Access Control in Ubiquitous Environments Based on Subjectivity Eliminated Trust Propagation

Omar Hasan
INSA Lyon, France
omar.hasan@insa-lyon.fr

Jean-Marc Pierson
IRIT, France
pierson@irit.fr

Lionel Brunie
INSA Lyon, France
lionel.brunie@insa-lyon.fr

Abstract

The first challenge that we tackle in this paper is how to conduct access control in ubiquitous environments where sites have to handle access requests from their own users as well as unknown users from foreign sites. We present a solution based on trust propagation. A recommendation from one site to another about the trustworthiness of an entity is the basis of trust propagation. An issue that we identify with this technique is that since the perception of trustworthiness is subjective, the meaning of a trust recommendation from one site to another may get misinterpreted. The result of such misinterpretations would be inaccurate trust propagation and hence inaccurate access control. Thus the second challenge that we address is how to use trust propagation without the negative effect of subjectivity. We use a method for eliminating subjectivity from trust recommendations which relies on the notion of percentiles. We illustrate the problem and the advantage of our access control model with the help of examples.

1. Introduction

One of the visions of Ubiquitous Computing is that users are able to roam freely and access resources at foreign sites as seamlessly as they would at their home site. Security is one of the main challenges when realizing such an environment [9]. Access control is an important component of security. At their home site, a user can be granted access to resources based on their pre-determined rights. However, a foreign site does not have any pre-defined access rights associated with an unknown user thus access control becomes a problem. The foreign site may be able to grant access to the user after some extra steps such as manual intervention by the user and an administrator however that renders the access control process non-ubiquitous.

We present a solution based on the notion of trust management and propagation. Instead of allowing access to resources based on roles (as in RBAC [3]) or identities (as in IBAC [8]), it is granted based on the trustworthiness level of the user. Roles or identities that exist at one site may not exist at another site. Ubiquitous access control is possible with trustworthiness since it is a universally recognized notion.

A site has direct knowledge of the trustworthiness of its own users. The trustworthiness of an unknown user can be determined through trust propagation. Trust propagation is a technique that enables the foreign site to acquire trust in the unknown user through a path of trust recommendations that link the site to the user. For example, a site X may acquire trust in an unknown user u, if u's home site Y which is trusted by X, makes a recommendation to X about u. A trust recommendation from a site takes the form of a quantitative value such as 0.8 on the interval [0,1].

An issue with this approach is that due to the subjective nature of trustworthiness, a value given as a trust recommendation may have different interpretations for the recommender site and the site that receives the recommendation. For example, it is possible that the recommender site considers 0.8 as an average value of trustworthiness, where as the receiving site considers 0.8 as a very high value of trustworthiness. Thus the true meaning of the recommendation is not conveyed due to subjectivity. The Merriam-Webster online dictionary [12] defines subjectivity as a judgment that is "modified or affected by personal views, experience, or background" and is "peculiar to a particular individual". The result of this particular scenario could be that the user receives access to more sensitive resources at the foreign site than at his home site. As discussed in [5], using qualitative labels instead of quantitative values does not resolve the problem.

Using trust propagation for access control is by no means a novel idea. Works such as [16, 9] have introduced similar schemes. However, the approach that we present is novel in the sense that it recognizes subjectiv-

ity as an issue and eliminates it from trust propagation. The hypothesis is that eliminating subjectivity would lead to more accurate trust propagation and hence more accurate access control.

Authentication is another important component of security, which is closely associated with access control. However, in this paper we do not address authentication. We assume that users are authenticated using one of the existing authentication schemes for ubiquitous environments such as [17]. Our focus is on the ability of a site to determine whether an authenticated user should be permitted or denied access to a particular resource.

The remainder of the paper is organized as follows: The next section outlines the problem setting. In section 3, we present our access control model for ubiquitous environments. Section 4 comprises of an example which illustrates the advantage of the model. We discuss future work and present concluding remarks in section 6 and section 7 respectively.

2. Problem Setting

The environment comprises of n sites given as the set $S = \{s_1, s_2, \ldots, s_n\}$. A site is defined as a geographically bounded collection of resources with an autonomous administration and access control policy. Some examples of sites include university campuses, corporate offices, airports, etc.

