An Access Control Model for Mobile Physical Objects

Florian Kerschbaum
SAP Research
Karlsruhe, Germany
florian.kerschbaum@sap.com

ABSTRACT

Access to distributed databases containing tuples collected about mobile physical objects requires information about the objects' trajectories. Existing access control models cannot encode this information efficiently. This poses a policy management problem to administrators in real-world supply chains where companies want to protect their goods tracking data. In this paper we propose a new access control model as an extension to attribute-based access control that allows trajectory-based visibility policies. We prove the security properties of our novel authentication protocol for distributed systems that can supply the decision algorithm with the necessary reliable information using only standard passive RFID tags. As a result companies will be able to improve confidentiality protection and governance of their object tracking data and more trustingly engage in data sharing agreements.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection—*Access control*; C.2.4 [**Computer-Communication Networks**]: Distributed Systems—*distributed applications*

General Terms

Security, Algorithms

Keywords

Access Control, Distributed Databases, RFID, Supply Chain Management

1. INTRODUCTION

Imagine a set of mobile physical objects $O_1, \ldots, O_m$ each traversing a (potentially different) subset of players $X_1, \ldots, X_n$. Each player X_i collects information about each object O_j it handles, e.g., time, place, type of action, etc., and stores this information in its local database. Later other players may ask for access to an object's data in this database.

SACMAT'10, June 9–11, 2010, Pittsburgh, Pennsylvania, USA.

This scenario is common place in modern supply chains [40]. Companies are adopting object-level tracking in their supply chains, either because of the business benefits, such as some retailers, or because of regulations, such as the pharmaceutical industry. Radio frequency identification (RFID) technology [16] provides the means to equip and capture each object with an unique identifier. Data commonly collected includes time, location and type of handling, e.g., packing, unpacking, receiving, or shipping.

On the one hand, combining this data from many companies (just predecessor and successor is almost always insufficient) along the supply chain enables or improves many economically attractive collaborative applications, such as batch recalls [46], counterfeit detection [43], benchmarking and analytics [27, 28, 29] or estimated arrival forecasts [12]. We therefore expect an increasing interest by companies to adopt object-level tracking technology. On the other hand, too liberal sharing of this information allows espionage on one's business operations [32, 39]. We observe this as a major obstacle to wider adoption.

Companies are usually part of many supply chains (even for the same product) all managed using the same database. Specifying access control rules for this database can be very delicate. Consider the following two examples:

It is common place, e.g., in the automotive industry, that suppliers sell their products to competing companies. Imagine a supplier S_1 selling a product p_1 to buyers B_1 and B_2. If B_1 has access to all scheduled orders for p_1, he can infer the volume of future business with B_2. This can be very sensitive, in case S_1 has to cancel some orders due to a temporary capacity reduction, e.g., a machine failure. B_1 could then infer whether B_2's orders are treated preferentially.

While this decision can be based on local information in the case of bridging only one supply chain stage, it becomes difficult in case of a tier-2 supplier. Imagine a supplier S_2 selling product p_2 to S_1 which is then used to produce p_1. If either B_1 or B_2 contacts S_2 requesting data, S_2 cannot decide which object was shipped to which buyer. If S_2 would grant access to all items, B_1 could infer again the volume of business of B_2.

A naturally emerging access rule is to share data with partners about shared objects, i.e. objects both partners have possessed. This implements the important business concept of visibility, i.e. each partner gains (additional) information about how its (entire) supplies are produced and how its (entire) products are used, but still provides a separation between different supply chains merging at one company. Furthermore it can be easily adopted reciprocally, i.e.

"I give you access, if you give me access", providing a fair allocation of cost, risk and benefits.

We distinguish between down-stream and up-stream visibility. In down-stream visibility a company is allowed to access data associated with its objects shipped to its supply chain partners (at those partners). Up-stream visibility is the reverse and a company is allowed to access data associated with objects it has received from its supply chain partners (again at those partners).

Setting these visibility policies correctly using existing access control models can be excruciatingly difficult, since the access control matrix can be huge ($n \times m$) and each object can have a different trajectory (Section 2.2). First, we show how these policies can be implemented using a novel attribute in the framework of attribute-based access control (Section 2.3) and how to encode it using XACML (Section 2.4) Then we show how to implement this attribute using a novel protocol with standard passive RFID tags (Section 3). Finally we compare our work to existing access control models (Section 4) and outline future extensions (Section 5).

Our summarized contributions are

- Definition of visibility policies.
- Analysis of the complexity managing these policies using existing access control models, e.g., role-based access control (RBAC).
- Integration of the policies into the framework of attribute-based access control which enables companies to combine them with existing models (including RBAC).
- A novel protocol for implementing the necessary attributes on standard passive RFID tags without relying on secret information.

2. SUPPLY CHAIN VISIBILITY POLICIES

2.1 Definition

We first formally define the trajectory of an object O_j and then define upstream and downstream visibility policies.

Let there be n players $X_i \in \mathbb{X} = \{X_1, \ldots, X_n\}$.

We model the trajectory $\mathcal{L}(O_j) = \langle \mathbb{L}_j, \mathbb{R}_j \rangle$ of object O_j as a totally ordered set consisting of elements in the set $\mathbb{L}_j \subseteq \mathbb{X}$ and a binary relation $\mathbb{R}_j \subseteq \mathbb{L}_j \times \mathbb{L}_j$. The players represent the spatial domain of the trajectory and the players in $\mathbb{L}_j$ are those that have handled (possessed) the object O_j. The relation $\mathbb{R}_j$ models the temporal domain of the trajectory. Simply speaking, a player X_i is ranked lower than a player $X_{i'}$ in $\mathcal{L}(O_j)$, i.e. $\langle X_i, X_{i'} \rangle \in \mathbb{R}_j$, if X_i handled the object O_j earlier than $X_{i'}$. We write $\sigma(X_i, \mathcal{L}(O_j))$ for a predicate that can be used to compute the rank of player X_i in $\mathcal{L}(O_j)$ and $|\sigma(X_i, \mathcal{L}(O_j))|$ for the evaluated rank itself. I.e. $|\sigma(X_i, \mathcal{L}(O_j))| < |\sigma(X_{i'}, \mathcal{L}(O_j))|$ iff $\langle X_i, X_{i'} \rangle \in \mathbb{R}_j$. If player X_i did not handle the object O_j, then $|\sigma(X_i, \mathcal{L}(O_j))|$ is undefined and any order relation on the natural numbers, e.g. both $<$ and $>$, should always evaluate to false. We say the least element in $\mathcal{L}(O_j)$ is the source of object O_j and the top most element is its destination.

