

Context-Based Humanized and Authorized Personalization in Mobile Commerce Applications

Christos K. Georgiadis, Ioannis Mavridis and Athanasios Manitsaris
Department of Applied Informatics, University of Macedonia, 156 Egnatia Str.,
540 06 Thessaloniki, GREECE

Abstract: *Given the existing limitations and advantages on the mobile Internet, the preferences of users for mobile commerce content and services are noticeably affected. Context-awareness of mobile devices emphasizes the importance of personalization technology. Personalization is more and more used as a way to accelerate the delivery of information to each user, making the site convenient and attractive to return to. A promising approach to maintain different (personalized) permissions for different users is to examine personalization considerations along with adequate security and privacy mechanisms (authorized personalization). We focus on how the various customization and authorization concepts influence specific user interface design elements, namely content, presentation, connection, communication, community and commerce. Adapting an appropriate context-sensitive model for authorizations, the overall flexibility of the established personalization mechanisms is preserved without compromising the stability of the required security precautions.*

Keywords: *M-commerce, context, personalization, and authorizations.*

Received: July 30, 2005 | **Revised:** August 10, 2005 | **Accepted:** August 25, 2005

1. Introduction

Mobile commerce (m-commerce) is concerned with the use, application and integration of wireless telecommunication technologies and wireless devices within the business systems domain. It relies on the same core information technologies of e-commerce, such as the Internet and the World Wide Web, but typical m-commerce client devices (cell phones or personal digital assistants-PDAs) have certainly limited input/output facilities and restricted computational power resources. These constraints elevate the importance of context-aware approaches in m-commerce applications and underline the benefits of these approaches on the personalization technology.

The central objective of personalization is to supply users with what they want or need, without requiring them to ask for it explicitly. The efficiency of m-commerce sites in allowing users' easier access to the required information in the most suitable form and at the right time can be realized by focusing on particular individual needs and providing tailored products and services. But the success of personalization depends on the ability of the providers of personalization in promoting responsible use of that technology [1]. How personalized services can manage to balance between facilitation, security and privacy concerns, will determine the future of this field.

Security considerations affect the decisions concerning the personalized behaviour in m-commerce applications. From that point of view, the ability of user interfaces to form and arrange the proper authorization rules is of great importance. In our work we outline how the various personalization techniques influence

m-commerce users' interfaces specific design elements. A comprehensive method to understand personalization technology is by distinguishing the coexisting and jointly responsible features of the humanized (or flexibility-oriented) personalization from the authorized (or security-oriented) personalization. So, finally we approach authorized personalization from an access control viewpoint and we study the applicability of an appropriate context-sensitive model for authorizations, namely the Context-based Team Access Control.

2. Mobile commerce

Nowadays, m-commerce focuses more on the facilitation of enhanced information network access and less on supporting and realizing transactions. The use of wireless technologies extends the nature and scope of traditional e-commerce by providing the additional aspects of mobility (of participation) and portability (of technology) [2]. The wireless medium influences all areas of society: how employees work and how businesses run, advertising opportunities, personal communications, consumer purchases, location-aware services, information locating and retrieval etc. In time, consumers and businesses, citizens and organizations will be able to conduct all information transactions from mobile devices.

By far, the most promising and one of the most rapidly spreading applications within the m-commerce world is the mobile Internet: the wireless access to the contents of the Internet using portable devices, such as PDAs and particularly mobile phones. M-commerce applications vary considerably from e-commerce

applications. In fact, mobile Internet does not act as if to duplicate the wired Internet. Most wireless interfaces display only condensed text and basic graphics. By contrast, wireline communications offer full-colour multimedia enriched sites. In particular, cellular phones continue to shrink in size and weight, and compared to desktop computers have minor multimedia facilities, inconvenient input/output components (smaller screens/keyboards), limited memory capacity and slower connection speeds. Keyboard and mice operations (in e-commerce setting) are being replaced with keypads and buttons in the mobile setting. Devices are difficult to use with only one hand and changing environmental conditions (weather, noise level, brightness) affect also the use of mobile devices. Complexity using devices can transform into errors, wasted time and user disappointment. And last but not least, wireless transmissions are less secure than wireline transmissions.

In spite of these drawbacks, m-commerce offers significant benefits. It possesses the ability to reach users effectively, anywhere and anytime. It allows users instant access to business-critical communication and information. Users can communicate, access corporate databases, and manage responsibilities and administrative tasks (such as scheduling meetings and answering e-mails) during idle time – while standing in line at a bank or waiting for a bus) [3]. Mobile devices, through their common availability and use, encourage business organizations to seek wireless mobile commerce opportunities to engage with the user. An example of such opportunities is the capability to directly market products or services to a customer via the mobile Internet to a mobile phone, or to provide location-dependent information on demand to mobile phone users.

