Journal of Information Security and Applications 34 (2017) 63–75

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Access control for secure information sharing in smart content spaces

Brian Greaves, Marijke Coetzee*

Academy for Computer Science and Software Engineering, University of Johannesburg, Johannesburg, South Africa

ARTICLE INFO

Article history:
Available online 26 January 2017

Keywords:
Access control
Mobile content sharing
Personalization
Context
Smart content space
Local policy
Global policy

ABSTRACT

Sophisticated mobile devices are becoming more compact, powerful and cheap to produce, leading to the implementation of smart applications that enable users to create and share large amounts of data on the go. Services such as Wi-Fi Direct support device-to-device communication, enabling peer-to-peer networks called smart spaces that support the sharing of information and resources between peers. In line with current research on personalization of the security of smart spaces, this paper introduces the concept of a proximity-based local personal smart space (LPSS) that presents new security challenges such as secure content sharing. An evaluation of current research on access control for smart spaces highlights that personalized context-based access control can provide better control over shared content. A local personal smart space access control framework is proposed focusing on the very nature of local personal smart space environments, namely, the enforcement of access control using personal preferences of users that are defined using policies. A prototype is presented that implements the access control model. Finally, the paper is concluded with some insight into future improvements.

1. Introduction

Today, the sophistication of smart devices makes it possible to share information directly between two devices, and create entirely access-point-less networks of devices (Adiba et al., 2004). Generally, as users possess more than one device, they need these devices to intelligently share content between themselves and the devices of friends and colleagues with minimal intervention (Gallacher et al., 2012). Currently, cloud-based applications such as DropBox, Box, and iCloud are commonly used for sharing content between devices. Even though these solutions are very popular, users have concerns regarding the security of their data in the cloud and the upload and download costs involved when the communication medium is not free.

To address the concerns introduced by cloud-based applications, peer-to-peer mobile storage and content sharing solutions are a current focus of research. Solutions such as Haggle (Nordström et al., 2014) and Mobistore (Fleming et al., 2014) demonstrate how content can be shared automatically between devices using local connections such as WiFi or Bluetooth. Without any doubt, these solutions can offer new benefits, but also introduce new threats for users making use of their services. Users may store a variety of personal content which they may want to share selectively with others who are in range. As it is not always possible to verify someone's identity visually due to the increasing strength of radio antennae, security is important to consider when sharing mobile content or resources with others (Manaf et al., 2009).

To date, not much research on access control for peer-to-peer mobile storage and content sharing solutions has been done. The distribution of information across devices makes it difficult to control access to resources using well-known access control models, such as discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC) as the nature the environment dictates that access control should be dynamic in nature (Kashevnik et al., 2013). The amount of sensory and other data available on smart devices can enable the measurement of the context of interactions (Adiba et al., 2004). Devices can respond to their operational environments and change the parameters of their operation based upon their context.

Research shows that smart spaces can make people's lives easier as they provide new types of applications and capabilities. This research extends previous research (Greaves and Coetzee, 2015) to describe local personal smart spaces and their access control requirements in more detail. An access control framework is presented that uniquely addresses personal and group preferences of users who are in possession of a number of mobile devices. The research makes a contribution by demonstrating how local and global group preferences are used together.

* Corresponding author. Academy for Computer Science and Software Engineering, University of Johannesburg, Johannesburg, South Africa. Fax: +27866499344.
E-mail address: marijkec@uj.ac.za (M. Coetzee).

http://dx.doi.org/10.1016/j.jisa.2016.12.002
2214-2126/

The paper is structured as follows: The concept of the local personal smart space is introduced, followed by a scenario. A set of access control and other requirements are identified. The topics of context and policy are examined to determine how they can be used to protect a local personal smart space by evaluating recent literature. Finally, the paper proposes a context-aware access control model which uses two dimensions of policy, namely local and global. Then access control enforcement is described using scenario-based examples used to highlight access control policy usage. Finally, a prototype implementation is described and the paper is concluded.

2. Local personal smart spaces

Pervasive computing (Satyanarayanan, 2001) is an important research focus that has attracted much interest due to the increasing number of devices that users are confronted with in their environment such as sensors, computers and smart phones. When pervasive computing is applied to a local domain it is referred to as a smart space. A smart space is a physical environment within a specific dimension containing adaptive devices that are automatically managed (Gallacher et al., 2012). Smart space research focuses on systems for fixed smart spaces, or systems supporting mobile users. Research on fixed smart spaces such as smart homes, smart buildings and smart cities has produced intelligent applications that dynamically manage infrastructure and sensors to suit the needs of users without application pre-configuration (Gallacher et al., 2012). In order to be able to provide the user with an intelligent environment where services and resources are managed on their behalf, the personalization of the environment is required. Personalization ensures that a system behaves differently when the user or the context changes (Gallacher et al., 2010). For example, if the location of a mobile user changes, a different set of services or resources may be made available. The system thus needs to track changes and adapt its behavior as specified by user preferences for different contexts.

