Int. J. Inf. Secur. (2014) 13:571–581
DOI 10.1007/s10207-014-0229-x

REGULAR CONTRIBUTION

A conceptual model of security context

Vladimir Jovanovikj · Dušan Gabrijelčič · Tomaž Klobučar

Published online: 8 March 2014

Abstract Ubiquitous environments which embrace the trends of enterprise mobility and the consumerization of IT have an increasing social importance. In these environments, the same device and applications are simultaneously used for both personal and professional purposes. Such usage blurs the boundaries between personal and professional domains and presents many challenges for information security. Context-aware security has been proposed as a solution for many of them. We argue that the existing approaches are limited and mainly deal with targeted use cases. They do not provide a clear and complete understanding of the context relevant for security, and use contextual information with an arbitrary level of abstraction. In order to address these issues, we propose a conceptual model of security context. The model identifies important concepts of security context and takes related social aspects into account. It represents the security context through a set of concepts at the appropriate level of abstraction. We show that our model is suitable to analyze various situations from the perspective of security and compare them with the existing approaches. The model promises to facilitate the specification and management of security policies containing contextual information as well.

Keywords Security · Context · Ubiquitous computing

1 Introduction

Ubiquitous computing is an intelligent coalition of the physical and virtual world, integrated for the purpose to assist people in their everyday life [60]. Contemporary mobile devices are bringing us closer to this vision as a single device capable of supporting multiple functionalities of it [52]. Indeed, it has been shown that a mobile device can facilitate the interaction between people and objects and helps the user to access ubiquitous services [44]. Today, people are already extensively using mobile devices for communication, education, and entertainment, and enterprises are incorporating them into their practices to increase the efficiency, effectiveness, and convenience of their business processes [7,8]. As people became attached to their own mobile devices, they insist using them, together with their familiar services, in their professional life as well. Initial positive experiences in the form of lower costs and increased employee productivity and satisfaction have recently caused this to develop into a modern enterprise trend known as the consumerization of IT [15,18,29,42].

The ubiquitous environments encompassing the trends of enterprise mobility and the consumerization of IT has an increasing social importance. It means a user-owned mobile device is used to perform both personal and professional activities, anywhere and anytime. Many of these activities are often performed simultaneously, usually with the same consumer-oriented applications, and this blurs the boundaries between the domains of personal and professional life. As people increasingly work for more than one organization and in complex collaboration patterns [30], these environments will span over many administrative domains. We refer to these environments as ubiquitous social systems.

Ubiquitous social systems present three main challenges for information security. First, the enforcement of corporate security policies becomes difficult because enterprises have less control over the devices and applications used in their business processes. Since employees are the owners of the devices, enterprises cannot demand they use the strongest security outside the enterprise domain and do not install

V. Jovanovikj (✉) · D. Gabrijelčič · T. Klobučar
Laboratory for Open Systems and Networks, Jožef Stefan Institute, Jamova cesta 39, 1000 Ljubljana, Slovenia
e-mail: vladimir@e5.ijs.si

various applications on their devices. Second, the protection of resources becomes complicated as users make increased interactions with their devices. These interactions are often ad hoc, unplanned and with possible leakages of implicit information due to the modern forms of communication [13,45,47]. Finally, the security provision should understand the trade-off between security, performance, and efficiency in order to better utilize the limited hardware resources of mobile devices and operate with minimal human involvement [28,45,50,58].

Many researchers have proposed context-aware security provisioning as a possible solution to overcome the challenges of ubiquitous social systems. However, their approaches provide only limited solutions. They deal only with targeted use cases (e.g., smart spaces: home [16], workplace [3], or hospital [2,17,37], mobile workers [23,34,59], or network communication [6,36]) and mainly provide a single security service (e.g., access control [2,16,17,23,34,37,59], authentication [25,46], secure channel communication [36,48], or identity management [24,56]). The consequences from this are twofold.

First, the existing context-aware security approaches are not based on a clear and complete understanding of the context relevant to security. They usually consider it identical to the context in general (e.g., [2,4,16,23,27,36,37,59]), although it arises from activities relevant to security and is thus specific to the security domain. At the same time, they rarely specify what contextual information they take into consideration. Because of the variety of possible contextual information, it is difficult to understand what they are aware of and adapt to. In addition, the existing approaches (e.g., [2,4,16,34,36,41,54,59]) utilize only part of the available contextual information and omit important contextual information, for example the social context.

Second, the existing context-aware security approaches (e.g., [4,6,16,34,46]) adapt to an arbitrary level of abstraction of contextual information. This can be cumbersome, error-prone and can jeopardize the validity of the security service. Since there is a vast amount of information which can be used as the context, researchers have pointed out that it is more sophisticated for context-aware systems to adapt to contextual information with a higher level of abstraction [10,19,61]. These information meaningfully interpret raw sensor data through the process of context reasoning. They better represent the human perception of reality and are more stable than sensor data which can be uncertain and change frequently.

As a solution for ubiquitous social systems, we envision a security system with the following capabilities. Such system should manage various security mechanisms in order to provide several security services (e.g., access control, data confidentiality and integrity, auditing). It should support different levels of security and multiple security mechanisms for a single security service. Moreover, it should adapt these security levels and mechanisms depending on the domain in which the mobile device is used, and the surroundings. Several tasks are challenging in the designing and developing of such a security system, and in this paper, we point out the specification of the context relevant for security. A conceptual model of the security context is required as prerequisite for this task.

This paper addresses the above issues and helps towards a better understanding of the security context. We propose a definition and conceptual model of the security context. The model identifies important concepts of the security context, at different levels of abstraction. It introduces several concepts which take into account the socially related aspect. The model represents the security context as a set of concepts which we consider to be at the appropriate level of abstraction. We evaluate the flexibility and sufficiency of the model using two methods. First, we use the model to analyze the diverse use cases of ubiquitous social systems. Then, we compare it with the existing approaches, especially with their understanding of the security context. In addition, we point out several gaps in the existing approaches that elicited from the comparison. Our model promises to facilitate the specification of the security context in context-aware security systems that are applicable for ubiquitous social systems as a whole.

