

# Context Sensitive Access Control

R.J. Hulsebosch<sup>†</sup>, A.H. Salden, M.S. Bargh, P.W.G. Ebben, J. Reitsma

Telematica Instituut  
P.O. Box 589  
7500 AN Enschede  
The Netherlands

<sup>†</sup> Corresponding author: Bob.Hulsebosch@telin.nl

Telephone number: +31-53-4850498

## ABSTRACT

We investigate the practical feasibility of using context information for controlling access to services. Based solely on situational context, we show that users can be transparently provided anonymous access to services and that service providers can still impose various security levels. Thereto, we propose context-sensitive verification methods that allow checking the user's claimed authenticity in various ways and to various degrees. More precisely, conventional information management approaches are used to compare historic contextual (service usage) data of an individual user or group. The result is a relatively strong, less intrusive and more flexible access control process that mimics our natural way of authentication and authorization in the physical world.

## Categories and Subject Descriptors

C.2.0 [Computer-Communication Networks]: *General – Security and Protection*; D.4.6 [Operating Systems]: *Security and Protection—Access controls, Authentication, and Verification*; K.6.5 [Management of Computing and Information Systems]: *Security and Protection—Authentication and Unauthorized access*

## General Terms

Security, Verification

## Keywords

Access Control, Context Sensitive, Service Usage Patterns, Authentication, Context Verification

## 1. INTRODUCTION

The emerging, pervasive and ubiquitous computing environments need security services that are non-intrusive and easily adaptable to changing user or environmental contexts. Traditional security services are context insensitive. They require a complex and static authentication infrastructure in which a user has to identify himself by username and password or via certificates. In ad-hoc or roaming situations, access control to e.g. train services [1] could rather preferably depend on a group of users' contexts than on their identities. By coupling access control to such user or group context information, security services can become far more user-friendly and flexible.

Context-based security has already been applied in various settings [1, 2, 3]. As commonly deployed Role Based Access Controls or Access Control Lists are too static and therefore not suitable for context aware or smart environments, other solutions have been proposed for context-based access control. One of them is Generalized RBAC [4]. The GRBAC paradigm for access control incorporates the concept of *environment roles*. Environment roles (conditions) capture environmental information, such as time of day or weather conditions, which can be used to mediate access control. Compared to the commonly used role-based access control schemes, GRBAC offers more expressiveness and ease of use, making it suitable for context aware authorization schemes [3, 5]. However, GRBAC may not be feasible in practice because the potential large amounts of environment roles make the system very hard to maintain manually. Zhang and Parashar therefore have proposed a Dynamic RBAC model that extends the role based access control model and 'dynamically' adjusts static *Role Assignments* and *Permission Assignments* based on context information [6]. Alternatively, the OASIS access control system for open, inter-working systems in a distributed environment has the notion of appointment, whereby the role activation conditions of a service may include environmental constraints [7]. In the Web Services area, several mechanisms for controlling access to web services have been proposed. An XML access control language (XACL) for web services has been discussed by Hada and Kudo [8]. XACL does not support roles and does not handle context information. The OASIS eXtensible Access Control Markup Language (XACML)

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SACMAT'05, June 1–3, 2005, Stockholm, Sweden.

Copyright 2005 ACM 1-59593-045-0/05/0006...\$5.00.

specification is based on an extension of XML to define access control specifications that support notions similar to context-based privilege assignments [9]. It, however, does not directly support the notion of roles. Bhatti et al. [10] describe a framework for enforcing role based access control in dynamic XML-based web services. Their solution includes concepts of roles and context.

The type of context information that is used for access control depends on the situation. It could be based on location, velocity, age, device and/or network capabilities, temperature, time of day, etc. More advanced solutions even take into account the user's intentions as a measure for access control. Ways to determine the user's intentions are for instance to make use of behavior recognition or service usage patterns. Classification and recognition of these patterns is considered an effective security approach in real life [10, 11].

Advanced security services for access control purposes exist that take the intentions of a user or a group into account [1]. Those intentions can be associated with specific user or group behavior that manifest themselves e.g. in recorded GPS-location and service usage history patterns. We claim that classification of such patterns into various hierarchies enables us to create different access control policies of various strengths (for a thorough exposition on how to arrive at such hierarchical categorization the reader is referred to previous work by the authors [12]). Such patterns of a group of users allow us to define various methods for verifying context information provided by an individual user. For example, an individual train traveler is given access to train services on the basis of the fact that he belongs to a group of train travelers using similar services in the same train. This way we obtain a very flexible solution for context sensitive and therewith personalized access control that extends beyond the current state of the art.

However, several issues have to be resolved before context sensitive access control will be effective. The most important issue concerns fraudulent generation of context claims. An impostor can rather easily construe location information as credentials for gaining access, even without a GPS-receiver or other positioning technology. It is clear that verification of such context claims made by a user or device/sensor is essential. A second major issue concerns the reproducibility, volatility and dynamics of contextual information. Access authorization to devices in offices based on sporadic location determination can be very tricky in particular if the user is constantly moving around. A third issue concerns the privacy sensitivity of transactions on contextual information. An end-user may be willing to provide his location information to a service provider, but he may not wish to reveal his identity.

