

Network Security Assignment

Group 32 Members :-

IIT2018156 Kartik Nema

IIT2018163 Bhupendra

IIT2018172 Prakhar Srivastava

IIT2018175 Ashish Patel

IIT2018177 Shubham Soni

Theory :- Compare and contrast the nature of certificates in PGP and S/MIME. Explain the web of trust made from certificates in PGP and in S/MIME. (8)

Practical:- Create a simple mail server using S/MIME. (3)

Theory



(i) PGP

A public key certificate is digitally signed from one identity which confirms that the public key of another entity has a certain value. Public key refers to the value associated with an identity, which is known to everyone.

Pretty Good Privacy (PGP) uses the X.509 certificates and PGP certificates while S/MIME uses the X.509V3. Protocols that use X.509 certificates depend on the hierarchical structure of trust. Hierarchical structure here implies that there is a single path from fully trusted authority to any certificate, the CA at the root level issues certificates to the CAs at second level, the CA at second level then issues certificates to CAs at third level and so on. A X.509 certificate contains a public key, digital signature, information about the identity associated with the certificate and the issuing certificate authority.

X.509 certificates

X.509 is a digital certificate that uses the X.509 public key infrastructure used to verify that a public key belongs to a user. This certificate contains information of both the identity to which certificate is issued and identity which issues the certificate. This certificate contains following components :-

Certificate format version	version 3
Certificate serial number	12345678
Signature algorithm identifier for CA	RSA with MD5
Issuer X.500 name	c=US, o=ACME
Validity period	start=01/08/96, expiry=01/08/98
Subject X.500 name	c=US, o=ACME, cn=John Smith + ...
Subject public key information	 RSA with MD5
<small>version 2</small> Issuer unique identifier	
<small>version 2</small> Subject unique identifier	
CA Signature 	

Structure of X.509 certificate

(source :

<http://ftp.gnome.org/mirror/archive/ftp.sunet.se/pub/security/docs/PC A/misc/Entrust/x509v3.pdf>)

All X.509 certificates have the following data :-

- (i) Version: The version of X.509 which is used in the certificate.
- (ii) Serial number: The authority creating the certificate assigns a serial number to differentiate from other certificates.
- (ii) Algorithm information (signature algorithm): Algorithm used by the identity which issues the certificate to sign the digital certificate.
- (iv) Issuer's unique name: The name of the identity which issues the certificate.
- (v) Subject Public Key Information: It has 2 fields :-
 - The value of the public key owned by the subject.
 - Algorithm identifier :- Specifies the algorithm with which public key is used. It specifies both the public-key algorithm and hashing

algorithm.

(vi) Validity period of the certificate – start/end date and time

The X.509 certificates are used in web browsers which support TLS browsers, it is also used in some code-signing schemes (eg. Microsoft Authenticode), it is also used in E-mail standards such as PEM and in SET (a E-Commerce protocol).

PGP certificates

In PGP there is no need for CAs, i.e. anyone in the ring can sign a certificate for anyone else in the ring. So there can be multiple paths from fully or partially trusted authorities to any subject. The mechanism of PGP is based upon