We can now capture the notion of being part of multiple supply chains that we briefly informally introduced in the introduction. A player X_i is part of multiple supply chains, if at least two objects that it handled have been handled by at least one player each – both upstream or downstream – which did not handle both objects. Formally iff X_i is part of two supply chains, then there exist two other players $X_{i'}$ and $X_{i''}$ and two objects O_j and $O_{j'}$, such that

$$X_i \in \mathbb{L}_j, X_i \in \mathbb{L}_{j'}$$
$$X_{i'} \in \mathbb{L}_j, X_{i'} \notin \mathbb{L}_{j'}$$
$$X_{i''} \notin \mathbb{L}_j, X_{i''} \in \mathbb{L}_{j'}$$

$$\begin{aligned} \big(|\sigma(X_i, \mathcal{L}(O_j))| &< |\sigma(X_{i'}, \mathcal{L}(O_j))| \wedge \\ |\sigma(X_i, \mathcal{L}(O_{j'}))| &< |\sigma(X_{i'}, \mathcal{L}(O_{j'}))|\big) \vee \\ \big(|\sigma(X_{i'}, \mathcal{L}(O_j))| &< |\sigma(X_i, \mathcal{L}(O_j))| \wedge \\ |\sigma(X_{i''}, \mathcal{L}(O_{j'}))| &< |\sigma(X_i, \mathcal{L}(O_{j'}))|\big) \end{aligned}$$

For simplicity we omit modeling a player handling an object more than once (e.g. product returns), although visibility policies are still valid and applicable.

Now a player X_i is requesting information from player X_v (verifier) about object O_j stored in X_v's database. Player X_v intercepts this request and performs an access control decision. The intercepting component is called a policy enforcement point (PEP) and the information about the request, e.g. the identity of the requestor X_i and the unique identifier of the object O_j are forwarded to the policy decision point (PDP). The PDP compares the information to the policies in its store and returns its evaluation decision (grant or deny) to the PEP.

DEFINITION 1. *An* up-stream visibility policy *grants (or denies) access to X_i for O_j based on the predicate evaluation*

$$|\sigma(X_i, \mathcal{L}(O_j))| < |\sigma(X_v, \mathcal{L}(O_j)|$$

DEFINITION 2. *A* down-stream visibility policy *grants (or denies) access to X_i for O_j based on the predicate evaluation*

$$|\sigma(X_v, \mathcal{L}(O_j))| < |\sigma(X_i, \mathcal{L}(O_j)|$$

2.2 Management of Visibility Policies

Existing access control models are faced with a serious scalability problem when protecting object-level data with visibility policies. There is a huge number of items (m) and each item requires unique protection corresponding to its trajectory. Its authorization matrix

$$\textit{player} \times \textit{object} \times \textit{access}$$

is therefore huge and diverse at the same time, since there exists no natural grouping of objects.

The most successful method to reduce the complexity of an authorization matrix, role-based access control (RBAC) [38], does not help in this case, although very often proposed for this purpose [20, 33, 47]. RBAC divides the authorization matrix by introducing a level of indirection via the role concept:

$$\textit{player} \times \textit{role} \qquad\qquad \textit{role} \times \textit{object} \times \textit{access}$$

Although RBAC does not help solving the problem, it fortunately does not hurt either, such that we can integrate its benefits into our model without detrimental effects.

In a supply chain one can assign roles vertically or horizontally. If the roles are assigned vertically as in the left picture of Figure 1, i.e. each stage (e.g., distributor or manufacturer) has its own role, then there is no distinction between companies at one stage and each company can read

the data for each object, even if it was not handled by him. This lack of distinction can be particularly sensitive, since the companies on one stage are often competitors and the gained information is particularly likely to be abused. If the roles are assigned horizontally as in the right picture of Figure 1, i.e. each trajectory through the set of players has its own role, then access control cannot be assigned before the good has been shipped to the final stage and each company needs to be informed about every shipping process. Also there are as many roles as trajectory which is more than there are players in the system.

It is almost needless to point out that access control models that further extend the authorization matrix provide no help in managing mobile objects, e.g. Task-Based Authorization Control (TBAC) [45] or Generalized Temporal Role-Based Access Control (GTRBAC) [25] to name a few. In order to simplify administration of visibility policies we can reduce the authorization matrix. Since the concept of visibility is independent of the players on the trajectory of an object, we can abstract from players in the authorization matrix and reduce it to

$$\textit{object} \times \textit{visibility policy}$$

Being even more restrictive we could further group objects, e.g., one can set a visibility policy for all objects of one product group. This reduces the authorization matrix to

$$\textit{object-group} \times \textit{visibility policy}$$

While this model is very restrictive, it is definitely also very simple and the administration effort is easily practically manageable in many real-world supply chains.

2.3 ABAC Integration

Fortunately we can combine this visibility policy authorization matrix with the expressiveness of sophisticated access control models without necessarily sacrificing simplicity of administration. The unifying model is attribute-based access control (ABAC) [35].

This unification is important, since visibility policies can efficiently express access control policies necessary in many supply chains, but they are not sufficient in many cases. Companies may want to grant access to their object data to players outside of the supply chain. Examples are auditors or other service providers that provide outsourced services operating on object data. Also companies may want to restrict access to partners, although they are part of the supply chain. Examples are competitors or otherwise non-cooperating organizations.

We therefore integrate the notion of visibility policies into the ABAC framework. Our integration is efficient and does not re-introduce the scalability problems described in Section 2.2. The ABAC framework integrates the features and expressive power of many access control models, including the classics RBAC, discretionary access control (DAC) and mandatory access control (MAC). We briefly review the policy model from Yuan and Tong [49] in a simplified form – we leave out environments and their attributes which are necessary to also include access control models such as TBAC or GTRBAC.

- There are subjects and resources.
- $SA_l (1 \leq l \leq L)$ and $RA_m (1 \leq m \leq M)$ are the existing attributes for subjects and resources, respectively;
- $ATTR(s)$ and $ATTR(r)$ are attribute assignment relations for subject s and resource r, respectively:

$$\begin{aligned} ATTR(s) &\subseteq SA_1 \times SA_2 \times \cdots \times SA_L \\ ATTR(r) &\subseteq RA_1 \times RA_2 \times \cdots \times RA_M \end{aligned}$$

- A policy rule that decides on whether a subject s can access a resource r, is a Boolean function of s's and r's attributes:

$$access(s, r) \leftarrow f(ATTR(s), ATTR(r))$$

  Given the attribute assignments of s and r, if the function f evaluates to true, then access to the resource is granted; otherwise access is denied.