We present a framework for context-sensitive access control that tackles the above problems (see section 2). Thereto, we first present an access control architecture underlying context-aware service provisioning. Secondly, we define access control on the basis of an inextricable relationship between user/device and service. Thirdly, we propose verification methods for anonymous access based on location and service usage history patterns of a user and groups of users. Next we implement context-sensitive access control for in particular train services (see section 3). Furthermore, we discuss the pros and cons of our context-based

access control approach (see section 4). Finally, we conclude and pose challenges for future work.

## 2. ACCESS CONTROL FRAMEWORK

We present a framework for context-sensitive access control to resources. The framework consists of setting up an access control architecture related to context-aware service provisioning, conceiving context-sensitive access control, and user authentication on the basis of context verification.

### 2.1 Access Control Architecture

A context-sensitive access control (CSAC) architecture should deal with all issues related to access, collection, storage, processing, and distribution of context information. Thereto, a CSAC architecture should reflect the business roles, relations and federations in context-aware service provisioning (see Figure 1).

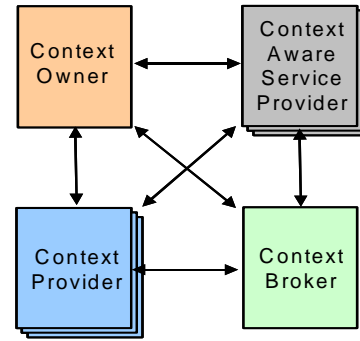


Figure 1: CSAC Roles, relations and federations.

In a simplified version of a context-aware service provisioning value network the following roles can be distinguished: a Context Owner (CO), a Context Provider (CP), a Context Broker (CB), and a Context-Aware Service Provider (CASP).

The CO collects and owns the contextual data or information, e.g. a user receives and possesses GPS-location information. He or she decides which, why, when, where, how and by whom context data or information may be stored, distributed and processed. Even if another party, like a telecom operator knowing your whereabouts, collects context information associated to the CO, this party has to comply with legislation concerning e.g. the privacy of the CO. A CO role can be assigned to a party also playing the role of user, customer or CASP. Of course, users, customers and CASPs all have their own privacy and security concerns. However, they will probably enable and permit provisioning of contextual information as credentials via COs – roles that users, customers and CASPs may play themselves – to CPs in return for personalized services. In our scenario, anonymous train travelers play the role of CO. They are willing to share their GPS-location and service usage patterns for authentication purposes.

The CP looks not only after user and group management issues such that e.g. context access control and usage policies are in line with privacy and security requirements of the COs. The CP also takes care of context management issues by providing categorization means for context indexing, retrieval, querying, inferential and association purposes. Therewith, those context provider functions can provide insight in e.g. service usage history patterns of COs. In this way specific context information (e.g., time, location, speed, etc.) provided by the CO allows the CP to infer a role (e.g., train passenger, visitor). This information in turn

can form for anonymous users sufficient and necessary credentials to authenticate them. Note that in addition the *CP* performs and permits storage, distribution and processing of contextual data and information on behalf of the *CO* by third parties in line with the *CO*'s privacy and security requirements. The *CO* via policies that the *CP* enforces on his behalf for instance specifies these requirements.

The *CB* provides service publishing mechanisms to *CPs*, and service discovery mechanisms to the *CASPs*. How the *CPs* publish their services to the *CB* and the *CASP* is up to them but it will be compliant with the privacy and security requirements of the *CO*. The *CB* will enforce these requirements, e.g. anonymity of train travelers, when intermediating between the *CASP* and the *CPs*.

The *CASP* provides services to a user or customer that are tailored to his or her requirements that he or she has communicated as *CO*, and are adapted to specific user-service contexts, e.g. being on the train. On behalf of the context-aware service owner, the *CASP* performs access control by applying authentication and authorization measures.

## 2.2 Context Sensitive Access Control

Access control should prevent unauthorized usage of resources [13]. It involves an *Access Controller* who grants or denies *Subject* to perform *Operation* on an *Object* according to an *Access Policy*. The Subject identifies an entity, e.g., a specific user or group who are *COs*, and can be *any* (context) attribute of such an entity. Like an executable program, Operation upon its invocation makes information to flow to/from the Object or causes the consumption of an exhaustible system resource represented by the Object. The Operation involves not only access, but also collection, storage, processing, and distribution of (context) information or other resources. The Access Policy specifies the usage rights or *Permission(s)* of the Subject to perform the Operation on the Object. The Access Controller executes *Subject Authentication* and *Access Authorization*. The Access Controller performs Subject Authentication on the basis of a *Token (T)* and a *Subject Identity (S<sub>ID</sub>)*. The Access Controller performs Access Authorization by determining the Permission of the Subject to execute the Operation on the Object. Subsequently, the Access Controller allows or disallows the Subject to carry out the Operation on the Object after identifying the Permission of the Subject. For example, Access Controller denies the Subject to access the Object if the Subject is neither authenticated nor authorized, but grants the access if the Subject is authenticated and authorized (see Figure 2).

