UNTRACEABLE ANONYMOUS SERVICE CONSUMPTION IN SaaS

Vinícius Pacheco and Ricardo Puttini
Department of Electrical Engineering, University of Brasília - UnB, Brasília, Brazil

Keywords: Cloud Computing, Software as a Service, Privacy, Multi-layer Security, Anonymity, Untraceable Communication, E-cash.

Abstract: Several cloud computing providers are emerging to provide web services that encapsulate common business logic in the cloud. However, these Software as a Service (SaaS) offers are currently based in trust relationships between cloud consumers and providers. Consumer must trust the provider not to disclose sensitive data exchanged during service provision, as such leak can compromise consumer's privacy and threaten its business. In this paper, we propose a privacy enhancing framework to protect consumer information privacy against excessive exposure to cloud computing providers. Our design is essentially based on anonymity technology, as conventional encryption and authentication security mechanisms do not supply enough protection to consumer's privacy; particularly, when the provider itself is considered a threat. The design consists in a multi-layered framework, where different anonymity techniques are employed together to protect the privacy of different types of consumer information, during both administrative (e.g., legal contracting and financial transactions) and technical (e.g., message exchanges) interactions. We also describe a complete connection anonymity SaaS service consumption scheme based on e-cash as the main tool for generating and managing anonymous credentials in the cloud.

1 INTRODUCTION

Software-as-a-Service (SaaS)[1] is a cloud computing delivery model where a cloud provider offers and provides application-level software services that encapsulate parts of the consumer's business logic. SaaS service consumption is done through message exchanges between the cloud consumer and the cloud provider. Messages contain consumer's data and metadata and can often carry sensitive information about the consumer's business.

In this paper, we present an approach to protect cloud consumer's information privacy using anonymity technology. We aim at establishing an anonymity framework that enables message exchanges in SaaS to happen anonymously and the consumer's consumptions to remain untraceable. Still, the consumer has proper access to services and the provider can correctly authenticate, account, and charge for service usage.

Díaz *et al.* in (Claudia Díaz *et al.*, 2002) divide anonymity, inside the context of privacy, into data anonymity and connection anonymity. Data anonymity relates to removing any identifying information from the data itself, and, on the other hand, connection anonymity focuses on protecting the identities of source and destination during communications.

The main contribution of our work consists in the provision of connection anonymity in SaaS service consumption. In short, our proposal consists in establishing a pay-as-you-go service consumption scheme in which the services are anonymously paid for at the same time of service consumption, using electronic cash primitives that are embedded in the message metadata.

Although not in the focus of this research paper, we acknowledge that data anonymity and network-level connection anonymity are important building blocks of a cloud computing anonymity framework.

[1] Although the term SaaS, as a cloud computing service model, applies to a broad type of applications that can be accessed and utilized as a service, this framework focuses in a particular subset of the SaaS paradigm, where services are understood as decoupled parts of business logic that are accessible through simple request-response message exchange patterns (MEP), expressed in a service contract, most likely available as SOAP or REST web services.

Pacheco V. and Puttini R..
UNTRACEABLE ANONYMOUS SERVICE CONSUMPTION IN SaaS.
DOI: 10.5220/0003930700960101
In *Proceedings of the 2nd International Conference on Cloud Computing and Services Science* (CLOSER-2012), pages 96-101
ISBN: 978-989-8565-05-1

Appropriated considerations about these issues are pointed out in our formulation.

2 SERVICE CONSUMPTION IN SaaS

Our target scenario consists in an enterprise organization (consumer) making use of a particular service that a provider organization (provider) offers in the cloud as SaaS. This service consumption will be made through message exchanges, performed through the network. Our goal is to improve information privacy in SOAP (and potentially, REST) web services consumption. In this case, there is a technical contract for each service that specifies simple request-response message exchange patterns (MEP) for each operation provided in the service. Without loss of generality, our analysis concentrates in the case of decoupled point-to-point interactions using simple MEPs, but more complex compound MEPs can also benefit from the proposed framework.

The typical scenario for SaaS cloud computing model starts with the service provider publishing the service along with the respective service usage conditions.

