X. 509 and PGP Public Key Infrastructure methods: A critical review

Shahin Fatima[#1], Shish Ahmad[*2], Shadab Siddiqui[#3]

[#]*Computer Science and Engineering Department, Integral University*
Kursi Road Lucknow (UP) India.

shiish@iul.ac.in

[*] *Computer Science and Engineering Department, Integral University*
Kursi Road Lucknow (UP) India.

***Abstract*—Public Key Infrastructure methods consists of a group of policies, processes, server platforms, software and workstations which is used for the purpose of administering certificates and maintaining pairs of public-private keys. These pair of keys is able to issue, maintain, and revoke public key certificates. The goal of a Public Key Infrastructure (PKI) is to ensure secure, convenient and efficient discovery of public keys. There are various types of PKI that are deployed. This discussion is centred on X.509 certificate, creation of certificate, revocation of certificate, its authentication procedures and PGP certificates. The goal of this analysis is to highlight the differences between both systems and to provide the reasons for their usage.**

***Keywords*—public key infrastructure, X.509 certificate, certificate authority (CA), PGP format, authentication, confidentiality**

I. INTRODUCTION

The development of public-key cryptography is the greatest revolution in the entire history of cryptography. Public-key cryptography provides a radical departure from all that has gone before. Public-key algorithms are based more on mathematical functions than on substitution and permutation. Furthermore, public-key cryptography is asymmetric, i.e. it involves the use of two separate keys, in comparison to symmetric encryption, which uses only one key [1]. The use of two keys has major consequences in the areas of confidentiality, integrity, and authentication, as we will see. One misconception about asymmetric encryption is that it is more secure from cryptanalysis attack than symmetric encryption.

Moreover, the security of encryption scheme depends on the length of the key and the computational work involved in breaking a cipher text. There is nothing said about either symmetric or public-key encryption that makes one superior than another from the point of view of resisting cryptanalysis. A second misconception about public-key encryption is that it has made symmetric encryption obsolete. Because of the computational overhead of current public-key encryption methods, there seems no foreseeable likelihood that symmetric encryption will be abandoned.

A. Applications for Public-Key Cryptosystems

Before proceeding, we need to clarify one aspect of public-key cryptosystems that can otherwise lead to some confusion. Public-key systems uses cryptographic algorithm with two keys, one is called private and the other one is public [1]. As per the application, the sender uses either the sender's private key or the receiver's public key, or both, in order to perform some type of cryptographic functions. In broad terms, we can classify the use of public key cryptosystems into three categories:

• Encryption /decryption**:** The sender encrypts a message with the recipient's public key.

• Digital signature: In digital signature sender "signs" a message with its own private key. This process of signing is achieved by using cryptographic algorithm applied to the small block of data that is a function of the message.

• Key exchange: In key exchange both sides cooperate to exchange a key. Many different approaches are proposed, which involves the private key(s) of one or both parties

The remainder of the paper is organized as follows. Section II describes the X.509 certificate. Section III gives the overview on PGP. Section IV gives the relative comparison between them. Finally section V offers some concluding remarks and future work.

II. X 509 CERTIFICATE

X.509 defines a framework for the provision of authentication services to its users. Each certificate contains the public key of the user and it is signed with the private key of a trusted certification authority (CA) [1]. In addition, X.509 defines alternative authentication

Manuscript received May 5, 2015
Manuscript revised May 20, 2015

protocols based on the use of public-key certificates. X.509 is an important standard because of its certificate structure and various authentication protocols defined in X.509 are used in a variety of contexts. X.509 uses the concept of public-key cryptography and digital signatures.

An X.509 Certificate is issued by the Certification Authority
(CA) and is duly signed with the private key of CA.
It includes:

- Owner's public key
- Owner's name
- Expiration date of the public
- Name of the issuer (the CA that issued the Digital Certificate)
- Serial number of the Digital Certificate
- Digital signature of the issuer

The most widely accepted format for digital certificates is defined by the CCITT X.509 international standard [2]. And the most widely used standard for digital certificates is X.509 certificate. Digital Certificates are the framework for identifying information, and bind their identities with public keys. An electronic signature duly issued by the certifying authority that shows the authority of the person who is signing the e-form. Each Certificate contains the public key of the user and is signed with the private key of the certification authority.

