SCIS 2006 The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

Design and Implementation of a Live-CA CD/DVD on an Open Source Environment

鄭佩技* 楊中皇† 櫻井幸一†
Pei Chi Cheng* Chung Huang Yang† Kouichi Sakurai†

Abstract— Nowadays, people gather and exchange information through internet prevalently. The increasing use of electronic means of data communications, coupled with the growth of computer usage, has extended the need to protect information. PKI can enhance the mechanism of user's authentication, provides the electronic signature of electronic document and protect data with non-repudiation. So, making a secure management system to coincide PKI is a very important issue. In this paper, we present our effort in the design and implementation of a Live-CA CD/DVD on an open source environment to build a CA management system very quickly and develop CA client software by using the Borland C++ Builder 6 to manage every operation of certificate authority with IC card to enhance the security of user's private key.

Keywords PKI, Certificate Authority, Electronic Signature, Live CD, Digital Signature

1 Introduction

Nowadays, the whole world population of accessing the Internet reaches several hundred millions and the management of the organizations can't leaves without computer and the network system. When the enterprise or the organizations want to extend the business scope by the Internet, the most important thing is how to protect the security of information and identify user identification authentication. As long as the user identification authentication question can be solved, the network security problem also can be easily solved. Considerable progress has been made in the techniques for encryption, decryption, and fending off attacks from intruders over the last decade. [1][9]

Public-key infrastructures (PKI) [1] are comprised of supporting services that are needed for using public-key technologies on a large scale. A public-key [4][8] certification system works by having a certification authority (CA) [3][7] for the generation and management (application, storage, renewal, revocation, and inquiry) public-key certificates. Both CA and PKI [1][3] are crucial parts of many secure network applications such as VPN, secure email, online stock trading, time-stamping, etc.

The OpenCA PKI Development Project [6] is a collaborative effort to develop a robust, full-featured and Open Source out-of-the-box Certification Authority implementing the most used protocols with full-strength cryptography world-wide. The project development is divided in two main tasks: studying and refining the security scheme that guarantees the best model to be used in a CA and developing software to easily setup and manage a Certification Authority.

KNOPPIX [5] is a bootable CD with a collection of GNU/Linux software, automatic hardware detection, and support for many graphics cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. Due to on-the-fly decompression, the CD can have up to 2 GB of executable software installed on it.

In this paper, we present our effort in the design and implementation of a Live-CA/PKI CD/DVD on an open source environment. We make a Live CD [5][10] with OpenCA [6] to enable that every unit could install a CA quickly and effectively and develop a CA

* Kaohsiung County Chu Woei Elementary School, Taiwan, No.1, Daren N. Rd., Gangshan Town, Kaohsiung County 820, Taiwan (R.O.C.) cloudsea@m1.cc.ks.edu.tw
† Institute of Information, Computer and Education, National Kaohsiung Normal University, Taiwan, No.116, Heping 1st Rd., Lingya District, Kaohsiung City 802, Taiwan (R.O.C.), chyang@computer.org
† Dept. of Computer Science and Communication Engineering, Kyushu University, Hakozaki, Fukuoka 812-81, Japan , sakurai@csce.kyushu-u.ac.jp

client software with IC card by Borland C++ Builder [2] to administer the operations of the CA and protect user's private key.

2 Design and Implementation of CA/PKI Live CD

2.1 System Structure

In this paper, the certificate management system mainly divides into two major parts. The first one builds the certificate management server on Linux OS environment and makes the OS into a Live CD. The other one builds the CA client software developed by C++ Builder. Figure 1 shows system diagram of our PKI.

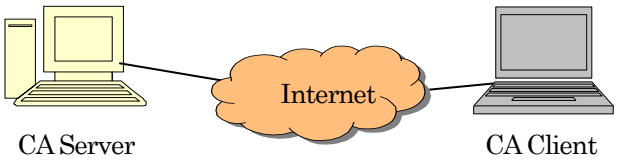

Figure 1: Client-server PKI over Internet

In order to realize the design of the certificate management system, this research divides into following two steps to accomplish it.

1. Use the KNOPPIX to customize a Live-CA CD. Then, people could test and use the CA system easily and quickly.

2. Use Borland C++ Builder 6 [2] as a software tool to develop Internet-based client. The CA client software integrates the main functions of CA server, such as certificate/revocation request, certificate/ revocation approve, certificate download, search function, and database backup. It provide the function of saving user's private key into IC card.

