Secure User Authentication in Cloud Computing Management Interfaces

Liliana F. B. Soares, Diogo A. B. Fernandes, Mário M. Freire and Pedro R. M. Inácio
Instituto de Telecomunicações, Department of Computer Science, University of Beira Interior
Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal
Emails: {lsoares,dfernandes}@penhas.di.ubi.pt, {mario,inacio}@di.ubi.pt

I. Introduction

The degradation of the security of password-based mechanisms, combined with the increasing number of perils on the Internet, is rendering one-factor authentication outdated. This threatens the security of online operations for enterprises and end users, and consequently affects *cloud computing* solutions. Although cloud computing provides appealing benefits in terms of costs reduction, while increasing productivity, it introduces uncharted security issues (*e.g.*, see [1]) beyond the ones inherited from the Internet. The emergence of mobile computing also makes authentication a priority, and has been reinforcing the need to build stronger and more resilient mechanisms; and simultaneously providing the means to develop new authentication mechanisms, namely Multi-Factor Authentication (MFA) schemes. The convergence to Single Sign-On (SSO) models is being used to eliminate or decrease password management complexity. MFA mostly appears in the form of Two-Factor Authentication (2FA) mechanisms based on One-Time Passwords (OTPs) for the second factor after standard password authentication. Such mechanisms can be based on public-key cryptography and may resort to several technologies to improve user experience, namely Quick Response (QR) codes, Short Message Service (SMSes), Trusted Platform Modules (TPMs), or even contactless Near Field Communication (NFC). Another trend leans to the adoption of risk-based authentication. Efforts for securing authentication are mainly being undertaken by the Initiative for Open AuTHentication (OATH) and the Fast IDentity Online (FIDO) alliance.

The awareness regarding authentication is changing. Because the security state of cloud computing is a hot topic nowadays, it is critical to address its issues in the short-term. There is the need to harmonize and unify authentication into a solid and secure approach. This extended abstract overviews briefly cloud computing security and how authentication is evolving, and summarizes a work on the construction of a model for carrying out authentication securely in cloud computing management interfaces. A prototype of the model is also described, together with some recommendations.

II. Security

Cloud computing is a promising technology. Its public deployment model implies moving on-premises Information Technologies (IT) to outsourced clouds managed by a cloud provider. As such, costumers need to trust the providers, since they may hold potentially sensitive data. In Software-as-a-Service (SaaS) clouds, authentication is limited to the software they offer, contrarily to what happens in Platform-as-a-Service (PaaS) that allows customers deploying what they best see fit. In Infrastructure-as-a-Service (IaaS) clouds, Virtual Machines (VMs) may be grouped in virtual data centers and can be accessed via remote connection protocols. The configuration and management of the virtual data centers is done in management interfaces, to which customers have access to.

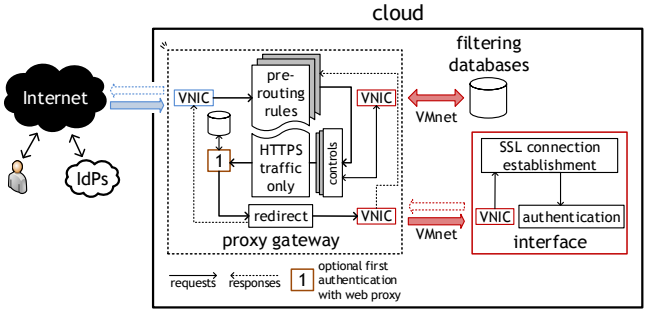

Figure 1. The model for secure user authentication on management interfaces.

The usage of one-factor, password-based authentication is becoming less secure because (i) password breaches culminated in huge password lists and efficient cracking, and (ii) processing units are getting faster. As such, MFA should include distinct factors, otherwise little security would be complementarily achieved. The awareness on password security has not always been the best as well, which is particularly critical for cloud management interfaces, since they comprise a weak method when compared with schemes based on digital signatures or Zero-Knowledge Protocols (ZKPs). Such interfaces open up the front door for the IT of a customer, thereby embodying attractive attack points that are exposed to the outside on public clouds, contrarily to traditional IT network perimeters. But, even emerging authentication trends show a few security caveats. For example, Twitter and Dropbox did not reviewed application workflows while having in mind their 2FA implementations, which resulted in vulnerable 2FA systems [2], [3]. These may be seen as a warning, authentication should be taken into account every step of the way.

III. The Model

The proposed model aims at minimizing the impact of the aforementioned threats by engineering a cloud infrastructure for carrying out authentication on cloud management interfaces. The infrastructure is inspired on the Whonix architecture, and determines placing a VM—the *proxy gateway*—between the connection to the outside and the management

978-1-4799-3214-6/13/$31.00 ©2013 IEEE

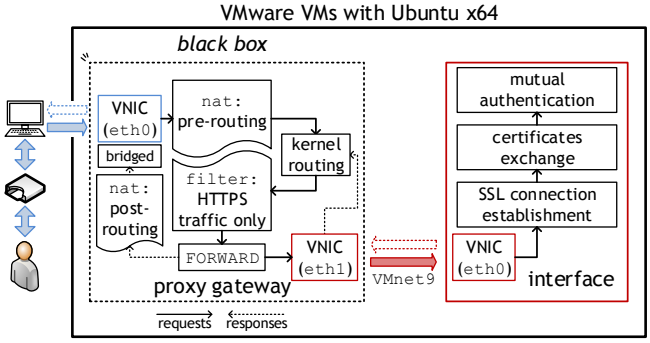

Figure 2. The prototype for strong and mutual authentication.