B. Security of document requires:

- Authenticity
- Confidentiality
- Integrity
- Non-repudiation

C. Generation of a public-key certificate

The heart of the X.509 scheme is the public-key certificate associated with every user. These certificates are generated by a trusted certification authority (CA) and they are recorded in the directory by the CA or by the user to whom the certificate is issued. The directory server is not responsible for the creation of public key or for the certification function rather it merely provides an easily accessible location for users to obtain certificates.
Figure 1 shows the normal use of a public key certificate by both sender and receiver and the use of keys for encryption and decryption.
Figure 2 depicts the general format of a X 509 certificate, which includes the following elements.

- Version: It differentiates among successive versions of the certificate format; and by default the version is 1. The value of version must be 2 if the issuer unique identifier or subject unique identifier are present, and if one or more extensions are present, then the value of version must be 3.
- Serial number: Serial number is an integer value which is unique with the issuing CA and that is associated with this certificate.

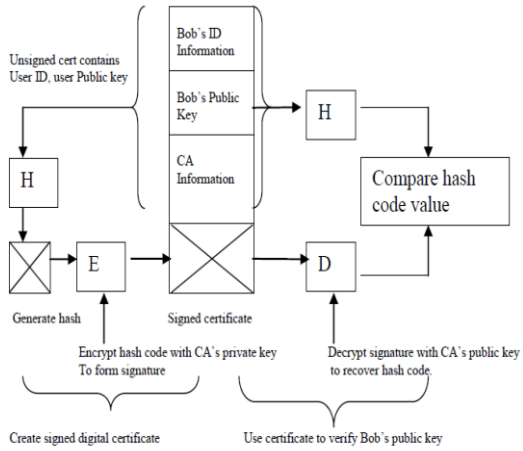

Fig 1: Public Key certificate use

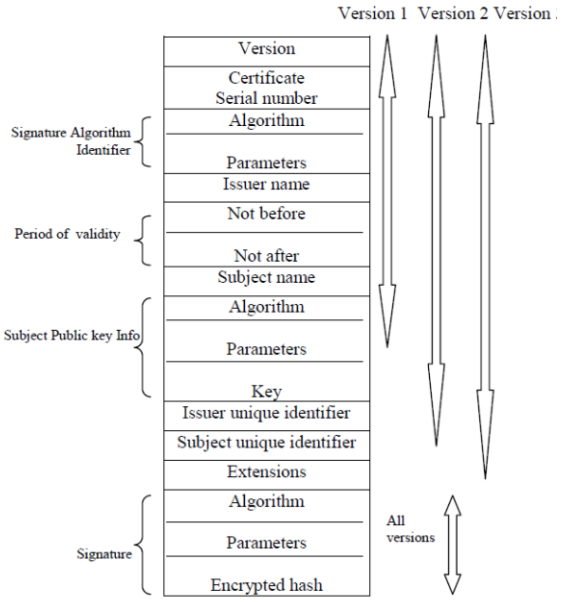

Fig 2: Format of X 509 Certificate

- Signature algorithm identifier: It includes the algorithm used to sign the certificate along with any associated parameters. Since this information is repeated in the signature field at the end of the certificate, therefore this field has little or no utility.
- Issuer name: Issuer name is the name of the CA that has created and signed this certificate.

• Period of validity: It consists of two dates: the first date and last date within which the certificate is valid.

• Subject name: It is the name of the user to whom this certificate is issued. That means this certificate certifies the public key of the subject who holds the corresponding private key.

• Subject's public-key information: It contains the public key of the subject, and an identifier of the algorithm for which this key is to be used, along with any associated parameters.

• Issuer unique identifier: It is an optional-bit string field and consists of an identifier which is used to uniquely identify the issuing CA.

