M.J., Ahamad, M., Essa, I., Venkateswaran, H.: Parameterized Authentication. In: Samarati, P., Ryan, P.Y A, Gollmann, D., Molva, R. (eds.) ESORICS 2004. LNCS, vol. 3193, pp. 276–292. Springer, Heidelberg (2004)
6. Levin, T.E., Irvine, C.E., Spyropoulou, E.: Quality of Security Service: Adaptive Security. The Handbook of Information Security. In: Threats, Vulnerabilities, Prevention, Detection and Management, vol. III, John Wiley & Sons, Inc, Chichester (2005)
7. Marcus, L.: Local and Global Requirements in an Adaptive Security Infrastructure. In: International Workshop on Requirements for High Assurance Systems (RHAS), Monterey Bay, California (2003)
8. Kouadri Mostéfaoui, G., Brézillon, P.: A Generic Framework for Context-Based Distributed Authorizations. In: Blackburn, P., Ghidini, C., Turner, R.M., Giunchiglia, F. (eds.) CONTEXT 2003. LNCS, vol. 2680, pp. 204–217. Springer, Heidelberg (2003)
9. Hulsebosch, R.J., Salden, A.H., Bargh, M.S., Ebben, P.W.G., Reitsma, J.: Context sensitive access control. In: SACMAT 2005. Proc. of the tenth ACM symposium on Access control models and technologies, Stockholm, Sweden, pp. 111–119. ACM Press, New York (2005)
10. Ranganathan, A., Al-Muhtadi, J., Campbell, R.H.: Reasoning About Uncertain Contexts in Pervasive Computing Environments. In: Pervasive Computing, vol. 3(2), pp. 62–70. IEEE, Los Alamitos (2004)
11. Belovin, S.M.: On the Brittleness of Software and the Infeasibility of Security Metrics. IEEE Security and Privacy 4(4) (2006)
12. van Kranenburg, H., Bargh, M.S., Iacob, S., Peddemors, A.: A Context Management Framework for Supporting Context Aware Distributed Applications. IEEE Communications Magazine 44(8), 67–74 (2006)
13. Ranganathan, A., Al-Muhtadi, J., Chetan, S., Campbell, R., Mickunas, M.D.: MiddleWhere: A Middleware for Location Awareness in Ubiquitous Computing Applications. In: Jacobsen, H.-A. (ed.) Middleware 2004. LNCS, vol. 3231, pp. 397–416. Springer, Heidelberg (2004)
14. Jøsang, A., AlZomai, M., Suriadi, S.: Usability and Privacy in Identity Management Architectures. In: Brankovic, L., Steketee, C. (eds.) Proc. Fifth Australasian Information Security Workshop Privacy Enhancing Technologies (AISW 2007), Ballarat, Australia, pp. 143–152 (2007)
15. Bardram, J.: The trouble with login: on usability and computer security in ubiquitous computing. Personal and Ubiquitous Computing 9(6), 357–367 (2005)

16. Hager, C.T.R.: Context Aware and Adaptive Security for Wireless Networks. PhD thesis, Virginia Polytechnic Institute and State University (2004)
17. Yee, G., Korba, L.: Context-Aware Security Policy Agent for Mobile Internet Services. In: Proc. of the 2005 IFIP International Conference on Intelligence in Communication Systems, Montréal, Québec, Canada, pp. 249–260 (2005)
18. Yee, G., Korba, L.: Negotiated Security Policies for E-Services and Web Services. In: ICWS 2005. Proc. of the 2005 IEEE International Conference on Web Services, San Diego, California, pp. 605–612. IEEE Computer Society Press, Los Alamitos (2005)
19. Covington, M.J., Fogla, P., Zhan, Z., Ahamad, M.: A Context-Aware Security Architecture for Emerging Applications. In: ACSAC 2002. Proc. of the 18th Annual Computer Security Applications Conference, Las Vegas, Nevada, pp. 249–258 (2002)
20. Abowd, G.D., Battestini, A., O'Connell, T.: The Location Service: A Framework for Handling Multiple Location Sensing Technologies (2002), http://www.awarehome.gatech.edu/publications/location_service.pdf
21. Bohn, J., Vogt, H.: Robust Probabilistic Positioning Based on High-Level Sensor-Fusion and Map Knowledge. Technical Report No. 421, ETH Zurich (2003)