Each site has a number of member users associated with it. The set of users associated with a site x is given as $U_x = \{u_{x,1}, u_{x,2}, \ldots, u_{x,|U_x|}\}$, where $|U_x|$ is the number of users. For simplicity we assume that the set of users of any two sites x and y are disjoint, that is $U_x \cap U_y = \phi$.

Each site also has a number of resources under its ownership. The set of resources of site x is given as $R_x = \{r_{x,1}, r_{x,2}, \ldots, r_{x,|R_x|}\}$, where $|R_x|$ is the number of resources. A user may request access to a resource at his home site or he may roam in the environment and request access to the resources of foreign sites. Each site has an access control policy that determines if a user is qualified to access a resource that he has requested.

The first goal is to make the access control process for a user as ubiquitous at a foreign site as it is at his home site. The solution given to this problem is based on trust propagation. The second goal is that the trust propagation based solution should not suffer from the effects of subjectivity.

3. The Access Control Model

In this section we present our model for access control in ubiquitous environments based on trust propagation. We include two versions of the function for trust propagation. The first version (section 3.2) is conventional in the sense that it does not account for subjectivity. The second version (section 3.3) builds upon the first one but incorporates subjectivity elimination. We first begin with laying out the general framework of the model.

3.1. General Framework

We define a set, $V = \bigcup_{x \in S} U_x \cup S$. The set V contains all the users and all the sites in the environment.

We define a binary relation, $T = \{(x,y) : x \in S \wedge y \in V\}$. The relation T represents the *trusts* relation between a site and another site or a user. We will use the notation $x \ T \ y$, $x \ trusts \ y$, and (x,y) interchangeably.

A Web of Trust is defined as a weighted directed graph, $G = (V,T)$. The sites and their users form the vertices of the graph. The trust relations between the members of set V given as ordered pairs in the set T form the edges of the graph. An edge that is incident from x and incident to y, implies (x,y) or $x \ trusts \ y$.

A weight is associated with every edge (x,y) in the graph, which represents the amount of trust that entity x holds for entity y. The weight associated with an edge (x,y) is given as the function $t(x,y)$. $t : T \rightarrow X$. The set X is defined as $X = [0,1]$.

The range of $t(x,y)$ is real numbers bounded by 0 and 1. 0 implies "minimum trust" and 1 implies "maximum trust". Real numbers between 0 and 1 give us infinite resolution for expressing trust. $t(x,y) = 0$ in our model implies "minimum trust" and not "no trust". "No trust" between entities x and y is the absence of (x,y) in T. We do not address distrust in this model.

(x,y) exists for all x,y where $x \in S$ and $y \in U_x$. This implies that a site has direct trust relationships with all of its users.

A path $p = \langle x_1, x_2, \ldots, x_m, u \rangle$ from a site x_1 to a user u is said to exist if $x_1, x_2, \ldots, x_m \in S$ and $u \in U_{x_m}$ and $(x_1,x_2),(x_2,x_3),\ldots,(x_{m-1},x_m),(x_m,u) \in T$.

3.1.1. Trust Recommendation and Propagation. If $(x_1,x_2),(x_2,x_3),\ldots,(x_{m-1},x_m),(x_m,u) \in T$, then $t(x_2,x_3), t(x_3,x_4), \ldots, t(x_{m-1},x_m), t(x_m,u)$ may be considered as recommendations to x_1 from $x_2, x_3, \ldots, x_{m-1}$, x_m respectively. Taking into consideration this "chain of trust", x_1 may choose to establish (x_1,u) and $t(x_1,u)$. We say that the trust of x_m in u is propagated to x_1.

To facilitate the discussion we establish the following terminology:

Source site – the site from which the path originates; the site that may establish trust in a previously unknown user based on a recommendation

Recommender site – a site that recommends a site or one of its users to the source site

Target user – the user at whom the path terminates; the user whom the source site may choose to trust

In the preceding case, x_1 is the source site, $x_2, x_3, \ldots, x_m$ the recommender sites, and u the target user.

3.1.2. Access Control. With each resource $r_{x,j}$, the site x defines a threshold value which is given as the function $h(r_{x,j})$. $h : R_x \rightarrow X$. The access control policy of a site lists all its resources and associated thresholds.