2.2 CA Server

In this paper, we modify the open source code of OpenCA to install a server on Linux OS. Among the supported software is OpenSSL, Apache Project, Apache mod_ssl, perl5 and MySQL. After the installation of OpenCA, you must use it by a browser. There are three interfaces provided by OpenCA, which let the user and the RA/CA administrators to carry on the application of certificate and the management of certificate system movement, describe as following.

1. The Public interface (Figure 2) provides these operations which a user can view current certificate lists, manage certificates and download CA and revocation certificates from these screens. A user can use it to generate CSRs (certificate signing request) for browser, client independent requests and private keys, receive PEM-formatted PKCS#10 requests from servers, enroll certificates and CRL, and it support two different methods revocation, search certificates, and test user certificates in browsers.

Figure 2. Public Interface

2. The RA interface (Figure 3) lets an RA administrator to manage certificate requests, view certificate information and manage the RA server from these screens, such as editing requests, approving certificate and revocation requests, deleting wrong requests and email users. The RA administrator verifies applicant's material here, authorizes the data which pass the verification, and delivers applicant to the higher hierarchy of CA server.

Figure 3: RA Interface

3. The CA interface (Figure 4) has all function which you need create certificates and CRLs (Certificate Revocation Lists) and to change the configuration via a web interface. The CA administrator uses it to manage the CA server, to issue users' certificates and CRLs on the server end proceed all operations about CA.

Figure 4: CA Interface

2.3 CA Live CD Customization

In this paper, we use KNOPPIX as the base Operation System environment adding Chinese packages, fonts and input to supply Chinese interface and removing some packages we don't need to economize more disk space. Then, build the CA system of OpenCA which has modified its source code into the KNOPPIX system and add booting scripts which lets every unit could enter their own information about their CA server and the email of administrator. Finally, using the compression technology remaster a CA Live CD with Chinese interface. Figure 6 shows the booting of the OpenCA Live CD.

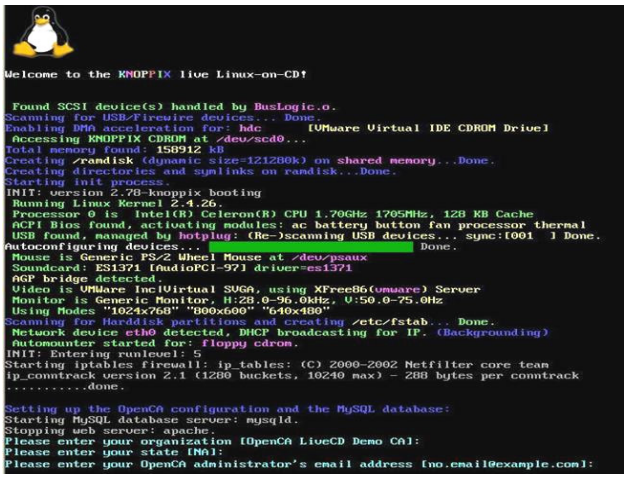

Figure 5: CA Live CD Startup Picture

2.4 CA Client

We use C++ Builder to develop our software (Figure 7) of CA system to make the procedure of certificate and revocation request easily and fast. This software integrates main functions of CA which provide an accordant interface to carry on each item of certificate system work and avoid the users and administrator to operate by changing among these web pages.

Figure 6: CA Client Software

The design of this software divides into four major parts: request work, certificate work, RA management and CA management. In order to guarantee the system security, the first two works could use for any person but the latter two items must confirm the identification as CA/RA managers who can use the management of RA and CA from IC card. In order to enhance the security of user's private key, we also design a function which can save user's private key into IC card.

The main functions of request work used by user are generating CSRs (Figure 7) and revocation request (Figure 8) which provide a user to request a certificate. The user fills in his data in the request and presses down the "Submit" button, and then the request will be sent out to RA which could check the data of a user by a RA manager. The user also can query his request progress to confirm whether the certificate has issued or the application has been rejected. The certificate work contains the downloading suitable form of the CA certificate and the users' certificates and exporting the certificate into storage such as USB storage.