Given the existing limitations and advantages of the mobile Internet, the preferences of users for m-commerce content and services are evidently affected: they tend towards to low-intensity content (ring tones, weather reports, screen icons, etc.) and low-risk products or services [4]. An obvious motivation for these inclinations is the previously mentioned devices' constraints, such as memory capacity, bandwidth and display screen size/resolution. Generally, users of m-commerce applications avoid transmitting large quantities of information. An important reason too, is cost. Mobile telephony providers frequently charge by the minute, which is not economically advantageous to 'surfing' the Internet via a wireless device. So, to avoid the costly extra connection time for accessing descriptive informative material, orders of simple products and services are mainly given.

Furthermore, users have usually limited attention as they operate their mobile devices. This is because they regularly are concerned at the same time with other tasks (e.g. car driving), and they getting involved in a

mobile transaction as in a peripheral task. Therefore, this (usually) limited user concentration during mobile devices operations increases the 'uncertainty' associated with most high-risk products/services. Especially for the preference on low-intensity content, an additional reason has to be noted: users tend to treat their mobile device in a quite personal and emotional way. The majority of them think of it as a declaratory part of their personality, so they keep on searching and downloading further individually customized content.

Finally, security is another important explanation of users' preferences concerning mobile commerce content and services. The mobility of devices amplifies the jeopardy of losing the device and its data. So, users prefer m-commerce applications which do not require storing and processing of sensitive data on mobile devices. In addition, the nature of wireless technology presents new opportunities through which security may be compromised. Communication channel threats and the relevant radio interface risks are significant network-centric aspects of m-commerce that need to be considered. But, what wireless technology actually does do is lower the threshold separating people from temptation [2]. Ease of use can lead to ease of abuse. Mobile device's instant connectivity and user-friendliness make it an ideal tool for e-crime activities. On the other side, malicious users can easily find their unsuspected victims, because security awareness in mobile environment is in its infancy. Consequently, the opportunities for misuse of the system can be greatly increased, if adequate measures enforcing a proper access control policy are not taken to prevent them.

3. Context-awareness in m-commerce environments

With the arrival of mobile devices, context becomes a more considerable influence on the requisite behaviour of computer systems. People are using m-commerce applications in extensively varied environments that are relatively unstable from one moment to the next. The notion of context is often equated simply with location, but is actually more complex. Context concept attempts to contain all changing circumstances and often contradictory user needs. And the most exciting thing is that mobile devices are context-sensitive, that is they are capable to detect the user's setting (such as location, resources nearby etc.) and as a result to offer this information to the application.

Contextual information can be categorized [5] in:

- Environment – includes the properties of objects in the physical environment. Representative characteristics are location and orientation of objects, brightness and noise levels, availability,

quality of devices, quality of communication and physical properties.

- Participants – covers the status of the user(s) and other participant entities. Representative examples are personal properties (age, gender, education, preferences, expectations, etc.), mental state and physical health, location and orientation.
- Activities – is concerned with the tasks and goals of user(s) and participants, as well as environmental activities (such as weather or temperature).

As contextual information is also considered the interactions or relationships that may exist among environment, participants, and the activities (such as collaboration and teamwork, co-location, season situations, worker/workplace relationships, time-of-day or day-of-the-week etc.). Furthermore, it must be underlined that time is considered as an important factor which influences all categories of context as well as their interactions. Practically, all context characteristics are not important to an m-commerce application at a given time. However, increased usability and functionality may result for applications that are able to sense and pick those context characteristics that are relevant.

Context may affect beneficially m-commerce applications in many ways. First, it can be used as a means to manage devices' usability constraints. Context-based approaches are capable of modelling data adaptively for devices with varying capabilities and multiple heterogeneous networks. Applications and devices may adapt themselves automatically to changing contexts. To overcome the physical limitations of mobile devices, modified interaction practices may be required. Flexibilities of input and output modalities can allow adaptation to changing user needs as these are produced from contextual information. So, context can also be exploited for managing the distracting user setting in mobile Internet. Aside from the mobile application itself, a large number of additional objects, people and activities compete for user's attention. Therefore, as users' priorities may change unpredictably in dynamic outside environment, the amount of the concentration that they can provide to a mobile application will be different over time. Context-sensitivity provides solutions (e.g. viable alternatives such as speech input or sound output may be utilized depending on the context parameter of noise level).