The paper is structured as follows. First, we describe a motivation scenario to illustrate ubiquitous social systems, in Sect. 2. Next, in Sect. 3, we make an overview of related works defining and describing the security context. Afterward, we give our working definition of the security context in Sect. 4. Then, we present our conceptual model of the security context in Sect. 5. This is followed by a discussion about the applicability of the model and the security requirements of the security context in Sect. 6. We evaluate the model with two methods, and for one of them, we use the scenario from Sect. 2. Finally, we conclude the paper in Sect. 7.

2 Motivation scenario

We present a typical scenario for ubiquitous social systems. It concentrates mainly on activities performed within the professional domain, since they are the more attractive targets for attacks and thus more challenging for security. However, its translation to the personal and other domains is quite straightforward. The scenario includes general and simple use cases originating from the area of enterprise mobility. Similar use cases have been described in several works [7,26,57] and encountered in common practice. The use cases are further enriched with the characteristics of the IT consumerization, which are a major influence for security. In addition, they take

into account the security guidelines for enterprise mobility as presented in standardized security documents [32].

The scenario centers around Alice, a researcher working for the ACME company. Alice is allowed to use her personal mobile device for professional purposes, as well as various consumer applications that she finds productive. She is satisfied with this—her favorite file manager and office applications are on the company's list of allowed applications. However, she feels work to be a bit more difficult without the help from her favorite intelligent personal assistant.

The ACME company requires relevant parts of its security policy to be implemented on Alice's device, although it is aware that it does not have full control over the device. In particular, it is interested in using appropriate security mechanisms and having control over its resources that are accessed through the device. Mobile malware is on the rise lately, and applications routinely require extensive permissions during installation [38]. Therefore, the company wishes to limit certain functionalities of some applications, such as access to data, sensors, and networks, while completely forbidding applications whose core functionality is a threat to its resources. For example, intelligent personal assistant applications are forbidden because they send audio recordings to remote servers and can potentially leak confidential company conversations.

Alice is currently participating in several research projects, in which the company collaborates with other partner organizations. For one of them, a meeting is scheduled during a larger conference event hosted by the company. Alice is supposed to present her work at this meeting. The rest of the scenario centers around that particular conference day.

Scene 1: At Alice's home: Alice is making the final revision of her slides for the presentation. She is using her favorite office app on her mobile device for this purpose. While editing, Alice opens a personal document with the same app. The app should be allowed to only read this document, but not edit it. This prevents it from transferring company data into the personal document. Alice leaves her apartment, while both documents remain open. The presentation slides should be closed automatically.

Scene 2: Coffee break at the hall: Alice and her colleague Bob are reviewing the slides for the meeting on their mobile devices. Alice sends Bob the latest version of the slides over a wireless channel, with her favorite file manager app. Usually, the transmission of unencrypted company documents between colleagues is allowed in company premises, as long as there are only company employees around. However, at that moment, many visitors to the event are present in the hall. Some of them may be from a competitive company, trying to capture an unencrypted communication between ACME employees. Therefore, a secure channel between Alice's and Bob's mobile device must be established prior to the transmission.

Scene 3: Project meeting at a conference room: Alice is about to present her slides to the project members, using her mobile device. She activates the slideshow from the office app, and this activates the transmission to the projector. As outside the conference room there are people who are not members of this project, a secure channel with the projector is established first. During the presentation, the janitor suddenly enters the conference room. Since he is not a project member, he is not allowed to see the confidential project data on the screen. Therefore, the presentation should be automatically terminated.

Scene 4: On the way home: Alice leaves the company's premises. According to the company's security policy, logging is mandatory during work. Since Alice has finished work, this should be turned off automatically. Also, all open company documents and intranet pages should be closed. Alice starts her intelligent personal assistant app and requests it to start playing her favorite song. While walking home, she receives a call from her colleague. Prior to taking the call, the assistant app should be terminated and the logging should be turned on again. In addition, Alice should be warned to be careful as she is making a confidential conversation in insecure environment and somebody might listen to it.

3 Related work

The notion of context has been widely discussed during the past years by many researchers from various disciplines, such as computer science, linguistics, and psychology [9]. Although their understanding of context strongly depends on their specific domains, some characteristics of context appear to be common. Context acts as a set of information that influences the behavior of a system, such as the system's description, the system's users, and the environment in which the system operates. However, it arises from activity and includes only those items that are relevant to the particular activity at hand [1,20].

Only a few works have explicitly defined security context. Johnson [35] combined acknowledged definitions of context and security, and defined the security context as any information that characterizes the situation of an entity and has security implications. As an entity, she considers the user, the user's computing device, and the surrounding environment. Kouadri-Mostefaoui [41] defines the security context as a set of information from the user's and application's environments that are relevant for the security process. She further describes it as the state of these environments requiring security interventions. In addition, Bandinelli et al. [6] are concerned only with contextual information which originates from the communication between entities and is useful for providing end-to-end security.

Existing definitions of the security context are incomplete and do not represent the full nature of the context. They specify only information about part of the relevant entities, namely the user and the particular device that hosts the context-aware system. This is insufficient for ubiquitous social systems, for which contextual information about other surrounding entities (people and devices) need to be also taken into consideration. Moreover, current definitions describe only the static nature of the context, omitting the notion of activities which guide the creation of the security context.

Furthermore, a few works also tried to more precisely describe the security context with taxonomies. Johnson [35] classifies the security context along two dimensions—the relevant entity and the affected security objective—and provides simple guidelines to identify the relevant security context. Evesti and Pantsar-Syväniemi [22] define important concepts for the security context and classify them into three groups: (i) the situation context, which contains concepts describing the usage of applications, (ii) the digital context, which contains concepts describing the surrounding environment, and (iii) the physical context, which contains concepts describing the execution platform. Cuppens and Cuppens-Boulahia [17] recognize several types of security context in their taxonomy: the temporal, the spatial, the user-declared, which is related to the user's intention, and the prerequisite and the provisional contexts, which are related to the preconditions and obligations of activities. In addition, Bandinelli et al. [6] divide the possible security context into several categories: user, device, communication, and application, depending on their origin.