Identity itself and roles become attributes of the subject and ownership in DAC becomes an attribute of the resource. Also, in MAC clearance becomes an attribute of the subject and classification an attribute of the resource.

In our case subjects are the players X_i and the resources are objects O_j, but for mobile physical objects the situation is unfortunately slightly more complicated. The predicate $\sigma(X_i, \mathcal{L}(O_j))$ in visibility policies depends on both player (X_i) and object (O_j). Therefore if we want to express upstream or downstream visibility as an attribute, we need to introduce a new type of attribute into the ABAC model. Our extension of the model is as follows:

- $SRA_k (1 \leq k \leq K)$ are the existing attributes for pairs of subjects and resources.
- $ATTR(s, r)$ is the attribute assignment relation for a pair of subject s and resource r:

$$ATTR(s, r) \subseteq SRA_1 \times SRA_2 \times \cdots \times SRA_K$$

- We extend the Boolean function for policy evaluation to s's, r's and both s and r's attributes:

$$access(s, r) \leftarrow f(ATTR(s), ATTR(r), ATTR(s, r))$$

We instantiate our ABAC model for visibility policies with the following two attributes: one for downstream and one for upstream partners.

$$SRA_h = \text{“}\textit{downstream}\text{”} \qquad SRA_{h+1} = \text{“}\textit{upstream}\text{”}$$

We can implement the assignment of these attributes as an evaluation of the predicates. When receiving $s = X_i$, $r = O_j$, $\sigma(X_v, \mathcal{L}(O_j))$, and $\sigma(X_i, \mathcal{L}(O_j)$ in an access request, player X_v can evaluate the predicates and assign corresponding attributes.

$$|\sigma(X_v, \mathcal{L}(O_j))| < |\sigma(X_i, \mathcal{L}(O_j)| \implies$$

$$ATTR(s, r) = \{\text{“}\textit{downstream}\text{”}\}$$

$$|\sigma(X_i, \mathcal{L}(O_j))| < |\sigma(X_v, \mathcal{L}(O_j)| \implies$$

$$ATTR(s, r) = \{\text{“}\textit{upstream}\text{”}\}$$

Our visibility policies can then be formulated as

$$\begin{aligned} access(s, r) \leftarrow\ & \text{“}\textit{downstream}\text{”} \in ATTR(s, r) \vee \\ & \text{“}\textit{upstream}\text{”} \in ATTR(s, r) \end{aligned}$$

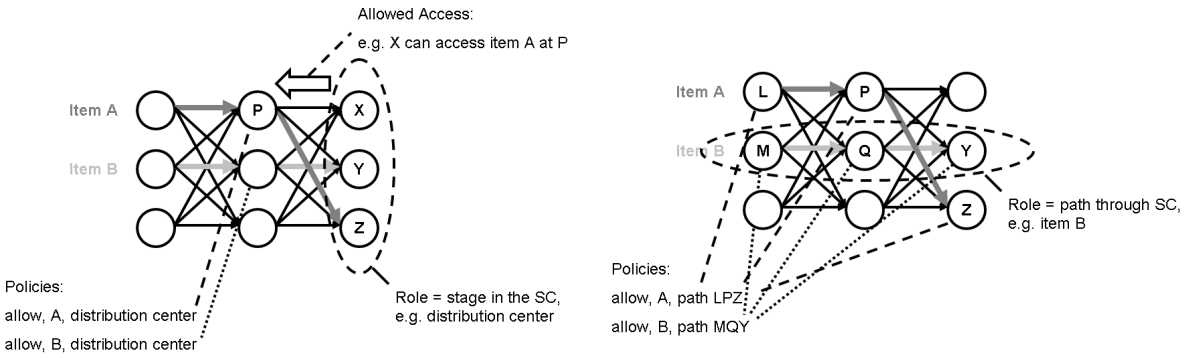

Figure 1: Vertical and horizontal assignment of roles

We can also include or exclude supply chain partners as in our examples above

$$\begin{aligned} access(s,r) \quad \leftarrow \quad & \text{“}auditor\text{”} \in ATTR(s) \vee \\ & \Big((\text{“}downstream\text{”} \in ATTR(s,r) \vee \\ & \text{“}upstream\text{”} \in ATTR(s,r) \Big) \wedge \\ & \text{“}competitor\text{”} \notin ATTR(s) \Big) \end{aligned}$$

2.4 XACML Encoding

Given such an abstract model the challenge of access control administration now becomes to be able to efficiently and flexibly specify the Boolean function f. Yuan and Tong [49] provide an implementation to express their attributes in XACML [36]. Following their example we encode our visibility policy example in XACML, but since XACML also does not support attributes on subjects and resources combined either, we encode them as environment attributes and check them using a condition. The condition encoding for predicate evaluation is very intuitive, but we need to extend it with expressions tying the predicate attributes to the subject and resource attributes in order to preserve the integrity of the predicate. In the example the evaluation of the values (ranks) of the predicates could be even omitted, since it always evaluates to true. Listing 1 shows the example in a simplified form for readability.

We show the details of the request in Section 3.4. The other policy aspects regarding subjects in our example can be specified using independent rules in a straightforward manner. We encode the exclusion of the competitor as a separate rule due to the lack of a “not-equal” matching function, but an administrator must take care that such translations do not change the effect.

```
<Policy RuleCombiningAlgId="first-applicable">
 <Rule Effect="Permit">
  <Target>
   <Subject>
    <SubjectMatch FuncId="string-equal">
     <AttrValue>auditor</AttrValue>
     <SubAttrDes AttrId="subject"/>
    </SubjectMatch>
   </Subject>
  </Target>
 </Rule>
 <Rule Effect="Deny">
  <Target>
   <Subject>
    <SubjectMatch FuncId="string-equal">
     <AttrValue>competitor</AttrValue>
     <SubAttrDes AttrId="subject"/>
    </SubjectMatch>
   </Subject>
  </Target>
 </Rule>
 <Rule Effect="Permit">
  <Condition>
   <Apply FuncId="and">
    <Apply FuncId="string-equal">
     <SubAttrDes AttrId="subject"/>
     <EnvAttrDes AttrId="req-pred-player"/>
    </Apply>
    <Apply FuncId="string-equal">
     <ResAttrDes AttrId="resource"/>
     <EnvAttrDes AttrId="req-pred-object"/>
    </Apply>
    <Apply FuncId="or">
     <Apply FuncId="integer-greater-than">
      <EnvAttrDes AttrId="req-pred-value"/>
      <EnvAttrDes AttrId="own-pred-value"/>
     </Apply>
     <Apply FuncId="integer-less-than">
      <EnvAttrDes AttrId="req-pred-value"/>
      <EnvAttrDes AttrId="own-pred-value"/>
     </Apply>
    </Apply>
   </Apply>
  </Condition>
 </Rule>
 <Rule Effect="Deny"/>
</Policy>
```

Listing 1: Simplified Example XACML Policy

In summary, we can integrate the many access control models covered by ABAC and our visibility policies. Our integration promises to be still efficiently manageable for administrators, since both traditional access control and visibility can be expressed with a few rules in the same standardized language of XACML. In the next section we show how to implement the predicates in a distributed system.