4. Customization and personalization: Issues and mechanisms

Context setting (the implicit information about the environment, situation and surrounding of a particular communication) is of great importance. However, typically each and every person receives the same information under the same context condition. What is

even more challenging is the adaptability of mobile applications to the interests, the conditions and the preferences of the individual user. Indeed, a particular m-commerce technology, namely personalization, focuses on making a site more receptive to the unique and individual needs of each user [6]. Undoubtedly, delivering personalized information is a critical factor concerning the effectiveness of a site: it has the ability to treat people based on their personal qualities and prior history with it, and moreover has the ability to change (customize) its resources (products, information or services) to better fit the needs of each user.

The goal of m-commerce applications is to increasingly make their service offerings more personalized towards their users. In addition, they support mechanisms to learn more about customer desires, to recognize future trends or expectations and hopefully to amplify customer "loyalty" to the provided services. Personalization and customization, is considered as an important m-commerce technology on marketing, which potentially enable product and service differentiation down to the level of the individual, and thus strengthening the ability of marketers to create brands [7].

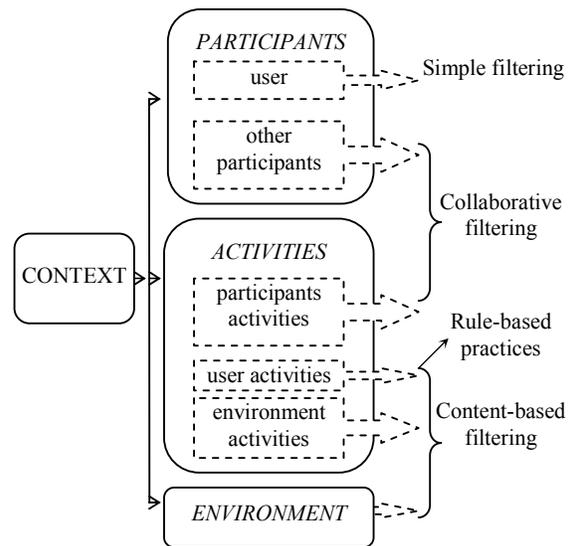


Figure 1. Impact of Context Categories on Personalization Mechanisms.

Personalization mechanisms initially gather user information in order to construct a profile that demonstrates a set of descriptors essential to the site owner (e.g. user's interest, navigation paths, entitlements and roles in an organization, purchases, etc.). The ordinary methods of this process are: explicit profiling (asking each user to fill out questionnaires), implicit profiling (tracking the user's behavior) and using legacy data (e.g. previous behavior, credit applications etc.). The core

personalization mechanisms analyze user information to recommend specific actions. To develop the best recommendation, rule-based practices are usually combined with filtering methods [8]:

- Manual decision rule-based practices consist of allowing business administrators to specify rules for business applications or marketing campaigns (e.g. cross-selling) to impel personalization.
- The filtering methods utilize algorithms to analyze user profiles:
 - The most *simple filtering* technique is based on predefined groups of users, classifying their accounts by age groups, asset value etc.
 - *Content-based filtering* is a more complex mechanism, as it tries to outline a representation of the user's interest. It works by analyzing the content of the site's objects, trying to identify key attributes for each object and assign them the proper attribute values (e.g. documents based on keywords).
 - *Collaborative filtering* is another advanced filtering approach. As an alternative to locating objects comparable to those a user was fond of in the past (the process of the content-based filtering approach), collaborative (or social) filtering builds up recommendations by discovering users with similar inclinations. The collection of users' opinion on a set of objects (explicitly or implicitly), is used to structure like-minded and well-suited peer groups. These groups are used to predict a particular user's concern in an item.

5. Humanized personalization in m-commerce applications

Existing m-commerce applications provide the users a reasonably easy, browser-based interface to access available services. Generally speaking, user interfaces for m-commerce sites represent the site's theme, which should be easy to navigate, and pleasing to the site's visitors. It is therefore important to examine how the users' interfaces can be supported with personalization mechanisms. Rayport and Jaworski in [9] presented an elaborated framework for e-commerce customer interfaces based on seven design elements - the 7C framework: customization (site's ability to be personalized), content, context/presentation, connection (the degree of formal linkage from one site to others), communication (the type of dialogues between sites and their users), community (the interaction between users) and commerce (the interface elements that support the various business transactions).