interface on another VM, as depicted in Figure 1. The proxy gateway mediates access to and conceals the inner VM, transparently forwarding traffic. This approach is useful for attaching arbitrary security controls (*e.g.*, firewalls and intrusions detection/prevention systems) to the proxy gateway as desired, so as to inspect traffic to prevent attacks. A first factor of authentication can be setup on the proxy gateway, and only then access to the management interface would be provided, on which more factors could be evaluated. Both VMs are secured by an isolated private virtual network.

IV. The Prototype

The proof-of-concept prototype uses only readily available and open-source technology, except for the Portuguese citizen card, and it follows the specifications of the model. The proxy gateway VM is connected through `VMnet9` to the VM holding the interface. VMware hypervisors were used with the 64-bit versions of the Ubuntu operating systems running within VMs, as shown in Figure 2. The gateway is hardened with the Linux firewall, configured with `iptables` to act as a *black box*, allowing only HyperText Transport Protocol Secure (HTTPS) traffic, and redirecting requests and responses to the interface accordingly. The management interface uses standard web technology, namely the Apache server with Secure Sockets Layer (SSL) activated for mutual authentication. For testing purposes, the certificate on the server side was created with OpenSSL and the certificates for the path validation of the Portuguese citizen card were dully added to the SSL module. Mozilla Firefox was used to access the interface, after being configured with the required middleware of the smartcard.

The Portuguese identity card is a cryptographic smartcard containing a digital certificate for authentication, protected by a Personal Identification Number (PIN). After swapping the card into a common reader and accessing the interface via HyperText Transport Protocol (HTTP), Firefox asks for the PIN to access the private key. Strong and mutual authentication is then performed at the SSL level enjoying, either way, 2FA (possession of the card and knowledge of the PIN). Access is then mediated by checking if the identity on the certificate of the citizen is registered on a local database or not.

V. Recommendations

MFA decreases the effectiveness of data breaches through compromised accounts. Turning mobile devices into personal authenticators comprises and interesting option for improving user experience by utilizing, for example, QR codes for one of the factors (*e.g.*, Google Authenticator). Nonetheless, the cryptographic material stored in such devices should be encrypted, which is not the case in Authentify xFA [4]. Such would also adhere to the Bring Your Own Device (BYOD) paradigm, while enforcing corporate policy. Special care should also be taken when using biometric data for MFA. Since it is immutable, someone who gets hold of signatures correspondent to some biologic trait may be able to bypass authentication.

For web-based sessions using cookies, perhaps the most promising solution is to cryptographically bound them to the underlying Transport Layer Security (TLS) channel [5]. This avoids cookie theft and can be extended for bounding SSO security assertions. It is also recommended to generate cryptographic material on the user side, like MEGA and unlike Amazon Elastic Compute Cloud (EC2), in order to put the cloud operation more close to the customer. On IaaS clouds, the Linux Pluggable Authentication Module (PAM) can easily integrate 2FA for securing remote connections or root commands. Finally, all password-based systems should favor slow hashing algorithms, instead of fast ones.

VI. Conclusions and Future Work

Computing perceptions are changing with the emergence of cloud and mobile computing. Likewise, authentication is evolving to device-centric and user-centric, combating the efficacy of spam and phishing techniques. If the efforts of major organizations succeed, interoperable and universal protocols will make authentication more secure and perhaps more transparent. This extended abstract summarizes a study concerning the importance of authentication on cloud management interfaces, emphasizing some of the related issues and presenting a model that, by resorting to cloud computing technology, may enable the construction of more resilient, securer and backward compatible authentication systems. A prototype using readily available tools shows the feasibility of implementing such a model in practice using smartcard-based authentication, in this case. This approach adheres to the trends discussed herein. The fact that the model offers backward compatibility may help in the process of gradually replacing password-based mechanisms in the future. As for future work, possible lines of research include evaluating the effectiveness of the proxy gateway under atypical scenarios (*e.g.*, a packet flood), and check its resiliency against a number of threats by using various security controls, while utilizing various authentication mechanisms.

References

[1] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security Issues in Cloud Environments — A Survey," *Int. J. Inf. Secur.: Security in Cloud Computing*, pp. 1–58, 2013. [Online]. Available: http://link.springer.com/article/10.1007\%2Fs10207-013-0208-7

[2] M. Hypponnen, "Twitter's 2FA: SMS Double-Duty," http://www.f-secure.com/weblog/archives/00002560.html, May 2013, accessed Aug. 2013.

[3] D. Kholia and P. Węgrzyn, "Looking inside the (Drop) box," in *7th USENIX Workshop on Offensive Technologies (WOOT)*, Washington, DC, USA, Aug. 2013, pp. 1–7.

[4] Authentify, "xFA," http://www.authentify.com/xFA/, accessed Sep. 2013.

[5] D. Balfanz, "Channel-Bound Cookies," Available in http://www.browserauth.net/channel-bound-cookies, 2012, accessed May 2013.