Sealed Cloud - a novel approach to defend insider attacks

Hubert A. Jäger and Arnold Monitzer
Uniscon universal identity control GmbH
Agnes Pockels-Bogen 1, 80992 München, Germany

preprint 15. December 2010*

Abstract

Security and privacy have been turning out to be major challenges of the further evolution of the Internet in general and cloud computing in particular. This paper proposes a novel approach to defend previously unimpeded insider attacks, which is referred to as Sealed Cloud. A canonical set of technical measures is described, which in conjunction complicate and thus economically prevent insider access to unencrypted data in the computing infrastructure.

1 Introduction

The concerns of security in information technology have been focusing for a long time on perimeter security and assumed the provider of software as a service (SaaS) or the provider of a cloud and cloud-based services respectively as trusted entities. Statistics of data theft and privacy violations however reveal [1] and [2] that at least every fourth harmful attack origins from the inside of these organizations. This data only confirms what many potential customers of SaaS and cloud-based offerings have been anticipating about the level of security for their data. Therefore mission critical applications have not been outsourced to cloud resources and privacy enabling and privacy enabled services have not been established on a significant scale so far [3]. This means that an integrated security approach is needed as stipulated by many IT security experts recently, e.g. [4]. Moreover, a technical break-through in protecting user data processed in the computing infrastructure of providers is wanted.

This work was elaborated in the context of the development of an Internet privacy enabling service [5], where in a SaaS architecture a data security requirement was ex-
tended to consistently embrace also the server components. Only after that the resulting set of technical measures appeared as equally suited to also solve the issue of missing means to defend insider attacks in general computing infrastructure.

Outline The remainder of this article is organized as follows. Section 2 gives account of previous work. The Sealed Cloud proposal is presented in Section 3. Finally, Section 4 gives the conclusions.

2 Previous work

In literature there are several approaches to secure computing infrastructure, employing Trusted Platform Modules (TPM), e.g. [6] or [7] for improved software integrity. In [8] a closed box execution environment is used to protect the virtual machines against an unauthorized access by an administrator. According to [9] this method has not been implemented yet.

These approaches secure the integrity of the software and thus substantially restrict administrators liberty to abuse infrastructure and data, however do not fundamentally impede access to unencrypted user data while being processed. E.g. if the operation kernel of a processor fails, or is provoked to fail, unencrypted data is written to core dumps.

Similar ideas to clean-up data as presented in this paper when perimeter security has been surmounted can be found in literature on tamper-proof hardware, e.g. [10].

The sole alternative to the Sealed Cloud concept known to the authors at this point in time is homomorphic encryption [11], [12], an enabling technology still in stage of research. In this approach data are processed in encrypted form and therefore cannot be copied in a readable form during processing by the operator or administrator of the service.

The following proposal employs only off-the-shelf components and is thus ready for implementation.

3 Proposal

A processing infrastructure is assumed, which hosts applications that process personal data. Personal data is considered to be any data associated with users of such applications and is assumed to be worthy to be protected against unauthorized access.

Unauthorized access is considered all access of parties, which have no business directly related to the functional logic of the applications nor a legally justified access right.

Unauthorized parties are external attackers but also internal staff of the operator of the service or the infrastructure, as long as no human interaction is needed for the functional logic of the application. Often solely the user of an application and a legal entity – within the narrow latitude of law – are the only persons with authorized access.

In the following a set of measures is proposed, which aims at protecting the personal data from unauthorized access. This protection of data for sensitive and mission critical applications has to be sufficiently effective by
technical means only. The potential impact of human deviance should be minimized.

**Basic idea** Based on the fact that current computing infrastructure is normally secured with state-of-the-art perimeter protection and in addition a complex set of measures to insure integrity of the software, still the administrators of the computing infrastructure has access to unencrypted personal data as illustrated in Figure 1.

![Figure 1: Classical set of technical measures to defend insider attacks.](image1)

Of course, operators of such infrastructure and operators of services implemented on such infrastructure are well aware of this weakness and complement the protection of unencrypted processing data with non-technical means, i.e. properly defined processes and staffing of these processes with upright personnel they can trust, as illustrated in Figure 2.

![Figure 2: Practical set of technical and non-technical measures to defend insider attacks.](image2)

A good example for such a full set of processes is described in [13]. The best combination of technical, formal and informal measures to maximize security is elaborated.

