International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 2 Issue 5, May-2013, pp: (44-47), Available online at: www.erpublications.com

Securing Database using Public Key Infrastructure A Proposed DB PKI Architecture

Ashmeet Kaur
Master of Technology, Amity School of Engg. & Tech, Amity University, Noida, India

Abstract: **Database security concerns the use of a broad range of information security controls to protect databases potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical. To secure information and data against threats such as intrusion or unauthorized access, the Public Key Infrastructure (PKI) has been developed. It realizes basic concept of PKI i.e. PAIN, where P stands for Privacy, A stands for Authentication, I stands for Integrity, N stands for Non-Repudiation A public key infrastructure (PKI) provides the framework of services, technology, protocols, and standards that enable you to deploy and manage a strong and scalable information security system based on public key technology. In our paper we proposed PKI architecture for Database. Based on the type of table access right given to the user certificates are issued to them. The access rights are categorized into three different groups of user. First group of users can execute all the quires including truncate delete etc… Second group can add and modify the database without deleting data and the third and last group can only view the information stored in the database. Simple authority PKI models is used to implement our DB-PKI architecture.**

Keywords: **PKI (Public Key Infrastructure), Certificate Authority, CRL, Simple Authority.**

1. INTRODUCTION

Database security is a specialist topic within the broader realms of computer security, information security and risk management. To secure data against threats such as intrusion or unauthorized access, the public Key infrastructure (PKI) has been developed. It realizes authentication and confidentiality using public key cryptography technology.

The DB PKI architecture has to accommodate the limitations imposed by the methods of access controls on database. In PKI we issue certificates to the users with different privileges depending upon their access rights. A certificate is just like an electronic passport that validates the identity of a user or a device that wants access to the network. The certificate ensures the public key actually belongs to an entity and checks entity's information is correct. When a trusted identity (a certificate authority) [2,3] signs an entity's public key[1] only then a certificate is created. A certificate contains information such as:

- User name of the certificate
- An expiry date
- A unique serial id number provided to the certificate by the CA
- The user's public key
- Information about the rights and uses associated with the certificate
- The name of the CA that issued the certificate
- The signature of the CA.
- An algorithm that was used to sign the certificate.

This paper combines basic data structures for certificate revocation, PKC, Certificate Revocation List (CRL) and the authenticated dictionary such as Certificate Revocation Tree (CRT), into a single framework. CRL management using our suggested scheme enables higher security because it does not require trusted entities other than the CA; 2) it improves scalability and performance because it does not require responses to be signed; and 3) it can interoperate well with the existing CRL framework.

In this paper we proposed a new PKI architecture for Database which is based on the type of table access right given to the user. The access rights on the database are categorized into three different groups. First group of users can execute all the quires including truncate delete etc… Second group can add and modify the database without deleting data and the third and last group can only view the information stored in the database. Trusted certificate authority will issue certificates to these three different groups of users and according to the type of certificate the user can execute the query on the database.

2. PUBLIC KEY INFRASTRUCTURE

The PKI approach is an alternative means of source for achieving security. PKI provides a method to ensure that the sender can encrypt a message, which the receiver can decrypt, while preventing anyone who intercepts the message from reading it. The sender and receiver get a pair of public and private keys. These keys are mathematically related. To encrypt a message for a certain receiver, the sender uses the receiver's public key for encryption. Only the intended receiver can decrypt this message with his private key. PKI requires a certification authority for issuing digital certificates, a registration authority maintaining the records of the PKI users in a directory service, a policy framework governing certificate issuance and cancellation, and PKI-enabled applications [11].

The advantages of PKI [5,6,7] makes it suitable for securing industry standard like for securing Internet and e-commerce applications. PKI is also a standards-based technology. It allows the choice of trust provider. It is highly scalable. Users maintain their own set of certificates, and certificate authentication will involve exchange of data between client and server only. No third party authentication server needs to be online. Thus there is no limit to the number of users who can be supported using PKI. PKI provides delegated trust [3]. That is, a user who has obtained a certificate from a recognized and trusted certificate authority can authenticate himself to a server the very first time he connects to that server, without having previously been registered with the system. Since PKI is not a single sign-on service, it can be implemented in a way so as to enable single sign-on.

3. CERTIFICATE-BASED AUTHENTICATION OF PKI

Primary concern in distributed environments is establishing user identity. The most common authentication method in use is Passwords [7.8], but we need to employ stronger authentication services for particularly sensitive data. This section describes: Certificates and Certificate Authorities. Having a central facility authenticate all members of the network (clients to servers, servers to servers, users to both clients and servers) is one effective way to address the threat of nodes on a network falsifying their identities. This method deals with certificates and certificate authorities [6].