Access is granted to a user u that requests a resource r at a site x if $t(x,u) \geq h(r)$. In other words, access to a resource is granted if the site has equal or greater trust in the requesting user than the threshold for that resource.

It is important to note that the user u may or may not be a member of site x. If u is a member of site x then the site has direct knowledge of the user's trustworthiness. In case u is not a member then access may still be granted if $t(x,u)$ can be established through trust propagation and $t(x,u)$ passes the trustworthiness threshold.

What makes the model ubiquitous is that a site does not need to have pre-defined access rights for a certain user to be able to grant them access to resources. The site can establish trust in a previously unknown user through trust propagation and it can grant them access based on that acquired trust. From the user's point of view access to resources at foreign sites is as seamless as at their home site.

3.2. Trust Propagation without Elimination of Subjectivity

3.2.1. Trust Propagation Function. We define a function *ptrust* (abbreviation of "propagated trust") that given a path $\langle x_1, x_2, \ldots, x_m, u \rangle$, suggests a weight for the edge (x_1, u). The value suggested by the function is an estimate of the amount of trust in u that may propagate to x_1.

$$\begin{aligned} t(x_1,u) &= ptrust(\langle x_1, x_2, \ldots, x_m, u \rangle) \\ &= t(x_1,x_2) \times t(x_2,x_3) \\ &\quad \times \ldots \times t(x_{m-1},x_m) \times t(x_m,u) \\ &= \prod_{i=1}^{m-1} t(x_i,x_{i+1}) \times t(x_m,u) \end{aligned} \quad (1)$$

3.2.2. Reasoning for Using Multiplication. The suggested propagated trust value is the product of all the trust values on the path. We implement the function as such for its simplicity and intuitiveness. We consider a few examples to illustrate our point.

Let's assume that all the trust values on the path are 1. The trust value suggested by the function in this case would be 1, which reflects the fact that absolute trust exists throughout the chain.

As another case let's consider that any one or more of the trust values on a path are 0. That is, one of the sites has no trust in the entity that it has a trust relationship with. The trust value suggested by the function would be 0. Thus the fact that one of the sites does not trust an entity on the path is appropriately reflected in the suggested value.

Let's now consider a path of length 3 with each of the trust values as 0.9. The suggested trust value would be $0.9 \times 0.9 \times 0.9 = 0.73$. Although each of the sites has a high trust of 0.9 in the recommended site or user, the suggested trust value is a lower 0.73. This value is reflective of the degree of separation between the source site and the target user. Intuitively, trust attenuates as the degree of separation between the source site and the target user grows.

As the final example we consider the path $\langle x_1, x_2, x_3, u \rangle$ with $t(x_1,x_2) = 0.1$, $t(x_2,x_3) = 0.8$, and $t(x_3,u) = 0.9$. The suggested trust value would be $0.1 \times 0.8 \times 0.9 = 0.07$. Although x_2 and x_3 have very high trust in x_3 and u respectively, since x_1 has low trust in x_2, the propagated trust value remains low.

3.3. Subjectivity Eliminated Trust Propagation

3.3.1. Disposition to Trust. Disposition to trust is the inherent propensity of an individual to trust or distrust others. An individual's disposition to trust does not vary for specific entities but is a stable characteristic of their personality that governs how they view the trustworthiness of every other entity that they encounter.

McKnight et al [11] define disposition to trust as the "extent to which a person displays a tendency to be willing to depend on others across a broad spectrum of situations and persons".

Rotter [14, 15] notes that an individual's "generalized attitude" towards trust is a product of life experiences, such as interactions with parents, peers, and authorities. Boone and Holmes [2] suggest that good experiences lead to a greater disposition to trust and vice versa.

A study in the context of ecommerce by McCord and Ratnasingam [10] has demonstrated that there is a strong relationship between an individual's disposition to trust and the trust related decisions that they make.

Clearly, the disposition to trust of an individual is a factor that contributes to subjectivity in their opinion

about the trustworthiness of an entity. An individual with a high disposition to trust is likely to assign a relatively high value of trust to an entity. Whereas an individual with a lower disposition to trust is likely to assign a lower value of trust to that same entity.

