Network Identity Management Platform Based on eID

ZOU Xiang[1], CHEN Bing[1,2,a]*

[1]The 3rd research institute of ministry of public security (key laboratory of information network security, Ministry of Public Security), Shanghai, China

[2]Dept. of computer engineering of Tongji University, Shanghai, China

[a*]bing_chen2000@163.com

Keywords: Electronic identity(eID); Network identity; Identity management; Massive data

Abstract. With the prompt evolution of Internet, network identity management is getting more and more basilica. Personal electronic identities in cyberspace associated in reality have been one significant and urgent task as online life becomes real. So this paper presents a network identity management platform architecture based on electronic identity (eID). Identity verification and attribute verification services are introduced as the most typical services with security and privacy to be used by personal users, enterprises, websites and foreign clouds. The architecture and related technology could be widely applied to all kinds of real identity verification for personal security and privacy protection in cyberspace.

Introduction

As online worlds become more and more engrossing in our realism, personal identity in cyberspace will be more and more important. Changes in technology, politics and governance, environment, demographics and economics will deeply affect the notions of identity. There are different kinds of Internet identities such as username for instant messaging, email account, online game account and third party payment account etc. But these identities lacking authority and security protection mechanism, it is unable to represent one's true identity in cyberspace and might leak one's identity privacy. SK Telecom Co., Ltd. (South Korea) announced that personal information about 35 million online users had been hacked in July 2011, marking South Korea's worst online security breach. The hacked personal information involved SK users' names, phone numbers, email, resident registration numbers and passwords. The registration details about 40 million users of tianya.cn, one of the biggest social website in China, were found leaked in December 2011. Quickly websites such as Renren, CSDN and Mop etc. were also reported attacked by hackers. It is estimated that over one hundred million usernames and passwords have been leaked.

Academy community, enterprise and government have more and more focused on identity management and electronic identity (simply called eID) to provide identity in cyberspace with authority and security. The electronic identity card or EIC is a government-issued document for online and offline identification [1]. Countries including Belgium and Italy have issued identity cards comprised of conventional identities and identities of digital signature. Most European countries will issue eID in the future. EID and identity management in cyberspace will be one important task for the future development of most countries in the world.

Related Research

Recently research about eID mainly focuses on identity management technologies and systems by governments, enterprises and academic institutions.

Identity management (IDM) is related to how persons are identified, authenticated and authorized in cyberspace[2]. Isolated IDM, Centralized IDM, and Federated FIM[3] are the major identity management models widely used. Isolated IDM is the most common identity management model that the service provider plays the role of service provider and identity provider. This approach simplifies trust complexity but is problematic for users as the number of service providers transacted with increases. Most websites mentioned in Section I implement their Isolated IDM systems. In Centralized models, all the service providers share the global unique identity provider that implements user identity storage and user authentication for all intra-domain users. Users have little control over identity, and privacy protection mechanism is weak in most Centralized IDM systems. Federated IDM aims to enable a group of service providers to recognize user identifiers and entitlements from other service providers in a federated domain. Each service provider knows which services are allowed to use by its employees. A Federated IDM system makes this information available to the service providers on demand, online and with low delay. Federated IDM has been widely accepted because it enhances security and the protection of privacy while reducing costs and redundancy of authorization information management. The major Federated Identity Management standards are SAML [4], Liberty Alliance [5] and WS–Federation [6]. OpenID [7] implements the federated authentication which a user can be authenticated in several web sites by submitting the password of OpenID to the authentication server only once.

Design of Network Identity Management Platform Based on eID

As shown in figure 1, the network identity management platform based on eID consists of four layers: hardware infrastructure layer, resource virtualization layer, eID core management layer, eID identity service layer.

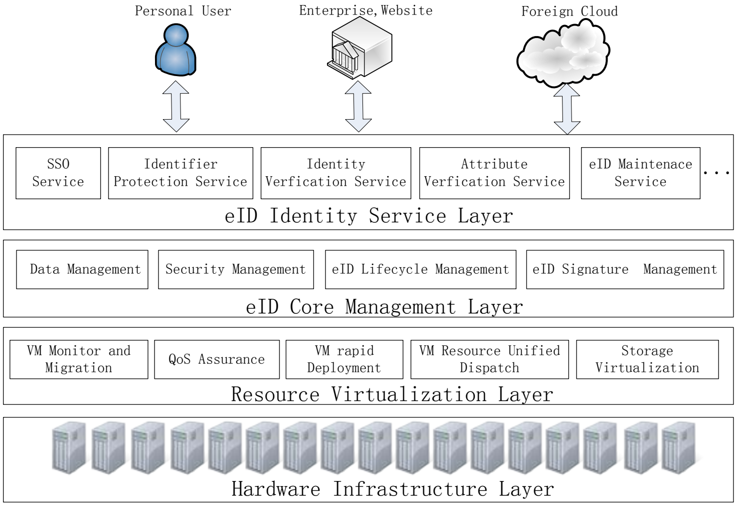

Figure 1. The network identity management platform based on eID.