3. AUTHENTICATION USING RFID

In order to enforce visibility policies the player must be able to reliably compute the predicate $\sigma(X_i, \mathcal{L}(O_j))$ of an object's trajectory and supply it as attributes in the access request to the PDP. This is challenging, since the necessary

information about the trajectory is distributed across multiple players and need not be known to the player. Each player knows by default only his predecessor and successor from physically moving the object which is even insufficient to determine its own rank in the trajectory. Therefore the requestor must supply the predicate, but of course the information is unreliable, since he should not necessarily be trusted. The player must verify the supplied predicate.

This problem is an extension of the authentication problem in distributed systems. Clearly authentication is a prerequisite for any access control, but as seen before our predicate is an attribute of subject and resource, and as such common identity verification mechanisms fall short of solving the problem. Nevertheless, similar to the most common solutions for the authentication problem in distributed problems, we can resort to cryptographic techniques.

We are concerned about physical objects (equipped with an RFID tag each) and a player needs to prove possession of this object. Differently from the ownership authentication factors – "something you have" – our authentication must succeed even if the player is no longer in possession of the object – "something you had". This complicates the problem, since it rules out solutions of simply interactively using RFID for access control [7, 41].

The notion of (current) possession has been explored before and extended to securely verifying ownership of an RFID tag [34, 42]. This concept already has many applications for mobile physical objects in supply chains, but, e.g. for any form of analytics, authentication and possession are decoupled. Also as pointed out in [13] these protocols still suffer from security flaws.

The problem of authenticating based on (past) possession of RFID tags has been first considered in [30]. Yet these protocols do not allow implementing our predicate, but simply allow a decision whether an item has been in possession. They therefore do not allow a distinction between upstream and downstream.

Our authentication relies on a similar mechanism as the proofs of possession from [18]. A proof of possession is in our terms a verifiable predicate which can be supplied during the access request. Unfortunately all solutions proposed in [18] are either not reliable in our attacker model or are not realizable in our system model. A different design is therefore needed.

3.1 System Model

We continue our model with multiple players, but restrict ourselves in this section to one object O_j which is the one considered in the access request. One player (X_v) is the designated verifier of the predicate.

We assume each player is uniquely identifiable and the availability of a public-key infrastructure to securely distribute public keys for each player.

Besides the basic capabilities for communication, we only assume the availability of re-writeable permanent storage on the RFID tag. Passive tags (without own source of power) with up to 64 KBytes of storage are available [17] and follow the EPC Gen 2 protocol which is commonly used in supply chains [1].

Note that we do not consider cryptographic capabilities on the RFID tag, such as symmetric encryption [15] or public-key cryptography [5, 8, 21]. We emphasize that is a very strong restriction of the solution space. It implies that the RFID tag cannot manage secret material, such as cryptographic keys or even passwords. It therefore rules out any solution transferring common concepts from distributed systems authentication. E.g., signing challenges by the RFID tag using message authentication codes or public-key signatures which significantly simplify the problem cannot be implemented in our model. We do this in order to address the security problems of existing and currently emerging deployments of RFID in supply chains which do not yet have these cryptographic capabilities.

Before the access request and the problem of authentication, several operations are performed using the RFID tag. We use a simplified model from [30].

Assume Trent (T) is a trusted third party that supports players in obtaining RFID tags. A natural choice is the RFID manufacturer. Note that Trent does not obtain any additional information about the supply chain operation than any RFID manufacturer already does now. Our authentication consists of the following algorithms or protocols.

Initialize: A player Alice requests a (or a set of) RFID tags from Trent. She can later use those to attach to newly created objects.

Move: A player Alice moves an object to another player Bob. She updates the information stored on the attached RFID tag. We emphasize that this operation does not require network access to Trent or Bob.

Authenticate: The requestor sends a verifiable predicate $\sigma(X_i, \mathcal{L}(O_j))$ for access to the verifier. The verifier makes an access control decision based on this predicate (and its policies).

3.2 Security Model

We assume secure and authenticated communication over the network, i.e. between the players and Trent. We assume insecure communication with the RFID tag attached to the object.

Our attacker controls the requestor (X_i) and may control any other player except the verifier (X_v) and Trent, i.e. we consider almost *arbitrary collusion*. Our attacker is *adaptive*, i.e. the set of controlled players may change over time.

Definition 3. *An admissible attacker A is a sequence of subsets $\mathbb{A}_l \subset \mathbb{X}$ $(l = 1, \ldots, \lambda)$ of players none of which contains the verifier (X_v) or Trent:*

$$\mathbb{A}_l \cap \{X_v, T\} = \emptyset$$

Our main security guarantee is the non-forgeability of the verifiable predicate $\sigma(X_i, \mathcal{L}(O_j))$. We state the following theorem.

Theorem 1. *No admissible attacker can forge a verifiable predicate $\sigma(X_i, \mathcal{L}(O_j))$ for $X_i \in \bigcup_l \mathbb{A}_l$ without possession of object O_j by any $X_{i'} \in \bigcup_l \mathbb{A}_l$.*

We defer the proof to Section 3.5 after the description of the protocols.

Note that it is impossible to prevent forgery for an attacker in possession of object O_j. He can simply physical move the object to X_i. Even without physical movement, it is impossible prevent an attacker from forgery, since he has access to all information (no trusted hardware) and can e.g. relay signals from the RFID tag.

An interesting problem not captured by Theorem 1 arises when considering an adaptive adversary. Assume that at

time t_1 X_i has possession of the object O_j and the attacker A has not compromised X_i, i.e. $X_i \notin A_{t_1}$. Later at time $t_2 > t_1$ A compromises X_i, but now he should not be able to perform forgery of predicates for object O_j. We call this property non-transferability, since the attacker wants to transfer the predicate from X_i to another player $X_{i'}$. This property is similar to forward secrecy in key agreement protocols [14]. Non-transferability is important, since it also prevents information leakages in the supply chain by otherwise trustworthy partners.