3.3.2. Quantitative Representation of a Site's Disposition to Trust. We adapt the notion of disposition to trust for sites. It is easy to imagine that a site such as a university would have a higher disposition to trust than sites of more sensitive nature such as airports and banks. The trust decisions at sites are made either directly by the administration or through policies that the administration has defined. Thus the trust decisions made by a site are reflective of the disposition to trust of its administration.

Several examples from the computer science literature may be cited where historical patterns are used to predict future behavior with considerable success. Instances include Self-Customizing Software [7] and Branch Predictors in Microprocessors [4].

We propose an approach based on similar lines for determining the disposition to trust of a site. The trust values that a site has assigned to its users and other sites may be considered as an indication of its disposition to trust. For example, given a site that has a pattern of assigning high values of trust, we may infer that the site has a high disposition to trust, and vice versa. We thus propose to represent a site's disposition to trust by the collection of its trust value assignments in the environment.

3.3.3. The Method for Eliminating Subjectivity from Trust Recommendation. The approach that we use for eliminating subjectivity from a trust recommendation is to report a trust value not as an absolute value but as its percentile value in the disposition to trust of the recommender site. The percentile value indicates the recommender site's perception of the recommended entity in relation to the others that the recommender site has rated. This approach is covered in further detail in [6].

Going back to the example discussed in the Introduction, if site Y conveys to site X an absolute value such as 0.8, site X does not know if according to site Y the value 0.8 is an average value or a high value of trust. However, if the trust is reported as a percentile value, site X does have this information. For example, if the percentile value is in the vicinity of 50%, site X would know that according to site Y, user u has an average trustworthiness. If the percentile value is around 80% or 90%, it is clear that site Y regards user u as highly trustworthy. The absolute value that site Y locally assigned to user u becomes irrelevant.

To convert the percentile to a local absolute score, a site reads the value that is at the given percentile in the collection of trust values that it itself has assigned to other sites and users. This absolute score holds perfect meaning for the site since it is in the context of its own disposition to trust. Thus going through a relative value as an intermediary, the subjectivity and misinterpretation associated with an absolute trust value are eliminated.

3.3.4. Formal Description of the Method. d_x is a vector of the weights associated with the outgoing edges of site x, that is, all $t(x,y)$ where y is a vertex adjacent to x. As discussed in section 3.3.2, the collection of trust values previously assigned or d_x represents the disposition to trust of site x.

The values in d_x are arranged in ascending order and indexed $1,2,\ldots,n_x$, where n_x is the number of outgoing edges of site x (as well as the number of values in d_x). The j^{th} value in d_x is referred to by $d_x[j]$. We define a function $first(k,d_x)$ that returns the index of the first occurrence of a value k present in d_x.

$c(x,y)$ is the percentile of $t(x,y)$ in d_x. The function which calculates $c(x,y)$ is given as:

$$\begin{aligned} c(x,y) &= percentile(t(x,y),d_x) \\ &= \frac{100 \cdot first(t(x,y),d_x)}{n_x+1} \end{aligned}$$

As an example, consider $d_{Alice} = \langle 0.4,0.4,0.5,0.6,0.8,0.8,0.8,0.8,0.8,0.9,0.9\rangle$ and $t(Alice,Carol) = 0.8$. Then $n_{Alice} = 11$ and $first(t(Alice,Carol),d_{Alice}) = 5$. $c(Alice,Carol)$ is calculated as follows:

$$\begin{aligned} c(Alice,Carol) &= percentile(t(Alice,Carol),d_{Alice}) \\ &= \frac{100 \cdot first(t(Alice,Carol),d_{Alice})}{n_{Alice}+1} \\ &= \frac{100 \cdot 5}{11+1} = 41.67 percentile \end{aligned}$$

$t(x,y)_z$ is defined as the value in d_z at the $c(x,y)^{th}$ percentile. The function which calculates $t(x,y)_z$ is stated as:

$$\begin{aligned} & t(x,y)_z \\ &= trustvalue(c(x,y),d_z) \\ &= \begin{cases} d_z[i] + f \cdot (d_z[i+1] - d_z[i]) & \text{if } 0 < i < n_z \\ d_z[1] & \text{if } i = 0 \\ d_z[n_z] & \text{if } i = n_z \end{cases} \end{aligned}$$

where,

$$i = \left\lfloor \frac{c(x,y) \cdot (n_z + 1)}{100} \right\rfloor$$

and,

$$f = \frac{c(x,y) \cdot (n_z + 1)}{100} - i$$

i is an integer and f is a fraction greater than or equal to 0 and less than 1.

