PKI-Lite: A PKI System with Limited Resources

Oğuz Yayla, Sedat Akleylek

Abstract— ***The aim of this study is to give some ideas about how to construct a PKI system with limited resources. Such a PKI system can be applied for some compact organizations which don't have requirements for complying with industry or government standards. Such a PKI system provides safeguarding user information, protecting against malicious users, providing a safe domain environment and others. An example to such system is an educational organization. This study covers the topics to people for whom a PKI is appropriate for their organization, and how PKI can be deployed most effectively.***

***Index Terms*— Public Key Infrastructure (PKI), PKI architecture, PKI Design, Certificate Authority (CA).**

I. Introduction

A Public key infrastructure (PKI) is a foundational technology that allows organizations to build security solutions that leverage a common trust. Because of this, the PKI can help organizations operate more securely and at lower costs over the long term. However, PKI is not an all encompassing solution to an organization's security challenges such as virus infections.

PKI has been adapted to many security providing systems. This is because of two reasons. First, there exists a dislike for other security technologies. For example, a dislike for password-based authentication, but, may result in a stronger preference for PKI solutions. Secondly, public-key technology offers some important benefits that are not similarly offered by other technologies, such as digital signatures, smart card logon, secure e-mail, software code signing, IP security, secure 802.1x connection, software restriction policy, internet authentication, encrypting file system and many others.

There are many choices in implementing PKI system. Even there are many standardized and commonly used versions such as X.509 [1], PGP [10], AADS/X9.59 [11], and SPKI [12].

In Section 2, some concepts related to PKI components are described briefly in order to determine design strategy to construct a PKI system in section 3. Then, in section 4 a PKI system example is constructed according to definitions.

II. PKI Components

PKI has standard procedures for registration, initialization, certification, key generation, recovery, update, expiration, compromise, cross-certification and revocation of certificates. The architectural model consists of five components as specified in [3]:

- Certificate Authority (CA) acts as the root of trust in PKI and confirms the identities of parties sending and receiving communications. It is needed for the management and signing certificates. Therefore, it is similar to notary.
- Registration Authority (RA) that vouches for the binding between public keys and certificate holder identities or other attributes. RA is trusted by CA for these transactions.
- Public Key Certificates (PKC) owners that can sign digital documents and decrypt documents using private keys. These certificates are private for each identity, conforming that the identity has the appropriate credentials.
- Clients that validate digital signatures and their certification paths from a known public key of a trusted CA and encrypt documents using public keys from certificates of PKC holders.

Repository is a database of active digital certificates for a CA system. That stores and makes available PKCs and Certification Revocation Lists (CRLs).

III. RESULTS

PKI may take a variety of forms, determined by the trust relationship between its components. PKI architecture planning and designing need to consider each component to be correctly working. If one of the components leaks a security threat, the whole system will not work. Therefore, there are different issues when planning and designing PKI [4]. For our design, all necessary but simplest design criteria are taken into account.

Manuscript received September 25, 2007; revised November 23, 2007.

Oğuz Yayla is with the Institute of Applied Mathematics, Middle East Technical University, Ankara, 06531 Turkey. (e-mail: e118296@metu.edu.tr).

Sedat Akleylek is with the Institute of Applied Mathematics, Middle East Technical University, Ankara, 06531 Turkey. (e-mail:akleylek@metu.edu.tr).

A. Policy Design

Policy is a generic problem within the area of information security. It is the specification of local requirements and process for specified levels of trusted operation. Policy applies to the PKI since it describes the user identification process, private key management, the process for responding to lost or compromised private keys, certificate enrollment and renewal requirements, and the maximum value for transactions. X.509v3 gives CA the ability to include with the certificate a list of policies that were followed in creating the certificate. Hence, while designing the policies X.509v3 can be implemented [5,13]. Policies are intended to help users decide if a certificate is suitable for a particular purpose. For example, a policy might indicate that a certified key can be used for casual email messages but not for ensuring the identity of a remote computer.

Besides certificate policies, one needs to accomplish computer security objects registry which defines security services, identifies applications to secure by using certificates, and defines security services to offer by using certificates.

Next step is developing certification practice statement (CPS). A CPS describes the details of the system and the practices employed by a CA to issue certificates, and it details the procedures used to implement the policies identified in the certificates issued by a CA, including the means used to identify certificate subjects. The CPS also states the means used to protect the private key of the CA, and the other operational practices followed by the CA to ensure security [5,13].