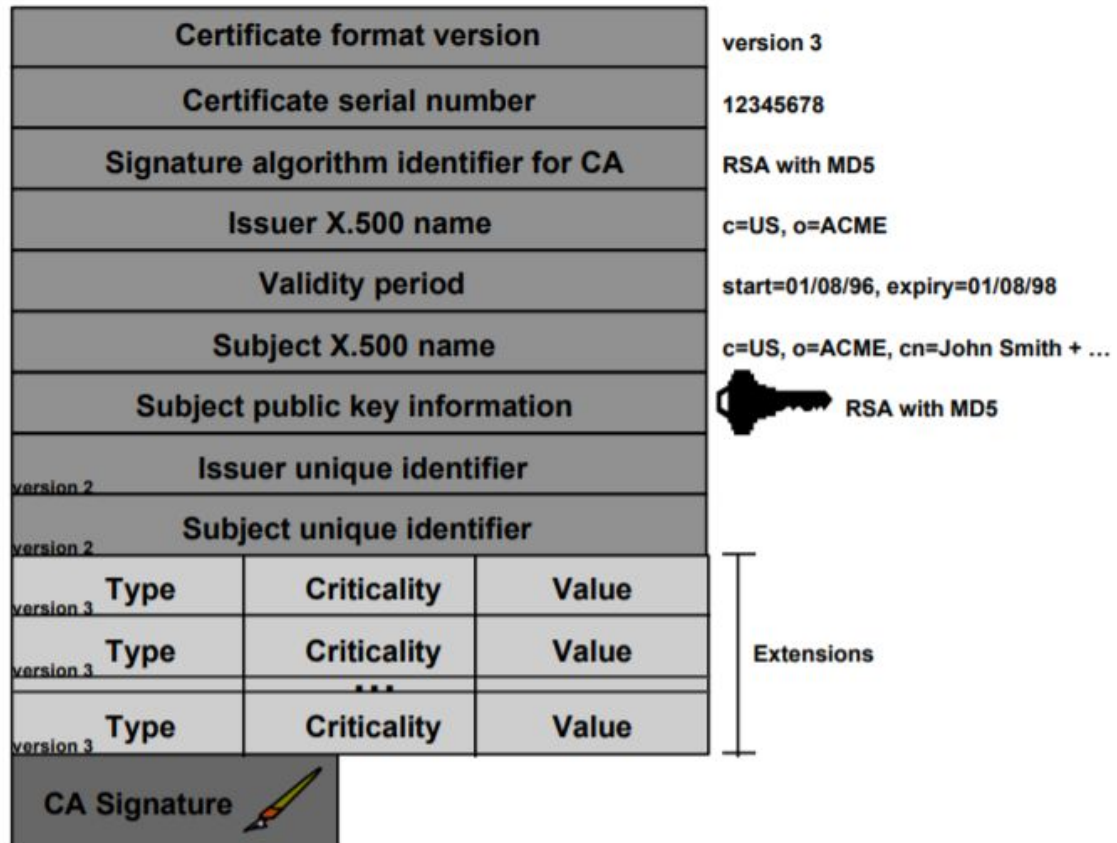
1. Introducer Trust
2. Certificate Trust
3. Legitimacy of the public keys

(ii) S/MIME

X.509V3

X.509V3 introduces a mechanism by which the certificate can be extended to include additional information.

Each extension consists of three fields: type, criticality, and value.



Structure of X.509V3 certificate

(source :

<http://ftp.gnome.org/mirror/archive/ftp.sunet.se/pub/security/docs/PC A/misc/Entrust/x509v3.pdf>)

The extension value field contains the actual data for the extension, the type field is used to specify the type of data in the extensions. Type could be string, numeric or complex. Criticality bit is a single-bit field. Which when set it indicates the extension value has important information, this information can not be ignored.

The extensions provided by this certificate are categorized into 4 groups :- key information, policy information, user and CA attributes, certification path constraints.

The common extensions include KeyUsage :- to limit the use of keys to a particular purpose only for example to sign in only, Alternative Names to allow other identities to be associated with public keys.

In summary, X.509V3 has the following attributes for all extension fields-

- (1) extnId - Used to uniquely identify the extension
- (2) critical - If set indicates extension is vital
- (3) extnValue - the actual extension value

Web of Trust Model:

In cryptography Web of Trust model is used to authenticate the binding between the public key and its owner. During a network communication many people will receive different keys and as time goes on many keys will be accumulated and to prove oneself there would be many key exchanges. This would cause a fault in the network

Operation of WOT:

Let's say Alice trusts Bob and Bob gives a key and says that this is Stacy's key. Since Alice trusts Bob therefore she will sign the key for Stacy proving that the key is of Stacy. So we can say that if a person trusts person B then he trusts anyone B trusts.

