ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Survey on Digital Certificates

Sujata Gawade, Vina M. Lomte

ME Student, Dept. of Computer Engineering, RMD Sinhagad Institute of Technology, Warje Campus, Pune, India

Head, Dept. of Computer Engineering, RMD Sinhagad Institute of Technology, Warje Campus, Pune, India

ABSTRACT: The most common use of certificate is in websites to provide secure communication. As CA is responsible for issue, revocation and reissue of certificate, the certificate management task gains a lot of importance. There are many issues in certificate management such as revocation in case the certificate got compromised before expiry, handling anonymous digital certificates, fast revocation and reissue of certificate and much more. The most common way of managing certificate revocation is use of **Certificate Revocation List (CRL)**. However, due to above issues, the revocation of certificate cannot be completely automated. Again we have to consider burden on CA for certificate management. Another approach to handle the overhead of certificate management on CA is to distribute the part of CA responsibilities (such as reissue and revocation) to user, in controllable manner so that the basic rights of CA (such as issue of certificate) remain untouched. In this paper we explore various techniques used in digital certificate generation as well as management of those certificates such as short lived certificate, multi-certificate PKI etc. We also review the ways by which we can enhance security for application specific use without using CA model (e.g. using certificate transparency for emails.).

KEYWORDS: Certificate Revocation list; Certification authority; multi-certificate PKI

I. INTRODUCTION

The number of people and businesses online is continuing to increase. As access becomes faster and cheaper people are spending even more time connected to the Internet for personal communication and business transactions. The Internet is an open communications network that was not originally designed with security in mind. Criminals have found they can exploit its vulnerabilities for fraudulent gain. If the Internet is to succeed as a business and communications tool users must be able to communicate securely. All security properties can be achieved and implemented through the use of Public Key Infrastructure (in particular Digital Certificates). Digital Certificates are a means by which consumers and businesses can utilize the security applications of Public Key Infrastructure (PKI). PKI comprises of the technology to enables secure e-commerce and Internet based communication. Existing systems make use of public key infrastructure for certificate issue, private key storage, publication of certificates, key update, backup recovery, key escrow and certificate revocation list etc.

The most common standard for digital certificates is the X.509 standard. Each certificate is associated with a public key and a private key. The public key is incorporated into the X.509 certificate and is always available with the certificate itself. The private key is always kept private and never transmitted. In general, Certificate authority (CA) verifies the authenticity of certificate. In most common scenario, CA is third party like VeriSign which is trusted by certificate owner as well as relying party.

Recent work on area of digital certificate has major contribution towards certificate management and security. The main tasks in certificate management include certificate revocation and certificate reissue. Further, the security of application is also major aspect. This paper gives overview of existing certificate based systems and various problems identified with them. It also discusses various advantages and disadvantage of existing work in this area.

Certificate revocation is important task in certificate management. CA issues a certificate with some validity period. However, the certificate may become bad before expiry due to compromise of its key. In such case the certificate need to be revoked before expiry. Another reason for revocation of a certificate before expiry is change in user's name, company or any other information in the certificate. Revocation of such a certificate is done manually or through certificate revocation list. The time of certificate revocation is major factor that need to be considered so as to avoid any

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

use of certificate after its expiry or compromise. If CA goes through CRL once in month then maximum time required for revocation of certificate can be one month. In such a case user can use the certificate for a month.

To avoid above said issue, short lived certificates can be used. In this method the certificate with shorted duration are created. When user request CA for issue of a certificate; CA respond this request with an URL. This URL is active for year or more. With this URL, user can have number of certificates with validity period of few days.

Another approach for fast revocation is to use semi-trusted mediator. Before decrypting/signing any message user have to contact SEM for token. Without this token, it is not possible to decrypt/sign messages. Whenever there is need of certificate revocation the user informs SEM for not assigning token. This avoid use of certificate after its revocation.

Generating correlated certificates is also a way to provide better certificate management. In this depending on the basic key, correlated certificates are generated by forming a correlation tree. In this approach, CA issues only one certificate however user can have more than one certificate per issued certificate. The security of correlation tree is major concern in this application. Hence online creation/storage of correlation tree is not done.

To address the security shortcomings of CAs as trusted third parties vouching for the identity-key binding, certificate transparency is proposed. The core idea behind the concept is a public, verifiable, and append-only log. Another way is use of RIKE. RIKE is integration of PKI and identity based encryption. It is used to address conflicting requirements of confidentiality and nonrepudiation.

