PKI Endorsement Functions for Network Users

Sreekanth D
Department of Computer Applications
Westfort Higher Education Trust
Thrissur, Kerala,India

ABSTRACT

Computer Business Systems and automated business transactions require robust and rigorous security measures. Public key cryptography supports security mechanisms such as confidentiality, integrity, authentication and non-repudiation. A Public Key Infrastructure (PKI) is a foundation on which other applications, systems and Network components are built.

Gatefree is a user endorsement gateway system network which is opened to public. This system can be used for controlling the campus wide open network.

In this research, we implemented PKI endorsement functions for Network Users, and we enabled the certificate based endorsement via a web browser.

Keywords

PKI, Certificate management.

1. INTRODUCTION

The omnipresence of the Internet Technologies presents many opportunities, but also poses security and integrity issues. Improvement of network infrastructure, we can use services to intend for an autherised individual on the internet or on the internal network of organizations, for example shopping on the internet, web mail, e-commerce, reporting of the university lectures etc.

The endorsement services are commonly done with user ID and Password with low cost widely because it doesn't need any special hardware or software. The user ID and Password endorsement has many problems for user side, for example in case of multiple services, management of User ID and Password becomes complicated and users may set same password as all services to simplify them, that causes several security issues.

Instead of maintaining this user ID and password endorsement, there is the endorsement using electronic certificate based on PKI. The PKI based authentication can provide multiple services with one certificate. Therefore management for the users simplifies and usability improves.

In this research we supposed that each organization utilize certificate base PKI as authentication and authorization platform. Based on this we implement PKI authentication functions for Network Users and enabled the certificate based authentication on web browser. By this way we increase the usability of PKI Endorsement functions for Network Users.

2. PKI ENDORSEMENT FUNCTIONS

2.1 Overview

The internet becomes the infrastructure of the society. Nowadays most of the people want to access the inter network wherever they goes. In order to fulfill this requirement we are using wireless LAN, Network Sockets and Public terminals in wide area, but there are many troubles caused by inadequate or illegal use of internet. So the authentication systems are required to restrict users and to take usage log.

On basis of this demand, PKI Endorsement Functions for Network Users is a system to authenticate network users and to record the usage logs. The system allows user nodes to connect the internet without a special application forms or software setups. It has simply an Interface to authenticate with web browser and use authentication server, such as LDAP, RADIUS, and POP3 and so on. After the endorsement the user terminal will start to use the internet. The PKI Endorsement Function observed it and if the user ends the usage of network it closes the connection to the internet.

2.2 Work Flow

PKI Endorsement Functions acts as a gateway (here after the function called as Gatefree) of the network where the user terminals are connected. A user accesses to an external site with a web browser from his/her terminal the gatefree forwards the user authentication details to the local web server and the local web server returns the authentication. Then the interface program inserts the gatefree rules to pass the packet relating the node. After that, the node can use network freely.

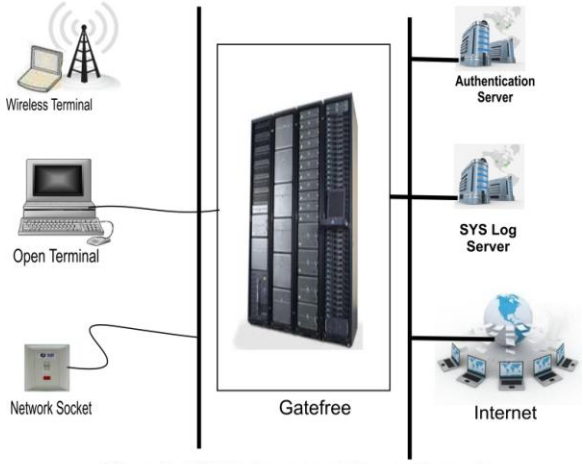

Figure 1: **PKI Endorsement Server Example**

2.3 Endorsement

Authentication means verifying that the identity of entities is provided by the use of public key certificates and digital signature envelopes. The primary goal of authentication in a PKI is to support the remote and unambiguous authentication between entities unknown to each other, using public key certificates and CA trust hierarchies. Authentication in a PKI environment relies on the mathematical relationship between the public and private keys. Messages signed by one entity can be tested by any relying entity. The relying entity can be confident that only the owner of the private key originated the message, because only the owner has access to the private key. The user authentication can be performed with external authentication servers. Various protocols are supported for authentication, such as POP3, POP3S, RADIUS, LDAP, LDAPS and PAM.

2.4. Tracking the IP Address and Monitoring the User Terminal

Gatefree gets the (IPv4 and IPv6) IP address of the user terminal from the Web server, and opens and closes the communication path using the terminal's IP address. The completion page of authentication is displayed on the user terminal after authentication, and a Watch-Process script (JavaScript or Java Applet) is downloaded to the user terminal. This script establishes a TCP connection to the
monitor process forked from the Program Interface. Gateway verifies status of using network for user by this connection. When the script does not answer a response message from the monitoring process, the system judges the termination of use and the communication path is closed.

