Use of Digital Certificates in the Information Security of Small-Medium Business's Internal Processes

Reyes Cruz Jorge Alberto[1], Shabo Li[2] and WeiJie Pan[2]

[1]School of Computer Science and Information, Guizhou University, 550025, Guiyang, Guizhou, China

[2]Key Laboratory of Advanced Manufacturing Technology, Guizhou University (Ministry of Education), 550003, Guiyang, Guizhou, China

Abstract: This article presents a summary and analysis of the use of digital certificates and the considerations that we need to have when we use this kind of infrastructure in the internal business processes of companies. A brief summary of the elements involved in the use of a PKI solution is presented, and also presents the design of a PKI solution for use in small-medium enterprises, explaining the operation of each one of the elements involved in the design proposed.

Keywords: information security; database; certificates.

1. INTRODUCTION

In modern times, due to the continued growth of Internet users and the increase of online transactions (online banking, electronic commerce, etc.), as well as the type of information that is handled during these transactions, the issue of network security becomes increasingly important. This information is not unique to the area of online transactions and operations. Critical information such as the management of the internal processes of companies often needs to be handled and transferred. This establishes security as one of the most important points to be considered.

The use of digital certificates in order to identify people and resources on networks (such as the Internet) and enabling confidential and secure communication between two parties through the use of encryption has been adopted amply in protocols such as SSL (Secure Socket Layer) or TLS (Transport Layer Security) [1]. However, despite d\the use of digital certificates in Internet transactions (such as the annual return of individuals to Mexico and access to the tax office in Madrid [2]), further exploration in the use of technology for the internal business processes of enterprises should be performed.

It is clear that there are many elements that must be considered when we do this kind of analysis. Elements such as PKI (Public Key Infrastructure), certificate management, protection and distribution of the keys and certificates, etc.., deserve an evaluation to establish its common usage in the business activities, and not just for the use in transactions on the Internet. Although these elements have already been investigated previously [3-5], little has been specific about the approach to use it to contribute to the achievement of internal business processes.

2. PKI BACKGROUND

PKI is a robust technology based on asymmetric public key cryptography which provides strong authentication, encryption, data confidentiality, and data integrity. The public/private key is issued and operated as inverse pairs; an operation performed by one of the keys can be reversed or verified by the other. One of the keys is kept as a secret key for the owner, and the other is made available through emails, shared folders, website exchanges of public keys, etc., in order to allow other operations that only the private key owner can access. However, the use of an asymmetric public key cryptography introduces the problem of transmitting, storing, and safely distributing public keys to the users. To resolve these problems centralized entities called Certificate Authorities, transmit and check the keys and signatures. Among the key components belonging to the public key infrastructure (PKI), we find the following [6]:

- Final Entities: refers to any entity that can be identified by a public key certificate.
- Certification Authority (CA): is responsible for issuing the certificates. It can support a variety of administrative functions.
- Registration Authorities (RA): optional component that assumes some of the functions of the CA.
- Repository: generic term used to denote any method to store certificates and CRLs (Certificates Revocation List) and can be obtained by the entities.
- CRL issuer: an optional component that the CA may delegate to publish CRLs.

In PKI, the certificate authority is responsible not only for storing the user keys in a safe way, but also to carry out authentication processes in order to distribute the public keys to other users. However, the complexity of PKI lies on the establishment of the certifying authority, creation of keys for users, key management, authentication, secure storage and transmission of the keys, among many other processes.

Despite the maturation and stability of PKI, companies are reluctant to implement a security strategy based on certificates, possibly due to the perceptions of experiences of the early adoption of this technology [7]. From solutions offered by outside vendors, to solutions that can be implemented internally within organizations, there are plenty of current options for PKI deployments. This paper is a presentation of a proposal design for the implementation of this technology in small-medium enterprises. Through this implementation, information will be transferred securely within the internal processes of enterprises.

3.1. DIGITAL CERTIFICATES

Being able to perform the encryption through the use of an asymmetric system allows the encryption of documents, e-mails, etc. However, receiving the public key of an entity does not guarantee that the relationship between this entity and the key are true. This is where the use of digital certificates, which provide assurance that the public key really belongs to the bearer of it, links the identity of the owner to the public key.

A digital certificate is an electronic document which certifies the authenticity of the identity of a person, company, or other form of identity (such as the URL of a Web site [8]), through a third party called certification authority. These certificates provide the users with security credentials for both identification as well as encryption, which provide greater security than traditional methods such as the use of password authentication or encryption systems. These certificates are issued to enterprises through certification authorities. Major certification authorities include Go Daddy, VeriSign, Comodo, and several others [9]. However, for the internal activities of a business the best option is to establish their own certification authorities which are responsible for issuing these certificates to the employees. As mentioned above, certification authorities are just one element of the PKI infrastructure and are responsible for the publication of these certificates and the administration of the keys. However, it still requires the administration of other PKI's components.