In this survey, Section II gives the Literature review for certificate management and security. It also lists their pros and cons.

II. RELATED WORK

In paper [1] author proposes fast revocation of certificates using security mediator called SEM. The paper addresses the issues in time required to revoke a certificate such as late revocation may allow user to access his or her messages though he or she is no more intended to use those anymore. SEM is online semi-trusted server. The idea behind SEM is, to decrypt any message the user has to acquire a token from SEM. Though user have private key, he/she cannot decrypt the message without this token. In case of revocation, the administrator stops SEM from issuing token. Due to lack of token, user no longer is able to decrypt/sign the message.

The disadvantage of this system is SEM replication. SEM replication may cause an exposure of SEM key which further lead to unrevoked certificates. Further SEM performance, security and fault tolerance are major concerns.

This paper [2] presents a concept of short lived certificates. In existing systems the CA issues the certificate with longer validity period, generally more than a year. However, thecertificate can go bad before its validity period. Google proposed short lived certificates which has validity period of few days which can be obtained on demand basis through the URL provided by CA. However, CA provides URL which is active for a year or more.

The disadvantage of this system is; compromise of root CA certificate is not handled. Further, as certificate authorities are online; there is risk of generation of fake certificates or stealing of keys. However, due to chrome, the window of vulnerability will be shortened.

This paper [3] proposes certificate transparency model for ensuring the security of mails. In Certificate transparency approach, certificate authorities are prevented from issuing public key certificates for a domain without being visible to the owner of the domain. The underlying concept is; public log is maintained which has list of all issued certificates. The certificate is accepted if there is entry on the certificate in log. Revocation management is done by sending these logs periodically to browser. It uses merkel tree algorithm to maintain certificate transparency.

The disadvantage of this system is spam handling should be done on client side.

This paper [4] discusses the unlinkability of certificate attributes and possible associated attacks. The use of certificate metadata in covert channel attack can be learnt in this paper. It proposes U-prove architecture to solve this problem.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

This paper [5] proposed a generalized digital signature model. In this user has no public key, in contrast it has secret token based security. It proposes discrete logarithm based and integer float based protocols to implement this functionality.

It uses user's personal information such as driving license, birth certificate in digital certificate. In this system, certificate authority still has role of issuing the certificate. This paper addresses user authentication and key establishment problems.

In [6], the problem of certificate revocation is addressed. It uses authenticated data structures to address these problems.

The main construction is 2-3 trees with leaves corresponding to the revoked certificates' serial numbers in increasing order, so that proving a certificate is revoked or not reduces to proving the existence of certain leaves in the sort tree. A centralized directory maintains the tree and responses to the CA's updates as well as relying parties' queries. The system is robust to the changes in parameters however it does not reduce communication cost with CA.

This paper [7] presented various ways by which we can remove the use of certificate revocation lists. It proposes approaches like certificate transparency, OCSP responders to avoid CRL. OCSP is already almost outdated as it is suitable for middle scale infrastructure and certificate transparency has its own limitations of spam handling. However it is still possible to avoid the CRLThis paper [8] focused on analysis of Heartbleed OpenSSL bug. This bug made it possible for attacker to view server's memory contents. It made possible for attacker to steal the private keys residing in server memory. This paper provides us best learning allowing us to measure how completely and quickly administrators took steps to secure their keys.

This paper [9] presents an alternative for Public Key Infrastructure. This paper addresses the conflicting requirements on key escrow. If the certificate is used for non-repudiation and signatures, key escrow is prohibited by laws. If the certificate is used for confidentiality and to encrypt messages, key escrow is usually required. RIKE provides solution which eliminates these drawbacks. RIKE is an integration of Identity Based Encryption (IBE) and PKI. The basic idea is to let each user has only one certificate. This certificate is used for only non-repudiation, and the private key is not escrowed. Then, the certificate is inputted to IBE as an identity to derive another public key. The second key pair is inherently escrowed and used for confidentiality only. The main issue in this paper is building hierarchical RIKE through integration of hierarchical IBE and hierarchical PKI.

This paper [10] gives a survey on various security issues with HTTPs. The basic learning from this paper gives understanding of severity in various attacks independently.