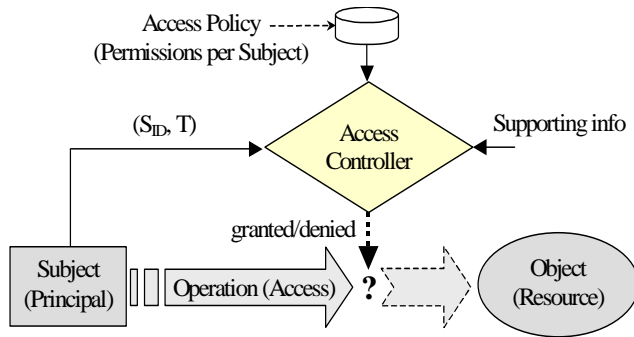


Figure 2: An illustration of the access control process.

Table 1: A juxtaposition of access control methods.

Approach	Subject Identity $S_{ID}$	Token T	Authenti- cation	Mapping	Access Policy - Permission P
Conventional Access Control	User-name	Password	Is $S_{ID}$ a valid user- name, given T?	-	$(S_{ID}, P)$
Public Key Based Access Control	Certificate (public key)	Signature (private key)	Does $S_{ID}$ represent a valid user, given T?	-	$(S_{ID}, P)$
Role-Based Access Control	Username	Password	Is $S_{ID}$ a valid user, given T?	$S_{ID} \rightarrow$ $Role_{ID}$	$(Role_{ID}, P)$
Context-aware Role Based Access Control	Username	Password	Is $S_{ID}$ a valid user- name, given T?	$S_{ID} \rightarrow$ $Role_{ID}$ $S_{ID} \rightarrow cxt$	$(Role_{ID},$ $cxt, P)$
Context Sensitive Access Control	User pseudonym	Context information	Is T a valid context, given the available context info?	-	$(cxt, P)$

Access control based on user-specific contextual information, i.e., our CSAC, requires on the one hand that the Access Controller – for Subject Authentication purposes – verifies the contextual attributes T, provided by the Subject. On the other hand, it requires that the Access Controller – for Access Authorization purposes – binds Permissions in the Access Policy to (parts of) those attributes. Analogous to the way that an Access Policy binds a Permission to organizational roles of the Subject in RBAC [14], an Access Policy binds a Permission to the contextual attributes of the Subject in our CSAC. In particular, Subject Authentication in our CSAC is based on verifying whether or not the situational context claimed is a valid context attribute of the Subject, e.g. being really a train traveler. Furthermore, Subject Authentication by context verification (see section 2.3) enables the Access Controller to decouple context attributes from the identity of an entity. In our CSAC an Access Controller does not need to know the exact or reference to the legal identity of the Subject. On the contrary context verification enables the Access Controller to simultaneously enforce various levels of access control, user anonymity or privacy. In Table 1 we juxtapose our CSAC access control to conventional user-name/password access control, public key based access control, RBAC [14], and context-aware

RBAC [3, 15]. The non-uniqueness ( $S_{ID}, T$ ) in our access control method proves its flexibility compared to the other methods. Moreover, it also displays the robustness of our method. For example, forgetting username and/or password is no issue anymore. However, our CSAC access control method can be combined with other methods, such as user-name/password based Access Control, to ensure higher security or privacy levels. This does not mean that our method cannot sustain similar security or privacy levels as the more conventional ones or even outperform those.

### 2.3 Authentication by Context Verification

Although context information, e.g. location information, is often publicly and freely available, its verification is essential when it is used for security purposes. For instance, an impostor might deceive a train service by asserting he is in the train by providing location information related to a train track. This authentication method by verification of context information resembles a lot those based on user's username via a password. To ensure higher levels of context authenticity and reliability of the claimed context information there are several verification options:

- Checking the source. The source of context information is the premier criterion for its credibility and quality. The source can be a trusted subject/user, trusted context provider or broker.
- Using cryptography. Context-based digital signatures can be used to protect the authenticity (integrity) of the (context) information. For example, for location authentication purposes, GPS-location and -time information can be integrated into data encryption and decryption processes for specific locations or areas [16].
- Using round trip times. Round-trip time measurements can be used to gain and verify location information about a user in different contexts [17, 18, 19, 20]. It has the drawback that this location information is associated with a rather large area, that the errors are considerably, and that it works poorly in routed networks.
- Using proximity. Proximity is a common technique to also prove the user's location, i.e. (s)he is in the neighborhood of a trusted reference point. A nearby beacon can transmit a security token known to the authenticator of the access controller that can be used by the user to prove (s)he is in the proximity of the beacon. Balfanz et al. have proposed using location-limited short-range channels for location-based access control [21], and many others have also proposed use of limited-range radio broadcast as a way to verify proximity [22].
- Using user context history. A claim of a user's context can be validated against a reference database containing history information of earlier claims made by users. If such a new claim is in line with what is expected based on the history database, it could be trusted. For example, the use of location history and movement patterns can improve location-tracking techniques [23]. Furthermore, Kalman filtering can improve the accuracy of context information such as the current and future movements based on GPS-information [24]. Despite the uncertainty of context information probabilistic logic,

fuzzy logic, Bayesian network and other mechanisms still allow to reason about that information [25].