Lee and Benbasat in [10] describe in detail the influence of mobile Internet environment to the 7C framework. In both of these works, the focal point was a particular users' category, the customer. So, their

observations are free from security considerations, which naturally appear when other categories of users are getting involved. Certainly, their conclusions are significant concerning the 'humanized' dimension of the personalization technology. On the other hand, Pierrakos et al. in [8] present a comprehensive generic classification scheme for Web personalization systems in which personalization functions are distinguished in four basic classes: memorization, guidance, customization and task-performance support. Regarding this scheme, we argue that the personalized access rights of the memorization class must be separated to form a distinct security class, responsible for all authorized personalization functions. We deal with them in the next paragraph, where we analyze all security relevant issues. Also, the task-performance support class (with functions as personalized errands, personalized negotiations, etc.) presents indeed interesting challenges in m-commerce applications. We believe that these personalization functions when applied in m-commerce environments can be categorized in the commerce design element of the 7C framework. Given the diversity of all these tasks, seems an attractive process to examine them in the light of the authorized personalization category, and we plan to do it as a future extension of this work.

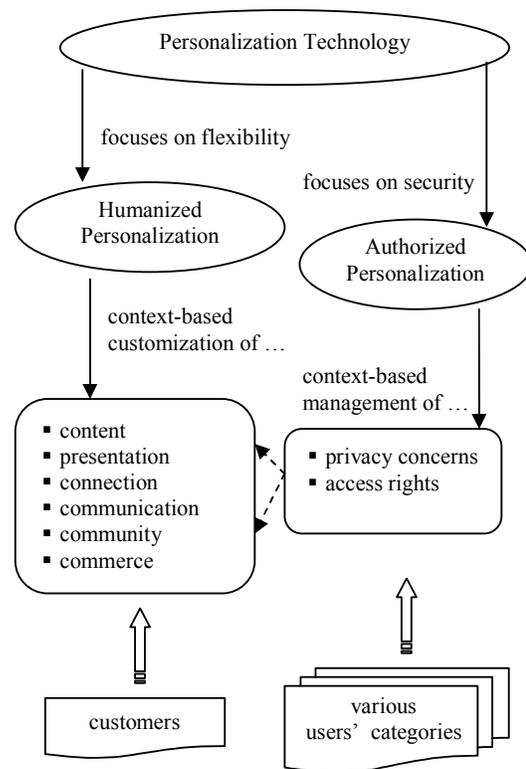


Figure 2. Perspectives of Personalization Technology.

In this paper we are concerned mainly for the customization class, and to a certain degree, both the guidance class and the non-security oriented

memorization class (user salutation and bookmarking) can be studied according to the customization/personalization design element [9] [10] of m-commerce interfaces. Thus, flexibility-oriented personalization can be examined by re-evaluating the remaining elements of the 7C framework from a customization viewpoint:

- *Content*: Personalization may work as a sieve which allows the delivery of low-intensity content that users appreciate and rejects the rest. Thus, active adaptation of content is strongly related to customization. A resembling significant consideration that deals also with personalized content is that the portable devices may offer task-relevant information and service.
- *Presentation* is related to customization in two main ways:
 - The *aesthetic nature* of interfaces: Visual and audio characteristics (such as color schemes, screen icons, ring melodies etc.) have been proved for mobile users as a favorite way of making their phones more personal.
 - The *layout* which refers to two aspects: section breakdown (how a part of information is separated into sets of Web pages) and link issues with the sub-categories of the linking structure (how each page is linked to the others) and of the navigation tools (in what ways the moving throughout the site is supported).
- *Connection* concerns links with external sites. Context-awareness of mobile devices may influence the connection (e.g. the choice of a particular external link among a set of similar ones may depend not only from its content, but also from its availability and efficiency under the specific conditions of user's setting).
- *Communication* is defined as having one of the following forms or a combination of them: broadcast (a one-way information transmission from a site to users) and interactive (a two-way information exchange between a site and a user). M-commerce administrators should make use of information about users' mobile setting to catch the right type of communication for the right moment, taken into account also the choices of each user concerning the most wanted type of communication between him and the site.
- *Community*: In many cases users seek information from other users about some products or services. So, supporting interactive or non-interactive communication between users enables opinion exchange about current transactions and network accesses. Undoubtedly, such functionality may provide useful material for collaborative filtering techniques, resulting in more successful personalized sites.

- *Commerce*: Shopping cart, negotiations, order tracking or delivery options are some of the potential interface issues that must be designed taking into account the preferences of mobile users for low-intensity content and low-risk transactions. Also, given the distracting user setting in mobile Internet, the interface should call for only minimal attention in order to complete successfully critical transaction steps (such as the checkout process).

