Cloud Service Security using Two-factor or Multi factor Authentication

Jubin Luckose[1], Sameer Chindarkar[2], Dhanamma Jagli[3]

[1,2] Final year student MCA, V. E. S. Institute of Technology, University of Mumbai, India.
[3] Assistant Professor, V. E. S. Institute of Technology, University of Mumbai, India.

---***---

Abstract - *Due to the recent security infringement incidents of single factor authentication services, there is an inclination towards the use of multi-factor authentication (MFA) mechanisms. These MFA mechanisms should be available to use on modern hand-held computing devices like smart phones due to their big share in computational devices market. Moreover, the high social acceptability and ubiquitous nature has attracted the enterprises to offer their services on modern day hand-held devices. In this regard, the big challenge for these enterprises is to ensure security and privacy of users. To address this issue, we have implemented a verification system that combines human inherence factor (handwritten signature biometrics) with the standard knowledge factor (user specific passwords) to achieve a high level of security. The major computational load of the aforementioned task is shifted on a cloud based application server so that a platform-independent user verification service with ubiquitous access becomes possible. Custom applications are built for both the iOS and Android based devices which are linked with the cloud based two factor authentication (TFA) server. The system is tested on-the-run by a diverse group of users and 98.4% signature verification accuracy is achieved.*

Key Words: **Cloud Security, Two-Factor Authentication, Multi-factor Authentication, Security, Authentication Process, Cloud Service.**

I. INTRODUCTION

With the increasing trend towards ubiquitous computing and Internet technology, remote access to services and private networks is becoming a peculiar feature of today businesses. These advances in technology have facilitated both the enterprises and their targeted user-groups or clients. In a recent report by Gartner, it is estimated that the user authentication services used by enterprises will rise from less than 10% as of today, to more than 50% by 2017. However, the associated security challenges related to user authenticity and safety of private data have opened new avenues for malevolent activities. The emerging requirement is to provide better security solutions that could efficiently cater-for the possible risks and loopholes endangering security of Smartphone users.

Using static passwords for user authentication is a risky venture. This is evident from the recent incidents of security infringement faced by major corporations. Around 6.5 million unsalted SHA1 hashed LinkedIn passwords were leaked in June 2012. A data breach in an FTP server owned by the IEEE resulted in leak of 0.1 million plaintext passwords in September 2012. Drop box confirmed that it got hacked in July 2012 and therefore offered two-factor authentication from October 2012. Twitter, Skype, New York Times and Wall Street Journal suffered security breaches during the last one year. Adobe said it was investigating how 150 million customer records were stolen during October 2013. Therefore, the recent trend is to shift towards TFA, which is more robust to security breaches and identity thefts. US Federal Financial Institutions Examination Council (FFIEC) recommends the banks to use TFA, in order to monitor monetary transactions. The user credentials presented for remote validation for TFA schemes take a number of forms such as one time issued pass-codes, biometric traits, Key Fob hardware authenticators and digital certificates. In this work, we propose to use dynamic handwritten signatures in a TFA framework that runs on interactive hand-held devices.

Human biometrics can be defined as the automatic methods of recognizing different humans based on measurable anatomical, physiological and behavioral characteristics. Physiological biometrics are derived using invasive methods that are based on some physical parameters coming directly from human body. Non-invasive biometric traits that are characteristic of the concerned person are termed as Behavioral biometrics. We prefer to use behavioral biometrics (i.e., handwritten signatures) in the current work because of their high acceptability due to less cumbersomeness and ease in data collection. We argue those behavioral biometrics are more suitable to use in TFA systems because unlike the Key Fob tokens, user does not have to carry the issued identity all the times. Moreover, risk of identity loss/theft is negligible and these are difficult to replicate.

Among all the biometric measures, handwritten signature is an old, tested and most commonly used person authentication metric. Recent advances in sensing technologies and efficient touchable interfaces present in modern hand held devices have also made it an easily deploy-able authentication metric. Mobile devices are easily available to use and thus any authentication framework using biometric data collectible through these devices is of paramount importance. In contrast to traditional scanners and dedicated electronic devices for signature acquisition, newly available mobile devices are pervasive, equipped with high computational resources and also have extra features to attract consumers. Touch screen enabled smart phones and personal digital assistants (PDA's) can use signature verification for making on-line transactions, remote client authentication, signing legal documents and accessing various other online services. Signatures verification is possible both in static and dynamic modes. In current work, instead of using static signature data, we prefer to use dynamic signatures because of their better verification performance, robustness against forgery and ease in data collection through touch screen enabled hand-held devices.

Although mobile platforms pose a promising area for signature based biometric authentication, there are several challenges associated as well. Restricted writing area, comparatively lower computational power of mobile devices and limitations in data collection are the key challenges for achieving high performance. The question of how the constraints put by hand-held devices on the user specific signature characteristics are studied in. It has also been noted that device-to-device variability has a significant effect on the acquired signature dynamics and user specific traits as depicted in acquired data. The high intra-user variability due to poor capturing conditions at different times can also not be ruled out. The signing surface may not be familiar to many people who are accustomed to perform signatures on paper. This in turn can have an impact on verification system's performance. It has also been reported for the case of hand-held devices that various dynamic features (such as, time, speed and acceleration) have relatively low discriminative power. Time required to perform computations during training and testing is also high due to resource constraints.