- By comparison/uniqueness. Maybe the most often used method to prove the authenticity of physical objects is simply to compare it to another authentic object. As digital security and physical security become increasingly interdependent in context aware environments, this method could also be used to verify context information that is used for security purposes, e.g., context claims of several train travelers can be compared with each other. Logically, all travelers in the same train should have the same velocity. So if traveler X claims to be in train Y with velocity  $V1=60$  km/hour and five other travelers also claim to be in train Y with velocity  $V2=75$  km/hour, then it can be concluded that traveler X is faking his velocity and possibly his location [26]. This example of togetherness for verifying the context claims has been proposed [1]. Assuming that a commonly agreed context may be more reliable than that of a single device/sensor, they describe a method for collaborative context recognition.

Requiring a subject to present various types of context information of various levels of accuracy provides a very powerful and flexible measure for access control and trust management. In our opinion, therefore, just comparing context information can be very effective and efficient in verifying the raw context claimed by a subject. Moreover, the comparison/uniqueness method is most often used in our physical every day life for the verification of information and therefore seems most natural and powerful to implement. In our implementation this method is reflected by the use of trusted or collective reference sources for the verification of context information of context owners. For example, a train traveler providing his location information and claiming to be in a train can be verified by comparing his claimed context with that of a trusted context information like that the train guard or driver.

## 3. A CONTEXT-SENSITIVE ACCESS CONTROL INFRASTRUCTURE

In our Mobile & Wireless 2004 project, an IEEE 802.11 WLAN network along the train track is rolled out. In this project a scenario is envisioned in which train travelers enjoy anonymous access to online services. To ensure that *solely* train travelers have access, their common contextual information is compared to that of other travelers and/or railway personnel like train guard and driver. In the following, we describe the technical and information requirements needed to gain access to train services, and present a corresponding system architecture. We conclude this section providing implementation details of our context sensitive access control mechanism.

### 3.1 Requirements and System Architecture

We require that each train traveler and railway personnel has a GPS-receiver and a laptop with WLAN-card for making use of Internet services. Internet connectivity is obtained via Wireless LAN that has been rolled out along a railway track.

The contextual information elements that are required are location and velocity (including its direction). These elements are obtained from the GPS-receiver of the travelers and railway personnel. Verification of those elements is done either via comparison/uniqueness with a trusted reference point like the train guard or via comparison/uniqueness with other anonymous

train travelers in the same train. Anonymous access to these services is based on the GPS-location and -velocity (i.e. context) of the travelers that they obtain via their GPS-receivers.

On the basis our CSAC depicted in Figure 1 the roles, relations and federations are associated and mapped to infrastructural entities that can (partially) automate access control on behalf of the stakeholders. These entities and their collaboration are depicted in Figure 3. For privacy purposes, the true identity of the context owner (*CO*) must be decoupled from his context information. Therefore two types of tickets are required: the Context Ticket and the Context Granting Ticket. The *CO* and the trusted context broker (*CB*) know both the Context Ticket and Context Granting Ticket. The Context Ticket is issued by the *CB* to the *CO* and contains a pseudonym that the *CB* uses to link the

*CO* and her context provider (*CP*), i.e., it contains the Owner ID and Context Provider ID tuple. The Context Granting Ticket is issued by the *CB* and instantiates the association between the *CO* and his *CP*. Only the mediator *CB* has access to the Context Granting Ticket. The *CB* uses this ticket to create new Context Tickets when the *CO* decides to use other context-controlled services. The *CASP* only knows the Context Ticket and uses it for communication with the *CB*.

The messages that are sent between the parties for the exchange of anonymized location information are shown in Figure 4. The exchange of context information between the involved entities is done via http put/get primitives.

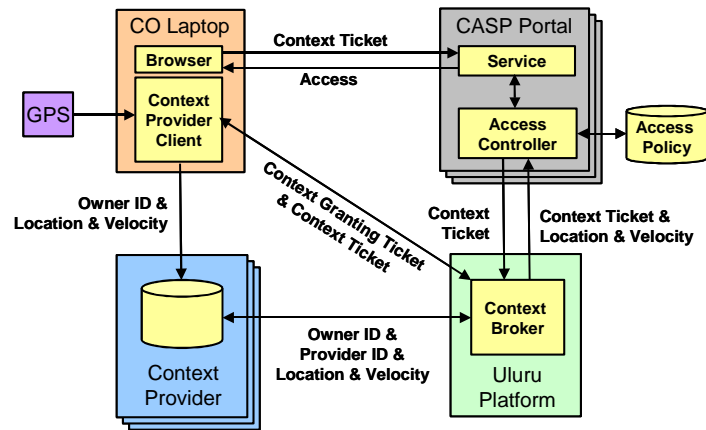


Figure 3: A CSAC infrastructure.