6. Context-based authorized personalization

Undoubtedly, user convenience and user satisfaction are the main goals of personalized user interfaces. For that reason, quite often the term humanized personalization is used to emphasize the emotional dimension of the previously mentioned customization elements. For example, restaurant information related to user's location (content element), favourite links or ring tones (presentation element) etc. At the same time, a careful study on those elements, speaks for the inseparable dependence between security and personalization.

Personalization opens up the possibility of intensive invasion of privacy for commercial and governmental purposes that is unprecedented [7]. Future expansion of m-commerce services will depend in part on the ability of m-commerce firms to transform their customized services into truly and therefore reliable personalized services (such as providing unique consultation based on an automated, yet intimate understanding of the client). So, authorized personalization is setting privacy as a first priority: personal intrusion by misusing sensitive users' information must be avoided.

In order to be more effective, authorized personalization requests in particular a different perspective: it demands a strong access control engine, which is able to grant authorizations in order to securely manage the appropriate personalization mechanisms. Thus, the concepts of authentication and authorization are of critical importance in security-oriented personalization. Authentication is the process where a networked user establishes a right to an identity, in reality, the right to use a name. A large number of techniques exist, able to authenticate users: passwords, biometric techniques, smart cards, and certificates. Authorization is the process of determining whether an authenticated identity is permitted to access a resource. Authentication and authorization decisions can be made at different points, by different organizations. Using authorized personalization in the interface design, any interaction with the resource is performed via specific interface components that present the set of all actions available

for the resource and thus we provide different users with different access rights. So, what is really needed as an underlying infrastructure is a flexible and context-sensitive access control model, in order to support the proper authorization decisions for secure personalized m-commerce services.

6.1. Context-based Team Access Control

A mixture of contextual information (like time, user's location, device's characteristics, etc.) has to be considered when influencing the desirable behaviour in m-commerce applications and the underlying access control system during runtime. Personalization enlarges the applications' complexity since every individual's options have to be considered and implemented. It results in a massive amount of variant possibilities: target groups, output formats, mobile end devices, languages, locations, users joining and leaving the network in unpredictable way, etc. Thus, manual selection and composition of content and services is not practical. As a consequence, the authorizations requirements are difficult to define in a static way. An 'authorized personalization engine' is needed to dynamically provide secure context-dependent personalized services. Context-based Team Access Control (C-TMAC) is an active access control system that supports context-based permission activation. Passive access control models are those that primarily serve the function of maintaining permissions assignments, such as in role-based ones, where permissions are assigned to roles. On the other hand, active access control models, as C-TMAC, approach security enforcement from the perspective of activities and therefore provide the mechanisms for the active runtime management of authorizations as tasks progress to completion. C-TMAC, can actually facilitate the content-based filtering personalization mechanisms. In addition its remarkable suitability for collaborative environments (as it is testified in recent credible survey [11], where it was classified first in all criteria among seven competitive models) makes it also an ideal security tool for supplementary personalization approaches based on the collaborative filtering.

In a C-TMAC model, a variety of factors are considered in order to formulate the appropriate context associated with a particular task. The team concept is used mainly as a mechanism that associates users with contexts. Even when a user is acting alone, we may consider the user as the single member of a private team. Context thus identifies the specific need-to-know requirements of each member of the team [12]. C-TMAC model is based on Role-based Access Control (RBAC) [13] approach. It consists of users, roles, permissions, teams and contexts, as well as a collection of sessions. A role is a job function within the organization with some associated semantics regarding

the authority and responsibility conferred on a member of the role. Permissions or authorizations are approvals of a particular mode of access to one or more resources.

The team entity is used to represent a group of users having specific roles with the objective of completing a specific activity in a particular context. The use of a team as a mediator to enable a user to acquire a context is analogous to the use of role as a mediator between users and permissions. A team can also be seen as a mapping to multiple users. The roles activated by these users identify the permission set available to the team as a 'combination' of permissions from all roles participating in that team. Context-to-team assignment and user-to-team assignment are both many-to-many relations.

Authorizations are granted using role-based permission assignment and team-based permission activation. Teams can be seen as groups of current task contexts. This means that when a user participates in a team he obtains also the context of team's task. The team context is expressed in terms of ranges of values. For every team, there are a variety of system variables that can hold sets of values for chosen contextual information (factors). The binding of these variables to actual values is accomplished during the runtime. Team contexts can be seen also, as filters or restrictions on objects, conditions and services. Thus, the final permission set of a user is generated after a filtering process based on the current context of his team. It must be noticed that we must not confuse the filtering process here with the previously referred personalization filtering algorithms.