The content of digital certificates is prescribed by the X.509 standard [10], developed by the International Standards Organization (ISO). The latest version is now the X509 v3, where the main elements of the digital certificate are [11]:

- Version number of the certificate format
- Serial number of the certificate
- Signature algorithm identifier
- Issuer of digital certificate: a certificate authority with URL
- Validity period
- Unique identification of certificate holder
- Public key information

3. PROPOSED DESIGN

We already have mentioned before that the establishment of a PKI infrastructure in a business is not an easy process. One of the main problems in trying to establish a PKI-based solution is the planning. Important issues to be considered by companies are issues such as security policies, creation of policies for the certificates, and the establishment of practices for creating certificates.

Currently, there are a lot of tools that allow businesses to establish their own certification authorities. However, we need to determine what the real needs of the company are, and based on these considerations, choose the one that best suits them. Below there is a design solution for establishing a PKI infrastructure which could be adopted by small-medium enterprises, and contribute to their operations by using digital certificates to enhance the secure transfer of critical information between different members of the company.

It is assumed that the design presented will be used in an internal network (LAN), because it is designed for internal data transfer within the company. Because of this, external issues regarding network security out of the same company and the transfer of information between various branches have not been taken into consideration.

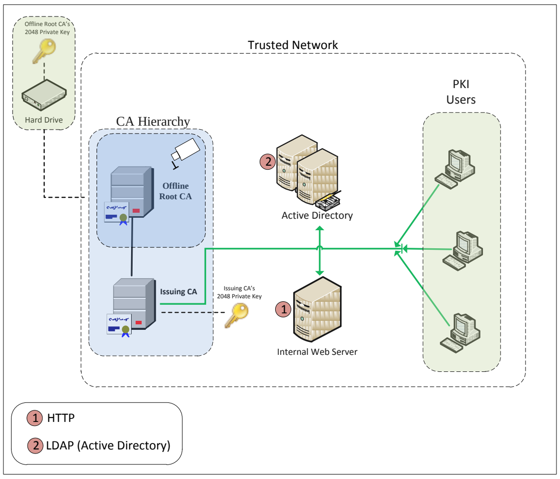

Figure 1. Proposed design of a PKI infrastructure for small-medium enterprises.

3.1. CERTIFICATION AUTHORITIES

The number and levels of certification authorities to consider was made based on the security and availability requirements of the small-medium business. Because of this, we have chosen to use two hierarchical levels which take into account considerations such as hardware costs, server license costs, HSM (Hardware Security Modules), etc.

Although a single certificate authority, functioning as Offline Root and Issuing CA could be considered for the design, the two roles have been separated because of safety issues. With this configuration, the private key of the certification authority is better protected from being compromised because the Root CA is offline. This allows for more flexibility and the integration of a new Issuing CA subordinate to the Root CA if this is required.

The Root CA should never be connected to the network and needs to stay offline and physically secure. The Root CA will be responsible for issuing certificates to subordinate CAs. Both the certificates and the CRL will be manually published and made available to users through a distribution point as HTTP and LDAP.

3.2. KEYS SIZES

The length of the keys is definitely one of the most important factors to be considered. The selected length directly affects the security of the information protected by that key. The Private Key for both the Root CA as well as for the Issuing CA is a selected key of 2048 bits. Although the ideal selection could be the use of a key of 4096 bits for the Offline Root, it was taken into consideration that there are some products that have trouble handling keys bigger than 2048 bits, for instance some of Cisco's products [12]. However, this point could be modified and adapted, with consideration from the same companies, for the use of a key of 4096 bits for the Root CA, depending on the equipment that was selected for the Root CA.

Another factor that was considered in the selection of the key size process was the space required by these keys (major keys also require more space) as well as the consideration of the processing time required to sign the certificates (which generates an extremely low performance in most of the Issuing CAs [13]).

3.3. PROTECTION OF THE PRIVATE KEY

There is a need to add extra measures that allow enhancement to the security of the private keys, especially in the Root CA (despite the fact that the Root CA is offline all the time), because of the importance of private keys in a PKI infrastructure. This helps to protect the private key. One option to ponder would be the use of SmartCards [14]. However, this is not an option to consider because the smart card should remain in the reader to use. Another potential alternative is the use of a Hardware Security Model (HSM) [15], which would allow for a great increase in the security of the private key by encrypting the same key. However, the use of this type of hardware in the design makes this solution not viable for small-medium enterprises due to the high cost of such hardware. The solution adopted for this design makes use of hard disk storage of the Root CA in a safe place. Despite being a simple solution, through the control of access to the hard disk, the chances that the key could be compromised are significantly reduced using this method.