3.1 Certificate Authorities

A certificate authority (CA) [6] is a trusted third party that certifies that other entities--users, databases, administrators, clients, servers--are who they say they are. When it certifies a user, the certificate authority verifies the user's identity and grants a certificate, signing it with the certificate authority's private key. The certificate authority has its own certificate and public key, which it publishes, as well as a private key, which is securely maintained. Servers and clients use the CA's root certificate to verify signatures that the certificate authority has made. A certificate authority might be an external company that offers certificate services, or an internal organization such as a corporate MIS department.

4. SIMPLE AUTHORITY

Simple Authority [6,8] is a fully functional Certification Authority, or Certificate Authority (CA), that is designed to be very easy to use. It generates and manages keys and certificates that provide cryptographic digital identities for people and/or computer servers. These identities are designed to be used in other applications such as for:

- Secure two factor authentication - using a technology like Key Vault for controlling access to Web resources
- Secure email - for digital signing and encryption of email
- Document signing - including PDF, Word and Open Office documents
- VPN access - to provide a much higher level of security than username/password access
- Client SSL authentication - to control access to an online service such as a subversion repository or wiki
- Server SSL authentication[8] - to authenticate a Web server to people within a known community
- Code signing - including Java archives, Windows executables, etc.

Simple Authority is free and contains no nag screens when used to manage up to 4 users. If you want to manage more users, or if you require advanced features, then you need to purchase.

- Simple Authority contains no adware or other nastiest.

