ARTICLE IN PRESS

Pervasive and Mobile Computing ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Fast track article

Anonymous end-to-end communications in adversarial mobile clouds

Claudio A. Ardagna [a], Kanishka Ariyapala [b], Mauro Conti [c,*], Cristina M. Pinotti [d], Julinda Stefa [e]

[a] University of Milan, Italy
[b] University of Florence, Italy
[c] University of Padua, Italy
[d] University of Perugia, Italy
[e] Sapienza University of Rome, Italy

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Anonymity
Mobile cloud computing
Wireless network

ABSTRACT

Today's mobile devices have changed the way we interact with technology. Internet, cloud access, online banking, instant messaging, and file exchange through the cloud are just a handful of the myriad of smartphone services that we make use of every day. At the same time, the very enablers of these services – mobile internet providers and cloud platforms that host them – pose several threats to the anonymity of our communications. In this paper, we consider the problem of providing end-to-end anonymous communications and file exchange under the cooperative privacy threat of involved parties including network operators and cloud providers, which actively tamper with the communication. We propose a solution for delay-tolerant applications (similar to Whatsapp or Email) and prove the security properties of the protocol under this strong attack model. Finally, we present an experimental analysis of the efficiency of our protocol in terms of performance overhead.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

Mobile cloud computing is the paradigm that was built with the goal to save a resource very precious to mobile devices—their battery. The idea is simple: Pushing the execution of (parts of) mobile apps to remote servers residing on the cloud in order to avoid the energetic cost coming from the local execution on the device. The paradigm works best with computation-intensive applications with very limited access to device local resources like sensors, data. In fact, the more computation-intensive a given task, the more the device will benefit from executing it remotely. The less a given task needs to access local resources, the smaller is the device–cloud communication overhead to execute it remotely. Through the years, researchers have proposed offloading frameworks that take smart decisions on what to execute remotely [1–3], and solutions that boost the security of our devices [4–6] or enable efficient data/application backup [7]. Also, solutions that create virtual peer-to-peer networks of smartphone software clones in the cloud enable unprecedented and efficient, complex distributed protocols on mobiles [8,9].

* Corresponding author.
E-mail address: conti@math.unipd.it (M. Conti).

http://dx.doi.org/10.1016/j.pmcj.2016.09.001
1574-1192/© 2016 Elsevier B.V. All rights reserved.

Please cite this article in press as: C.A. Ardagna, et al., Anonymous end-to-end communications in adversarial mobile clouds, Pervasive and Mobile Computing (2016), http://dx.doi.org/10.1016/j.pmcj.2016.09.001

The nature of the mobile apps, but most importantly, their typical complexity, makes it very hard, if not impossible, to use privacy-preserving execution mechanisms like homomorphic schemes. In fact, these mechanisms, designed to operate in hostile environments (e.g., the untrusted cloud) over encrypted user data, are not suitable for application scenarios considering remote execution of mobile apps [10]. While offloading to the cloud, a mobile user has then to fully trust the cloud-side of the process. Not only is the cloud aware of which data and jobs the user is running, but it also knows exactly who is communicating to whom and what information is being shared.

In this paper, we advocate that communication and file-exchange privacy among mobile cloud computing users is achievable, even under very powerful attacks. To this aim, we propose a protocol that, while supporting storage and computation offloading, implements anonymous end-to-end communications for mobile devices in adversarial mobile clouds. Specifically, we consider a strong attack model (Section 3) in which smartphones, cloud clones, the network operator, and the cloud provider are all adversarial entities and can collude to de-anonymize a communication. The cloud provider can both monitor the traffic from/to the user's cloud clones, and have access to the memory within the machines hosting them. Under this powerful and multifaceted attack model, all previous solutions for anonymous end-to-end communication in a mobile cloud computing setting, including ours [11], are unable to provide the requested privacy (Section 2). In this paper we challenge the common belief and come up with a solution that provides anonymity and unlinkability to the users (Section 4). We discuss the security properties of the protocol according to this new challenging attack model (Section 5). We finally investigate on possible slow-down effects in the system and show, through experimental evaluations, that the overhead incurred is affordable (Section 6).