Current taxonomies do not seem very helpful for context specification. Although their category types are related to important concepts of the security context, they are still mostly useful only to describe the security context. Moreover, they rarely take into account the related social aspect. Only a few of them, [17,22], try to use social concepts, such as the role of the user and environment and the objective of the user. However, this is done only arbitrarily, without any attempt to define these concepts in a consistent manner.

4 Definition of security context

Our definition of security context combines the notions of security and context. It is based on one of the widely accepted definitions of context given by Day et al. [1]. It further emphasizes the dynamic nature of context and the role of activities. For clarity, we do not include any explicit definition of security in it. We refer to security as the protection of resources in order to attain the objectives of confidentiality, integrity, and availability [11,55]. Our definition of the security context is given below.

Security context is a set of contextual information considered relevant for the process of security, regarding a particular task or activity.

Contextual information is any information that can be used to characterize the situation of an entity. An entity can be a person or a device, which can be seen as a composition of its resources.

Analogously to systems in general [14], security systems can utilize the security context in two ways. Systems that can only present information about the security situation of the resources of interest, depending on the current security context, can be referred to as passive context-aware security systems. On the other hand, systems that automatically adapt their behavior during runtime in accordance with the discovered security context, in order to provide a more relevant service, are called active context-aware security systems. In the rest of the paper, the usage of the term context-aware security systems refers to the active ones.

5 Conceptual model of security context

We propose a conceptual model of security context in order to define its notion more precisely. The conceptual model identifies important concepts that constitute the security context and the relations between them (Fig. 1). Many of these concepts elicit directly from the motivation scenario in Sect. 2. For example, there are persons (e.g., Alice and Bob) who use devices (e.g., their mobile devices) and perform various

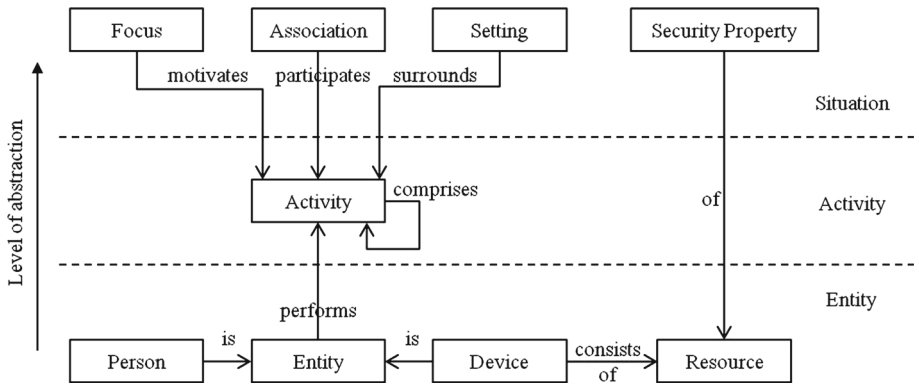

Fig. 1 Conceptual model of security context

activities (e.g., share work documents) which are more precisely described with the persons' intention, social relation, and surrounding environment (e.g., sharing work documents with a colleague at a public event while working). We separate the identified concepts into three layers: entity, activity, and situation (Fig. 1). Each of them has a different level of abstraction from the perspective of a context-aware system—concepts from a lower layer are used to derive concepts from a higher layer and thus need to be determined beforehand. In fact, this represents how a system becomes aware of the context in which it operates, through the process of context reasoning.

5.1 Entity

An entity performs an activity and thus is the subject whose situation needs to be characterized. Our model centers around two types of entities—a person and a device. A person is a human individual that operates with devices, whereas a device is an object with computing and communication capabilities. We denote the set of entities, $E = P \cup Dev$, as a union of the set of persons P and the set of devices Dev. Two entities are of particular importance for our discussion: the device that hosts the context-aware security system—the host, $h \in Dev$, and the person operating this device—the user, $u \in P$.

A device can be seen as a composition of three types of resources: data, channel, and method [40]. The data represent an information in a form understandable to devices or persons. It can be kept as a file, read from a sensor, or received from another entity. A channel represents a pathway through which the user or any other device communicates with the host. Examples of such pathways are sockets and named pipes. A method represents a software component that implements a certain functionality, which can be executed through its interface (API). Methods are usually combined in applications, which enable achievement of more complex functionalities. We recognize security mechanisms as methods in our model We denote the set of resources as $Res = D \cup M \cup C$, where D is the set of data, M is the set of methods, and C is the set of all active channels that a device, for example h, has.

Entities can be described with various contextual information that can be acquired from physical and virtual sensors. Physical sensors are hardware components, such as GPS, camera, microphone, accelerometer, and many others which can be already present in contemporary mobile devices, whereas virtual sensors are software components providing contextual information taken from various sources [5], such as applications, protocols, social networks. Contextual information can be acquired either from sensors on the host or from an external context provider. Table 1 shows examples of contextual information, associated with the representing entities.

Table 1 Examples of contextual information, associated with entities

Entity	Contextual information
Person	Age, gender, relations, religion
Device	OS information, owner, location, time
Resource	Data value, protocol, sec. mech. strength

5.2 Activity

An activity is the process in which an entity executes organized operations while trying to accomplish certain goals. It is performed either explicitly by the user while interacting with the host or implicitly by the host itself. An activity whose goals are related to the protection of resources is called security activity.

Generally, activities are performed with an application by executing a specific method over resources. Some activities are more complex than other and comprise several activities that are consecutively performed. We represent an activity in our model as a tuple of tuples (app, op, obj), where $app \subseteq M$ is the application used for performing the activity, $op \in M$ is the method that implements the operation of the activity, and $obj \subseteq Res$ are the resources upon which the activity is performed, i.e., objects of an activity. We denote the set of all activities as A. For clarity reasons, in the rest of the paper, we represent activities with their description in words. For example, an activity described as "$offapp$ reads data d_1" is represented as a tuple $(offapp, read - data, d_1)$.

As an example of complex activity, consider an activity described as "$offapp$ presents data d_1", which comprises several other activities: "$offapp$ reads data d_1", "$offapp$ opens channel c_1", and "$offapp$ shares screen through channel c_1". Similarly, a complex security activity is "app_1 establishes confidential channel c_1", which is comprised of several (security) activities that are executed during the SSL protocol handshake.

