Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective

Franco Callegati, Saverio Giallorenzo, Andrea Melis, Marco Prandini

Università di Bologna, Via Zamboni, 33, 40126 Bologna, Italy

INRIA, France

ARTICLE INFO

Article history:
Available online 21 November 2017

Keywords:
Mobility-as-a-Service
Federated platforms
Insider threat
Cloud-of-Things
Internet-of-Things

ABSTRACT

Mobility-as-a-Service (MaaS) applies the everything-as-a-service paradigm of Cloud Computing to transportation: a MaaS provider offers to its users the dynamic composition of solutions of different travel agencies into a single, consistent interface. Traditionally, transits and data on mobility belong to a scattered plethora of operators. Thus, we argue that the economic model of MaaS is that of federations of providers, each trading its resources to coordinate multi-modal solutions for mobility. Such flexibility comes with many security and privacy concerns, of which insider threat is one of the most prominent. In this paper, we revise and extend previous work where we classified the potential threats of individual operators and markets of federated MaaS providers, proposing appropriate countermeasures to mitigate the problems. In addition, we consider the emerging case of Cloud-of-Things (CoT) for mobility, i.e., networks of ubiquitous, pervasive devices that provide real-time data on objects and people. Automation and pervasiveness of CoT make an additional attack surface for insiders. In an effort to limit such phenomenon, we present an overlay networking architecture, based on gossip protocols, that lets users share information on mobility with each other. A peculiarity of the architecture is that it both constrains the quality and quantity of data obtainable by insiders, optimizing the routing of requests to involve only users that are able to answer them.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

The term Cloud Computing denotes a dynamic infrastructure where users access services without regard to where the services are hosted (Buyya et al., 2009). The concept of Mobility-as-a-Service (MaaS) (Pippuri et al., 2016) takes inspiration from such a model and brings it into the context of transportation. In Cloud Computing, the architecture that runs the services is dynamic and transparent to users. Likewise, MaaS hides a dynamic composition of solutions provided by different travel agencies behind a consistent interface. Hence, MaaS users experience traveling over complex itineraries as if they were provided by a single agency.

Due to regulatory and logistic issues, mobility resources are administrated and owned by a scattered plethora of mobility operators (traditional travel agencies and providers of data for mobility). Thus, we argue that the leading economic model of MaaS markets is that of federations of mobility operators, each trading its resources. In such a federated market, operators can dynamically partner with each other, still preserving their individual autonomy and without the need for a centralized
regulation authority. On these premises, we are currently developing a service-oriented platform, called Smart Mobility for All\(^1\) (SMAll), built on the concept of federated Cloud Computing (Buyya et al., 2010; Rochwerger et al., 2009) and purposed to support liquid markets for transportation.

During the development of SMAll and through the collaboration with our industrial partners (public administrations, local travel agencies, etc.), we identified and analyzed many security issues spanning from a single operator to a federation of operators. In this context, we deem malicious insider activity one of the most prominent threats, spanning from standard threats against cloud installations (Kandias et al., 2013) to insider issues specific to the contexts of mobility and of markets of services.

**Motivation.** Fig. 1 depicts a cross section of an instantiation of SMAll, where the colored entities outside of the boundaries of SMAll (bordered with double lines) are public transportation agencies, private companies, on-line communities, and MaaS Operators.

Even when considered in isolation, the agents in the platform already entail well-known threats due to insider activity. For example, the City Bus Operator represents a threat to the privacy of drivers since GPS positioning can reveal sensitive information on their conduct, which is forbidden under some legislation; however, also drivers represent an insider threat to the Bus Operator: they can disable the GPS device on their vehicles, compromising the reliability of the GPS positioning system and that of the other services that depend on it\(^2\) (e.g., the Bus Delays service that estimates bus arrivals based on vehicle GPS positions). Finally, employees can manipulate the services and their data, damaging the company by extracting restricted information or causing outages.