2.5. SYSLOG for User Information

Gatefree records the user's information using a SYSLOG function. It allows separation of the gateway that generates messages from the system that stores them and the gateway that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate, a means to notify administrators of problems or performance.The stored Information are the ID, terminal IP address, MAC address, start time and end time of the user.

3. DESIGN OF PKI GATEWAY

Several users expressed concern about the complexity involved in the key and certificate setup process. One user proposed a certificate-vending-machine type mechanism for which the only user interface task consisted of entering some form of authenticator and clicking a button labeled "Click here to generate a key and obtain a certificate". This was to be implemented using an HTTPS interface to the CA, submitting the public key and reading the resulting certificate back from the certificate store.

This section describes the design of PKI Gatefree with the function, PKI for network users.

3.1. Functions

The basic certificate management system is built on the top of the database of choice and uses HTTP or HTTPS interface for communication. Certificates are generally identified by users ID and password. The actual questions that followed were broken down into five groups covering enrolment, identification of certificates, storing and obtaining certificates, checking certificate validity, and a miscellaneous section. Two functions are mainly required in the Gateway for certificate based authentication.

1. User's certificate submission from the client terminal.
2. Endorsement functions between Gatefree and authentication server.

Gateway uses Web browser as user interface. In this research, users submit their certificate from Web browser because Gatefree -PKI keeps compatibility with PKI endorsement functions. We use EAP-TLS protocol to implement Certificate based authentication and to use RADIUS authentication server for authenticate with EAP-TLS.

Web browser can't send packets for authentication to RADIUS server directly. Therefore, Gatefree -PKI gets SSL handshake packets in HTTPS from Web browser of the client. The system converts them into packets for EAP-TLS authentication of RAIDUS. Using these packets, the user is authenticated by RADIUS server (Figure.2).

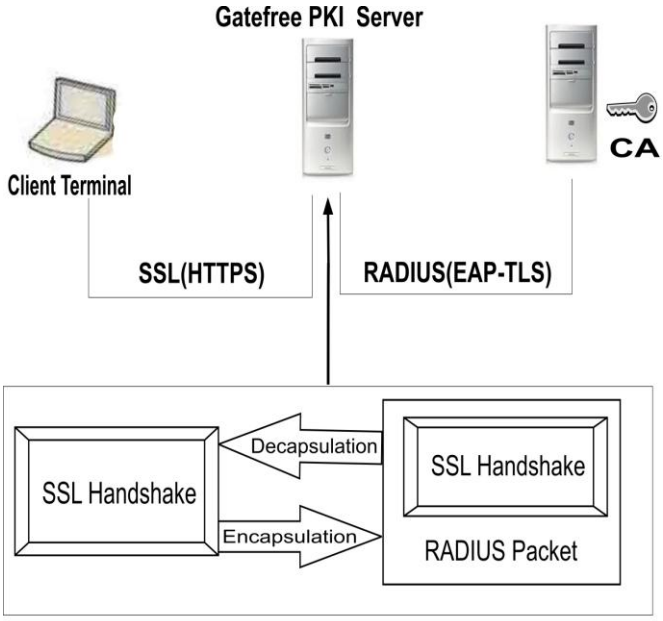

Figure 2 : Packet Conversion

3.2. Configuration

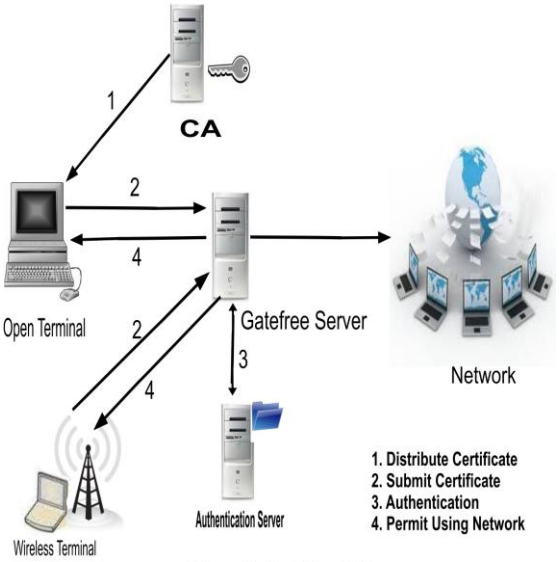

Figure 3: Gatefree PKI

The PKI Endorsement functions for certificate based authentication works as follows

1. CA issues and distributes the user certificate to the user.
2. The user submits his/her certificate to Gateway-PKI server by Web browser.
3. Gatefree -PKI server gets the user certificate and authenticates the user based on it with RADIUS authentication server.
4. If the authentication is success, user's terminal can use the network.
5. If Certificate-based authentication failed, Gatefree-PKI changes the authentication method from Certificate-based authentication to ID/Password-based one.