•Subject unique identifier: It is an optional-bit string field and consists of an identifier which is used to identify uniquely the subject [1].

• Extensions: It consists of a set of one or more extension fields. Further extensions are added in version 3.

• Signature: Signature covers all other fields of the certificate; it contains the hash code of the other fields which is encrypted with the private key of CA. This field also includes the signature algorithm identifier.

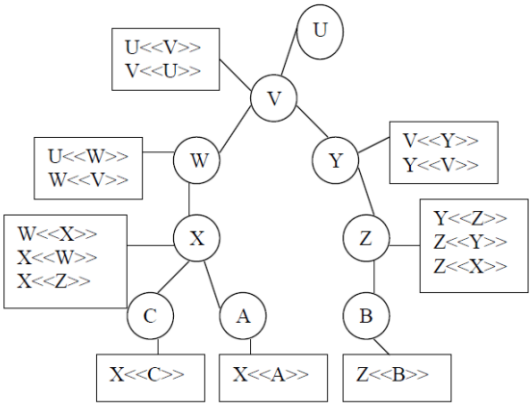

Fig 3: X 509 Hierarchy

Figure 3, taken from X.509, is an example of a hierarchy. The connected circle shows the hierarchical relationship among the CAs, the boxes shows certificates maintained in the directory for each CA entry. The directory for each CA includes two types of certificates:

• Forward certificates: These are the certificates of X generated by other CAs

• Reverse certificates: These are the certificates generated by X that are the certificates of other CAs

In this example, user A can acquire the following certificates from the directory to establish a certification path to B:

When A has obtained these certificates, it can unfold the certification path in sequence in order to recover a trusted copy of B's public key. By using this public key, A can send encrypted messages to B. Now, if A wants to receive encrypted messages back from B, or to send signed messages to B again, then B needs A's public key. B can obtain this set of certificates from the directory, or A can provide them as part of its first message to B.

Algorithms
Parameters
Issuer Name
This Update date
Next Update date
User Certificate serial #
Revocation date
- - - -
User Certificate serial #
Revocation date
Algorithms
Parameters
Encrypted

Fig 4 Certificate revocation list

D. Revocation of Certificate

Each certificate has a valid period such as in an ATM card or a credit card. Furthermore, a new certificate is issued just before the expiration of the old one [2]. Additionally, it may be desirable on occasion to revoke a certificate before it get expires, for one of the following reasons: 1.When the user's private key is assumed to be compromised. 2. When the user is no longer certified by this CA. 3. When the CA's certificate is assumed to be compromised. Every CA should have a list that contains all revoked but not expired certificates issued by that CA, which includes both of those issued to users and to other CAs. This list be posted on to the directory. Each certificate revocation list (CRL) posted to the directory is signed by the issuer and includes the name of the issuer, the date at which list was created, the date at which the next CRL is scheduled to be issued and an entry for each revoked certificate. Each entry in the directory consists of the serial number of a certificate and revocation date for that certificate. Since the serial nos. are unique within every CA, therefore this serial no. is sufficient to identify the certificate. When a user receives a certificate with the message, the user must determine whether the certificate has been revoked or it is the original certificate. The user can also check the directory each time it receives the certificate. In order to avoid delays associated with

directory searches, the user should maintain a local cache of certificates and list of revoked certificates.

III. PGP

PGP is a public key cryptographic package, which is intended for public usage. It provides confidentiality, authenticity, integrity and non-repudiation of the sender. Although PGP can encrypt any data or files, it is most commonly used for e-mail which has no built-in security as originally implemented. It was originally designed and developed by Phil Zimmermann in 1991[3]. For that time it has been sufficiently influential that its algorithms and data formats have been standardized for interoperability between different pieces of software. Eventually, the PGP design was made in Internet standards-track specification known as Open PGP. It is described in RFC2440 [4]. PGP combines symmetric and asymmetric cryptography. The user generates a pair: (public key, private key) that is associated with his unique ID. Public keys are stored on public key rings and private keys are stored on private key rings. On the sender's side, PGP creates a session key, which is random number generated by the keystroke characteristics of a user. Once the data is encrypted with this key, the session key is encrypted with the recipient's public key and sent together with the cipher text to the recipient. The recipient's copy of PGP uses her private key to recover the session key, which then allows the recipient to decrypt the cipher text. PGP uses pass phrase to encrypt the private key on its owner's machine. Pass phrase is longer and more complicated version of the password. The private key is encrypted on the disc using a hash of the pass phrase as a secret key. In order to use her private key, user has to decrypt it using the pass phrase. The distribution of public keys is usually done by key servers. They are mirrored at various locations around the world. They possess the recipients' public keys and on the demand of sender, they give the sender the recipients' public key.