For the formal definition we synchronize the time between the attacker and the trajectory. For each rank $l = 1, \ldots, |\mathbb{L}_j|$ in the trajectory $\mathcal{L}(O_j)$ there is a corresponding subset $\mathbb{A}_l$ of the attacker A. Since we cannot rely on cryptography on the RFID tag, we need to resort to different security measures. We cannot achieve cryptographic security for non-transferability in our model, because the attacker has access to all necessary information in the system at time t_1 to produce a new system state for time t_2 which cannot be disproved easily. Instead we rely on detection and traceability where more information is available. We refine Theorem 1 as follows.

THEOREM 2. *Let Σ be the set of valid verifiable predicates $\sigma(X_i, \mathcal{L}(O_j))$. No admissible attacker can prevent detection of $X_i \in \bigcup_l \mathbb{A}_l, \sigma(X_i, \mathcal{L}(O_j)) \in \Sigma$ after using a verifiable predicate $\sigma(X_{i'}, \mathcal{L}(O_j)) \notin \Sigma$ as long as*

$$\forall \sigma(X_i, \mathcal{L}(O_j)) \in \Sigma . X_i \notin \mathbb{A}_{|\sigma(X_i, \mathcal{L}(O_j))|}$$

3.3 Protocols

The protocols implementing the authentication are actually quite simple. We only use public-key signatures. Let $S_X()$ denote the signature with X's public key. Since we store the signatures on the RFID tag, it is beneficial to use very short signatures, e.g. [9].

Our protocols chain the information along the object's trajectory. Each supplier is vouching for his buyer, similar to fourth factor authentication [10]. Fourth factor authentication relies on somebody you know in case other authentication factors have failed. Clearly a supplier knows his buyer and they trust each other at least to the extend to engage in business. We therefore use this fourth factor to replace the typical cryptographic authentication factor of knowledge – "something you know" – which is not available on the RFID tag.

Initialize: The trusted third party Trent T sends to player Alice an RFID tag with identifier j which contains in its storage the signature $S_T(j, A)$.

Move: A player Alice (A) wants to move an object to another player Bob (B). She appends to the storage on the RFID tag the recipient's identity (B) and her signature $S_A(j, B)$. Due to storage restrictions on RFID tags we recommend to compress the identity information as much as possible, e.g. using similar approaches as for abbreviation of URLs.

Authenticate: Let $s_1, \ldots, s_k$ be the sequence of signatures stored on the RFID tag attached to object O_j. The requestor X_i sends as the verifiable predicate $\sigma(X_i, \mathcal{L}(O_j))$ this sequence $s_1, \ldots, s_k$. The verifier X_v verifies that

1. s_k conforms to $S_{X_{i_k}}(j, X_i)$.
2. For all $l (1 < l < k)$ s_l conforms to $S_{X_{i_l}}(j, X_{i_{l+1}})$.
3. s_1 conforms to $S_T(j, X_{i_2})$.
4. For all $l (1 \leq l \leq k)$ s_l is valid signature from X_{i_l}.

If all checks are successful, then it evaluates its policies to make the access decision.

3.4 Example

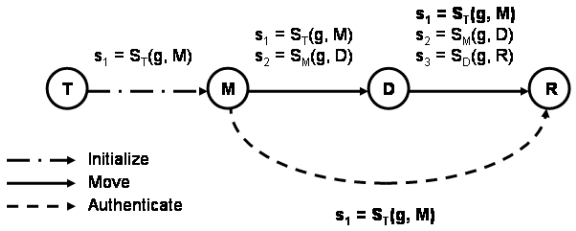

Figure 2: Example of an object traversing a supply chain

We present an example detailing the interactions. Assume a manufacturer M produces a good G. He first starts the **Initialize** protocol by contacting the trusted third party Trent T and requesting an RFID tag. T chooses a tag with identifier g, stores on the tag's memory $s_1 = S_T(g, M)$ and sends the RFID tag to M. M reads $\langle s_1 \rangle$ from the tag, stores it in its database and attaches the tag to the good G.

Now M intends to ship G to its distributor D. He starts the **Move** protocol and appends $s_2 = S_M(g, D)$ to the tag's memory. M can then ship G to D.

When D receives the good G he reads $\langle s_1, s_2 \rangle$ from the tag and stores it in his database. Later D may ship G to the retailer R. In this **Move** protocol he appends $s_3 = S_D(g, R)$ to the tag's memory.

R reads $\langle s_1, s_2, s_3 \rangle$ from the tag of the received good G and stores it in his database. First consider the situation of a downstream request when M requests information from R, e.g., in order to collect sales data or analyze product returns. Figure 2 shows the interations and exchanged data.

M and R run an **Authenticate** protocol. M reads $\langle s_1 \rangle$ from his database and sends it along with g, M to R. R's PEP verifies the data in $\langle s_1 \rangle$ as described in Section 3.3. It extracts M, g and the number of signatures (1) from $\langle s_1 \rangle$. Then it looks up its corresponding predicate $\sigma(R, \mathcal{L}(G)) = \langle s_1, s_2, s_3 \rangle$ in its database and similarly extracts R, g and the number of signatures (3). Listing 2 shows the resulting XACML request sent to the PDP with the predicate information encoded as environment attributes and subject (M) and resource attributes (g).

```
<Request>
 <Subject>
  <Attribute AttributeId="subject">
   <AttributeValue>M</AttributeValue>
  </Attribute>
 </Subject>
 <Resource>
  <Attribute AttributeId="resource">
   <AttributeValue>g</AttributeValue>
  </Attribute>
 </Resource>
 <Environment>
  <Attribute AttributeId="req-pred-player">
   <AttributeValue>M</AttributeValue>
```

```
  </Attribute>
  <Attribute AttributeId="req-pred-object">
   <AttributeValue>g</AttributeValue>
  </Attribute>
  <Attribute AttributeId="req-pred-value">
   <AttributeValue>1</AttributeValue>
  </Attribute>
  <Attribute AttributeId="own-pred-player">
   <AttributeValue>R</AttributeValue>
  </Attribute>
  <Attribute AttributeId="own-pred-object">
   <AttributeValue>g</AttributeValue>
  </Attribute>
  <Attribute AttributeId="own-pred-value">
   <AttributeValue>3</AttributeValue>
  </Attribute>
 </Environment>
</Request>
```

Listing 2: Simplified Example XACML Request

An upstream request needs not change the algorithm, although the verifier could rely on the supplied verifiable predicate in order to extract his own predicate information instead of retrieving it from his database. In the next section we will prove the proposed theorems validating our security claims.