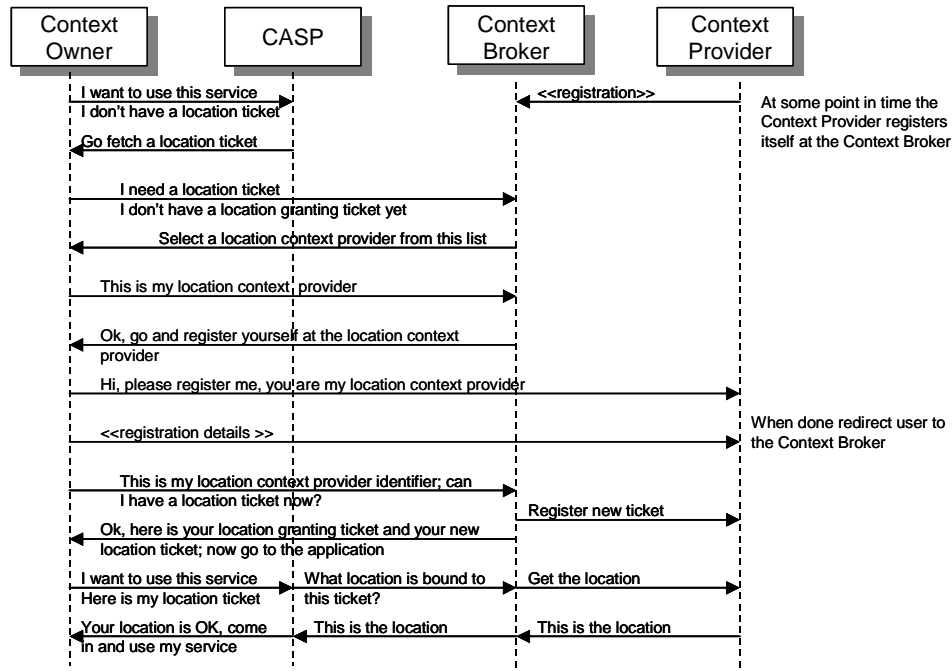


Figure 4: A CSAC message sequence chart.

### 3.2 Implementation Details

We limit ourselves to location information of the user as the relevant context parameter. We use a commodity GPS-receiver (an Emtac CRUX II BTGPS) for obtaining our location. This receiver communicates with a laptop via a Bluetooth connection, using the Bluetooth Serial Port profile. A small Java application on the laptop interprets the NMEA 0183 sentences emitted by the GPS-receiver and transfers the coordinates to a central store using the HTTP protocol. This setup is the actual Location Provider; we refer to it as GPS-over-web.

The location information of (potentially) multiple context providers (*CPs*) is managed by the context broker (*CB*) service running on the Uluru Platform [27]. The location *CP* service is an Enterprise Java Session Bean running inside the JBoss application server. Currently we have implemented two location provider mechanisms:

1. Using external location information obtained as actual location information from outside the Uluru platform as described above.
2. Using a Jabber Instant Messaging (with a location extension).

When using Jabber, the laptop must run a Jabber client capable of distributing the GPS-location to the Jabber server.

The location *CB* is a Java web application, also running in JBoss (using an embedded Tomcat 5 servlet container). The location *CB* is used for defining the location *CP*, and creating location tickets. The latter are created silently when the *CP* is known, i.e. the user does not notice, although under water a few HTTP redirects are taking place. The Context Granting Ticket is implemented using the cookie mechanism. Due to the nature of the cookie mechanism, the cookie is available to the broker only and stored in the browser of the context owner (*CO*, i.e., the user). Optionally, the *CB* can encrypt the cookie, as it contains potentially sensitive information.

The Portal application, the actual application that demonstrates the use of context-sensitive access control, is a Java web application running in a separate Tomcat 5 servlet container. Through the use of a so-called Servlet Filter all requests to the portal are intercepted. A location based access policy determines whether authorization is needed for the requested resource.

Several types of access policies could be implemented. The access controller can define a geographical area that grants anybody who is inside this area access to a service. If the traveler leaves the area access to the service will be lost or denied. Since this is a very coarse-grained access control, additional context constraints were put in place to only allow train travelers access to services. However, with such a location-based access control policy in place, other users that provide fake location information can still be able to enjoy Internet services. To enhance in a natural way our access control policies we have implemented a comparison/uniqueness method (see section 2.3). We could do so by using trusted reference sources for the verification of context information of train travelers and railway personnel, i.e.:

1. Verify the actual context *C* (GPS-location or -velocity) of the train against the context of the traveler:  $C_{\text{train}}$  (location,

velocity) =  $C_{\text{traveler}}$  (location, velocity). The train guard or driver can be used as alternative trusted reference resources.

2. Or, in case of an absence of trusted reference sources by comparing the context *C* of the traveler with the contexts of other travelers in that train:  $C_{\text{travelers}}$  (velocity) =  $C_{\text{traveler}}$  (velocity).

We have implemented the first option and require that the traveler must be in the vicinity of the train guard in order to gain access to restricted resources. For this option, the location of the train guard needs to be distinguished from those of the travelers. The train guard is therefore also equipped with a GPS-receiver in the same constellation as an ordinary traveler described above. Linking the location of the traveler with the right train guard is implemented via a unique identifier: the number of the train wagon associated with the train guard. During the activation of his GPS-account, the train guard enters the numbers of the train wagons he is controlling. These numbers are unique and typically displayed above the door inside the train. If the traveler enters the train, she also has to enter the number of the train wagon before access is granted to train traveler services. The train wagon number thus links the traveler with the train guard in the same train. Moreover, locating train guards and comparing their context with numerous travelers' contexts may impose a huge load on the access controller. The use of this identifier reduces this load.