PGP can also be used for 4 things:

• To encrypt a message or file so that only the intended recipient can decrypt and read it. The sender, after signing with PGP, also provides guarantee to the recipient, that the message have come from the authorized sender and not from any unauthorized person.

• Clear signing a plain text message guarantees that it can only have come from the sender and not an impostor.

• Encrypting computer files so that they can't be decrypted by anyone other than the person who encrypted them.

• Really deleting files (i.e. overwriting the content so that it can't be recovered and read by anyone else) rather than just removing the file name from a directory/folder.

A PGP certificate includes (but is not limited to) the following information [3]:

• PGP version number—PGP version number identifies which version of PGP was used to create the key associated with the certificate.

• Certificate holder's public key— It holds the public key , together with the algorithm of the key such as RSA, Elgamal or DSA.

• Certificate holder's information— This is the information about the user, such as his or her name, user ID, e-mail address, ICQ number, photograph, and so on.

• Digital signature of the certificate owner— It is also called a self-signature. It is the signature which uses the corresponding private key of the public key associated with the certificate.

• Validity period— It is the certificate's start date/time and expiration date/time which indicates when the certificate will get expire. If the key pair contains sub keys, then this includes the expiration of each of the encryption sub keys as well. Sub keys enable convenient use of separate keys for signing and encryption

• Preferred symmetric encryption algorithm for the key— This indicates the encryption algorithm through which the certificate owner prefers to get information encrypted. The supported algorithms can be CAST, IDEA, Triple-DES, and Blowfish etc.

IV.COMPARISON

The major differences between PGP and X.509 PKIs can be separated in three areas: differences in certificate, network of trust and revocation procedure.

1) Certificate Format: The PGP Certificate format contains self signature and can also obtain multiple signatures. X 509 certificate support only a single digital certificate to attest to the key.

2) Key: X 509 certificate has only a single name for key owner whereas PGP certificate has public key with different labels which identify the user in multiple ways.

3) *Introducer*: In X 509 Certificate introducer is always CA (Certification Authority) whereas in PGP it can use digital signature as the introducer.

4) *Chain of trust:* When any user signs another user's key, then he or she becomes an introducer of that key. With the flow of this process, it establishes a chain of trust, so any user can act as a certifying authority (CA). By this, many certification paths are formed to achieve fault tolerance in compensation for the fact that amateur certifiers are signing certificates. A PGP user public key certificate can also validate another PGP user's public key certificate. Moreover, such a certificate is only valid to another user if another party recognizes the validator as a trusted introducer. PGP user is the one that manages keys, while with X.509 CA does a managing of keys.

5) *Issue of Certificates:* In an organization using a PKI with X.509 certificates, the job of the RAs is to approve certificate requests and the job of the CA is to issue certificates to users - a process which generally entails responding to a user's request for a certificate. In an organization which is using PGP certificates, the job of the CA is to check the authenticity of all PGP certificates and then to sign the good ones.

6) *Revocation procedure:* In X.509 certificates, the revoked signature is almost the same as a revoked certificate given that the only signature on the certificate is the one that made it valid in the first place i.e. the signature of the CA. PGP certificates provide the added feature that user can revoke his or her entire certificate if user feels that the certificate has been compromised. The certificate's owner or revoker can revoke a PGP certificate. Only the certificate's issuer can revoke an X.509 certificate. Communication of revoked X.509 certificates is most commonly achieved via CRL, which is published by the CA.