This paper [11] focuses on credential revocation in an infrastructure less environment. The basic idea is; after detecting a node M engaging in some illegal activity, another node 'A' broadcasts a signed suicide note which includes the identities of both A and M. The other nodes in the network then verify the signature and, if correct, revoke both A and M. This can be achieved by adding both identities to a blacklist and deleting all keys shared with either node. This strategy is premised on the observation that if a node determines another node has cheated, there is no more convincing way to let its neighbors know of its sincerity than to transmit a signed self-revocation certificate. The disadvantage of this system is revocation of good node with bad node which seems to be desperate solution.

This paper [12] addresses the problem of certificate management. It proposes a framework for generating correlated digital certificates which can be used for applications like multi-certificate PKI or anonymous digital certificate. The system uses RSA, DSA algorithms to generate correlated certificates. However the drawback with this system is the certificate correlation tree cannot be built on online platform as disclosure of any certificate before activation may lead to security breach. Another drawback of this system is user need to be educated properly as the overhead of CA is moved to user's side.

III. PROPOSED SYSTEM

Correlated certificate generation framework [12] includes RSA, ECDSA, and DSA to better satisfy the security and privacy requirements of certificate users. The multi-certificate public key infrastructure (MCPKI) supports user certificates' spontaneous substitution as well as self-reissue after self-revocation. The anonymous digital certificate, features a self-service of de-anonymization, allowing the user to reveal her identity-key binding to preferred

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

communication peers only. The proposed framework is PKI-compatible and is ready to be integrated with existent PKI enhancements. To further enhance in security in MCPKI environment, the suicide for common good model [11] can be integrated along with above model wherein users have capacity to revoke the certificate of malicious node at the cost of own certificate.

IV. CONCLUSION AND FUTURE WORK

This paper analyses various techniques used for digital certificate management, security and generation. Also given the advantages and drawbacks present in the different studies performed by various researchers. It proposes to use correlated certificate generation framework to better meet security and privacy requirements.

V. AACKNOWLEDGEMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are also thankful to the reviewer for their valuable suggestions.

REFERENCES

1. D. Bonch, X. Ding, G. Tsudik and C.M. Wong "A method of fast revocation of public key certificates and security capabilities." in Proc.USENIX Secur. Symp. Aug. 2001Art. ID 22.
2. E. Topalovic, B. Saeta, L.-S. Huang, C. Jackson, and D. Boneh, "Towards short-lived certificates," in Proc. W2SP, May 2012, pp. 1–9.
3. M. D. Ryan, "Enhanced certificate transparency and end-to-end encrypted mail," in Proc. NDSS, Feb. 2014, pp. 1–14.
4. M. Ates, F. Buccafurri, J. Fayolle, and G. Lax, "A Warning on How to Implement Anonymous Credential Protocols into the Information Card Framework"
5. L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2372–2379, Jul. 2011.
6. M. Naor and K. Nissim, "Certificate revocation and certificate update," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 561–570, Apr. 2000.
7. R. L. Rivest, "Can we eliminate certificate revocation lists?" in Proc. FC, Feb. 1998, pp. 178–183.
8. L. Zhang et al., "Analysis of SSL certificate reissues and revocations in the wake of heartbleed," in Proc. ACM IMC, Nov. 2014, pp. 489–502.
9. J. Lin, W.-T. Zhu, Q. Wang, N. Zhang, J. Jing, and N. Gao, "RIKE+: Using revocable identities to support key escrow in public key infrastructures with flexibility," IET Inf. Secur., vol. 9, no. 2, pp. 136–147, Mar. 2015.
10. J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in Proc. IEEE SP, May 2013, pp. 511–525.
11. J. Clulow and T. Moore, "Suicide for the common good: A new strategy for credential revocation in self-organizing systems," ACM SIGOPS Oper. Syst. Rev., vol. 40, no. 3, pp. 18–21, Jul. 2006.
12. Wen-Tao Zhu, Member, IEEE, and Jingqiang Lin, Member, IEEE "Generating Correlated Digital Certificates: Framework and Applications" IEEE Trans. Information Forensics and Secur., VOL. 11, NO. 6, June 2016.

BIOGRAPHY

Ms. Sujata Gawade is a master of engineering student in the Computer Science and Engineering Department, RMD Sinhagad Institute of Technology, Savitribai Phule University Pune. She studying Master of Computer Science and Engineering (ME) degree from Savitribai Phule University, Pune, MS, India.

Prof. Vina M. Lomte is working as Head of Computer Science and Engineering Department in RMD Sinhagad Institute of Technology, Savitribai Phule University, Pune.