In this research, for the experimentation phase now, we built CA used self-singed certificate. We use NAREGICA as CA software and use Free RADIUS 1.1.7 as RADIUS server software using RADIUS endorsement.

3.3. Certificate-based Packet conversion

EAP-TLS protocol for Certificate-based authentication used in this research, EAP is a protocol that can authenticate users by encapsulating authentication method, such as MD5, LEAP, TLS and so on.

The client terminal communicates with Gatefree-PKI by HTTPS(HTTP over SSL/TLS) because HTTPS enabled authentication with certificate is supported by almost every Web browser. In HTTPS protocol SSL handshake is started to negotiate before communication by HTTP. The Certificate-based authentication on TLS is negotiated in this handshake.
The RADIUS server endorsement protocol was extended to support for EAP authentication. In this research, we use the EAP authentication and communicate between Gateway and authentication server.

The Gatefree Server converts HTTPS into RADIUS authentication protocol between clients and RADIUS authentication server. Gatefree processes authentication by this function.

At very first, Gatefree administrator set up PKI- Gatefree server to submit the client certificate with HTTPS and then, SSL handshake to process SSL clients authentication between the client and Gatefree -PKI begins. PKI server program gets this SSL handshake and encapsulates it into RADIUS packets. The encapsulation process converts SSL handshake to RADIUS attribute and splits RADIUS attribute.

4. DISCUSSION

4.1 Distribution and Revocation of Certificate

The operation rules for administrators are discussed in this section. The authentication of certificates is valid if the users who is authenticated only has private key. Therefore certain personal identification is needed when the administrator issues certificates from CA and distributes them to users.

In this system, users are authenticated on the assumption that Gatefree – PKI administrator distributes certificates and private key to users with the certain personal identification. The certificate and private key distributed in the PKCS#12 file formats. The private key is protected by the password. If revoking certificates is necessary then the administrator revokes quickly by CA and Administrator issues CRL used by the system.
In this research we supposed that each organization can utilize the system as authentication and authorization platform.

4.2 Certificate usage

This section describes operation rules of users. Gatefree-PKI users use his/her certificates distributed by the administrator via web – browser. The almost every web browser has functions of private key protection. The private key protection by these functions is recommended for users, but behavior of the private key protection is different according to web-browser, because it harms usability depending on a browser remarkably. We don't force the protection. When the private key is stolen or is missing, the user reports to Gatefree – PKI administrator quickly and stops authentication with his/her certificate and the user should delete completely the certificate or should restrict access to the certificate with encryption after loading the certificate in to web browser. This prevents missing private key or leaking private key to others.

4.3 Private Key Handling

The guidelines recommended using smartcards to manage private key. Obtaining smart card readers may require lot of costs. In the management of private key the problem is that the used don't know about the private key. It is important for the authentication with certificate to manage private key. Therefore a lot of costs for the education about them are necessary.

5. CONCLUSION

In this paper, we have been developed Gatefree - PKI that is added authentication functions with PKI for network user endorsement system. Mature technology and extensive experience that users have working with it.

6. REFERENCES

[1] "Solution and Problems: (Why) It's a long Way toInteroperability", Jürgen Schwemmer, *Datenschutz und Datensicherheit*, No.9, 2001 (September 2001).

[2] "PKI: An Insider View", Ben Rothke, *Information Security Magazine*, October 2001.

[3] "OpenPGP Message Format", RFC 2440, Jon Callas, Lutz Donnerhacke, Hal Finney, and Rodney Thayer, November 1998.

[4] "SPKI Certificate Theory", RFC 2693, Carl Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian Thomas, and Tatu Ylönen, September 1999.

[5] "Identity-Based Cryptosystems and Signature Schemes", Adi Shamir, *Proceedings of Crypto'84*,

[6] "Cryptography: A New Dimension in Computer Data Security", Carl Meyer and Stephen Matyas, John Wiley & Sons, 1982.

[7] "New Directions in Cryptography", Whitfield Diffie and Martin Hellman, *IEEE Transactions on Information Theory*, Vol.22, No.6 (November 1976), p.644.

[8] "Security for Computer Networks : An Introduction to Data Security in Teleprocessing and Electronic

Funds Transfer", Donald Davies and W.Price, John Wiley and Sons, 1984.

[9] "Replacing the Whois Protocol", Andrew Newton,*IEEE Internet Computing*, Vol.10, No.4(July/August 2006), p.79.116