2. Related work

The mobile cloud computing paradigm, though initially designed with the offloading of heavy computations in mind [1–3], brings multifaceted benefits in a large number of application scenarios. It can enable more complex security mechanisms for smartphones [6], or help exploit the cloud to optimize incoming data-traffic, minimize the device connections to remote servers, and ensure efficient data backup in the cloud [4,7,12]. It opens the way to complex peer-to-peer services on mobile devices [5,8,9], otherwise impossible to run on our battery-limited smartphones. All these solutions assume full trust on both the cloud and the network operators providing the device–cloud communication channel. Also, encryption can come to hand for the protection of the user data stored in the cloud. Unfortunately, if the data/application code is encrypted with a key known only to the user, the cloud cannot be exploited for offloading anymore. In addition, encryption does not guarantee full user privacy. Both the cloud and the network operator in fact know how often a user is: (i) Offloading computation to her cloud server (a.k.a. clone of the device [1,8,9]); (ii) storing data on her cloud server; (iii) exploiting the clone as a bridge to communicate/send the data previously stored on it to other users [8]. If the first two issues are unavoidable to achieve all the benefits of cloud computation offloading and backup, the user is increasingly concerned about her privacy when communicating with other users through the cloud.

Wired, wireless, and hybrid networked systems, have always brought the need of anonymous communication protocols [13–20]. Most applicable solutions exploit chains of proxy nodes [21,22], accumulating and forwarding source-encrypted messages in batches. Among them, TOR [22] is probably the most popular one. However, TOR is not applicable in the scenario in this paper because devices and clones on the cloud are uniquely coupled. Also, the communication among two devices directly involves the corresponding clones. If the latter are compromised, they will identify the sender (receiver) even if TOR is employed when communicating with the corresponding clone.

With the increasing popularity of social networks, several works put the trust among friends as a means to achieve anonymity of communications [14–20]. However, these solutions either not fit at all for mobile–cloud computing scenarios, or are computationally heavy for battery-limited devices. To the best of our knowledge, our previous work [11] was the first attempt to address the issue of anonymous communications through the mobile cloud. It provided a user-tunable level of anonymity to sender (indistinguishable among α users) and receiver (indistinguishable among β users), the (α, β)-anonymity, as defined Section 3, in presence of colluding adversaries, including both cloud providers and network operators. The protocol worked under the assumption that the cloud clones of friend users could trust each other, and rely on each other to thwart anonymity breaches of communicating users. Differently from [11], in this work we consider a much stronger attack model: The cloud provider is able to look into a hosted clone's memory and read encryption keys stored therein; other clones, even friend ones, are malicious and can collude with both the cloud provider and the network operator to de-anonymize other user's communication. Our solution also supports computation offloading, in addition to storage offloading, balancing it with data confidentiality.

Other works have addressed a variety of issues in research areas similar to the ones considered in this paper. Senftleben et al. [23] propose a decentralized privacy-preserving microblogging infrastructure based on a distributed peer-to-peer network of mobile users. The infrastructure, using device-to-device communications, is robust against censorship and provides high availability. Daubert et al. [24] present a solution to privacy-preserving sharing of smartphone sensor data and user-generated content via Twitter. The proposed solution ensures both confidentiality and anonymity of users and their messages. Finally, authentication, a milestone in sensitive-data handling platforms like the mobile cloud computing, is exhaustively reviewed in the survey in [25].

Please cite this article in press as: C.A. Ardagna, et al., Anonymous end-to-end communications in adversarial mobile clouds, Pervasive and Mobile Computing (2016), http://dx.doi.org/10.1016/j.pmcj.2016.09.001

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ 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 بهره مندی از سیستم هوشمند رهگیری سفارشات