We may think of $t(x,y)_z$ as the value $t(x,y)$ transformed such that instead of being in reference to the disposition to trust of site x, it is now in reference to the disposition to trust of site z.

Instead of reporting $t(x,y)$, a site x calculates $c(x,y)$ and communicates this percentile value to site z. Given $c(x,y)$, site z determines $t(x,y)_z$ and considers that as the recommended value.

Continuing the example from above, consider $d_{Bob} = \langle 0.2, 0.3, 0.3, 0.3, 0.5, 0.5, 0.5, 0.6, 0.8 \rangle$. Then:

$$\begin{aligned} t(Alice,Carol)_{Bob} &= d_{Bob}[i] + f \cdot (d_{Bob}[i+1] - d_{Bob}[i]) \\ &= d_{Bob}[4] + 0.17 \cdot (d_{Bob}[5] - d_{Bob}[4]) \\ &= 0.3 + 0.17 \cdot (0.5 - 0.3) = 0.33 \end{aligned}$$

where,

$$\begin{aligned} i &= \left\lfloor \frac{c(Alice,Carol) \cdot (n_{Bob} + 1)}{100} \right\rfloor \\ &= \left\lfloor \frac{41.67 \cdot (9+1)}{100} \right\rfloor = 4 \end{aligned}$$

and,

$$\begin{aligned} f &= \frac{c(Alice,Carol) \cdot (n_{Bob} + 1)}{100} - i \\ &= \frac{41.67 \cdot (9+1)}{100} - 4 = 0.17 \end{aligned}$$

The implementation of the functions *percentile* and *trustvalue* is based on the method for estimation of percentiles given by NIST [13].

3.3.5. Trust Propagation Function. We define a function *septrust* (abbreviation of "subjectivity eliminated propagated trust") that given a path $\langle x_1, x_2, \ldots, x_m, u \rangle$, suggests a weight for the edge (x_1, u).

$$\begin{aligned} t(x_1,u) &= septrust(\langle x_1, x_2, \ldots, x_m, u \rangle) \\ &= t(x_1,x_2) \times t(x_2,x_3)_{x_1} \times t(x_3,x_4)_{x_1} \\ &\quad \times \ldots \times t(x_{m-1},x_m)_{x_1} \times t(x_m,u)_{x_1} \\ &= t(x_1,x_2) \times \prod_{i=2}^{m-1} t(x_i,x_{i+1})_{x_1} \times t(x_m,u)_{x_1} \end{aligned} \quad (2)$$

The subjectivity eliminated propagated trust is the product of all trust values on the path which have been transformed such that they are in reference to the disposition to trust of the source site.

4. An Example

There are two sites, X and Y. X considers 0.5 as an average value of trustworthiness whereas Y considers 0.7 as an average value of trustworthiness.

Let's consider the path $\langle X, Y, u \rangle$, where $t(Y,u) = 0.7$. If Y recommends u to X and assuming that X has full trust in Y, that is $t(X,Y) = 1.0$, then the propagated trust value (from equation 1) of u would be 0.7. Since X considers 0.5 as an average value of trustworthiness, it would consider 0.7 as a high value of trustworthiness and would erroneously believe that u is highly trustworthy.

Let's consider $d_X = \langle 0.3, 0.5, 0.5, 0.5, 0.5, 0.6, 0.6 \rangle$ and $d_Y = \langle 0.5, 0.5, 0.7, 0.7, 0.7, 0.8, 0.8, 0.9 \rangle$. Then the propagated trust value using the subjectivity eliminated trust propagation (equation 2), the propagated trust value would be 0.5, which site X does in fact consider an average value of trustworthiness. Thus with subjectivity eliminated trust propagation, site X would have the correct information to make a judicious access control decision.

Considering that u had requested a resource r at site X, where $h(r) = 0.7$ implying that X allows access to r to highly trustworthy users. Without subjectivity eliminated trust propagation, X would have erroneously considered u as highly trustworthy and would have granted access. Whereas with subjectivity eliminated trust propagation, X would have reached the correct conclusion of not granting access since u has only average trustworthiness.