In our proposal this non-technical makeshift is attempted to be replaced by a well adapted encryption key distribution and tailored data clean-up procedures as indicated in Figure 3. Both measures used in conjunction with perimeter security and software integrity can close the gaps, such that in the Sealed Cloud no unencrypted processing data is easily accessible for unauthorized parties.

**Key distribution** An encryption of all data stored on persistent memory is assumed. In order to avoid an ability to access this encrypted data by the operator of the infrastructure or the operator of the services in an unencrypted form, it is necessary to either (a)
use an encryption method, were the operator – once the data is encrypted – does not have the option to decrypt the information again, i.e. asymmetric encryption, or (b) to delete the encryption key as soon as the encryption procedure has been completed. The latter method is suitable if the encrypted information is later to be used by the application in an unencrypted form again.

With these methods a division of power between the different parties involved with the business logic of an application can be achieved.

The most straightforward use case is the encryption of user data in the database of the service deployed in the Sealed Cloud with a key provided by the client of the application. If the data is supposed to be used later in the cloud again, no asymmetric keying is used and consequently the application needs to delete the key after the session or another unit representing the interaction with this data, is completed.

Another use case is an application, which needs to provide access to specific data for a third party. For example access of a business partner of the client organization is foreseen to have access to data needed to execute the partnership with the client organization. This data can be encrypted in the Sealed Cloud with the public key of the business partner, being exported in encrypted form to the partner, and there safely decrypted with the partners private key.

Such division of power – concerning the access to data – of course only remains functional, as long as no coalitions are built between the different parties within the business logic.

**Data clean-up** In the database of the Sealed Cloud is no unencrypted data. The keys for this data is only available for the parties the information belongs to according to the business logic. However, in the persistent and volatile memory of the processing infrastructure, unencrypted data is present. Planned access, i.e. planned maintenance sessions, to this memory is inevitable in order to practically maintain the processing infrastructure from an operational point of view. Also unplanned access cannot be excluded because perimeter security can alarm intrusion detection in most cases, but not always prevent it effectively.

Data clean-up as proposed here means that before planned or unplanned access to the persistent or volatile memory is possible the
personal data has been deleted or overwritten reliably. For this, triggering signals are required. For planned access new trigger signals have to be established, for unplanned access alarms from the perimeter security can be used as triggering signals.

**Dependencies** The data clean-up function as described in the previous paragraph depends on signals from the perimeter security. It also depends on trustworthy code, of which the authenticity is secured by software integrity measures, to execute the clean-up. These two examples already show that all measures have dependencies among each other. Similar dependencies exist between encryption as a means to control software integrity and software integrity to secure perimeter security etc. Nevertheless each technical measure can unambiguously be categorized into one of the given classes of measures. It should be mentioned that human integrity and processes are still important for the overall Sealed Cloud e.g. for software integrity. However this set of measures is, as illustrated in Figure 4, shifted to the second line of defence.

**Canonical set of measures** The presented set of measures is denoted to be canonical, because the entirety of technical measures, serving the purpose of protecting the unencrypted processing data, can be mapped into these four classes.

If for example a specific implementation of a Sealed Cloud is based on processing infrastructure without persistant memory the data clean-up comprises the clean-up in the volatile memory of the infrastructure only. If an other implementation uses also persistant memory a proper data clean-up also comprises a cleaning of the persistant memory, which imposes more demanding requirements on software integrity. However, all related measures can be mapped into the classes: Perimeter security, encryption & key distribution, software integrity, and data clean-up.

These four areas correspond to the attacks from outside and inside, as well as to attacks on encrypted and unencrypted data, respectively.
4 Conclusions

The presented proposal is a nice example for an integrated security approach in information technology. By technical means an unauthorized access of any kind is made complicated and is therefore prevented economically. The unauthorized parties include the operator of the infrastructure and the operator of services. The resulting Sealed Cloud is therefore a processing infrastructure on a new level of trust for the clients of hosted applications.

The current work is a proposal, which opens a field of research for the options to implement the suggested measures. In particular software integrity in environments with virtual engines and approaches to reliable data clean-up in standard cloud application interfaces are fields of research interest.

Prototyping of the Sealed Cloud is being persued by the Uniscon GmbH, the Fraunhofer Instute of Applied and Integrated Security and SecureNet GmbH, and will be co-funded by the German Ministry of Economics in the frame of the so called Trusted Cloud initiative [14].

References


topics in cloud computing, HotCloud09, Berkeley, CA.


