Chapter 12
Information Security Innovation: Personalisation of Security Services in a Mobile Cloud Infrastructure

Jan H. P. Eloff
SAP Innovation Center Pretoria, South Africa & Department Computer Science, University of Pretoria, South Africa

Mariki M. Eloff
University of South Africa, South Africa

Madeleine A. Bihina Bella
SAP Innovation Center Pretoria, South Africa

Donovan Isherwood
University of Johannesburg, South Africa

Moses T. Dlamini
University of Pretoria, South Africa

Ernest Ketcha Ngassam
University of South Africa, South Africa

ABSTRACT

The increasing demand for online and real-time interaction with IT infrastructures by end users is facilitated by the proliferation of user-centric devices such as laptops, iPods, iPads, and smartphones. This trend is furthermore propounded by the plethora of apps downloadable to end user devices mostly within mobile-cum-cloud environments. It is clear that there are many evidences of innovation with regard to end user devices and apps. Unfortunately, little, if any, information security innovation took place over the past number of years with regard to the consumption of security services by end users. This creates the need for innovative security solutions that are human-centric and flexible. This chapter presents a framework for consuming loosely coupled (but interoperable) cloud-based security services by a variety of end users in an efficient and flexible manner using their mobile devices.

DOI: 10.4018/978-1-5225-8176-5.ch012

INTRODUCTION

The increasing demand for cost-effective always on connectivity on all types of end-user computing devices (e.g. desktop computer, laptop, MP3 player, tablet, smartphone) results in the need for new business models (mobile, cloud, services, platforms) that increase the level of exposure to a company's assets. This creates new security challenges for networked businesses as a number of 3rd-party services and infrastructures within complex ecosystems are integrated. For instance, many actors are involved in the service provisioning ranging from the customer, the service provider, the content provider, the network provider, the cloud provider and the electronic or mobile payment provider. Each of these actors has an entry point to the service and therefore is a potential security risk.

Investigating a security breach thus requires the collection of data from all these different sources. In addition, the existence of various mechanisms to access the network (e.g. wired, wireless, 3G, modem, VPN) creates many access points that can be exploited for unauthorized access to and misuse of the company's information.

Detecting such events requires the continuous exchange of information between all service elements and network devices (Bihina Bella, Eloff, & Olivier, 2009). Furthermore, entities involved in the service provisioning can have conflicting security policies that need to be aligned to the company's policy.

In this collaborative environment, security risks shifts from the IT system as a whole to the services it offers to a multitude of independent users and to the data that travel across systems (e.g. in cloud computing applications hosted on public infrastructures). For example applications hosted on public cloud infrastructures are not only open to the general public but are also open to malicious individuals. Such applications become a public good and are susceptible to excessive and malicious use. Malicious or disgruntled individuals may decide to flood such applications with targeted distributed denial of service (DDoS) attacks so that the general public could not have access to them.

Maintaining a secure configuration in such heterogeneous IT landscapes is complex a security requirements are multi-lateral and diverse. This creates the need for innovative security solutions that are human-centric, flexible and also robust. Potential avenues for innovation within the information security domain include, amongst others, the following:

1. The definition of data-centric policies that travel with the services as well as the data.
2. The usage of privacy-preserving computing (Wang, Zhao, Jiang, & Le, 2009) to ensure the privacy of all parties involved.
3. Access control policies and mechanisms that take care of conflict management (Cuppens, Cuppens-Boulahia, & Ghorbel, 2007) between the members of an ecosystem.
4. The possible aggregation of different access control approaches such as usage and optimistic based access control (Padayachee, 2010).
5. Simple and basic authentication services on mobile devices.
6. Forensic tools for mobile-cum-cloud environments (Ruan, Carthy, Kechadi, & Crosbie, 2011) services utilization, using mobile devices.

This is an opportunity to capitalize on the advantages offered by cloud computing for accessing value-added business services, by end-users. In general, end-users are not concerned by the complexity of the technical infrastructure required to set up cloud-based services for large consumption but rather the intended business outcome offered by exposed services.