Next, the consumer interacts with the service directory to locate the appropriate service that provides the needed business functionality and evaluates the service consumption conditions in the service contract. This is the service discovery.

During service consumption, consumer requests and receives services from provider using message exchanges, which can, for example, be based on SOAP standard.

Finally, provider invoices the consumer according to the amount of service that was consumed and receives the due payment.

2.1 Threat Model

Consumer's information in the cloud is often subjected to an increased number of threats, most of them related to information exposure to the network, to the provider shared IT environment – which can allow access from other users (tenants) – and, in the end, to the provider organization itself.

Amongst the possible SaaS threat models, including, for instance, a network eavesdropper or a malicious user sharing the same IT environment with the consumer, none of these will have more access to consumer's information than the actual service provider. Thus, the focus of this work is to consider the provider as a possible origin of misuse of consumer's information. Providing information privacy in the interactions between consumer and provider will, in most cases, also enhance privacy against other less powerful adversaries.

2.2 Privacy Assessment

Roger Clarke (Clarke, 1997) defines information privacy as "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves." In the purpose of this research, we drill down into information privacy and present the following dimensions of the concept:

- **ID Privacy**: to conceal the subject's ID.
- **Location Privacy**: to not reveal the physical whereabouts of the subject.
- **Behavior Privacy**: to hide not the content but how this content is handled. Focuses in not disclosing the correlation of the subject's information over time.
- **Content Privacy**: to conceal the subject's information.

Considering the scenario described, various types of consumer information expose privacy, specifically, during the message exchanges. Following, we analyze how each can compromise the privacy dimensions presented.

2.2.1 Message Metadata

In SaaS message exchanges, the provider needs to authenticate, authorize and account (AAA) for the service consumption. This also enables the provider to correctly charge the consumer for service usage, on demand. AAA is usually based on identification credentials contained in message metadata.

Usual AAA credentials provide a direct link to consumer's ID. Besides, if this link can be done for all messages, the provider can correlate messages (and service usage) over time, compromising, consequently, behavior privacy. The provider can analyze these evidences to figure out when and how the consumer conducts its business. It is important to state that behavior privacy is affected even when the message payload is not available, as information about who is taking part in communications, along with communication volume and patterns, can reveal sensitive information. For message metadata, location and content privacy are not considered.

2.2.2 Message Data

Message Data refers to the message payload present

in the message exchanges. It is the information needed by the provider in order to perform the correct computations in the service consumption. Message payload, as an item of interest, impacts both ID and content privacy.

Vis-à-vis ID privacy, message payload can be inspected and analyzed to reveal the consumer's identification, as consumer's data can have semantic links to consumer's ID. As for content privacy, the message payload is comprised of the actual consumer's data. Location and behavior privacy are not considered in this type of consumer information.

2.2.3 Network-level Communications

Messages are sent through the network, typically in the Internet, which implies that both consumer and provider know each other's network credentials (e.g., IP addresses).

IP addresses affect both ID and location privacy. Current IP addressing schemes link easily the IP address to its owner and can be rapidly tied to a geographic position (Beresford and Stajano, 2003). Network traffic analysis, for instance, of TCP connections transporting service messages, can expose behavior privacy, revealing the correlation between successive service usages over time. Network protocols' payload eavesdropping (content and ID privacy) are not considered here, as this information is the same as those in message metadata and message data discussed before.

3 SaaS ANONYMITY FRAMEWORK

3.1 Multi-layer Design

Safeguarding the anonymity of the consumer during SaaS service consumption enables the protection of business' interests, avoiding the link between message requests and their respective consumer. However, as seen in the last section, ID, location, behavior and content privacy relate to various types of consumer information present in different layers of interaction between consumer and provider. Therefore, anonymity techniques can be employed in a multi-layer design, enabling the use of different and complementary techniques. In our framework, the overall anonymity is preserved by adding up the protection provided at each layer.

We are currently considering three different layers in our anonymity framework, corresponding to each type of consumer information described in the previous privacy assessment: Message Metadata, Message Data and Network.