In this regard, the PERSIST project (Cordis.europa.eu, 2008) aimed to provide a pervasive experience through an architecture based on the concept of a personal smart space. A personal smart space (PSS) is defined as a collection of devices that can be connected in a peer-to-peer manner to bridge the gap between mobile users and fixed smart spaces (Gallacher et al., 2012). In a PSS, devices and services are owned, controlled, or administered by a single user or organization. For example, QoSDream (Naguib et al., 2001) and Sentient Computing (Newman et al., 2001) are client–server, publish–subscribe PSS applications supported by a centralized approach, where clients subscribe to a location server that regularly polls their location to send them information about resources and other clients in their environment. Even though support for mobile users is provided, the system is dependent on centralized servers and requires mobile client devices to maintain a constant connection to the Internet. In more recent times, research in smart spaces have branched out from being solely dependent on fixed spaces to addressing applications such as tourist recommendations (Varfolomeyev et al., 2015) where software agents called knowledge processors run on devices to collaboratively collect and share information via semantic information brokers. The interaction between software agents leads to the construction of a service thereby decentralizing control within the PSS environment.

Moving further from fixed spaces, a mobile PSS is defined as a PSS that provides a mobile pervasive system around the user at all times (Gallacher et al., 2012). If the range of mobile device communication is limited by connections such as Wi-Fi Direct (Alliance, 2010) or Bluetooth (Haartsen, 2000), devices of a mobile PSS need to be in proximity to be able to interact. Such a proximity-based mobile PSS limits the physical dimension of the mobile PSS to a local scope with device-to-device communication (D2D). For this research, the architecture and operation of a proximity-based mobile PSS environment is a natural fit for the peer-to-peer content sharing solution required by this research.

Based on these constraints, this research now proposes the concept of a local personal smart space (LPSS) by extending the traditional concept of the mobile PSS. The foundation of the LPSS is a mobile PSS that is defined by a set of services, available within a dynamic space of connected mobile devices, owned, controlled and administered by a single user or organization, controlled by a set of personal preferences. This research adds a local dimension by requiring that mobile devices need to be in proximity of each other as they communicate in a peer-to-peer manner using technologies such as Wi-Fi Direct or Bluetooth. A LPSS is thus a proximity-based mobile PSS that can support services such as smart content spaces.

Important features of a local personal smart space are that it is owned by a specific user or organization and moves around with the user; their preferences are maintained by a set of rules; the physical boundary of the local personal smart space is determined by the proximity of devices from each other; and the local personal smart space must be able to identify and interact with other local personal smart spaces.

Unlike Personal Area Networks (Bourgeois et al., 2001), where mobile devices connect to each other in an ad-hoc manner when they are in close proximity, a local personal smart space is a smart space that enables the creation of groups of mobile devices that are governed by rules that have been defined by the owner of the group.

The relationships between users, mobile devices and content within a local personal smart space are now further investigated by means of a scenario.

3. Motivating scenario

In order to identify functional and access control requirements of local personal smart spaces, a scenario is presented next. The formation and use of both user and organizational local personal smart spaces is illustrated by considering three members of a family as individual owners of devices, and as a family group. A local personal smart space consists of a number of mobile devices, and is identified by a group name. As shown to the left of Fig. 1, John owns three mobile devices, namely a tablet, a smartphone for work, and a privately owned smartphone. His group is depicted as *group_J*. Mary has a smartphone and tablet (*group_M*) and Peter has a smartphone (*group_P*). At a global level, John, his wife Mary, and their son Peter are members of a family (*group_H*) that possess six personal mobile devices between themselves. Mark is a member of another local personal smart space group, *group_MK*.

Even though their mobile devices are not necessarily made by the same manufacturer, they would like to share content between the devices that they own, and also between all devices that are part of the family. As John has concerns about the security of cloud-based solutions and the associated costs incurred with uploading and downloading data, he wants content to be shared directly between devices when they are at home.

First, software is installed on each mobile device. The owner of a group of devices creates a group for those devices. John forms a group for this three personal devices, similarly Mary groups her two devices. As the designated owner of the family group, John creates the family group and invites all devices that should be part of the family group. Content can now be shared between devices in a personal group and between devices in the global family group. For example, John shares the pictures he takes with his phone with his tablet to have a backup of this content. Within the family group, John, Mary and Peter share selected family pictures between their devices so that they all have access to this content.