5.3 Situation

A situation better interprets an activity and gives more meaning to it. It describes the state of the relevant entities and the relationship among them [10,19]. We define several concepts suitable for representing situation. We separate them in two groups—social concepts and properties.

5.3.1 Social concepts

Social scientists have observed that during their life, people do not act simply as individuals in an undefined manner, but

take part of various social groups (communities) in order to achieve their goals more easily [21,43]. The common goals and interests of these groups shape the activities performed within them. Group members divide these activities among themselves according to the qualifications needed to accomplish them successfully, and this is represented as roles in the social group. The roles and the distribution of activities make social groups highly organized. Depending on these goals and roles, social groups can be categorized into social domains. Examples of social domains include family, friends, workplace, education, health care, research department, city, country, while examples of social groups include their particular realization. A research department social domain, for example, is defined by roles such as the head of the department, researcher, student or developer, and common goals such as solving scientific challenging problems, proving the feasibility of proposed solutions.

Devices and data can also be associated with social groups. Some devices perform important activities in ubiquitous social systems and are useful for a number of people, not just for a single person. Therefore, they can be considered as members of social groups and can have assigned roles that stem directly from the purpose of their use. Such devices are for example: printers, network access points, payment terminals, access control devices, attendance devices, information devices. On the other hand, a data can have assigned a social group according to the meaning of its content, which is especially important for protection of its confidentiality.

Since people (and devices) are often part of a single social group from a social domain, in the rest of the paper, we will refer to social groups by their social domains, to make things as clear as possible. For example, instead of referring to a particular family as a social group, we will refer to it as a family group, from the perspective of the user. Moreover, we will consider that by default all entities are part of a general social group called public social group.

We refer to an entity which can be a member of a social group as a social entity, $se \in SE$, $SE = P \cup SDev$, where $SDev \subseteq Dev$. Let G be a set of possible goals that can result from activities and Rol be a set of possible roles that can represent qualifications needed to successfully accomplish activities. A social domain $sd \in SD$ is defined as a tuple, $sd = (gls, rls)$, of specific goals $gls \subseteq G$ whose achievement is a reason for social entities to organize in a social group, and a set of specific roles $rls \subseteq Rol$ according to which activities that result in goals gls are divided between those entities. A social group, $sg \subseteq SE \times Rol$, is an implementation of a social domain and is defined as a set of tuples (se, rol) of social entities se and their assigned role rol, such that all roles are part of a single social domain sd. We represent the set of all social groups as SG.

Based on the notion of social groups, we define three social concepts: focus, association, and setting.

Focus People often consecutively perform activities from different social domains in ubiquitous social systems. Some activities and their related goals are more important than others at a given moment and are thus considered as primary. For example, while working, a person can quickly do something related to other social domains (e.g., call a friend or read personal email), but their work activities and goals remain primary. The focus describes the primary intention and orientation of the user and motivates their behavior at a given moment. We define focus, $focus \in SG$ as a primary social group for the user at a given moment.

Association Except the user, other entities can also be involved in an activity as participants. We denote the set of participants of an activity a as $par_a \subseteq SE \backslash \{u\}$. It is impractical to represent the participants individually as their number can be large for some activities. Instead, a social group common for all of them describes them better. Let $se_g \subseteq SG$ represents the set of social groups that a social entity se is part of. Also, let $common : 2^{SE} \rightarrow 2^{SG}$ be a function that maps an arbitrary set of social entities $B \subseteq SE$ to an intersection of social groups they are all part of, $common(B) = \{sg \in SG \mid \forall se \in B(sg \in se_g)\}$. Then, we define association of an activity $a, assoc_a \in SG$, as a common social group of the user and a non-empty set of participants in that activity, $assoc_a \in common(\{u\} \cup par_a)$, $par_a \neq \emptyset$. In case there is a single common social group, association is uniquely determined. However, in case of more than one common social groups between participants, focus can be of help in determining association. If $focus \in common(\{u\} \cup par_a)$, then $assoc_a = focus$, else $assoc_a = public$, since all entities are members of the public social group by default. In addition, if there are no participants in an activity, the association for it is null, $assoc_a = \emptyset$.

Setting Activities are performed in various environments, which can change dynamically in ubiquitous social systems. Except the participants, these environments can comprise many other social entities, referred to as observers. An observer of an activity is an entity that is near the user or is part of a channel used in that activity. We denote the set of observers of an activity a as $obs_a \subseteq SE \backslash \{u\}$. In a same way as participants, observers are better described with their common social group than individually. We define setting of an activity a, $sett_a \in SG$, as a common social group of the user and a non-empty set of observers of that activity $sett_a \in common(\{u\} \cup obs_a)$, $obs_a \neq \emptyset$. Same as for association, focus can be of help in determining setting. If $focus \in common(\{u\} \cup obs_a)$, then $sett_a = focus$, else

$sett_a = public$. In addition, if there are no observers for an activity, the setting for it is null, $sett_a = \emptyset$.

5.3.2 Property

A property is a quality that describes a resource or its usage. We define a property pr as a function that maps a resource $r \in Res$ to a certain value. In its simplest form, it is a function $pr : Res \rightarrow \{0, 1\}$. In this case, a value $pr(r) = 1$ denotes that the property of the resource is achieved, whereas $pr(r) = 0$ denotes the opposite. We denote the set of all properties as PR.

From all properties, security properties of resources are of special importance for our discussion. Generally recognized security properties are confidentiality, c, integrity, i, and availability, a [11]. We emphasize that evaluation of security properties of resources should not be seen as verification that security services, or their implementation, provide the particular security properties. Except as contextual information, security properties of resources are often used as an indicator of the security system operation. For an activity a, the current values of security properties of all resources that are of interest and are involved in a comprise a tuple, $sprop_a = (pr_1(r_1), pr_1(r_2), \ldots, pr_n(r_m))$, where $pr_i \in PR$ and $r_j \in Res$.

5.4 Summary

To sum up, the security context for a particular activity a is a tuple, $SecCon = (a, focus, assoc_a, sett_a, sprop_a)$, consisted of the activity itself, the focus of the user, $focus$, the social concepts that characterize a—association, $assoc_a$, and setting, $sett_a$, and the current values of the security properties of resources that are currently involved in a. For a continuous activity, the security context is dynamically updated as other activities are performed.