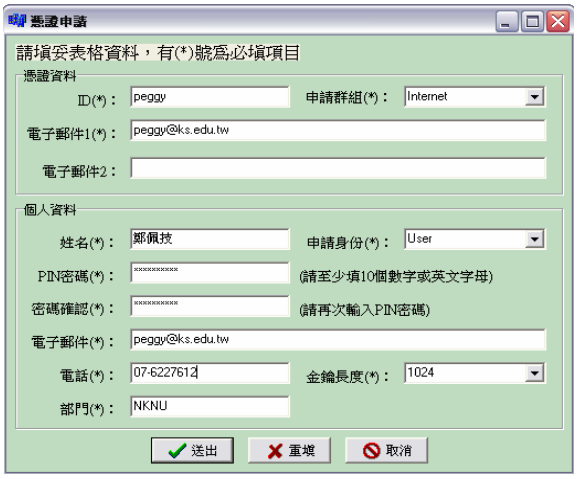

Figure 7: The Form of Certificate Request

Figure 8: The Form of Revocation Request

The RA management part (Figure 9) mainly does is to verify a user's data of application, approve the

request and send out to CA. The RA manager could check these applicants one by one and decide to approve or delete the requests. Then, the CA manager does the final certificate issue work, to issue or revoke the user's certificate and create a new CRL (certificate revocation list) on CA server.

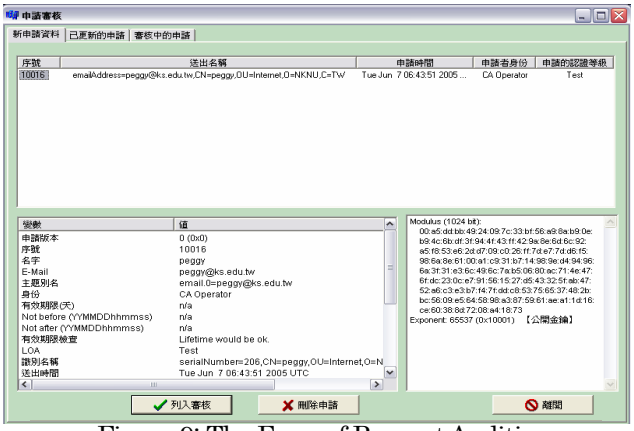

Figure 9: The Form of Request Auditing

Besides, we also provide IC card operation function and to restore database. IC card operation function is used to verify the identification of CA or RA user and save user's private key into IC card. This function of the recovery/backup of database is only used by CA manager.

3 Discuss and Conclusion

Public-key infrastructure is essential for large-scale secure network applications, where communication confidentiality, authentication, and non-repudiation services are made an integrated part of the systems. We have presented a design and implementation of CA/PKI with Chinese interface on the open source environment

Although OpenCA project mentioned about that they hope to guarantees the best model to be used in a CA and develop software to easily setup and manage a Certification Authority, it's not so easy to install and setup a Certification Authority. So we provide the Chinese interface and customize the KNOPPIX into a Live-CA CD, the user could save the complex steps to install and configure CA server and use it easily. And we develop client software to integrate all main functions on the section of management and use. Combining the advantage of KNOPPIX and the client software makes the OpenCA be easier to use. People could use it to build a CA management system very quickly and easily.

References

[1] Andrew Nash, William Duane, Celia Joseph, and Derek Brink, PKI: Implementing and Managing E-Security, McGraw-Hill, 2002.

[2] Borland C++Builder, http://www.borland.com/bcppbuilder/.

[3] C. Adams and S. Lloyd, Understanding Public-Key Infrastructure, Macmillan Technical Publishing, 1999.

[4] Dartmouth PKI Lab, http://www.dartmouth.edu/~pkilab/, Access time 2005/3/10.

[5] KNOPPIX, http://www.knoppix.org/, Access time 2005/3/10.

[6] OpenCA Labs, http://www.openca.org/, 1998.

[7] R. Housley, W. Ford, W. Polk, and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.ietf.org/ rfc/rfc2459.txt, 1999.

[8] Shashi Kiran, Patricia Lareau, and Steve Lloyd, PKI Basics-A Technical Perspective, http://www.pkiforum.org/pdfs/PKI_Basics-A_technical_perspective.pdf, Nov 2002, Access time 2005/3/10.

[9] Stallings W., Cryptography and Network Security Principles and Practices, Nov. 2002, 3/e, Prentice Hall.

[10] The Live CD List, http://www.livecdlist.com/, Access time 2005/03/10.