3.4. CERTIFICATES PUBLISHING AND REVOCATION LISTS

In regard to the distribution points and certificate revocation lists, the HTTP protocol from the point of view related with the protocols for publishing points (internal and external), is one of the best alternatives available to make public the certificates and the lists. The use of the LDPA protocol has been added, considering that the proposed design is focused to use in small-companies, which is typically used in situations where the company utilizes a Microsoft-based solution known as Active Directory.

Although some research has found deficiencies in the use of LDAP [16], solutions have been emerging over the years to solve these problems. There have been a large number of applications that currently make use of this protocol and a large number of studies have been done specifically on the use of LDAP [17, 18] and its use in PKI infrastructure.

4. FINAL CONSIDERATIONS

An important point that has not been mentioned in the elements to consider for the use of a PKI infrastructure in the small-medium business is the life time of the certificates. The validity period for the certificate of the Root CA should be two years due to the slight extension of the model proposed regarding this.

Regarding the features within the Root CA, in base with the analysis done with the different algorithms that could be possible to use, the encryption algorithm for the key to be used in the design is the 3DES algorithm, which has a minimum of 10 characters, and for the algorithm used for key generation is an RSA.

The Issuing CA will be responsible for the modification, approval and elimination of certificate requests made by users. The Issuing CA will be the only entity responsible for carrying out the validation of data received by users.

5. CONCLUTION

In this paper we have presented a proposal design for the use of a PKI infrastructure within the small-medium enterprises. We have defined points that should be considered during the establishment of such infrastructures. This proposal can be used in solutions based on Microsoft or some other type of internal solution. This raises the possibility that the same companies could adapt the design to achieve their needs by adding or removing elements (for example the removal of the LDAP) and using only the HTTP protocol.

The proposed design is not intended to meet the needs of various companies, yet it can serve as a base or template once adopted by a company. Said company would only need to determine what other requirements they may have, and add them to the proposed design. It is recommended that in the section related with the private key of the certification authority, assessing the possibility of using other technology, as might be the use of USB Token [19] and the use of a Hardware Security Model (HSM), of course, all this based on the resources of the company.

REFERENCES

[1] Entrust Securing Digital Identities and Information. Understanding Digital Certificates and Secure Sockets Layer [R] White Paper, 2007.

[2] Cámara Madrid. Certificación Digital para Empresas: identificación y firma electrónica [R] White Paper, 2007.

[3] Kasinath G. and Amstrong L. Analysis of PKI as a means of securing ODF documents [J]. Proceedings of 5th Australian Information Security Management Conference, Perth Western, Australia, December 4, 2007, pp.135-141.

[4] SANS Institute Info Sec Reading Room. A Business Perspective on PKI: Why Many PKI Implementations Fail, and Success Factors To Consider [R]. 2001.

[5] Liu M., Sun S. and Xing M. Study on Security Based on PKI for E-commerce of Statistics Information System [J] ACM, 2005, pp. 720-732.

[6] Nortel S., Lareau P. and Lloyd S. PKI Forum: PKI Basics – A Technical Perspective [J] November 2002.

[7] Peterson J. Enterprise effectiveness of digital certificates: Are they ready for prime-time? [D] (IN) SECURE Magazine, Issue 22, September 2009.

[8] Carro L. Certificados digitales. Implantación en centros educativos [D] Sociedad de la Información, Issue 23, Noviembre 2010.

[9] http://www.herongyang.com/PKI/Introduction-Most-Popular-Certificate-Authorities.html

[10] Curry I Version 3 X.509 Certificates [D] Entrust Technologies White Paper, 1997.

[11] Digital Certificate Infrastructure [D] Digital Library Federation.

[12] DEAL D. The Complete Cisco VPN Configuration Guide [R] December 15, 2005.

[13] http://technet.microsoft.com/en-us/library/cc962059.aspx

[14] CardLogix Coorporation Smart Card and Security Basics [D] pp. 30-33.
[15] SANS Institute Info Sec Reading Room, An Overview of Hardware Security Modules [D] 2002.
[16] Chadwick D. Deficiencies in LDAP when used to support Public Key Infrastructures [D] University of Salford, England.
[17] Karatsiolis V., Lippert M., and Wiesmaier A. Using LDAP Directories for Management of PKI Processes [J], Darmstadt, Germany.
[18] Karatsiolis V., Lippert M. and Wiesmaier A. Planning for Directory Services in Public Key Infrastructures [J], Darmstadt, Germany, pp. 349-360.
[19] Certified Security Solutions, Deploying Smart Cards in Your Enterprise [D] White Paper, 2005

SOCIEDAD DE LA INFORMACION

www.sociedadelainformacion.com

Edita:

Director: José Ángel Ruiz Felipe
Jefe de publicaciones: Antero Soria Luján
D.L.: AB 293-2001
ISSN: 1578-326x