7) *Formation of community:* With PGP certificates, the user usually posts the revoked certificate on a certificate server. X.509 standard does not provide any guidelines on the use of cross-certificates, certification paths and CRLs, so the users of X.509 certificates have to provide these procedures themselves. The result of this is that it takes longer to establish X.509 user communities than PGP user communities.

8) *Syntactic:* This means that PGP allows certificates to be in stack form, whereas in X.509 the certificates are linked one to another just as in an one-way linked-list (though X.509 could also include PGP syntax).

9) *Semantic:* This means that PGP allows an association between keys and real-world persons by web-of-trust rules, and not by transitive trust rules, whereas in X.509 it binds keys to names and accepts transitive trust even though a proper CPS could also forbid transitive trust in X.509 as a function of the CA's policies

IV. CONCLUSION AND FUTURE WORK

In our paper, we have explored what separates X. 509 from PGP Public key Infrastructure methods. It is very easy to understand the concept of Digital Signatures and the mechanism of how it works. The Digital Signature will definitely become an inevitable part of our future digital societies. An important aspect of the digital signature is verification of its authenticity Digital certificates ensure the property of confidentiality which ensures that messages can only be read by authorized recipient only. PGP ensures confidentiality for e-mail and other stored files, by using a private/public key pair, which includes sender authentication and data integrity, using digital signatures. The main drawback of PGP is how to distribute public keys. There are many public key servers from where we can retrieve other keys of other people and we can store our keys also. Moreover, they also do not check to ensure that the person who is storing the key is actually the same person indicated by the key identifier

I consider the X 509 method is more flexible and advanced than the PGP method because in PGP it requires that everybody that participates in it takes responsibility and makes decisions for himself. However I think that the X 509 is the right approach, because of personal privacy and security reasons.

In future work X. 509 can be a promising approach as compared to PGP, therefore can also be applied on various kinds of networks such as Adhoc Networks and Wireless sensor networks to provide authentication and confidentiality among nodes. X 509 can be applied on the nodes of adhoc network by reducing its size such that it consumes less energy which is the main constraint of adhoc networks.

REFERENCES

[1] William Stallings," Cryptography and Network security Edition 5.
[2] Mr. Vinod Saroha, Annu Malik, Madhu Pahal **,"**The Enormous Certificate: Digital Signature Certificate"; International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013 ISSN: 2277 128X
[3] "PGP User's Guide: An Introduction to Cryptography",
[4] J. Callas, L. Donnerhacke, H. Finney, R. Thayer, "OpenPGP Message Format",RFC2440,November1998,
[5] ITU-T Recommendation X.509, "Information technology – Open Systems Interconnection –The Directory: "Public-key and attribute certificateframeworks".
[6] H.L.Kesterson II, "Digital Signatures – Whom Do You Trust?", IEEE Electronic Database 0-7803-3741-7/97.
[7] R. Perlman, "An Overview of PKI Trust Models", IEEE Network, November/December 1999
[8] "VeriSign Certification Practice Statement" , version 3.0 , April 1, 2005,
[9] Cisco Systems, "Introduction to Secure Sockets Layer", White paper from Internet.
[10] D.W. Chadwick, A. J. Young, N. Kapidzic Cicovic, "Merging and IEEE Extending the PGP and PEM Trust Models – The ICE-TEL Trust Model",network, May/June 1997.
[11] "The GNU Privacy Project**".**
[12] J.Weise, "Public key Infrastructure Overview", Sun Blueprints Online, August 2001.
[13] "PGP User's Guide: An Introduction to Cryptography",
[14] H.L.Kesterson II, "Digital Signatures – Whom Do You Trust?", IEEE Electronic Database 0-7803-3741-7/97.
[15] D.W. Chadwick, A. J. Young, N. Kapidzic Cicovic, "Merging and Extending the PGP and PEM Trust Models – The ICE-TEL Trust Model", IEEE network, May/June 1997.