6 Discussion

We show the applicability of our model in an empirical manner. First, we use it to analyze the motivation scenario from Sect. 2. During this analysis, we describe a possible operation of a context-aware security system (CASS) that utilizes our model. Then, we compare it with the existing approaches, especially their understanding of the security context. Apart from showing the ability of our model in representing the security context, this comparison is also an evaluation of the understanding and specification of the security context in the existing approaches. Finally, we present the security requirements of the security context.

6.1 Model application in example scenario

We analyze two scenes from the motivation scenario into more detail. For our analysis, we assume that Alice is the user u and her mobile device is the host h of the context-aware security system that uses our model of security context. Alice is a member of four social groups: (i) the ACME company, $work = \{Alice, Bob\}$, in which she has a role of researcher, (ii) the particular research project, $project = \{Alice, \ldots\}$, in which she also has a role of researcher, (iii) her particular home, $home = \{Alice\}$, in which she has a role of inhabitant, and (iv) the particular city, $public = \{Alice, Bob, janitor, \ldots\}$, in which she has a role of citizen. We denote this as $u_g = \{work, project, home, public\}$. In addition, we assume that Alice's mobile device will keep information about the structure of the social groups she is member, i.e., about the members and their roles.

Scene 1 Alice registers to the company's time tracking software before she starts working. Based on this activity, the CASS changes her focus to her work social group, $focus = work$. In order to start reviewing her presentation slides d_1, she initiates an activity a_1: "$offapp$ edits data d_1", where $offapp$ denotes the office application. The CASS needs to examine the security context for this activity before allowing or denying it. One can imagine that this is done in the following way. Based on the facts that her focus is the work group and that d_1 is assigned for her project group, the CASS changes her focus to the project group, $focus = project$. For activity a_1, there are no other participants except Alice. Thus, the association for this activity is null. Setting is determined after the CASS scans the environment for wireless signals. Based on the recognized Alice's access point and TV, which are members of her home social group, as well as a previous activity of arriving home, setting for this activity is set to be Alice's home group, $sett_{a_1} = home$. The office app is authorized to edit project data during project focus in home setting. Therefore, CASS allows a_1 to be executed. After a_1 is started, confidentiality of d_1 is set in $sprop_{a_1}$ as achieved. Furthermore, Alice tries to read the home document with the office app. After examining the security context in similar manner, the CASS deduces that focus and setting remain the same. The office app has only permissions to read data from other groups during project focus, in order data leakage to be prevented. Thus, the CASS allows this activity too. Finally, Alice leaves her apartment with the documents remained opened. The CASS changes her focus to her public social group, $focus = public$. Since it is not allowed for the office app to edit project data in public focus, the confidentiality of d_1 is deprived. In response, the CASS closes this document.

Scene 3 Imagine that Alice uses her mobile device to authenticate at the conference room entrance. The project meeting is about to begin, so Alice's calendar notifies about the event start. Based on these two activities, the CASS is able to determine that the Alice's focus is her project social group, $focus = project$. The CASS recognizes that Alice is initiating a complex activity with the office application over the presentation slides, a_1: "$offapp$ presents data d_1". As described in Sect. 5.2, several activities precede this, during which a channel c_1 is established with a projector p_1. In order to decide whether to allow or deny a_1 (in fact the last initiated activity that led to its recognition), the CASS consults the security context for this activity. Association for a_1 can be determined based on information received from the conference room access control system (as a context provider) and the structure of Alice's social groups. As only people from partner institutions are currently present in the room, association for a_1 is set to be the project social group, $assoc_{a_1} = project$, which is their only common social group. Similarly, setting for a_1 can be derived based on various captured wireless signals. Except for the projector p_1, which is a member of the work social group $p_1 \in work$, the signals mainly come from unknown attendants outside the conference room. As a result, the setting for a_1 is set to be the public social group, $sett_{a_1} = public$. Presentation of project data in front of project association during project focus and in public setting is allowed only if confidentiality and integrity of the channel c_1 are achieved in advance. Security properties can be derived from previous activities. Since c_1 is unprotected, confidentiality and integrity of c_1 are not currently achieved. In order a_1 to be allowed, the CASS needs to adapt and establishes a secure channel over c_1, for example by using the SSL protocol. After the presentation is started, confidentiality of data d_1 is set to be achieved in $sprop_{a_1}$. Furthermore, when the janitor enters the room, the conference door access control system notifies the CASS. As a result, the security context for a_1 is updated. The association for a_1 now becomes the public social group, $assoc_{a_1} = public$. Since it is not allowed to present project data in front of public association, confidentiality of d_1 is deprived. In order to protect confidentiality of d_1, the CASS reacts by turning off the screen sharing with the projector.

6.2 Model comparison with existing approaches

We compare our model with various approaches of context-aware and adaptable security. In their characteristics and goals, they are very similar; the differences are mainly in their emphasis—the former are more concerned with the diversity of context and how to utilize it, whereas the latter mainly deal with the adaptation of their behavior. In particular, we map the security context that the existing approaches take into consideration, to our model. Moreover, we specify their adaptable behavior, which is in fact the security service these approaches provide. The results are presented in Table 2.

The comparison elicited several additional gaps in the existing approaches.

- The existing approaches seriously lack a context specification. Because of the variety of possible contextual information, it is difficult to understand what these systems can be aware of and adapt to. As a result, their applicability can become unclear.
- The existing approaches mainly adapt to low-level contextual information, acquired directly from sensors. On the one hand, this makes the definition of policies cumbersome and error-prone, because of the granularity, uncertainty, and the frequent change of this information. On the other hand, it gives an additional burden to policy evaluation and can compromise its performance, as it leads to performing context reasoning during this process.
- The existing approaches rarely use complex activities as contextual information, especially security activities. The creation of their security context is mainly guided by simple activities, which is a poor characteristic.
- Only few approaches [17,22,24,27,37,56] take contextual information from the social domain into consideration. They mainly use the concept of social relation. However, this is done only arbitrarily, without any attempt to define this concept in a consistent manner. Moreover, these approaches mainly use social contextual information to support and describe only activities, despite other possible applications.
- The existing approaches are mainly concerned only with the security properties they can achieve. They evaluate security properties on the basis of the characteristics of the security mechanisms that provide these properties, such as their strength or performance. An exception of this is [54], which tries to evaluate what specific security properties does a set of security activities achieve.
- The existing approaches mainly implicitly try to balance the trade-offs between security and other properties. Except for [46,48,51], none of the approaches track other properties more precisely.