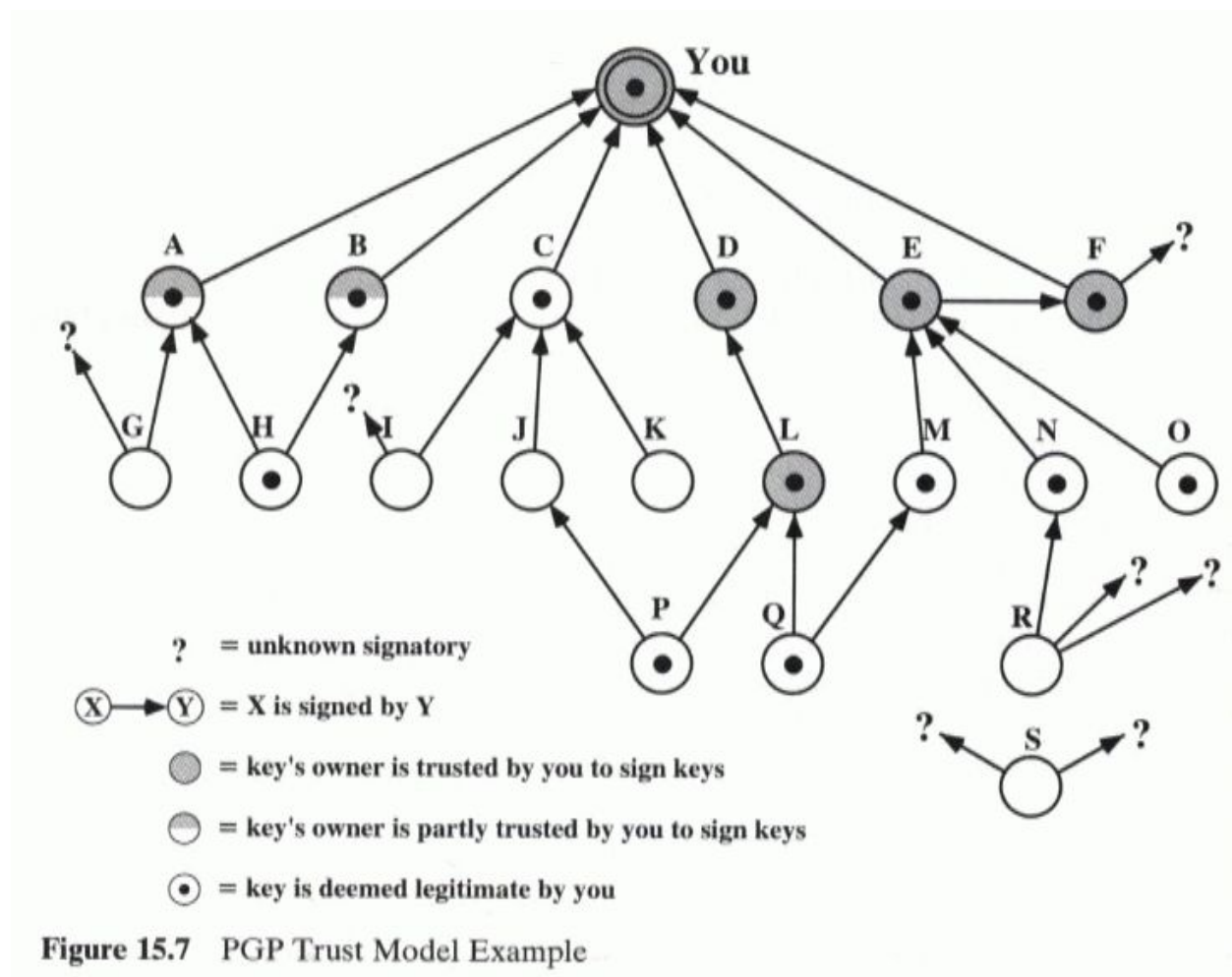
So in a PGP key signing event if Alice gets signed her key by someone. So the person who trusted the person who signed Alice's key can directly verify Alice's key and make sure that the key which was found online was of Alice.

Structure of a key:

A key in the public domain has the following attributes:

1. The owner
2. Owner trust given by the user. Values are:
 - (i) Ultimate Trust: Owner is the user
 - (ii) Complete Trust: The owner is always trusted
 - (iii) Marginal Trust: the owner is usually trusted
 - (iv) Untrusted: the owner is not trusted

3. Zero or more signatures, each one associated with a signatory trust.
4. Trust values calculated by PGP from the collection of signatory trust fields.



Source:-<https://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/PGP.html>

The figure illustrates how signature trust and key-signing combine to produce key legitimacy and user trusts on D, E, F, L to sign other keys and partially trusts A and B. Let's say the agent marked by You is Alice. Here are four cases.

1. Case for Alice and C: Alice and D are good friends. Therefore Alice can sign for D and also trust D.
2. Case for Alice and C: In this case, Alice says that the key is of C but Alice doesn't necessarily believe C.
3. Case for Alice and L: Here Alice may not have signed the key for L but trusts L but because of less electronic communication between them they were not able to sign keys.
4. Case for Alice and P: Alice may have not signed P's key and also has no trust in P since they don't know each other.