The challenging acquisition scenario in the case of hand- held devices put constraints on achieving good verification performance. The performance of signature verification systems on hand held devices cannot be evaluated on available datasets acquired using pen based tablets, hand glove or specialized signature pens, because of the difference in acquisition conditions. The users signing on capacitive touch screens of hand held devices normally use the tip of index finger. The finger contact can be lost during signing process, unclean touch screens can degrade sampled signal and natural factors like human skin sweating may also prove be a source of error. This acquisition scenario is challenging and completely different from subjects sitting on a chair and signing with pens or PDA stylus under controlled conditions. Bio secure signature evaluation campaign was launched in 2011 to test available online signature verification systems on two different evaluation tasks. Data was collected on a mobile platform (HP iPAQ PDA) as well and it was reported that the verification performance of systems decrease if data acquisition is carried out on a mobile device. In view of these challenges, we propose a robust, lightweight signature verification system that can provide high performance and better user experience on hand-held devices.

The aim of this work is to propose a TFA system for use on mobile platforms like PDAs, smart phones, tablets or other touch screen based interaction devices. The TFA system uses inherence factor (*something characteristic to a user*) along with the knowledge factor (*something user knows*) during the authentication purposes. We use handwritten signatures in combination with passwords to provide a user friendly authentication framework. Such an implementation of proposed security framework is both reliable and flexible and it can have adapted to various application scenarios in a *Software as a Service* (SaaS) paradigm. The major computational load of the aforementioned task is shifted on a cloud based application server so that a platform-independent user verification service with ubiquitous access becomes possible. Up to the best of our knowledge we are the first to propose and implement an online signature based verification system on smart phones that is linked seamlessly with the cloud. Custom applications are built for both the iOS and Android based devices which are linked with the cloud based two factor authentication (TFA) server. Using these smart phone based applications, we collect data from a group of users and test our scheme. Our system can also be used in conjunction with Security Assertion Markup Language (SAML) that enables multi-factor authentication by defining an open standard data format for exchanging sensitive data.

II. THE MODEL

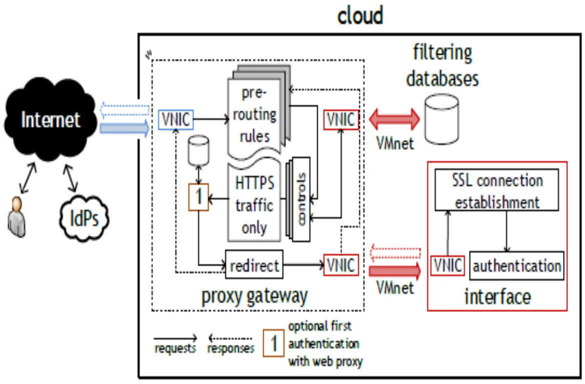


Figure 1. The model for secure user authentication on management interfaces

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

III. 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.

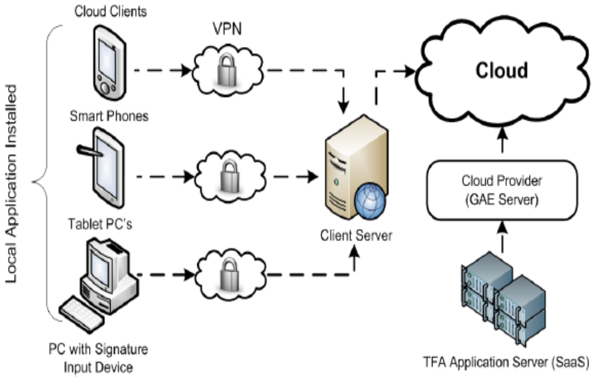
The usage of one-factor, password-based authentication is becoming less secure because password breaches culminated in huge password lists and efficient cracking, and processing units are getting faster. As such, MFA should include distinct factors; otherwise little security would be complementarily 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 inter- faces 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 review application workflows while having in mind their 2FA implementations, which resulted in vulnerable 2FA systems. These may be seen as a warning; authentication should be taken into account every step of the way.

IV. MECHANISM OF MULTI FACTOR AUTHENTICATION

Our system is composed of a simple-to-use library that can be included in Android and iOS applications. A flexible architecture of our scheme provides user interface in the form of a locally installed Smartphone application that connects with client server. Client server configuration is based solely on the application requirements and it may be hosting a SaaS, PaaS, IaaS, NaaS, STaaS, IDEaaS or an APIaaS. This client server needs to be registered at our TFA application server. Upon registration, our Representational State Transfer (REST) web API issues a key to the client. This key is used along with the *Nonce* (number used once) and *cNonce* (client number used once) to authorize the client for using the services offered by our API. The user using the client services must also be registered at the client server.