Each layer utilizes specific anonymity technology to enhance privacy of the respective items of interest. The multi-layer design is a salient feature of our framework: the anonymity technology used in each level can be replaced or adapted to meet specific requirements. Our goal is to make the design flexible enough so it can be adjusted and also evolve accordingly to privacy requirements, producing the best fit to the privacy needs.

The first layer, Message Metadata, is a distinguishing characteristic of the cloud computing scenario. As for the remaining layers, Message Data and Network, the approach can leverage on established anonymity technologies, not directly specific to the cloud computing model. Hence, in this Section, we discuss general solutions for each layer, but we present a detailed design only for the first layer, in the next Section.

In a companion paper, we consider the case of traceable anonymous service consumption, using group signatures as the main anonymity technology (Pacheco and Puttini, 2011).

The challenge in anonymous service consumption in a cloud computing environment relates to the need of the consumer to have access to services, with appropriate SLA, and the need of the provider to account and receive the payment related to service provision. In conventional SaaS scenarios, such as the one described in Section 2, SLAs are usually specified in the service contract (WSDL), which can be easily searched for and selected anonymously by the consumer. However, the service provision itself requires the consumer to be authenticated in order to allow the accounting and the billing for service usage. Moreover, consumer and provider are directly bond by the invoice-payment process, which represents a strong impairment to anonymity.

In our design, we aim at anonymous service consumption, implying consequently also in anonymous payment. The basic idea consists in using an anonymous electronic payment to be performed at the time of service consumption. Our approach is based on e-cash systems (Chaum, 1982), (Okamoto and Ohta 1992), (Camenisch *et al.,* 2005), which fulfills two basic requirements: (1) consumers must be able to obtain and use (pay for) e-cash anonymously; and (2) providers must be able to securely verify the payment immediately, during the service consumption, i.e., after receiving the service request (request message) and before providing the service (response message). Note that in this scheme, each service consumption instance is paid

for separately. This way, it is also desired that the anonymous payment system supports offline micro-payments (Camenisch *et al.,* 2005), whose value can be adjusted to the price of a single service consumption instance.

When using our anonymous electronic payment design, the consumer will simply include the payment credential (i.e., an electronic coin or bill) within the actual service request message metadata. Upon receiving the service request message, the provider verifies the payment and provides the requested service in return, accordingly to the SLA specified in the service contract. This simple interaction scheme excludes the need of any kind of previous bond between consumer and provider, which can compromise the anonymity of the interaction. The consumer is not even authenticated, so the service consumption remains untraceable by the payment transaction. However, if a more formal and even legal bond between consumer and provider is required, for instance, in order to limit the access to the services or to provide compensations in case of misuse or SLA unconformities, there is the alternative of using traceable anonymity, which is discussed in a companion paper (Pacheco and Puttini, 2011). Traceable anonymity cannot be based on e-cash systems, as those are usually untraceable, and the design presented in (Pacheco and Puttini, 2011) is based on group signatures, instead.

3.2 Message Metadata Anonymity

In typical SaaS service consumption, the messages being exchanged contains Message Metadata related to AAA credentials. A context specific characteristic of these credentials in the cloud computing model relates to the billing process. However, AAA credentials relate directly to the consumer's ID. In our design, these credentials are replaced by a simple e-cash credential that is also the payment for the service single usage. E-cash credentials are anonymous and cannot be traced back to the consumer.

3.3 Message Data Anonymity

Message Data anonymity relates to data anonymity and can build upon an appropriated combination of techniques to anonymize data.

Data anonymity can be challenging in cloud computing services, as there are many different types of data and data structures that are possible in business logic and service design. A service-by-service analysis may be required to establish the appropriated data anonymity technique in order to achieve efficient and effective data protection in relation to privacy.

3.4 Network Anonymity

Network level anonymity has been an important research topic since Chaum's mix-net design (Chaum, 1981).

Standing as a state of art low-latency MixNet system is The Second-Generation Onion Router - Tor – (Dingledine *et al*, 2004), an improvement over The Onion Routing project.