In case of an absence of trusted reference points the second option becomes valid. This option requires a database search for all travelers with a similar velocity and location. If travelers give the unique number of the train then the database search becomes much easier. In case there are no other travelers that have a corresponding profile, it depends on the policy whether the traveler is granted access or not.

We note that the privacy of the trusted, i.e., the train guard, and untrusted, i.e., the other travelers, reference parties is preserved in our scenario since the context broker anonymizes all context information. Train travelers will never have access to context information of the guard. Context information of the trusted reference parties, however, is flagged differently than that of the other context owners for better distinction. Normally, the service provider owns the context information of the trusted reference party.

The up-to-datedness of the contextual information is of crucial importance and must be verified frequently. The GPS-client software therefore typically updates the location information every few seconds.

### 4. CSAC EVALUATION

Comparing our CSAC solution with traditional measures we observe various benefits. The CSAC solution proposed does not require such complex but static mechanisms like PKI or username/password infrastructures. Furthermore, it offers access control mechanisms of various strengths that can adapt to user, group and environmental situational contexts. For example, access can be based upon comparison with context of a trusted reference party, the accuracy of the context information, the history of context information, or the number of different context sources such as e.g. location, speed, and heart beat frequency. Obviously, the trustworthiness of the reference party, the quality of the context, and the number of context sources will have an impact on

the level of access control. Additionally, it can be performed continuously and transparently without bothering the user – therefore it is less intrusive. Users don't have to remember numerous passwords any more. It can preserve various levels of privacy through anonymization by decoupling of context information from the user identity. It also can provide evidence to absolve innocent users. For instance, if an illegal activity has taken place from a user account at a certain location, the owner of that account might be able to prove he was at a different location at the time the activity took place. Last but not least, it can provide higher access control levels in combination with traditional measures like username/password or certificates.

Several drawbacks of our CSAC solution, however, can also be identified. It requires an infrastructure for the collection, management, interpretation, and controlled release of context information. Furthermore, if security solely depends on context information, the level of security might not be as high as traditional solutions. Additionally, the signaling overhead of periodic polling for fresh context information and the verification of it might be too much for many context-aware infrastructures. The frequency of the verification process depends typically on the type of context information and the policy of the service provider. Another drawback is that the flexibility of security that is introduced by using context information might result in complex security policies. Finally, context aware security requires verification of the context information. Useful verification methods strongly depend on the type of context and might be complex. For example, in the absence of a trusted reference party, collusion among train travelers might hamper the verification process. It might even introduce 'ghost trains' that exist based on false context claims of a group of users have a collusion. To prevent such situations, other context sources need to be used, like e.g. train schedules. It also depends on the access policy of the service provider and relates to the trade-off between security and economic usability.

It is difficult to explicitly discuss a cost-benefit trade-off of the usage of context information for security purposes. Such a discussion depends on the value of the services or resources that require access control. Our solution provides an additional security measure to enhance existing solutions, or may, in certain situations, serve as an alternative to the existing security solutions.

For our implementation we have chosen for a solution that includes a context provider and broker. At first sight, a more logical way would be to let the context owner directly provide the context information to the service provider. This option for direct context exchange between the context owner and service provider, however, will in a heterogeneous pervasive computing environment result in major scalability and interoperability issues. Moreover, a specific browser plug-in is required to be able to communicate context information directly to the service provider.

For the context information verification process it is important that both the train guard and the traveler are polled at more or less the same time. Polling the traveler 30 seconds later than the guard may result in location and velocity mismatches and loss of service access, even if they are on the same train. The context requester, however, doesn't have any influence on the up-to-datedness of the context information of the traveler that it obtains from the context broker. Time stamping of context information is therefore of utmost important for context-sensitive access control. Only then it

is possible to perform meaningful context verification and context history management. In general, comparing similar types of context information may result in conflicts. Conflict resolution of context information has to take into account the accuracy of the information, time aspects, and the trust level of the obtained information. Indulska et al. have presented a conflict resolution algorithm for location information [28].

Context information needs to be protected against unauthorized access and distribution to preserve the user's privacy. In the IETF GeoPriv Working Group requirements for a protocol-independent model for the access to geographic location information have been defined [29]. Similar requirements hold for other types of context information. For our prototype we have assumed that there is a trusted relationship between the context owner and broker. It is the context owner who decides if the context aware service provider is allowed to obtain context information via the Context Ticket. As all the context communication is done via http primitives, the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) could potentially be useful to specify the policies regarding access to context information [30].

We used a single train-traveler scenario to better explain our ideas about context sensitive access control. Nevertheless, the context sensitive access control concept might be applicable to medical or domestic settings as well:

- Medical records of a patient in a hospital can be read by a clinician when (s)he is in the proximity of the computer [2].
- Permission to talk to a resident in other room via the intercom may depend on the activity in which the resident is currently involved [3].