The activation of user permission is accomplished in accordance with the following two-step procedure:

- 1: Role-based Permissions =
= User Permissions \oplus Team Permissions
(symbol \oplus means "combined with")
- 2: Context-based Permissions =
= Role-based Permissions \otimes Team-Context
(symbol \otimes means "filtered by")

Team (role) permissions may be combined (\oplus) as follows:

- *Aggregation*: The set of access permissions of the team is the sum-up (union) of the individual assigned role-based access permissions of all team members.
- *Maximum/Minimum*: The set of access permissions is considered to be equal to the maximum or minimum permissions sets of the individual members of the team.
- *Current team structure*: The structure (formation) of the team is used to determine the credentials held by the team members. Individual users are not permitted to perform actions on their own but only in the presence of the other participants of the team.

We may consider the filtering process as a mechanism of extracting meaningful subsets of the role-based permissions based on the values of a team's contextual variable. For a more detailed description for C-TMAC model and relative implementation issues see [11][14].

6.2. Addressing the challenges of context: C-TMAC for personalization

An obvious area for exercising C-TMAC authorized personalization is during the analysis of user information and more precisely, when filtering approaches are used. It is worth mentioning that from a security viewpoint all users of m-commerce applications are not simply customers; some of them may have administrative authorizations to a certain degree. In addition, a crucial characteristic of users is their position in relation to the 'perimeter' of the organization that is going to be secured. Let us consider the following main categories:

- *External users:* external information providers who generate the information outside the organization, information consumers or customers, who want or need the information, and in some cases information sponsors who add their own advertising information.
- *Internal users:* internal information providers who generate the information inside the organization, information gatherers who gather and/or input the information, information editors, who decide what information to provide, information processors who format, process or modify the information to make it more useful to information consumers, information marketers who identify needs and consumers for information services and who market these services, and accountants who provide accounting services.

With C-TMAC, users according to their predefined responsibility are assigned to proper roles. Among them, customer role presents additional challenges if personalization mechanisms are going to be used. To be exact, first the set of available roles must be expanded. So, user-to-role assignments have to be further specified using additional sub-roles and based on certain criteria such as age, asset value, etc. Although these criteria are considered as contextual information (they consist the sub-category 'user' of the category 'participants' in previously described context scheme of fig.1), C-TMAC manipulates them differently from the other context categories. This is because it is the sole part of the contextual information that is not changing during runtime (static content). Thus, it is used as supporting material for passive security countermeasures and role assignment processes.

This kind of procedures is a necessary part of an access control system and in figure 3.A is depicted as the phase 'A' of authorized personalization. For every customer role CR_j , user interface holds the appropriate permissions which can be implemented in terms of authorizations for specific personalized content, presentation, connection, communication and commerce material. Therefore, all simple filtering techniques required by personalization mechanisms (extended in order to support additional security-oriented requirements of diverse users' categories-roles) are typical passive security issues that can be well supported from the RBAC component of C-TMAC.

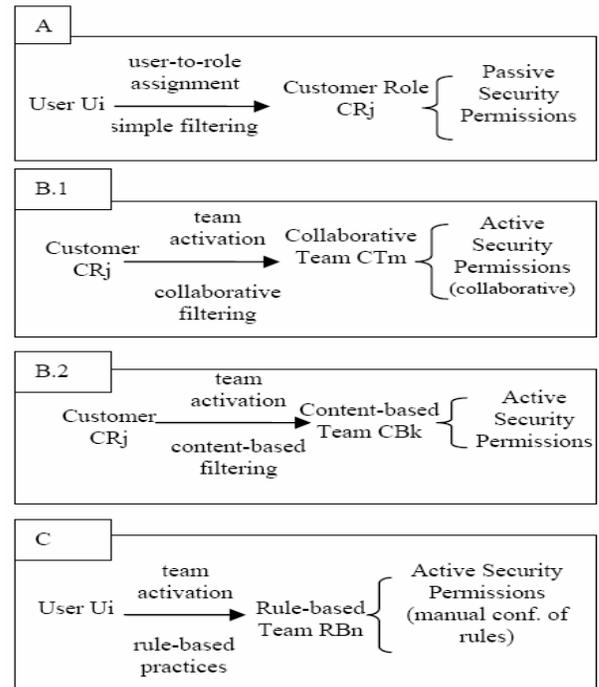


Figure 3. C-TMAC for Authorized Personalization.