6.3 Security requirements of security context

The correct operation of any context-aware system depends on how accurately the contextual information represents reality [12,39]. Since the contextual information directly influence the integrity of context-aware systems, their manipulation is an attractive attack vector for these systems. This applies especially to context-aware security systems, whose application is critical and can have rather severe consequences for its users. Any incorrect operation of these sys-

Table 2 Security context in context-aware security systems

References	Name	Context										Adaptable behavior
		Entity			Activity		Social			Property		
		Person	Device	Resource	Simple	Complex	Focus	Assoc	Setting	SP	OP	
Covington et al. [16]	Env. roles	✓	✓	✓	✓							AC
Al-Muhtadi et al. [3]	Cerberus	✓	✓		✓	✓				✓		A, AC
Johnson et al. [34]	Shrink-wrap. sec.			✓	✓					✓		AC
Toninelli et al. [59]	Proteus	✓		✓	✓	✓						AC
Hachem et al. [27]	Mob. Soc. ecosys.	✓		✓	✓			✓				AC
Riva et al. [46]	Progressive auth.	✓	✓	✓	✓					✓	✓	A
Evesti and Pantsar-Syväniemi [22]	Smart Space Arc.	✓	✓	✓	✓		✓	✓	✓	✓		Sev.Serv.
Spanoudakis et al. [54]	Serenity	✓	✓	✓	✓	✓				✓		Sev.Serv.
Ksiezopolski and Kotulski [36]	Adapt. PKI			✓	✓					✓		SC
Bandinelli et al. [6]	CASec for NGN	✓	✓	✓	✓							SC
Rocha et al. [48]	Adapt. protocols		✓	✓	✓					✓	✓	SC
Kulkarni and Tripathi [37]	CA-RBAC		✓	✓	✓			✓				AC
Bai et al. [4]	ConUCON	✓	✓	✓	✓							AC
Strimpakou et al. [56]	Daidalos	✓	✓		✓	✓		✓				IM
Frank et al. [24]	Persist	✓	✓		✓	✓		✓		✓		IM
Ahmed and Zhang [2]	CRAAC		✓	✓	✓							AC
Cuppens and Cuppens-Boulahia [17]	OrBAC	✓	✓	✓	✓	✓	✓					AC
Ganger [25]	Auth. Confidence	✓			✓					✓		A
Hulsebosch et al. [31]	CS Adapt. Auth.		✓	✓	✓					✓		A
Saxena et al. [51]	Auto. Sec. FW	✓	✓	✓	✓	✓				✓	✓	A, AC, SC
Kouadri-Mostefaoui [41]	CoDiS	✓	✓	✓	✓							Sev.Serv.
Feth and Jung [23]	Data UCON	✓		✓	✓	✓						AC
Zhang et al. [62]	RelBAC	✓	✓	✓	✓				✓			AC
Sabzevar et al. [49]	Chameleon	✓	✓	✓	✓					✓		AC

A checkmark (✓) denotes that the system takes into consideration this type of contextual information. Please note that a mark in the device column denotes that the system takes into consideration contextual information about the device as a whole
Assoc association, *SP* security property, *OP* other property, *AC* access control, *A* authentication, *SC* security channel, *IM* identity management, *Sev.Serv.* several services

tems can compromise them and cause an (easier) exploitation of resources of interest they are protecting.

Contextual information needs to be appropriately secured and verified prior to its use in context-aware security systems, in the same manner as data in general. In particular, three integrity properties of data need to be assured [53]: (i) data integrity, which is the property that the value contained in the data have not been changed in an unauthorized manner, (ii) source integrity, which is the property of the data to be trustworthy, based on its source, and (iii) correctness integrity, which is the property that the underlying information represented by the data is accurate and consistent. For this purpose, standard security mechanisms for data security can be used [33]. In addition, the confidence in correctness of contextual information can be built on the basis of their quality, usually represented through accompanying quality parameters [12,39].

7 Conclusion

Ubiquitous social systems require context-aware security provisioning. However, the existing approaches are not applicable as they do not have a clear and complete understanding of the security context and use contextual information with an arbitrary level of abstraction. We proposed a conceptual model of the security context to address these issues. The model identified the important concepts of the

security context, introducing several social concepts defined in a consistent manner. We demonstrated the flexibility and sufficiency of our model with two methods. First, we applied it to analyze a typical ubiquitous social system scenario from the perspective of security. Then, we compared it with the existing approaches, especially regarding their understanding of the security context. We observed several additional issues of existing systems from this comparison. Additionally, we discussed the security requirements of the security context.

Our conceptual model of the security context brings several benefits. It may facilitate the specification, management, and reuse of security policies for ubiquitous social systems, as it introduces meaningful concepts with a higher level of abstraction. At the same time, it may improve the process of policy evaluation, as it promotes the decoupling of this process from the context reasoning. As a result, our model promises to improve the design and development of context-aware security systems that overcome many of the security challenges of ubiquitous social systems.

Acknowledgments This work was supported by the Slovenian Research Agency (ARRS).