## 5. CONCLUSIONS AND FUTURE WORK

Security in context aware environments will require solutions very different from those of today's systems, which are predicated on relatively stable, well-defined, consistent configurations, static contexts, and participants of security arrangements. For instance, traditionally a user authentication mechanism is considered secure if it is a combination of something the user has, something the user knows, or something the user is. What is needed can be characterized by the term 'conformable security', in which the degree and nature of security associated with any particular type of action will change over time, with changing circumstances and with changing available information so as to suit the context [31].

We have added context awareness as a fourth dimension to security. Context sensitive security exploits the ability to sense and use contextual information to augment or replace traditional user attributes such as username/password for the purpose of authentication and access control by making security less intrusive and adaptable to situational or contextual changes. We have demonstrated this by regarding the access control process as a context aware service, whose objective is to grant or deny the access of a supplicant to a resource (e.g., a service) based on context information.

Smart usage of contextual information provides a powerful approach for controlling access to online resources that in many situations is more suitable than the current identity-based solutions. Recognition of behavior patterns and usage of togetherness principles make security smarter, more similar to our



natural security intuition, and therefore less intrusive. Context aware security solutions, however, should be viewed in their proper context. Different security approaches provide variable levels of protection for variable security properties at variable cost. The challenge is to find an acceptable level of security at an acceptable price (costs and user-friendliness).

Compared to traditional access control systems, context-sensitive access control introduces several challenges for future work:

- Context-based access control allows for multiple points of access (e.g. location, temperature and velocity) instead of a single one for conventional systems (identity). This offers flexibility but also complexity that should be dealt with in an appropriate way.
- The level of access security will be variable for a context-sensitive system and constant for a conventional system. The access levels to a service could be based on certain thresholds that depend on the user's behavior or contextual situation. Deviation from usual behavior or falling outside some context may alter the access level to prevent potential abuse of privileges. Introducing fuzzy logic in the access control process is an interesting topic for further research [32].
- Multiple administrative entities will be involved in a context-sensitive access control system, whereas only a single entity is involved in a conventional system. This requires an infrastructure that facilitates trusted cross-domain context exchange.
- Though we claim to be flexible, the implemented access policies are handcrafted in advance: they are not generated on the fly by an access control engine that explores context information concerning e.g. service usage patterns, learns and derives the most appropriate access control model. In order to make the access control process truly dynamic and transparent, context aware security policies need to be generated on the fly as well. Introducing context parameters as part of the policy ('user X has access to service Y if he is in the building') and using the access control model learned over time to functionally adapt those policies could result into more robust, flexible and scalable access control solutions. To obtain access control policies that relate to such control solutions and that depend on the situational context of individual or a group of users will be certainly one of our main challenges of the future.

## 6. ACKNOWLEDGMENTS

This work was carried out as part of the Mobile&Wireless2004 project and Freeband AWARENESS project, which is sponsored by the Dutch government under contract BSIK 03235.

## 7. REFERENCES

- [1] Hulsebosch, B., Salden, A., and Bargh, M. Context-Based Service Access for Train Travelers. In Proceedings of the 2<sup>nd</sup> European Symposium on Ambient Intelligence (EUSAI), Markopoulos et al. (Eds.), LNCS 3295, 84-87, Eindhoven, the Netherlands, 2004.
- [2] Bardram, J.E., Kjær, R.E., and Pedersen, M.Ø. Context-Aware User Authentication – Supporting Proximity-Based Login in Pervasive Computing. In Proceedings of Ubicomp 2003 – Ubiquitous Computing, Vol. 2864 of Lecture Notes in Computer Science. Springer-Verlag, Seattle, Washington, USA, 2003, 107–123.
- [3] Covington, M.J., Long, W., Srinivasan, S., Dey, A.K., Ahamad, M., Abowd, G.: Securing Context-Aware Applications Using Environment Roles. In Proceedings of the 6th ACM Symposium on Access Control Models and Technologies (SACMAT), Chantilly, Virginia, USA, 2001.
- [4] Moyer, M. and Ahamad, M. Generalized Role-Based Access Control. In Proceedings of the 2001 International Conference on Distributed Computing Systems (ICDCS), Mesa, AZ, 2001.
- [5] Wullems, C., Looi, M., and Clark, A. Towards Context-Aware Security: An Authorization Architecture for Intranet Environments. In Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshop (PERCOMW'04), March 14 - 17, 2004, Orlando, Florida, USA.
- [6] Zhang, G. and Parashar, M. Context-Aware Dynamic Access Control for Pervasive Applications. In Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), 2004 Western MultiConference (WMC), San Diego, CA, USA, Society for Modeling and Simulation International (SCS), January 2004.
- [7] Bacon, J., Moody, K., and Yao, W. Access Control and Trust in the Use of Widely Distributed Services. In Middleware 2001, volume 2218 of Lecture Notes in Computer Science, pages 295-308, Springer-Verlag, 2001.
- [8] Hada, S. and Kudo, M. XML Access Control Language: Provisional Authorization for XML Documents, October 2000, Tokyo Research Laboratory, IBM Research.
- [9] XACML 1.0 Specification, [www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf](http://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf).
- [10] Air Marshals Keep Close Eye on Travelers, NewsMax Wires, April 2004, Associated Press.
- [11] Waterman, S. TSA looking at new screening techniques, The Washington Times, 3 October 2004.
- [12] Salden, A. H. and Kempen, M. Sustainable Cybernetics Systems - Backbones of Ambient Intelligent Environments. In Remagnino, P., Foresti, G.L., and Ellis, T. (eds.), Ambient Intelligence, Springer, November 2004.
- [13] Ferraiolo, D.F., Barkley, J.F., and Kuhn, D.R. A Role-Based Access Control Model and Reference Implementation Within a Corporate Intranet. *ACM Transactions on Information and System Security*, February 1999, 2, 34-64.
- [14] Ferraiolo, D. and Kuhn, D.R. Role-Based Access Controls. In Proceedings of 15th NIST-NCSC National Computer Security Conference, pages 554-563, Baltimore, MD, October 13-16 1992.
- [15] Bhatti, R., Bertino, E., and Ghafoor, A. A Trust-based Context-Aware Access Control Model for Web-Services.