5. Experiments

5.1. Data Set

We generate a random graph [1] based web of trust as described in Figure 1. η is the number of sites, κ is the number of member users of each site, ε is the number of sites that are direct neighbors of each site, and G is the generated graph.

As discussed earlier, different sites may assign different trust values to a target entity. This occurs due to

GENERATE-WEB-OF-TRUST($\eta, \kappa, \varepsilon$)

```
1  create an empty weighted directed graph,
       G(V,E), where V is the set of vertices
       and E is the set of edges
2  populate V with η sites, labeled x_i,
       where i = 0,1,...,η−1
3  for each site x_i, add κ users to V
       labeled u_{x_i,j}, where j = 0,1,...,κ−1
4  with each vertex v ∈ V, associate a random
       trustworthiness value q_v
       from the interval [0,1]
5  with each site x_i, associate a random
       skew factor s_{x_i} from the interval [0,2]
6  for each site x_i
7      do create a set N_{x_i} = φ
8         add ε random distinct sites from V to N_{x_i}
9         add all u_{x_i,j} ∈ V to N_{x_i}
10        for each vertex v ∈ N_{x_i}
11            do create the edge (x_i, v) in E
12               assign the weight power(q_v, s_{x_i})
                     to (x_i, v)
13 return G
```

Figure 1. Pseudo code for generating the web of trust.

their different dispositions to trust even though their individual experiences with the target entity are the same.

These ideas are reflected in the generation of this web of trust. The trustworthiness value q_v represents the experience that other sites would have with an entity v. Since q_v remains constant for entity v, any site that interacts with it has the same experience. The skew factor represents the disposition to trust of each site. Although different sites have the same experience with a given entity v, they each assign it a different trust value based on their own disposition to trust. If the skew factor s_{x_i} is less than 1, q_v would be skewed upwards. Otherwise if the skew factor s_{x_i} is greater than 1, q_v would be skewed downwards. The resulting data set is a graph that approximately simulates trust relationships between sites and users in a distributed environment.

5.2. Experiment Design

The objective of this experiment is to test if users are able to ubiquitously access resources at foreign sites with our access control model based on subjectivity eliminated trust propagation.

We assume that every site in the environment has one resource. The resources in the environment have a uniform threshold given by τ. Each user in the environment visits every foreign site in the environment. At each foreign site, the visiting user requests access to the site's resource. The foreign site determines the trustworthiness of the user with the subjectivity eliminated trust propagation method. If it is able to determine the users trustworthiness and if the trustworthiness level satisfies its resource's threshold, the site grants access to the user. For each access granted in this manner, we count a "hit". We categorize the requests and hits according to the path length from the source site to the target user.

In a non ubiquitous environment, the users of a site can only access the resources at their home site in a ubiquitous manner. If we observe that users are able to access a considerable number of resources at foreign sites with this model, we would consider that a positive indication that the model is suitable for access control in ubiquitous environments.

Please note that this experiment does not compare trust propagation with and without subjectivity elimination. Such comparison is identified as part of future work.

5.3. Experiment Runs and Observations

We use a web of trust generated by the algorithm given in Figure 1, with $\eta = 100$, $\kappa = 10$, and $\varepsilon = 10$. We run the experiment for three different values of τ. The results are given in Table 1.

Table 1. Experiment runs.

Path length	*Requests*	*Hits,* $\tau = 0.2$	*Hits,* $\tau = 0.5$	*Hits,* $\tau = 0.8$
2	10000	5611	3376	1414
3	58450	22847	12688	4872
4	30540	8752	4615	1720
5	10	0	0	0
6	0	0	0	0

We note that with 10,000 requests made at foreign sites by users who were 2 trust relationships away, and with $\tau = 0.2$, the number of those requests that resulted in the user receiving ubiquitous access to the resource was a high 5,611. We observe considerable numbers of hits in various other columns as well.

6. Future Work

The example given in section 4 illustrates one scenario where our access control model would be effec-

tive. We would like to conduct an experimental study, preferably in a practical setting to gain further insight into its effectiveness. We would also like to conduct an experiment that compares the effects of trust propagation with and without subjectivity elimination in the access control model.