3.5 Analysis

The proof of Theorem 1 can be reduced to the cryptographic security of public-key signatures.

PROOF. Let $s_1, \ldots, s_k$ be the sequence of signatures for object O_j. Let Σ be the set of valid verifiable predicates $\sigma(X_i, \mathcal{L}(O_j))$. From the assumption in Theorem 1 and Definition 3 it follows that no player with a valid predicate has been compromised:

$$\forall X_i \nexists \sigma(X_i, \mathcal{L}(O_j)) \in Sigma \wedge X_i \in \bigcup_l \mathbb{A}_l$$

In order to forge a predicate $\sigma(X_{i'}, \mathcal{L}(O_j)) \notin Sigma$ the attacker must generate signature s_k, such that it conforms to $S_{X_i}(j, X_{i'})$ and is valid, but since no valid possessor has been compromised ($\nexists X_i \in \bigcup_l \mathbb{A}_l$), he cannot do so. □

The proof of Theorem 2 is more tricky and we start by describing the detection procedure. Assume there is an investigation for object O_j. This investigation can be triggered by an incident, reasonable suspicion, regular or random audit. All players reveal all verifiable predicates $\sigma(X_i, \mathcal{L}(O_j))$ they read from RFID tags or received during an authentication protocol. If there are two predicates $\sigma(X_i, \mathcal{L}(O_j))$ and $\sigma(X_{i'}, \mathcal{L}(O_j))$ from different players ($X_i \neq X_{i'}$), such that their ranks match $|\sigma(X_i, \mathcal{L}(O_j))| = |\sigma(X_{i'}, \mathcal{L}(O_j))|$, forgery has been detected. Let $s_1, \ldots, s_k$ and $s'_1, \ldots, s'_k$ be the sequences of signatures for the predicates $\sigma(X_i, \mathcal{L}(O_j))$ and $\sigma(X_{i'}, \mathcal{L}(O_j))$, respectively. The player X_i of the signature $s_l = S_{X_i}(j, X_{i''})$ where l is the highest index where both sequences of signatures match

$$l = \max\{l | \forall h.1 \leq h \leq l \wedge s_h = s'_h\}$$

will be blamed for forgery.

We can now prove Theorem 2 by showing that this procedure always reveals a compromised player $X_i \in \bigcup_l \mathbb{A}_l$.

PROOF. If X_i has been compromised, it follows from the assumptions in Theorem 2 that there is a valid predicate $\sigma(X_{i''}, \mathcal{L}(O_j)) \in \Sigma$, such that its rank is higher than that of the compromised player $|\sigma(X_{i''}, \mathcal{L}(O_j)) \in \Sigma| > l$. Since the last player X_{i_k} of the trajectory currently in possession of the object is currently not compromised $X_{i_k} \notin \mathbb{A}_k$, this predicate $\sigma(X_{i''}, \mathcal{L}(O_j)) \in \Sigma$ will be revealed during the investigation at least as a component of the last player's predicate read from the RFID tag. The attacker A used the forged predicate $\sigma(X_{i'}, \mathcal{L}(O_j)) \notin \Sigma$ which will also be revealed by its verifier. Therefore the detection procedure succeeds in revealing a compromised X_i.

If X_i had not been compromised, then according to Theorem 1 there cannot be a $\sigma(X_{i'}, \mathcal{L}(O_j)) \notin \Sigma$. □

The detection security mechanism appeals to the economic nature of business in supply chains. It intends to deter fraudulent behavior by imposing penalties, such as monetary fines or loss of business, combined with effective detection. The incurred risk of detection probability times expected loss provides an incentive for compliant behaviour. If the risk outweighs the gains from forgery, a rational player will behave honestly. The legal provisions for conducting business in supply chains, such as multilateral contracts between the players, can regulate the liability for these security breaches.

4. RELATED WORK

Another commercial separation access control model is the seminal Chinese Wall policy [11]. It prevents employees at companies dealing with competing clients to exchange information. In some sense our object trajectories are the inverse of their conflicting interest labels, i.e. they prevent access if they match, we prevent access if they do not. In addition, we have to deal with the difficulties of a distributed system, such as incomplete information about trajectories and verification of predicates.

The Chinese Wall policy has been applied to a distributed system in [4]. The system considered is a workflow system where all players are known and determined in advance. Its application to supply chains does not solve the visibility problem.

Our application area of RFID security and privacy has become a popular area of research in recent years. People are concerned about the impact RFID technology can have on their lives. A good survey over the current state of the art in research on RFID security and privacy is provided in [26], but as [26] states as well, little research is being performed on the security and privacy of RFID in business applications.

Most research has been performed in order to protect the access to the tag identifier and thereby provide privacy for the consumer. An example relating to access control is the jammer tag of [37]. Many authentication protocols for RFID tags that provide varying degrees of privacy have been proposed in the literature as well. A survey is given in [48]. Note that all these protocols operate in a significantly simpler system model of only RFID tag and reader.

Furthermore our security concern is less the protection of the consumer than that of the companies in the supply chain. In [23] the authors make a proposal for an access control model for object information where the access decision maker changes with the possession of the item. While this model is a very intriguing concept, the problem of efficiently specifying the access control itself has not been considered in this paper. Also the motivation for distributed databases is that the owner remains in control of the access decision.

The work of [19] considers the problem of specifying access control for parts of the object data. Instead of providing the entire object data only part of the object data is supposed to be revealed. This is orthogonal to our access control model and could be trivially integrated into ABAC as well. An expressive policy language for special case of EPCglobal data is proposed in the paper. Obviously this does not help with the problem of specifying different policies for a huge number of objects. Instead we believe that it is necessary to simplify policy specification in order to make handling a huge number of objects manageable. Our believe is supported by other research addressing the access control administration problem, e.g. in [24] the authors state that *"a wide variety of access control models have the expressive power to represent almost arbitrary policies, few are ever used by others due to their complexity"*.

An interesting and related concept for captured RFID data are visibility events [31]. In this case the data stored in the database is only trajectory data and the term visibility is taken more literally (line of sight). The data revealed to a principal is only data that is visible to him based on his related collected data. We extend their model with physical objects (they track principals) and define the relations between these data attributes. We also address the distributed data storage in supply chains.

Hippocratic databases [3] are capable of enforcing the access control policies to object-level data [2]. No specific access control model has been proposed.