References

1. Abowd, G.D., Dey, A.K., Brown, P.J., Davies, N., Smith, M., Steggles, P.: Towards a better understanding of context and context-awareness. In: Gellersen, H.W. (ed.) Handheld and Ubiquitous Computing. Lecture Notes in Computer Science, vol. 1707, pp. 304–307. Springer, Berlin (1999)
2. Ahmed, A., Zhang, N.: Towards the realisation of context-risk-aware access control in pervasive computing. Telecommun. Syst. **45**(2–3), 127–137 (2010)
3. Al-Muhtadi, J., Ranganathan, A., Campbell, R., Mickunas, M.D.: Cerberus: a context-aware security scheme for smart spaces. In: Proceedings of the IEEE International Conference on Pervasive Computing and Communications, PerCom '03, pp. 489–496. IEEE Computer Society (2003)
4. Bai, G., Gu, L., Feng, T., Guo, Y., Chen, X.: Context-aware usage control for android. In: Jajodia, S., Zhou, J. (eds.) Security and Privacy in Communication Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 50, pp. 326–343. Springer, Berlin (2010)
5. Baldauf, M., Dustdar, S., Rosenberg, F.: A survey on context-aware systems. Int. J. Ad Hoc Ubiquitous Comput. **2**(4), 263–277 (2007)
6. Bandinelli, M., Paganelli, F., Vannuccini, G., Giuli, D.: A context-aware security framework for next generation mobile networks. In: Schmidt, A., Lian, S. (eds.) Security and Privacy in Mobile Information and Communication Systems. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 17, pp. 134–147. Springer, Berlin (2009)
7. Basole, R.C.: The value and impact of mobile information and communication technologies. In: Proceedings of the IFAC Symposium on Analysis, Modeling & Evaluation of Human-Machine Systems, pp. 1–7 (2004)
8. Basole, R.C.: The emergence of the mobile enterprise: a value-driven perspective. In: International Conference on the Management of Mobile Business, ICMB 2007, pp. 41–41. IEEE (2007)
9. Bazire, M., Brézillon, P.: Understanding context before using it. In: Dey, A., Kokinov, B., Leake, D., Turner, R. (eds.) Modeling and Using Context. Lecture Notes in Computer Science, vol. 3554, pp. 29–40. Springer, Berlin (2005)
10. Bettini, C., Brdiczka, O., Henricksen, K., Indulska, J., Nicklas, D., Ranganathan, A., Riboni, D.: A survey of context modelling and reasoning techniques. Pervasive Mob. Comput. **6**(2), 161–180 (2010)
11. Bishop, M.A.: The Art and Science of Computer Security. Addison-Wesley, Boston (2002)
12. Buchholz, T., Schiffers, M.: Quality of context: What it is and why we need it. In: Proceedings of the 10th Workshop of the OpenView University Association: OVUA'03 (2003)
13. Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G., Mickunas, M.D.: Towards security and privacy for pervasive computing. In: Okada, M., Pierce, B., Scedrov, A., Tokuda, H., Yonezawa, A. (eds.) Software Security : Theories and Systems. Lecture Notes in Computer Science, vol. 2609, pp. 1–15. Springer, Berlin (2003)
14. Chen, G., Kotz, D.: A survey of context-aware mobile computing research. Technical report, Department of Computer Science, Dartmouth College (2000)
15. Clarke, J., Hidalgo, M.G., Lioy, A., Petkovic, M., Vishik, C., Ward, J.: Consumerization of IT: top risks and opportunities. Technical report, European Network and Information Security Agency (ENISA) (2012)
16. Covington, M.J., Long, W., Srinivasan, S., Dev, A.K., Ahamad, M., Abowd, G.D.: Securing context-aware applications using environment roles. In: Proceedings of the ACM Symposium on Access Control Models and Technologies, SACMAT '01, pp. 10–20. ACM (2001)
17. Cuppens, F., Cuppens-Boulahia, N.: Modeling contextual security policies. Int. J. Inf. Secur. **7**(4), 285–305 (2008)
18. D'Arcy, P.: CIO strategies for consumerization: the future of enterprise mobile computing (2011)
19. Dey, A.K.: Understanding and using context. Pers. Ubiquitous Comput. **5**(1), 4–7 (2001)
20. Dourish, P.: What we talk about when we talk about context. Pers. Ubiquitous Comput. **8**(1), 19–30 (2004)
21. Engeström, Y., et al.: Activity theory and individual and social transformation. Perspectives on activity theory, pp. 19–38 (1999)
22. Evesti, A., Pantsar-Syväniemi, S.: Towards micro architecture for security adaptation. In: Proceedings of the European Conference on Software Architecture: Companion Volume, ECSA '10, pp. 181–188. ACM (2010)
23. Feth, D., Jung, C.: Context-aware, data-driven policy enforcement for smart mobile devices in business environments. In: Schmidt, A., Russello, G., Krontiris, I., Lian, S. (eds.) Security and Privacy in Mobile Information and Communication Systems. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 107, pp. 69–80. Springer, Berlin (2012)
24. Frank, K., Kalatzis, N., Roussaki, I., Liampotis, N.: Challenges for context management systems imposed by context inference. In: Proceedings of the International Workshop on Managing Ubiquitous Communications and Services, MUCS '09, pp. 27–34. ACM (2009)
25. Ganger, G.R.: Authentication confidences. In: Proceedings of the Workshop on Hot Topics in Operating Systems, HOTOS '01, p. 169. IEEE Computer Society (2001)
26. Giessmann, A., Stanoevska-Slabeva, K., De Visser, B.: Mobile enterprise applications: current state and future directions. In: Proceedings of the 45th Hawaii International Conference on System Science, HICSS 2012, pp. 1363–1372. IEEE (2012)
27. Hachem, S., Toninelli, A., Pathak, A., Issarny, V.: Policy-based access control in mobile social ecosystems. In: Proceedings of the IEEE International Symposium on Policies for Distributed Systems