B. Certificate Hierarchy Design

There are two traditional certificate hierarchy to build PKI architecture, tree-base and cross-certification-based certificate hierarchies. In addition, bridge (a combination of formers) certificate hierarchy has been developed to accomplish the connection of one PKI to another. These hierarchy designs can be based on certificate usage, location, department's organizational structure. The simplest PKI architecture which is implemented in PKI-Lite is the single CA case whose end users are positioned at the next level.

C. Data Structure Design

Two basic data structures are used in a PKI system [5].

- Structure of a certificate is one of the basic data structures used in PKI. The certificate of a user is a collection of information, including the user's distinguished name and public key, as well as an optional unique identifier containing additional information about the user. This structure needs to be readable by any other entity. X.509 public key certificate format has evolved into a flexible and powerful mechanism. Eventually, X.509v3 certificate type is generally preferred all over the world.

- Certificates are usually given a fixed lifetime, after which they expire. However, it is possible that a certificate becomes invalid before its expiration. Certificate issuers need a mechanism to provide a status update for the certificates they have issues. One which can be implemented easily is the X.509 CRLs.

D. Physical Architecture Design

There are numerous ways in which PKI can be designed physically [5]. It is highly recommended that the major PKI components should be implemented on separate systems, that is, the CA on one system, the RA on a different system, and directory servers on other system. Since the systems contain sensitive data, they should be located behind an organization's unified threat management (UTM)/Firewall. The CA system is especially important as a compromise to that system could potentially disrupt the entire operations of the PKI and necessitate starting over with new certificates. Consequently, placing the CA system behind an additional organizational UTM/Firewall is recommended so that it is protected both from the Internet and from systems in the organization itself. UTM/Firewall would permit communications between the CA and the RA as well as other appropriate systems.

Moreover, using a secured server room with key access and minimizing services on the CA makes secure CA. Using software cryptographic service provider (CSP), smart cards or tokens with PIN numbers and hardware security modules (HSM) enables extra security of the private keys.

E. Administrative Design

Administrative staff is responsible for CA and HSM operation, and interaction with server management. Administrative staff approves or rejects requests for adding another certificate according to design policy. Therefore, administrative staff has a very important role to obtain security. Prohibiting remote administration of CA system, deploying CA system in restricted physical locations and placing them at major hubs of the networks enable centralized administration.

F. Key Length and Lifetime Design

Because of the reasons that CA is needed to have higher key lengths than its users and security level will be updated to higher bits soon, Root CA should use 4096 bits RSA key length issued by itself or by another trusted CA and the lifetime could expire 20 years later. End users could have 1024-2048 bits RSA key length. That is, for now, being adequate and their certificate could expire 1 month-1 year later.

IV. A PKI SYSTEM EXAMPLE

In this section, the most basic PKI system is given with single CA that provides all the certificates and CRLs for all users [6]. A single CA is a sensible solution for small organizations. Figure 1 in Appendix A illustrates the general architecture of PKI system. This architecture is proposed for as a suitable solution for the requirements of an educational organization.

The overall architecture is comprised of the following components:

- The user: The user easily obtains her digital certificates and generates his/her public/private key.
- Log system: The log system keeps logs of certificate requests and mediates the requests to CA.
- CA: CA performs signing certificates.
- Key and certificate institution: Key and certificate institution stores the private keys encrypted and certificates.
- UTM: UTM controls the network.

In this system new user firstly inserts his/her smart card into smart card reader. Then he/she should request a certificate and visit RA. If his/her transaction is not seen a threat for system, UTM will allow this request. While this operation is going on, RA registers the user and log system is saving this request with all detailed information. If CA accepts the certificate request, CA sends the signed certificate to log system. Log system saves this accepted certificate with all detailed information. Then, accepted certificate is sent to user again. Finally, certificate with key is backing up in the key store and certificate institution. Log system again saves this transaction. Key store and certification institution has a very critical role when the user does not have a smart card. In this scenario, user visits RA to authenticate himself/herself. Then, system generates one time password for him/her. He/She uses this password to request a certificate. Since he/she does not have his private key with himself/herself (he/she does not have smart card), he/she requests his private key from key store and certification institution with his/her one time password.

This PKI architecture provides a mechanism to allow the registration of users who cannot physically be in the organization. Moreover, this supports authentication using web based protocols. Security of this case is protected with one time passwords.