Some authentication mechanisms from the literature tackle similar problems. Proofs of possession techniques have been described in [18]. The paper considers only simple off-the-shelf approaches without any security analysis. None of the proposed approaches would verify in our security model. Better authentication has been proposed in [30], but it does not provide sufficient information to evaluate our visibility policies. The concept of vouching for authentication has been proposed in [10] for replacing lost credentials.

Secure ownership transfer protocols [34, 42] allow the verification of currently possessing an object equipped with an RFID tag. Most protocols have been broken in [13]. We extend the concept of ownership verification to verification after possession of the item.

In [22] the use of identity-based cryptography for protecting access to ubiquitous (object) data is proposed. They cannot yet implement our visibility policies efficiently, but focus on the exploitation of the hierarchical nature of the data.

5. CONCLUSIONS AND FUTURE WORK

We investigate the problem of access control for data collected about mobile physical objects. We showed that a new approach is required in order to combine the practically important confidentiality requirements with efficiently manageable administration. Commercial object-level data sharing systems are currently being developed in industry and the necessary access control policies will soon need to be installed and administered. Our access control model enables the administrator to easily set visibility policies potentially reducing the number of policies by several orders of magnitude. To the best of our knowledge there are no competing proposals for efficiently separating access to object-level data from different supply chains. We also presented a simple authentication protocol using RFID tags that reliably supplies the necessary information for making the access decision. We proved these protocols secure using standard cryptographic assumptions and rational behaviour. The RFID tags do not require any modification to commercially available ones with sufficient re-writeable storage.

We intend to improve our work as follows in the future.

Extensions to the Access Control Model

Using our predicates $\sigma(X_i, \mathcal{L}(O_j))$ we only specified two attributes: one for downstream visibility and one for upstream. We limit ourselves in this paper to these two visibility attributes, since they allow for a fair sharing of data revelation risks between players. In a "tit for tat" like manner, both players can share data for their common good without comprising their relation to other players. This lends itself to a viral adoption of these visibility policies, but in situations of imbalanced power players may be inclined to promote a different adoption strategy. This does not limit the technical capabilities of our model and clearly one can use the predicates to compute other forms of visibility, e.g. ϵ-visibility where the requestor should not be separated by more than ϵ stages in the trajectory:

$$-\epsilon \leq |\sigma(X_i, \mathcal{L}(O_j))| - |\sigma(X_v, \mathcal{L}(O_j))| \leq \epsilon$$

Also, in a central database one may want to compare the requestor's predicate with one different from the verifier's one.

Modifications to the System Model

As just mentioned one may consider a central database combining the information from all players. Our visibility policies from Section 2 are still applicable in unmodified form, but the authentication protocol Section 3 would be unnecessary, since all information is stored in the central database. Another common form of processing object-level data is in streams [44] which are transported between players using publish-subscribe networks [6]. Our visibility policies again remain necessary and useful unaltered, but there is no request for access any longer, such that our authentication protocol becomes obsolete. A different form of authentication and access control enforcement is required.

Improvements to the Authentication Protocol

Even without modifications to the system model several improvements to the authentication protocol seem advisable. First, the still existing need for a trusted third party albeit limited compared to [30] is questionable. While our trusted third party is not involved in moving objects and therefore remains oblivious to the supply chain operation, it remains an open problem to design an object-based authentication protocol without a trusted third party. Given the lack of a regular authentication protocol without trusted third party as a template, we are not aware of a promising idea for solving it. Adopting cryptographic primitives on the RFID tag seems to be the only solution.

Second, our authentication protocol may reveal the entire trajectory to a player. This is significantly more information than necessary to authenticate or make the access decision. Although our protocols already improve over proposals for standards [1] by revealing this information only to partners on the same supply chain and not any player in the system, approaches using modern cryptography [29, 46] show

that significantly better confidentiality protection is feasible. A more privacy-preserving protocol that only reveals the necessary information, such as the rank, seems like a welcomed improvement. The protocols in [30] are superior in this respect, such that a combination is likely to improve the situation.

6. ACKNOWLEDGEMENTS

The developments presented in this paper were partly funded by the European Commission through the ICT program under Framework 7 grant 213531 to the *SecureSCM* project.

7. REFERENCES

[1] EPCglobal. EPCglobal architecture framework, Version 1.2. *Available at* http://www.epcglobalinc.org/, 2007.

[2] R. Agrawal, A. Cheung, K. Kailing, and S. Schönauer. Towards Traceability across Sovereign, Distributed RFID Databases. *Proceedings of the 10th International Database Engineering and Applications Symposium*, 2006.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic Databases. *Proceedings of the 28th International Conference on Very Large Data Bases*, 2002.

[4] V. Atluri, S. Chun, and P. Mazzoleni. A Chinese wall security model for decentralized workflow systems. *Proceedings of the 8th ACM Conference on Computer and Communications Security*, 2001.

[5] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public-Key Cryptography for RFID-Tags *Proceedings of 4th IEEE International Workshop on Pervasive Computing and Communication Security*, 2007.

[6] K. Birman, and T. Joseph. Exploiting virtual synchrony in distributed systems. *ACM SIGOPS Operating Systems Review 21(5)*, 1987.

[7] P. Blythe. RFID for Road Tolling, Road-Use Pricing and Vehicle Access Control. *Proceedings of the IEE Colloquium on RFID Technology*, 1999.

[8] H. Bock, M. Braun, M. Dichtl, E. Hess, J. Heyszl, W. Kargl, H. Koroschetz, B. Meyer, and H. Seuschek. A Milestone Towards RFID Products Offering Asymmetric Authentication Based on Elliptic Curve Cryptography. *Proceedings of the Workshop on RFID Security*, 2008.

[9] D. Boneh, H. Shacham, and B. Lynn. Short Signatures from the Weil Pairing. *Journal of Cryptology 17(4)*, 2004.

[10] J. Brainard, A. Juels, R. Rivest, M. Szydlo, and M. Yung. Fourth Factor Authentication: Somebody You Know. *Proceedings of the 13th ACM Conference on Computer and Communications Security*, 2006.

[11] D. Brewer, and M. Nash. The Chinese Wall Security Policy. *Proceedings of IEEE Symposium on Security and Privacy*, 1989.

[12] S. Chou, and Y. Ekawati. Cost Reduction of Public Transportation Systems with Information Visibility Enabled by RFID Technology. *Proceedings of the 16th ISPE International Conference on Concurrent Engineering*, 2009.