Hardware Infrastructure Layer

Hardware infrastructure layer may contain one or several data centers that host thousands of servers, storage equipments, networking components and cabinets etc. coordinate tasks to deliver highly available cloud computing services.

Resource Virtualization Layer

Due to the consumption of node resources dynamically change under large-scale identity information service, different identity services as well as the cyclical changes in the verification request amount will lead to sharp fluctuations of resource utilization for request processing. So the efficiency of physical resources use is seriously affecting. Server virtualization [8] is applied to implement decoupling of physical resources and logical tasks as well as the dynamic load and rebuild of computing tasks. VM rapid deployment module keeps the virtual machine template of specific application in memory. Virtual machine could be waked up directly from memory template instead of disk mirroring consequently. VM monitor and migration module monitors the joining and exiting of compute nodes and the change of nodes performance and dynamically migrate virtual machines when current compute node fails. QoS assurance module avoids the degradation of application service quality based on service distribution policies. VM resource unified dispatch module dynamically adjusts the virtual machine configuration of CPU, memory, disk, and network bandwidth in order to achieve fine-grained resource scheduling. In addition to server virtualization, storage virtualization is applied to create a single pool of storage by abstracting different types of storage devices.

eID core management layer

eID core management layer is responsible for implementing core management functions including data, security, lifecycle and signature of eID.

Data management is to store, protect and maintain all data. SQL Server database is used to store important data including personal identity information, eID content information and eID carrier information. Memcached [9] is applied to cache database queries. Physical or virtual servers are divided into Memcached clients, Memcached servers and database servers, as shown in figure 2. Frequent accessed attribute of eID is selected as key of the key-value associative array maintained by Memcached servers. Memcached servers keep all keys and values in RAM. If a Memcached client wishes to set or read the value corresponding to a certain key, the client's library first computes a hash of the key to determine the Memcached server that will be used. Then it contacts that server to determine where to store or read the corresponding value.

As the core asset of cloud service platform, data security is the most important issue to take care of.

eID Identity Service Layer

eID identity service layer contains all services for personal users, enterprises, websites and foreign clouds, including identity verification service, attribute verification service, SSO (Single Sign-on) service, identifier protection service, eID maintenance service etc. Identify verification service could be used to verify the authenticity and validity of specific eID. Attribute verification service could be applied to ensure user attribute such as age, gender, reputation and credit etc. to meet specific requirements based on eID. SSO service could be implemented by taking the platform as OpenID identity provider. Identifier protection service is to protect different kinds of Internet identities such as username for instant messaging, email account, online game account and third party payment account etc. from theft or abuse. eID maintenance service is to maintain eID after it has been generated and issued to users, including support for activation eID before first time using through Internet, updating eID when it has expired or is going to be expired, the maintenance of bundled software et al.

Conclusion

This paper presents network identity management platform based on eID to implement management and service of eID with mass users, complexity terminal environment and provide different services to fulfill the demand of different online applications. Typical services including identity verification and attribute verification services are introduced with security and privacy capacity, which are to be used by personal users, enterprises, websites and foreign clouds. The architecture and related technology could be widely applied to all kinds of real identity verification for personal security and privacy protection in cyberspace.

Acknowledgment

The research work was sponsored by the National High Technology Research and Development Program of China 2012AA01A404 and the Key Program Project of Ministry of Public Security 201301ZDYJ023.

References

[1] Electronic identity card-Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Electronic_identity_card.

[2] X. Zou, B. Jin. “Identity Management with Trust Relationship and Privacy Preservation”. IEEE International Conference on Information Theory and Information Security (ICITIS), 2010.

[3] W. Hommel, H. Reiser. “Federated Identity Management: Shortcomings of existing standards”. In Proceedings of the 9th IFIP/IEEE International Symposium on Integrated Management, Nice, France, 2005.

[4] OASIS. “Assertions and protocols for the OASIS security assertion markup language (SAML) v2.0. organization for the Advancement of Structured Information Standards”, OASIS Standard, 15 March 2005.

[5] T. Wason, S. Cantor, J. Hodges, J.Kemp, P. Thompson, (Eds.): “Liberty alliance ID-FF architecture overview”. http://www.projectliberty.org/resources/specifications.php, 2004.

[6] C. Kaler and A. Nadalin. “WS-Federation specification”. http://www.ibm.com/developerworks/library/specification/ws-fed/, 2003.

[7] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in DIM '06 Proceedings of the Second ACM Workshop on Digital Identity Management, pp. 11-16, 2006.

[8] M. Steinder, I. Whalley, D. Carrera, I. Gaweda, and D. Chess, “Server virtualization in autonomic management of heterogeneous workloads,” in Proc. of the IEEE Sym. on Integrated Network Management, pp. 139–148, 2007.

[9] B. Fitzpatrick. Memcached: a distributed memory object caching system. http://www.danga.com/memcached/, 2009.