During the registration/log-in process, the subject is required to enter his/her username, password, signatures and the client specific Uniform Resource Locator (URL). Acquired data is stored in the *json* (JavaScript Object Notation) for- matted secure data. This data format is language independent and provides human readable text based data interchange. The log-in action will redirect the user to the client server who has the authority to forward the user data to our TFA application server. The TFA application server will first validate the client using its issued key and *Nonce*, *cNonce* and then the decision regarding the authenticity of user will be made according to the supplied biometric data and password. The biometric data consists of dynamic handwritten signatures from the user. The system requires one-time training so that a template of genuine biometric can be generated. This template is stored for authentication in future queries. The stored genuine template can be updated upon the request of client/user.

For the purpose of signature verification, two types of techniques are extensively used. These two major groups are Model based techniques and Distance based techniques. Model based techniques, such as Hidden Markov Models (HMM) generate a stochastic model of user handwritten signatures. These stochastic models adapt with respect to user specific dynamics and represent a robust representation using probability distributions of features. Among the distance based approaches, dynamic time warping (DTW) is the most popular one due to its flexibility and good performance over local features matching. We have used the DTW approach mainly because the model based techniques like HMM requires large test data, which does not suit our application situation. The elastic template matching technique - DTW - is used to compare the probe biometric with the genuine template stored on the TFA application server. The client server is addressed regarding the outcome of authentication process.



(a) Overview of Complete System

V. CLOUD SECURITY PRIVACY & CHALLENGES

Cloud services are mainly delivered through three main delivery models Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The current security and privacy challenges in a Cloud environment can be based on state of the art classification under five main categories

(a) Authentication and Identity Management

- Interoperability challenges in between service providers
- Inherited limitations in passwords
- Lack of clarification of multi-tenancy
- Multi-jurisdiction issues

(b) Trust Management and Policy Integration

- Semantic heterogeneity
- Jurisdiction issues
- Trust and interaction/sharing requirements
- Compose multiple services to enable bigger application services

(c) Secure Service Management

- Issues such as price, QOS, and SLAs
- Automatic and systematic service provisioning and composition framework that considers security and privacy issues

(d) Privacy and Data Protection

- Storing data and applications on systems that reside outside of on premise datacenters
- Shared infrastructure, risk of potential unauthorized access and exposure.
- Privacy-protection mechanisms must be embedded in all security solutions.
- Balancing between data provenance and privacy

(e) Organizational Security Management

- Shared governance
- Dependence on external entities
- Insider threat is significantly extended when outsourcing data and processes to Clouds.

VI. 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.

Authenticators comprise 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. 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. 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.

VII. 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 inter- faces, 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.

We propose a cloud based two factor authentication schemes that combines human biometrics and knowledge factor to enhance security. The proposed scheme is easily scalable and is available to use on mobile platforms such as smart phones and PDA's. The cost and resource requirements of the proposed SaaS are low and independent of the user end platform. We show that the implemented system performs well for a relatively small group of users. In future, we will evaluate our authentication framework on a larger-scale, with more clients and users registered on the cloud based service.

REFERENCES

[1] FFIEC. (2005, Feb.) Ffiec releases guidance on authentication in internet banking environment. [Online].

[2] S. H. Khan, M. A. Akbar, F. Shahzad, M. Farooq, and Z. Khan, "Secure biometric template generation for multi-factor authentication," Pattern Recognition, vol. 48, no. 2, pp. 458–472, 2015.

[3] D. Impedovo, G. Pirlo, and R. Plamondon, "Handwritten signature verification: New advancements and open issues."

[4] 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

[5] 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.

[6] Authentify, "xFA,"

[7] D. Balfanz, "Channel-Bound Cookies," 2012, accessed March 2017.

[8] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez- Rodriguez, "Hmm-based on-line signature verification: Feature extraction and signature modeling," Pattern Recognition Letters, vol. 28, no. 16, pp. 2325–2334, 2007.

[9] R. Martens and L. Claesen, "On-line signature verifica- tion by dynamic time-warping," in Pattern Recognition, 1996., Proceedings of the 13th International Conference on, vol. 3. IEEE, 1996, pp. 38–42.

[10] Google, "Google application engine for developers,"

[11] A. Allan, "Magic quadrant for user authentication," 2012.

[12] P. Kamp, P. Godefroid, M. Levin, D. Molnar, P. McKenzie, R. Stapleton-Gray, B. Woodcock, and G. Neville-Neil, "Linkedin password leak: Salt their hide," Queue, vol. 10, no. 6, p. 20, 2012.

[13] Norta, A. Kutvonen, L. 2012. A Cloud HUB for Brokering Business Processes as a Service. SRII Global Conference (SRII), 2012.

[14] Hassan, M.M. Song, B. Yoon, C. Lee, H.W. Huh, E.N. 2009. A Novel Market Oriented Dynamic Collaborative Cloud Service Infrastructure. SERVICES-2 '0 World Conference, 2009.

[15] Ferguson, D.F. Hadar, E. 2010. Constructing and evaluating supply-chain systems in cloud-connected enterprise. 22-24 July, 5th international conference on software and data technologies, 2010.