Broadening our scope to federated interactions, we focus on the MaaS Operator in Fig. 1 that, for example, deploys a Journey Planner service for providing dynamic multi-modal trips to users. The service orchestrates other federated services in SMAll: it uses information on scheduling, availability, disruptions, and the position of buses, trains, and on-demand cars. As expected, the threats highlighted for single operators surface (and possibly combine into new ones) to higher-level federated scenarios. Consider the case in which the City Bus Operator allows the MaaS Operator to access the Bus GPS Proxy service. With the raw data on the real-time position of buses, the MaaS Operator can undertake many malicious activities to the detriment of the Bus Operator, e.g., passing relevant information to its competitors. Another important threat comes from the extraction of sensitive information from aggregated/anonymized data. Consider the case of a Bus Operator, which is aware of the threat posed by the Bus GPS Proxy service, and thus it decides to market only its Bus Delays service. This countermeasure could be ineffective, since also aggregated data like the temporal approximation of the arrival of buses might let the MaaS Operator extract (Zhou et al., 2012) the actual position of vehicles (possibly optimizing the accuracy of the extraction (Mirri et al., 2016a)).

**Contribution.** As exemplified, in the context of MaaS Operators, the definition of what an insider is can assume subtle nuances depending on the considered scenario. In this work, guided by our experience with the development of SMAll, we describe the security issues concerning insiders within such a federated market of services. In doing so, we consider two distinct perspectives: i) the one of high-level services traded in an open platform and ii) the one of low-level data sources for mobility, focusing on the emerging case of Clouds-of-Things (Bandyopadhyay and Sen, 2011; Holler et al., 2014) for mobility. Our contributions are organized as follows.

**Insider Threats in MaaS Markets.** We consider the high-level perspective of services for mobility in MaaS markets. We integrate and extend material from Callegati et al. (2017a), where we introduced the case of MaaS markets and analyzed the possible emerging insider threats. Here, we present a revised version of the proposed analysis. To structure our exposition, we follow a tiered view of the MaaS markets called the MaaS Stack, presented in depth in Callegati et al. (2017b). In Section 2 we give a brief account of the MaaS Stack. Then, in Section 3 we discuss our findings: we consider each tier of the MaaS Stack, we define what an insider is for each of them, we analyze the related threats, and we describe the possible countermeasures.

**Cloud-of-Things for Mobility: Insider Threats.** We analyze insider threats in the context of Cloud-of-Things (CoT) for MaaS and we propose an architecture that constrains the quality and quantity of data that an insider could obtain from users. In doing so, the architecture also optimizes the routing of requests only to those users that are able to answer them. To achieve these results, the proposed architecture creates an overlay network among users, so that requests are bound to limited localities, guided by the capabilities (knowledge, proximity, etc.) declared by users, and spread following a gossip-based protocol (Boyd et al., 2006; Haas et al., 2006). In Section 4 we briefly illustrate the relationship between Mobility-as-a-Service and Cloud-of-Things, the latter being an increasing source of real-time data for mobility services. Since CoTs represent another attack surface for insiders, we analyze these threats in Section 4.1. From our analysis, in Section 4.2 we discuss how an overlay network of CoTs can mitigate some of the identified threats. Then, in Section 4.3 we give a brief account on gossip-based networks and describe how our overlay network employs gossip-based propagation of information to achieve both optimization of queries and locality of data. In Section 4.4 we present our overlay network. Finally, in Section 4.5 we report a thorough analysis on how and to which degree our overlay network mitigates some of the threats of MaaS, identified in Section 3, proposing possible future evolutions.

### 2. The MaaS Stack: An overview

In this section we briefly discuss an overview of the MaaS Stack (Fig. 2), a structured view that we assembled to guide the development of SMAll. In Section 3 we use the MaaS Stack to analyze the insider threats of each tier.

**Tier I eMobility Operators.** The first tier of the MaaS Stack is that of eMobility Operators. An eMobility Operator is an entity that owns, administrates, and exposes software functionalities regarding mobility, provided in a machine-readable form. In tier

---

2. The issues are far from being just speculative, as we actually encountered them collaborating with one of our industrial partners.
دریافت فوری
متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با پهربه مندی از سیستم هوشمند رهگیری سفارشات