In PGP model one user has the ability to give directly a public key to another user and vice-versa. So PGP does not mandate any policy for creating trust hence they are free to choose the length of trust. In S/MIME sender and receiver do not rely on shared keys rather they rely on a common certifier on which both can trust.

In short we say that PGP depends on each user key exchange while S/MIME uses hierarchically validated certifier for key exchange.

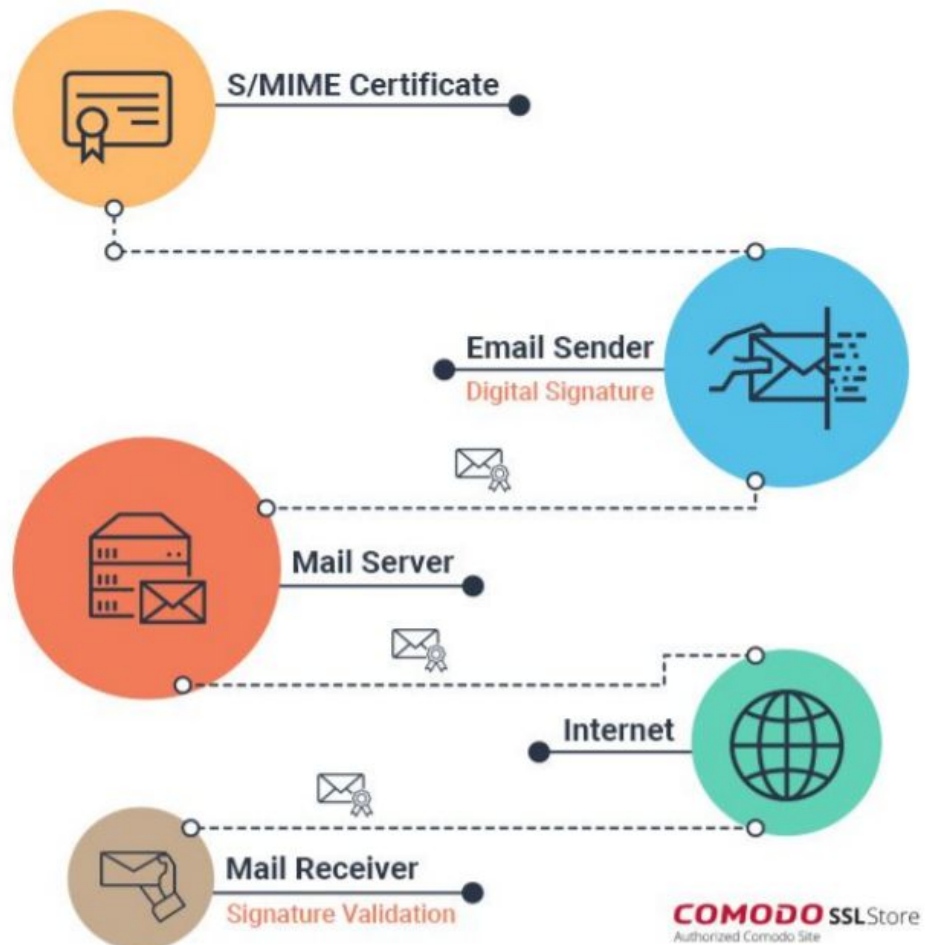
Practical:

Implementation: Create a simple mail server using S/MIME

What is S/MIME:

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a widely accepted method (or more precisely, a protocol) for sending digitally signed and encrypted messages. S/MIME allows you to encrypt emails and digitally sign them. When you use S/MIME with an email message, it helps the people who receive that message to be certain that what they see in their inbox is the exact message that started with the sender. It will also help people who receive messages to be certain that the message came from the specific sender and not from someone pretending to be the sender. To do this, S/MIME provides for cryptographic security services such as authentication, message integrity, and non-repudiation of origin (using digital signatures). It also helps enhance privacy and data security (using encryption) for electronic messaging.

Working of S/MIME:



WORKING OF S/MIME

References

<https://docs.oracle.com/javase/8/docs/technotes/guides/security/cert3.html>

http://ftp.gnome.org/mirror/archive/ftp.sunet.se/pub/security/docs/PC_A/misc/Entrust/x509v3.pdf