V. ISSUES AND RISKS IN PKI SYSTEM

There are some risks in PKI system during the verification of certificate user identity, certificate creation, distribution, acceptance and content, and managing digital certificates. Open risks relating PKI implementation can be listed as mentioned in [7]:

1. The certificates issued by a CA should not be automatically trusted.
2. The private key stored on your computer may not be secure.
3. Verifying machine may be an insecure computer
4. The name in a certificate may not be as valuable as it appears to be.
5. The CA may not be an authority on what the certificate contains
6. Security software may not be implemented correctly or used properly,
7. The RA+CA model may be in conflict of the certificate content.
8. The CA may not use good information to check the identity of the entity applying for the certificate, or may not ensure that this entity really controls the private key corresponding to the public key being certified.
9. Certificates must be used properly if one wants more security.
10. PKI does not solve all security problems.

As any PKI system, the one designed in this paper may also be vulnerable to these security issues and risks. All PKI users, also authorities and administrators, should take care of all consideration about these 10 issues and risks.

VI. CONCLUSION

In this work, an example PKI system is given. The design criteria are explained. It is emphasized that certification lies at heart of the any PKI. Moreover, issues and risks in CA system are described. From this point of view, it is obvious that the PKI system can be applied with limited resources to the compact organizations.

APPENDIX A

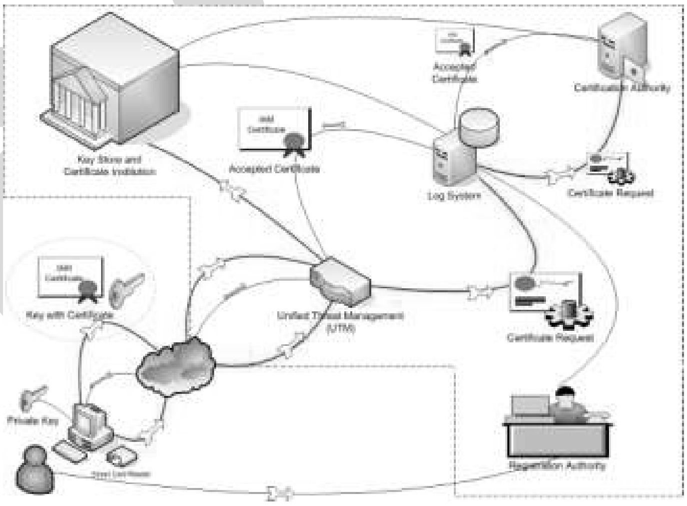

Fig. 1: PKI-Lite Architecture

REFERENCES

[1] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell System Technical Journal*, vol.28-4, pp. 656—715, 1949.

[2] J. Morello, “LSU PKI Architecture,” *CISSP Deputy Information Security Officer*, 2006.

[3] S. Berkovits, S. Chokhani, “Public Key Infrastructure Study Final Report,” *National Institute of Standards and Technology*, Gaithersburg, 1994.

[4] A. Arsenault and S. Turner, “Internet Draft PKIX: Internet X.509 Public Key Infrastructure: Roadmap,” January 2003.

[5] C. Adams, S. Lloyd, “Understanding PKI: Concepts, Standards, and Deployment Considerations,” Second Edition, *Addison-Wesley*, 2003.

[6] ITU-T Recommendation X.509. Information Technology – Open Systems Interconnection – The Directory: Public Key and Attribute Certificate Frameworks. March 2000 (equivalent to ISO/IEC 9594-8:2001).

[7] Digital Certificate Operation in a Complex Environment, J*oint Information Systems Committee*, UK, 2004

[8] C. Ellison, B. Schneier, “Ten Risks of PKI : What You’re not Being Told about Public Key Infrastructure,” 2002.

[9] P. Gutmann, “PKI: It’s Not Dead, Just Resting”, *IEEE Computer*, August 2002.

[10] L. Wheeler, “Account Authority Digital Signature and X9.59 Payment Standard”, slides presented at the *3rd CACR Information Security Workshop*, June 1999.

[11] J. Callas, “The OpenPGP Standard”, slides presented at the *3rd CACR Information Security Workshop*, June 1999. Avaliable : http://www.cacr.math.uwaterloo.ca/conferences/1999/isw-june/callas.ppt

[12] L. Wheeler, “Account Authority Digital Signature and X9.59 Payment Standard”, slides presented at the *3rd CACR Information Security Workshop*, June 1999. Avaliable : http://www.cacr.math.uwaterloo.ca/conferences/1999/isw-june/wheeler.ppt

[13] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylönen, “SPKI Certificate Theory”, *Internet Engineering Task Force (IETF) Request for Comments (RFC) 2693*, September 1999.

[14] 13. S. Chokhani, W. Ford, R. Sabett C. Merrill S. Wu, “Request for Comments: 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, 2003.