Furthermore, the collaborative nature of C-TMAC is able to support more complex and advanced filtering approaches, such as the collaborative filtering (phase 'B.1' of authorized personalization as depicted in figure 3.B.1). In reality, collaborative filtering deals with a particular form of collaboration (implicit collaboration), and requires the dynamic management of customer teams. Thus in C-TMAC, customers with comparable preferences are discovered and they form well-matched collaborative teams. For every collaborative team CT_m , user interface holds the appropriate context. The context categories (fig. 1) that influence this phase are 'other-participants', activities between 'user' and them, and all interactions among those and the 'environment'. Every team member gains additional authorizations from the customer roles of all his teammates (combination – first step) which may be specified in

more details with the context of his team (filtering - final step). As a result, items which were never presented to him before, it is predicted that they are proper and they actually are offered, because they belong in the context of his team (active security collaborative permissions).

Even when we are not interested for the community factor, C-TMAC and its context-sensitivity can obviously be utilized to support the supplementary form of advanced filtering, the content-based filtering technique (phase 'B.2' of authorized personalization as depicted in figure 3.B.2). In this case, we deal with another form of teams, the content-based teams (CBk). There is not users-to-teams assignment consideration, but more work has to be done for context-to-team assignment. The context categories (fig. 1) that influence this phase are 'environment', and 'environment activities' as we analyzed in previous paragraphs. In addition, 'user activities' influence also the construction and the authorizations of the content-based teams, because user's history (purchases, requests for extra information, navigation paths etc.) may also be taken into account during runtime, resulting in active security non-collaborative permissions.

Rule-based methods are actually authorizations on a user basis. C-TMAC can integrate this kind of personalization practices (phase 'C' of authorized personalization in figure 3.C). Simply, we may consider a third type of teams, the rule-based teams RBn, in which individual customers (users) are allowed to participate when their activities fulfill manually configured conditions. But it must be noticed that the resulting authorizations are by some means different. They surely can be categorized as 'active security permissions', because they are also context-based (influenced exclusively from 'user activities', context scheme in figure 1). On the other hand, they produce considerable administrative overhead, because the rules which govern the user-to-team participation have to be manually configured. Additional difficulties are originated from the fact that these rules must refer to individual customers and not categories (roles) of them. So, related disadvantages come from the very nature of these personalization mechanisms and not from the access control engine in use.

In general, phases 'B.1' and 'B.2' (if exist) are independent. But perhaps in certain m-commerce cases, it could make sense to describe precisely in what way user participation in a content-based team impacts his potential participation in a collaborative team. Also, 'B.2' and 'C' are in general self-sufficient phases which they can be applied autonomously and then to just combine their resulting authorizations. But similarly, sometimes the rules which build rule-based teams RTn can utilize conditions concerning user participation in collaborative teams CTK. On the

contrary, a semantic relationship exists between phases 'B.1' and 'C' (users in roles targeting specific objects and users in teams satisfying specific conditions on objects), and obviously between phases 'A' (role assignment) and 'B.i' (role participation in teams).

Finally, it is worth mentioning that implementing a context-sensitive access control system, has supplementary adjacent advantages for the personalization mechanisms: the initial process of accumulation of user information (tracking user's behavior) is facilitated by using model's (continuously recorded during runtime) enriched security metadata and log files.

7. Conclusion– Future work

Mobile devices are context-sensitive while accessing the wireless Internet. As user priorities, environmental conditions, participants' status, activities and interactions change, applications must function conveniently and properly configured. It is a challenging task to take the complexities of context into account during the design and use of m-commerce applications. On the other hand, this is a viable way to produce various business opportunities, such as the ability to offer highly targeted advertising or the ability to provide both Internet information and other services based on awareness of a user's location.

Adaptive services based on context-awareness are indeed a precious benefit of mobile applications: in order to improve their provided service, mobile applications can actually take advantage of the context to adjust their behaviors. Devices constraints, mobile setting's distracting environment and the 'personal' character of the mobile Internet (as it is expressed by the user's preferences for more personalized services), stand for the importance of adaptation and personalization technology in m-commerce systems.

In this work, we first present personalization issues independently from their security considerations. Then, we outline personalization in conjunction with access control reflections (authorized personalization). Based on previous reliable surveys for personalization technology, and on a particular and adequate context-sensitive authorizations model, we analyze the implications of personalization mechanisms on it, in order to achieve effective, secure and convenient m-commerce applications.

Future work includes a detailed case study concerning C-TMAC's influences on content-based and collaborative filtering operations. We will examine the applicability and the significance of the three distinct combination methods (aggregation, minimum/maximum, current team structure) for

customer role permissions in all three previously referred types of teams, and we will define team context (of all team types) according to the predefined context scheme. Also, we will examine the impact of personalization mechanisms on multimedia content and the mutual influence among digital rights management concepts and m-commerce's context-awareness.