[13] T. van Deursen, S. Mauw, S. Radomirovic, and P. Vullers. Secure Ownership and Ownership Transfer in RFID Systems. *Proceedings of the 14th European Symposium on Research in Computer Security*, 2009.

[14] W. Diffie, P. van Oorschot, and M. Wiener. Authentication and Authenticated Key Exchanges. *Designs, Codes and Cryptography 2 (2)*, 1992.

[15] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. AES Implementation on a Grain of Sand. *IEE Proceedings on Information Security, 152(1)*, 2005.

[16] K. Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. *John Wiley & Sons, Inc.*, 2003.

[17] Fujitsu. Fujitsu Develops World's First 64KByte High-Capacity FRAM RFID Tag for Aviation Applications. *Press Release. Available at* http://www.fujitsu.com/global/news/pr/archives/month/2008/20080109-01.html, 2008.

[18] E. Grummt, and R. Ackermann. Proof of Possession: Using RFID for large-scale Authorization Management. *Proceedings of AmI-07 Workshops*, 2008.

[19] E. Grummt, and M. Müller. Fine-Grained Access Control for EPC Information Services. *Proceedings of the 1st International Conference on The Internet of Things*, 2008.

[20] M. Harrison. EPC Information Service (EPCIS). *Proceedings of Auto-ID Labs Research Workshop*, 2004.

[21] D. Hein, J. Wolkerstorfer, and N. Felber. ECC is Ready for RFID – A Proof in Silicon. *Proceedings of the Workshop on RFID Security*, 2008.

[22] U. Hengartner, and P. Steenkiste. Exploiting Hierarchical Identity-Based Encryption for Access Control to Pervasive Computing Information. *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 2005.

[23] A. Ilic, F. Michahelles, and E. Fleisch. Dual Ownership: Access Management for Shared Item Information in RFID-enabled Supply Chains. *Proceedings of the 5th IEEE International Conference on Pervasive Computing and Communications Workshops*, 2007.

[24] T. Jaeger, A. Edwards, and X. Zhang. Managing access control policies using access control spaces. *Proceedings of the 7th ACM Symposium on Access Control Models and Technologies*, 2002.

[25] J. Joshi, E. Bertino, U. Latif, and A. Ghafoor. A Generalized Temporal Role-Based Access Control Model. *IEEE Transactions on Knowledge and Data Engineering 17(1)*, 2005.

[26] A. Juels. RFID security and privacy: a research survey. *IEEE Journal on Selected Areas in Communications 24(2)*, 2006.

[27] F. Kerschbaum. Practical Privacy-Preserving Benchmarking. *Proceedings of the 23rd IFIP International Information Security Conference*, 2008.

[28] F. Kerschbaum, D. Dahlmeier, A. Schröpfer, and D. Biswas. On the Practical Importance of Communication Complexity for Secure Multi-Party Computation Protocols. *Proceedings of the 24th ACM Symposium on Applied Computing*, 2009.

[29] F. Kerschbaum, N. Oertel, and L. Weiss Ferreira Chaves. Privacy-Preserving Computation of Benchmarks on Item-Level Data Using RFID. *Proceedings of the 3rd ACM Conference on Wireless Network Security*, 2010.

[30] F. Kerschbaum, and A. Sorniotti. RFID-Based Supply Chain Partner Authentication and Key Agreement. *Proceedings of the 2nd ACM Conference on Wireless Network Security*, 2009.

[31] T. Kriplean, E. Welbourne, N. Khoussainova, V. Rastogi, M. Balazinska, G. Borriello, T. Kohno, and D. Suciu. Physical Access Control for Captured RFID Data. *IEEE Pervasive Computing (6) 4*, 2007.

[32] C. Kuerschner, F. Thiesse, and E. Fleisch. An analysis of data-on-tag concepts in manufacturing. *Proceedings of the 3rd Konferenz Ubiquitäre und Mobile Informationssysteme*, 2008.

[33] H. Lee, K. Lee, and M. Chung. Enterprise Application Framework for Constructing Secure RFID Application. *Proceedings of the 1st International Conference on Hybrid Information Technology*, 2006.

[34] D. Molnar, A. Soppera, and D. Wagner. A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. *Proceedings of the 12th International Workshop on Selected Areas in Cryptography*, 2005.

[35] NIST. A Survey of Access Control Models. *Privilege (Access) Management Workshop*, 2009.

[36] OASIS. eXtensible Access Control Markup Language (XACML), Version 2.0. Available at http://docs.oasis-open.org/xacml/2.0/, 2005.

[37] M. Rieback, B. Crispo, and A. Tanenbaum. Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags. *Proceedings of the 13th International Workshop on Security Protocols*, 2005.

[38] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-Based Access Control Models. *IEEE Computer 29(2)*, 1996.

[39] B. Santos, and L. Smith. RFID in the supply chain: panacea or pandora's box? *Communications of the ACM 51(10)*, 2008.

[40] S. Sarma, D. Brock, and D. Engels. Radio frequency identification and the electronic product code. *IEEE Micro 21(6)*, 2001.

[41] S. Sarma, S. Weis, and D. Engels. RFID Systems and Security and Privacy Implications. *Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, 2003.

[42] B. Song. RFID Tag Ownership Transfer. *Proceedings of the Workshop on RFID Security*, 2008.

[43] T. Staake, F. Thiesse, and E. Fleisch. Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. *Proceedings of the 20th ACM Symposium on Applied Computing*, 2005.

[44] D. Terry, D. Goldberg, D. Nichols, and B. Oki. Continuous Queries over Append-Only Databases. *Proceedings of the ACM International Conference on Management of Data*, 1992.

[45] R. Thomas, and R. Sandhu. Task-Based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-Oriented Autorization Management. *Proceedings of the 11th IFIP International Conference on Database Securty*, 1997.

[46] L. Weiss Ferreira Chaves, and Florian Kerschbaum. Industrial Privacy in RFID-based Batch Recalls. *Proceedings of the 1st IEEE International Workshop on Security and Privacy in Enterprise Computing*, 2008.

[47] M. Wu, C. Ke, and W. Tzeng. Applying Context-Aware RBAC to RFID Security Management for Application in Retail Business. *Proceedings of the 2008 IEEE Asia-Pacific Services Computing Conference*, 2008.

[48] Y. Yousuf, and V. Potdar. A survey of RFID authentication protocols. *Proceedings of the 22nd International Conference on Advanced Information Networking and Applications Workshops*, 2008.

[49] E. Yuan, and J. Tong. Attributed Based Access Control (ABAC) for Web Services. *Proceedings of the IEEE International Conference on Web Services*, 2005.