Tor is being extensively used and tested by a dedicated community without major breakdowns, and is a suitable technique for network-level anonymity in cloud computing scenario. Also, as cloud computing service consumption is in most cases not tolerant to high latency channels, the fact that Tor is a low-latency anonymity system corroborates its selection.

4 UNTRACEABLE ANONYMOUS SERVICE CONSUMPTION

4.1 Description

In this Section, we present the detailed design of our untraceable anonymous SaaS service consumption approach. Our proposal aims at providing connection anonymity in order to protect consumer's ID, location and behavior privacy dimensions from the provider during service consumption. The requirements for that are threefold:

- **Anonymous Payment System**: consumer must be able to obtain and use (pay for) anonymous untraceable payment credentials, which can be readily verified by the provider, before authorizing the access to and supplying the requested service.
- **Message Metadata (ID)**: service consumption request messages contain anonymous payment credentials whose equivalent value in real currency equals the price for a single use of the service being requested. These credentials do not reveal the consumer's ID at the moment of the service consumption, and also cannot be traced back to the consumer later.
- **Correlation of Data and Metadata over time**: subsequent service consumptions are not linkable to each other, i.e., it is not possible for the provider to correlate any two different service consumptions to the same consumer.

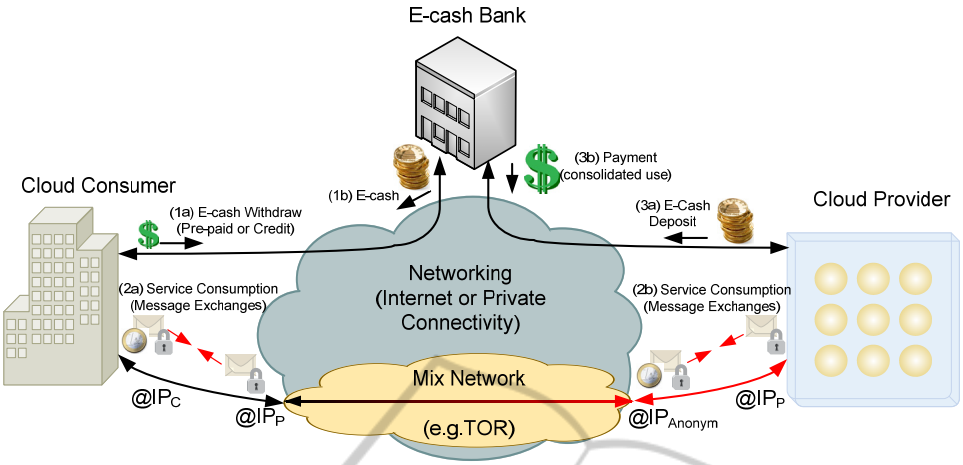

Figure 1: Untraceable anonymous service consumption.

Our proposal consists in including anonymous payment in the service consumption request message, in the form of untraceable electronic cash (e-cash).

A third party is needed to issue the electronic cash (e-cash), which is acquired by consumers in exchange for real money (withdraw operation), and to receive the e-cash used in electronic payments, which will be exchanged back by the provider for real money (deposit operation). This third party organization is called "E-cash Bank" or simply "**Bank**", and is usually an institution with ability to perform financial transactions electronically, i.e., operating in financial market place. Note that the Bank is a mere electronic payment processing entity and it does not take any other role in service consumption itself. Especially, the Bank has no access to the messages exchanged during service consumption. The scheme is shown in Figure 1.

Basically, consumer and provider will "open an account" with the Bank. This means that both consumer and provider recognize the e-cash credentials issued by the Bank. Before service consumption, the consumer must obtain the e-cash credentials with the Bank; this operation is called e-cash "withdraw". In this step, the consumer is exchanging real money (e.g., pre-payment or credit operation) (1a) for electronic cash issued by the Bank (1b). The consumer ("buyer") embeds the e-cash credentials in the service request messages (2a). During service consumption, messages are exchanged anonymously[2] . The provider ("seller"), upon reception of the service request (2b), verifies the payment credential, checks its validity and, if the credential is correct, stores the e-cash and provides the service. Finally, the provider will exchange the e-cash credentials back (3a) for real money with the Bank (3b). This operation is called e-cash "deposit". Note that the system uses a pay-as-you-go (on demand) pricing and the services are actually paid for anonymously at each service consumption instance.