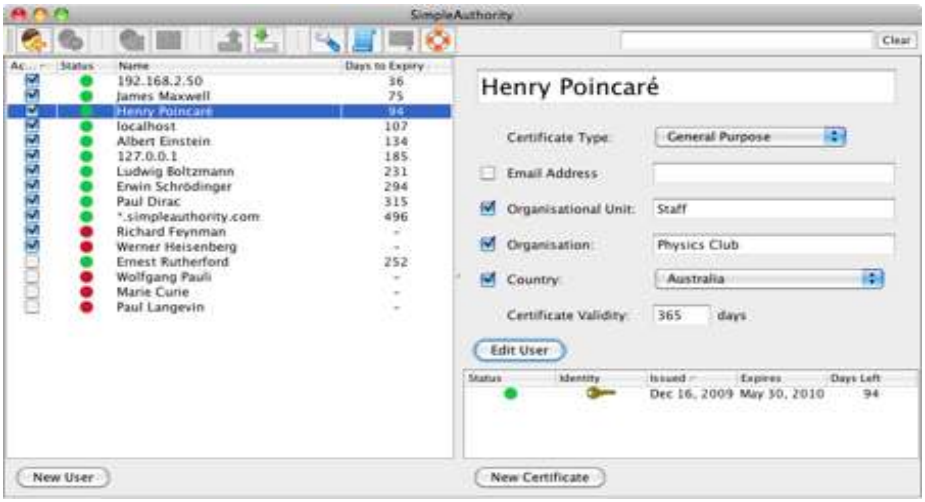

Fig 1: SimpleAuthority

5. PROPOSED DB PKI ARCHITECTURE

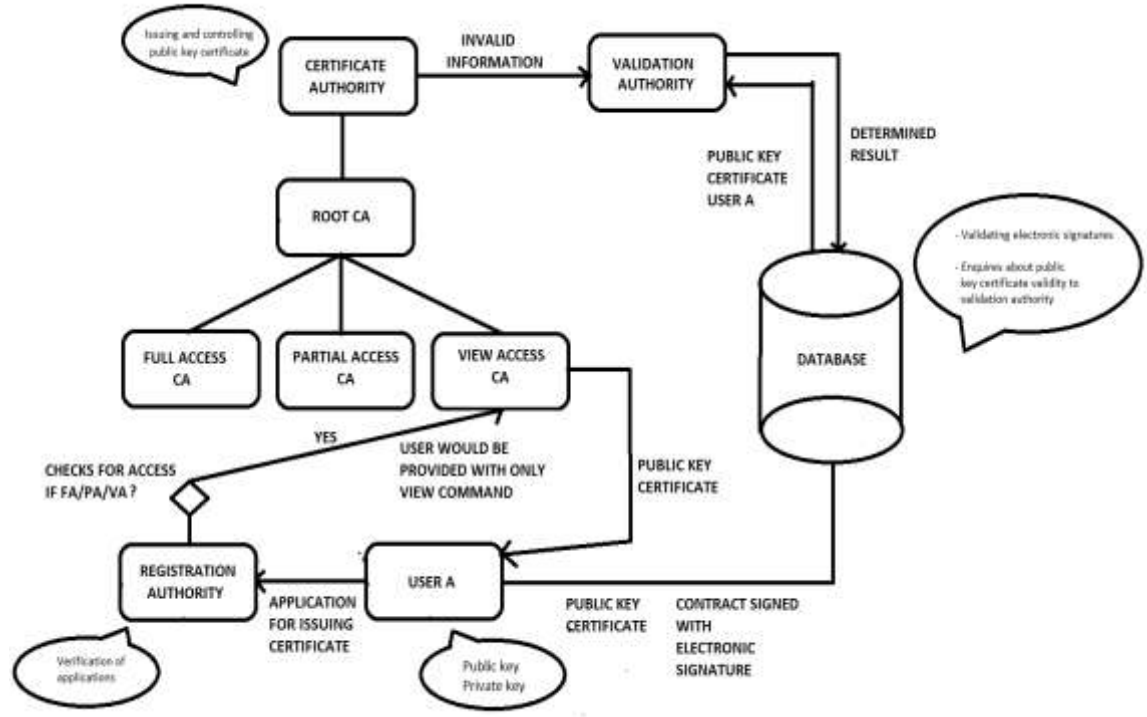

Fig 2: Proposed Architecture

The motive of this proposed architecture is that firstly the root CA makes many CA'S under its authority which can issue certificate to the valid and authentic users and let them access database according to their level.

A CA issues digital certificates containing a public key and the identity of the owner. The matching private key is kept secretly and not made available publicly, the secret is kept by the end user who generated the key pair. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates. CAs use a variety of standards and tests to do so. In essence, the Certificate Authority is responsible for saying "yes, this person is who they say they are, and we, the CA, verify that".

If the user trusts the CA and can verify the CA's signature, then he can also assume that a certain public key does indeed belong to whoever is identified in the certificate.

6. WHY PKI?

A solution to the problem of public authentication of public-key information is the web of trust scheme, which uses self-signed certificates and third party attestations of those certificates. The techniques and measures used earlier had many loopholes ,so providing certification using PKI stands out in providing security to database
A public-key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.[1]

In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The third-party Validation Authority (VA) can provide this information on behalf of CA. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). The RA ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation.

7. CONCLUSION AND FUTURE WORK

These approaches will reduce the threats against data such as intrusion or unauthorized access but will arise a lot of major issues regarding the CA, Certificate and CRL management, cost of implementing and managing PKI etc. One of the major obstacles of current PKI structure is safe storage of user's private keys. Thus what is really needed is a solution that would decrease cost of ownership while it would strengthen security of storage. Hence this approach still requires a lot more work to be done before its actual implementation.

It is very possible that many changes will be implemented on the structure of PKI. Many different ideas have been given regarding to technology, software, and organization of PKI.

One of the major obstacles of current PKI structure is safe storage of user's private keys. Thus what is really needed is a solution that would decrease cost of ownership while it would strengthen security of storage. The ideal solution would be to have a server centric approach with the strong factor authentication to a hardware based container, and biometrics is the mechanism with the strongest authentication factor. Thus one of the most popular ideas that has been given recently is to combine biometrics with server centric PKI, were user's private keys are kept and managed on a centralized file server. The authentication server determines the identity of the user by checking his/her biometric sample with the biometric sample saved at the central server . This technique has been implemented only in some research laboratories, as the cost is still too high and the solution is still not very practical.

REFERENCES

[1] Darrel R. Hankerson," Benefits of an Open–Source PKI implementation in Cryptanalysis of RSA and Its Variants in Guide to elliptic curve cryptography in 6th edition, New York.
[2] M. Jason Hinek, "Cryptanalysis of RSA and Its Variants" in PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks" in 3rd edition, Sydney.
[3] Luther Martin,"Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure" in Introduction to Identity-Based Encryption in 3rd edition.
[4] Francois Dessart, "Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations" in PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks in 4th edition.
[5] Menezes A, "PKI-Enabled Services" in Handbook of applied cryptography in 2nd edition, New Jersey.
[6] Erin Banks ,"Certificates and Certification" in Identity-Based Encryption,in 5th edition, 1992.
[7] Bill Ballad,"Trust Models" in Access Control, Authentication, and Public Key Infrastructure in 6th edition, Sydney.
[8] Roberto M. Avanzi ,"Electronic Signature Legislation and Considerations" in Pki: Implementing and Managing E-Security in 4th edition, Melbourne.
[9] Walsh G," Authentication Server Private Key Vault Biometric database", The Walsh Report, Accessed, 2004
[10] Whittle R, Rough critique of the 6 May Project Gatekeeper report. Office of Government Information Technology, ISBN 0 642 32032 2.,1998.
[11] Introduction to Public Key Technology and the Federal PKI Infrastructure" by National Institute of Standards and Technology, 2009.