The access control conditions that we have discussed are too simplistic. Only a scalar threshold is given as the condition for access to a particular resource. A more sophisticated language for defining access control conditions would be required for a practical deployment of the model. A few things that the language should handle, include: 1) different thresholds for different operations such as read, write, and execute, and 2) specifying contextual conditions such as those based on time, location etc.

7. Conclusion

In this paper we addressed the problem of providing access control in ubiquitous environments. The solution that we presented is based on trust propagation. Instead of granting access based on conventional criteria such as roles and identities, in our model access to resources is granted based on the trustworthiness of the user. What makes the model ubiquitous is that a site may be able to grant access to users even if they are previously unknown and it can do so without requiring any intervention from the users. The trustworthiness of an unknown user may be established through trust propagation. We identified that an issue with this approach is that when trust is propagated from one entity to another, its real meaning may become distorted due to the differences in perception or subjectivity between the two entities. We used a method that relies on the notion of percentiles for eliminating subjectivity from trust propagation. We give an example that demonstrates how eliminating subjectivity from trust propagation can lead to more accurate access control. The experiments provide a positive indication that the model can be effective for access control in ubiquitous environments.

References

[1] B. Bollobas. *Random Graphs*. Cambridge University Press, 2001.

[2] S. D. Boon and J. G. Holmes. *Cooperation and Prosocial Behaviour*, chapter The Dynamics of Interpersonal Trust: Resolving Uncertainty in the Face of Risk, pages 190 – 211. Cambridge University Press, 1991.

[3] D. Ferraiolo and R. Kuhn. Role based access control. In *Proceedings of the 15th National Computer Security Conference*, pages 554 – 563, October 13 - 16 1992.

[4] A. Fog. Branch prediction in the pentium family. http://x86.org/articles/branch/branchprediction.htm, 2008. Retrieved February 24, 2008.

[5] N. Griffiths. Task delegation using experience based multidimensional trust. In *Proc. Fourth Intl. Joint Conf. on Autonomous Agents and Multiagent Systems*, 2005.

[6] O. Hasan, L. Brunie, J.-M. Pierson, and E. Bertino. Elimination of subjectivity from trust recommendation. Technical Report TR-08-008, Department of Computer Science, Purdue University, IN, USA, March 2008.

[7] H. Hirsh, C. Basu, and B. D. Davison. Learning to personalize. *Communications of the ACM*, 43(8):102 – 106, August 2000.

[8] HP. Identity-based access control. Technical report, Hewlett-Packard, 2006. ProCurve Networking by HP.

[9] L. Kagal, T. Finin, and A. Joshi. Trust-based security in pervasive computing environments. *IEEE Computer*, December 2001.

[10] M. McCord and P. Ratnasingam. The impact of trust on the technology acceptance model in business to consumer e-commerce. In *Proc. Intl. Conf. of the Information Resources Management Association: Innovations Through Information Technology*, May 2004.

[11] D. H. McKnight, V. Choudhury, and C. Kacmar. Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3):334 – 359, September 2002.

[12] Merriam-Webster. Merriam-webster online dictionary. http://www.merriam-webster.com/, 2008. Retrieved February 24, 2008.

[13] National Institute of Standards and Technology (NIST). Nist/sematech e-handbook of statistical methods - percentiles. http://www.itl.nist.gov/div898/handbook/prc/section2/prc252.htm, 2008. Retrieved February 24, 2008.

[14] J. B. Rotter. A new scale for the measurement of interpersonal trust. *Journal of Personality*, 35(4):651 – 665, December 1967.

[15] J. B. Rotter. Generalized expectancies for interpersonal trust. *American Psychologist*, 26(5):443 – 452, 1971.

[16] R. Saadi, J.-M. Pierson, and L. Brunie. Authentication and access control using trust collaboration in pervasive grid environment. In *Proceedings of the International Conference on Grid and Pervasive Computing (GPC 2007)*, 2007.

[17] L. A. Staffans and T. Saridakis. An authorization and access control scheme for pervasive computing. In *Proceedings of the 2004 Conference on Software Engineering (SE 2004)*, Innsbruck, Austria, 2004.