The buyers (i.e., consumers) in e-cash systems enjoy untraceable anonymity, meaning that the e-cash credentials reveal no information about the consumer identity and even the e-cash issuer (Bank) cannot trace back the consumer's identity from the used e-cash. Therefore, the provider must have good security policies and measures in place because a malicious consumer carrying valid e-cash will not be prone to identification in any case.

5 PRIVACY ASSESSMENT

In this Section, we present the privacy assessment for the proposed SaaS anonymity framework. The analysis drills down into the influence of each layer of the framework, and the respective anonymity technique employed in the protection of consumer's information privacy.

5.1 Message Metadata

With e-cash credentials, the provider can authenticate service requests, but cannot distinguish which consumer has actually signed the message. Electronic money has the untraceability propriety.

[2] In order to leverage on the complete potential of the anonymity framework, message data shall be anonymized before sending it to the provider, and message should be delivered by the network through a network-level anonymity tool, such as Tor.

This is true, even for successive messages signed (paid) by the same consumer. This relates to the ID privacy dimension present in the AAA credentials; and the behavior dimension that could be grasped in the correlation of the MEPs over time.

5.2 Message Data

Content privacy dimension and the identification information that can be possibly unveiled by also inspecting the message payload have to be approached accordingly to the specific characteristics of each cloud service. This data anonymity customization need originates from the fact that each cloud service is provided differently and computes consumer data distinctively.

5.3 Network-level Communications

For the Network Anonymity layer there are two items of interests: IP and TCP connections over time. IP affects ID and location privacies and TCP connections over time influences the behavior dimension. However, Tor, as a mix-net scheme, can anonymize IP source addresses, and the addresses used are also changing over time. As a consequence, TCP connections over time become uncorrelated.

6 CONCLUSIONS

In this paper we have presented a privacy enhancing framework for SaaS service consumption, based on anonymity techniques. The design uses a multi-layer approach, allowing the combination of different anonymity techniques, in a flexible manner. Privacy assessments have shown that there are different types of consumer information that can compromise different privacy dimensions, while our multi-layer approach can be successful in protecting consumer privacy through anonymity.

The salient feature of the layered design is the flexibility to approach each level of interaction between consumer and provider, and the respective sensitive information and privacy dimensions, in a separate way. Privacy protection at each level adds up to increase consumer's privacy.

We presented a complete design for an untraceable anonymous service consumption scenario, where a Bank emits electronic cash to be used by the consumer and received by the provider.

ACKNOWLEDGEMENTS

The authors sincerely thank CDT of University of Brasília and the Swedish Institute of Computer Science for the support offered.

REFERENCES

Beresford, A., Stajano, F., 2003. Location Privacy in Pervasive Computing. In *IEEE Pervasive Computing journal, Volume 2 Issue 1*.

Camenisch, J., Hohenberger, S., Lysyanskaya, A., 2005. Compact E-Cash. In *Lecture Note on Computer Science, Eurocrypt 2005, pages 302-321, Springer Verlag*.

Chaum, D., 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. In *Communications of the ACM, Volume 24, Number 2*.

Chaum, D., 1982. Blind signatures for untraceable payments. In *David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, Advances in Cryptology — CRYPTO '82, pages 199– 203*.

Clarke, R., 1997. Introduction to Dataveillance and Information Privacy, and Definitions of Terms. In *http://www.rogerclarke.com/DV/Intro.html*.

Díaz, C., Seys, S., Claessens, J., Preneel, B., 2002. Towards measuring anonymity. In *Proceedings of the 2nd international conference on Privacy enhancing technologies*.

Dingledine, R., Mathewson, N., Syverson, P., 2004. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*.

Okamoto, T., Ohta, K., 1992. Universal Electronic Cash, 1992. In *Advances in Cryptology – Crypto '91, page 324-325, Springer-Verlag*.

Pacheco, V., Puttini, R., 2011. SaaS Anonymity Framework. Manuscript.