- In Proceedings of the 3rd International Conference on Web Services (ICWS), San Diego, July 2004.
- [16] Denning, D.E., and MacDoran, P.F. Location-Based Authentication: Grounding Cyberspace for Better Security. In *Computer Fraud & Security*. Elsevier Science Ltd. (1996).
  - [17] Brands S. and Chaum, D. Distance-Bounding Protocols, *Proc. Eurocrypt 1993*, Lecture Notes in Computer Science, no 765, Springer-Verlag, pp. 344,359.
  - [18] Waters, B. and Felten, E. Proving the Location of Tamper Resistent Devices, [http://www.cs.princeton.edu/~bwaters/research/location\\_proving.ps](http://www.cs.princeton.edu/~bwaters/research/location_proving.ps).
  - [19] Waters, B. and Felten, E. Secure, Private Proofs of Location, Princeton University Computer Science Technical Reports, TR-667-03, January 2003.
  - [20] Sastry, N., Shankar, U., and Wagner, D. Secure verification of Location Claims. *ACM Workshop on Wireless Security (WiSe 2003)*. September 19, 2003.
  - [21] Balfanz, D., Smetters, D.K., Stewart, P., and Wong, H.C. Talking to Strangers: Authentication in Ad-Hoc Wireless Networks. In *Proceedings of Network and Distributed System Security Conference*, February 6-8; San Diego; CA; USA. 2002.
  - [22] Kindberg, T., Zhang, K., and Shankar, N. Context Authentication Using Constraint Channels. *Fourth IEEE Workshop on Mobile Computing Systems and Applications*, June 20 - 21, 2002, Callicoon, New York, USA.
  - [23] Orr, R.J. and Abowd, G.D. The Smart Floor: A Mechanism for Natural User Identification and Tracking. In *Proceedings of the 2000 Conference on Human Factors in Computing Systems (CHI 2000)*, The Hague, Netherlands, April 1-6, 2000.
  - [24] Musolesi, M., Hailes, S., and Mascolo, C. Prediction of Context Information Using Kalman Filter Theory, UCL Internal Research Note. June 2004.
  - [25] Ranganathan, A., Al-Muhtadi, J., and Campbell, R. Reasoning About Uncertain Contexts in Pervasive Computing Environments, *IEEE Pervasive Computing Magazine*, volume 3, no. 2, April-June 2004.
  - [26] Mäntyjärvi, J., Himberg, J., and Huuskonen, P. Collaborative Context Recognition for Handheld Devices. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom 2003)*, pp. 161-168, Dallas-Fort Worth, Texas, USA, 2003.
  - [27] De Heer, J., Tokmakoff, A., Eertink, H., and Anijs, J. Uluru: Mobile Interactive Multimedia Experimental Service Environment. In *ERCIM News No 54*, Special issue on Applications and Platforms for the Mobile User, 2003.
  - [28] Indulska, J., McFadden, T., Kind, M., and Henricksen, K. Scalable location management for context-aware systems. In *Proceedings of the 4th International Conference on Distributed Applications and Interoperable Systems, DAIS 2003*, volume 2893 of *Lecture Notes in Computer Science*, pages 224-235, Paris, France, November 19-21 2003. ENST, Springer-Verlag.
  - [29] Cuellar, J., Morris, J., Mulligan, D., Peterson, D., and Polk, D. Geopriv Requirements, RFC 3693, IETF GeoPriv Working Group, February 2004.
  - [30] Rosenberg, J. The Extensible Markup Language (XML) Configuration Access Protocol (XCAP), draft-ietf-simple-xcap-04, work in progress, October 2004.
  - [31] IST Advisory Group, Trust, dependability, security and privacy for IST in FP6, European Commission, 2002, [ftp://ftp.cordis.lu/pub/ist/docs/istag\\_kk4402464encfull.pdf](ftp://ftp.cordis.lu/pub/ist/docs/istag_kk4402464encfull.pdf)
  - [32] Ghosh, S., Razouqi, Q., Schumacher, H.J., and Celmins, A. A Survey of Recent Advances in Fuzzy Logic in Telecommunications Networks and New Challenges, *IEEE Transactions on Fuzzy Systems*, Vol. 6, No. 3, August 1998, pp. 443-447.