References

- [1] Mulvenna D.M., Anand S.S., and Buchner G.A., "Personalization on the Net using Web Mining", *Communications of the ACM*, Vol. 43. No.8, pp. 123-125, 2000.
- [2] Elliot G., and Phillips N., *Mobile Commerce and Wireless Computing Systems*, Addison Wesley – Pearson Education, 2004.
- [3] Deitel H.M., Deitel P.J., Nieto T.R., and Steinbuhler K., *Wireless Internet and Mobile Business*, Prentice-Hall, 2002.
- [4] Bhatnagar A., Misra S., and Rao H.R., "On risk convenience, and Internet shopping behavior", *Communications of the ACM*, Vol. 43, No. 11, pp. 98–105, 2000.
- [5] Tarasewich P., "Designing Mobile Commerce Applications", *Communications of the ACM*, Vol.46, No.12, pp. 57-60, 2003.
- [6] Cingil I., Dogac A., and Azgin A., "A Broader Approach to Personalization", *Communications of the ACM*, Vol. 43, No.8, pp. 136-141, 2000.
- [7] Laudon C.K., and Traver G.C., *E-commerce: Business, Technology, Society*, Addison Wesley – Pearson Education, 2003.
- [8] Pierrakos D., Paliouras G., et al., "Web Usage Mining as a Tool for Personalization: A Survey", *User Modeling and User-Adapted Interaction* 13: pp. 311-372, Kluwer Academic Publishers, 2003.
- [9] Rayport J., and Jaworski B., *Introduction to E-Commerce*, 2nd Edition, NY: McGraw-Hill, 2004.
- [10] Lee Y.E., and Benbasat I., "A Framework for the Study of Customer Interface Design for Mobile Commerce", *International Journal of Electronic Commerce*, 1086-4415/2004, Vol. 8, No. 3, pp. 79–102, 2004.
- [11] Tolone W., Ahn G-J, and Pai T., "Access Control in Collaborative Systems", *ACM Computing Surveys*, Vol. 37, No. 1, pp. 29-41, 2005.
- [12] Georgiadis C.K., Mavridis I, Pangalos G., and Thomas R.K., "Flexible Team-based Access Control Using Contexts", *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies (SACMAT 2001)*, Chantilly, VA, USA , pp. 21-27, ACM Press, 2001.
- [13] Sandhu R., "Role-Based Access Control", *Advances in Computers*, V.46, Academic Press, 1998.
- [14] Georgiadis C., Mavridis I., Nikolakopoulou G., and Pangalos G., "Implementing Context and Team Based Access Control in Healthcare Intranets", *MED. INFORM. INTERNET*, Vol. 27, No. 3, pp. 185-201, 2002.



Christos K. Georgiadis is currently a Lecturer in the Department of Applied Informatics at the University of Macedonia, Greece. He received a Ph.D. in security for information systems & web databases from Aristotle University, Greece (2002); a postgraduate scholarship in informatics, Univ. di Pisa, Italy (1989); and a B.Sc. in mathematics from Aristotle University, Greece (1987). Dr. Georgiadis also worked in the University of Thessaly in Greece as a lecturer and in the Aristotle University, as a research associate. His research interests include the areas of e-/m-commerce technologies, multimedia databases, electronic and mobile commerce security, and web services technologies. He is a member of ACM – SIGEcom.



Ioannis Mavridis is a Lecturer in the Department of Applied Informatics of University of Macedonia (UoM). He has a Diploma in Computer Engineering and Informatics from the University of Patras (1985) and a Doctor's (Ph.D., 2000) degree in Mobile Computing Security from Aristotle University of Thessaloniki (AUTH), Greece. He has taught informatics and information systems security in UoM, AUTH, Hellenic Open University and TEI of Thessaloniki. He is a member of Greek Computer Society, Technical Chamber of Greece and WG 11.3 on Database Security of IFIP. His research interests include the areas of information system and network security, mobile computing, semantic web, and software engineering.



Athanasios Manitsaris is currently an Associate Professor in the Department of Applied Informatics at the University of Macedonia, Greece. He has a Ph.D. from University of Macedonia, Greece (1992); a DEA Mathématiques Statistiques, from Univ. de Paris VI, France (1977); and a B.Sc. in mathematics, Aristotle University of Thessaloniki, Greece (1975). His research interests include multimedia and Internet technologies, human-computer interaction and multimedia databases.