and Networks, POLICY '11, pp. 57–64. IEEE Computer Society (2011)
28. Haque, M., Ahamed, S.I.: Security in pervasive computing: current status and open issues. Int. J. Netw. Secur. **3**(3), 203–214 (2006)
29. Harris, J., Ives, B., Junglas, I.: IT consumerization: when gadgets turn into enterprise IT tools. MIS Q. Exec. **11**(3), 99–111 (2012)
30. Hines, A., Carbone, C.: The future of knowledge work. Employ. Relat. Today **40**(1), 1–17 (2013)
31. Hulsebosch, R., Bargh, M., Lenzini, G., Ebben, P., Iacob, S.: Context sensitive adaptive authentication. In: Kortuem, G., Finney, J., Lea, R., Sundramoorthy, V. (eds.) Smart Sensing and Context. Lecture Notes in Computer Science, vol. 4793, pp. 93–109. Springer, Berlin (2007)
32. ISO/IEC: ISO/IEC 27002:2005: Information technology—Security techniques—Code of practice for information security management. Technical Report 27002:2005, ISO/IEC (2005)
33. ITU-T: Security architecture for open systems interconnection for CCITT applications. Technical Report. Recommendation X.800, International Telecommunications Union (ITU) (1991)
34. Johnson, G., Shakarian, P., Gupta, N., Agrawala, A.: Towards shrink-wrapped security: practically incorporating context into security services. Procedia Comput. Sci. **5**, 782–787 (2011)
35. Johnson, G.M.: Towards shrink-wrapped security: a taxonomy of security-relevant context. In: Proceedings of the IEEE International Conference on Pervasive Computing and Communications, PerCom '09, pp. 1–2. IEEE Computer Society (2009)
36. Ksiezopolski, B., Kotulski, Z.: Adaptable security mechanism for dynamic environments. Comput. Secur. **26**(3), 246–255 (2007)
37. Kulkarni, D., Tripathi, A.: Context-aware role-based access control in pervasive computing systems. In: Proceedings of the ACM Symposium on Access Control Models and Technologies, SACMAT '08, pp. 113–122. ACM (2008)
38. La Polla, M., Martinelli, F., Sgandurra, D.: A survey on security for mobile devices. Commun. Surv. Tutor. IEEE **15**(1), 446–471 (2013)
39. Lacoste, M., Privat, G., Ramparany, F.: Evaluating confidence in context for context-aware security. In: Ambient Intelligence, pp. 211–229. Springer (2007)
40. Manadhata, P.K., Wing, J.M.: An attack surface metric. IEEE Trans. Softw. Eng. **37**(3), 371–386 (2011)
41. Kouadri-Mostefaoui, G.: Towards a conceptual and software framework for integrating context-based security in pervasive environments. Ph.D. thesis, University of Fribourg (2004)
42. Niehaves, B., Köffer, S., Ortbach, K.: IT consumerization: a theory and practice review. In: Americas Conference on Information Systems, AMCIS 2012 (2012)
43. Nissenbaum, H.F.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford Law & Politics (2010)
44. Papadopoulou, E., Gallacher, S., Taylor, N.K., Williams, M.H.: A personal smart space approach to realising ambient ecologies. Pervasive Mob. Comput. **8**(4), 485–499 (2012)
45. Ramakrishna, V., Eustice, K., Schnaider, M.: Approaches for ensuring security and privacy in unplanned ubiquitous computing interactions. In: Reiher, P., Makki, K., Pissinou, N., Makki, S., Makki, S. (eds.) Mob. Wirel. Netw. Secur. Priv., pp. 167–189. Springer, US (2007)
46. Riva, O., Qin, C., Strauss, K., Lymberopoulos, D.: Progressive authentication: deciding when to authenticate on mobile phones. In: Proceedings of the USENIX Security Symposium, Security '12, pp. 15–15. USENIX Association (2012)
47. Robinson, P., Beigl, M.: Trust context spaces: an infrastructure for pervasive security in context-aware environments. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing. Lecture Notes in Computer Science, vol. 2802, pp. 157–172. Springer, Berlin (2004)
48. Rocha, B.P., Costa, D.N., Moreira, R.A., Rezende, C.G., Loureiro, A.A., Boukerche, A.: Adaptive security protocol selection for mobile computing. J. Netw. Comput. Appl. **33**(5), 569–587 (2010)
49. Sabzevar, A., Sousa, J.: Chameleon: a model of identification, authorization and accountability for ubicomp. In: Hsu, C.H., Yang, L., Ma, J., Zhu, C. (eds.) Ubiquitous Intelligence and Computing. Lecture Notes in Computer Science, vol. 6905, pp. 326–339. Springer, Berlin (2011)
50. Sandhu, R.: Good-enough security. Internet Comput. **7**(1), 66–68 (2003)
51. Saxena, A., Lacoste, M., Jarboui, T., Lücking, U., Steinke, B.: A software framework for autonomic security in pervasive environments. In: McDaniel, P., Gupta, S. (eds.) Information Systems Security. Lecture Notes in Computer Science, vol. 4812, pp. 91–109. Springer, Berlin (2007)
52. Schmidt, A., Pfleging, B., Alt, F., Sahami, A., Fitzpatrick, G.: Interacting with 21st-century computers. Pervasive Comput. **11**(1), 22–31 (2012)
53. Shirey, R.W: Internet security glossary, version 2. Technical Report RFC: 4949, The Internet Engineering Task Force (IETF) (2007)
54. Spanoudakis, G., Kokolakis, S., Gomez, A.M.: Security and Dependability for Ambient Intelligence. Springer, Berlin (2009)
55. Stallings, W., Brown, L.V.: Computer Security: Principles and practice. Prentice-Hall, New Jersey (2008)
56. Strimpakou, M., Roussaki, I., Pils, C., Angermann, M., Robertson, P., Anagnostou, M.: Context modelling and management in ambient-aware pervasive environments. In: Strang, T., Linnhoff-Popien, C. (eds.) Location- and Context-Awareness. Lecture Notes in Computer Science, vol. 3479, pp. 83–94. Springer, Berlin (2005)
57. The Australian Signals Directorate: Risk management of enterprise mobility including bring your own device. Technical report, Australian Governament, Department of Defence, Intelligence and Security (2013)
58. Thomas, R.K., Sandhu, R.: Models, protocols, and architectures for secure pervasive computing: challenges and research directions. In: Proceedings of the IEEE Conference on Pervasive Computing and Communications, PerCom '04, pp. 164–168. IEEE Computer Society (2004)
59. Toninelli, A., Montanari, R., Kagal, L., Lassila, O.: Proteus: a semantic context-aware adaptive policy model. In: Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks, POLICY '07, pp. 129–140. IEEE Computer Society (2007)
60. Weiser, M.: The computer for the 21st century. Sci. Am. **265**(3), 94–104 (1991)
61. Ye, J., Dobson, S., McKeever, S.: Situation identification techniques in pervasive computing: a review. Pervasive Mob. Comput. **8**(1), 36–66 (2012)
62. Zhang, R., Giunchiglia, F., Crispo, B., Song, L.: Relation-based access control: an access control model for context-aware computing environment. Wirel. Pers. Commun. **55**(1), 5–17 (2010)