Topic 2: PKI

Topic 2 – Lecture 1:

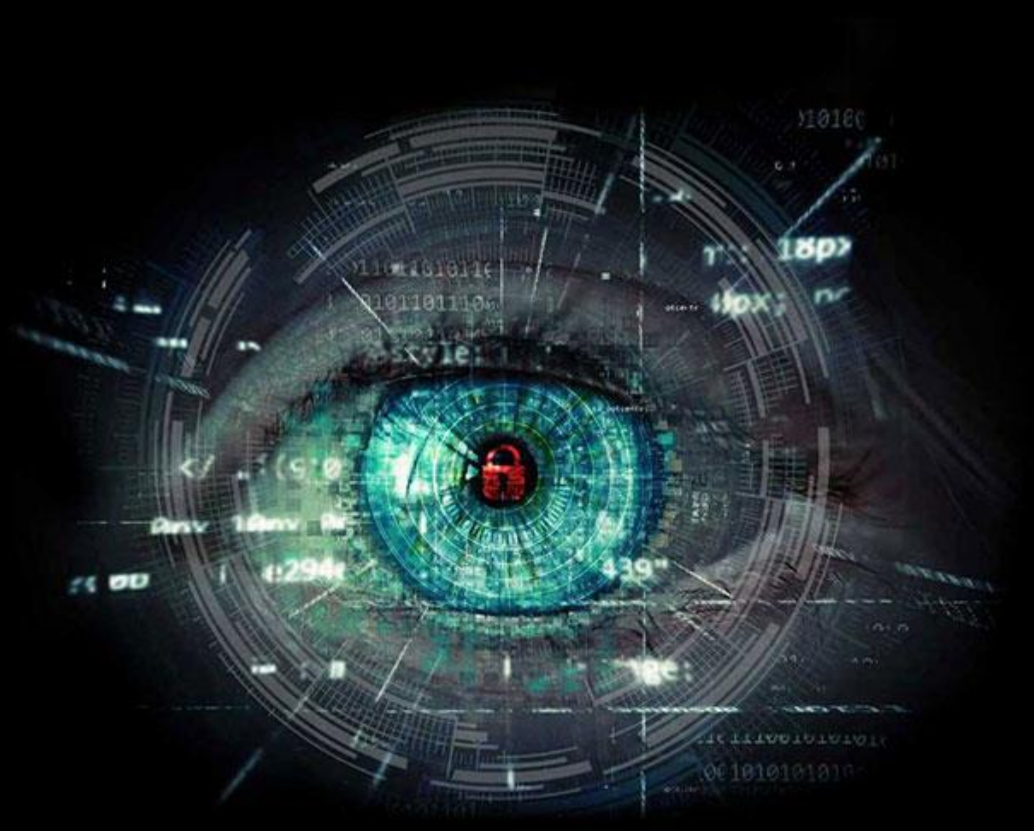
The Public Key Infrastructure

Network Security and Cryptography

http://www.freepowerpointtemplates-design.com

PKI Topic2 – 2.2

Scope and Coverage



01 The Public Key Infrastructure

02 Digital Signatures

03 Certification Authorities

04 Digital Certificates

PKI Topic2 – 2.3

Learning Outcomes

By the end of this topic students will be able to:

01 Describe the Public Key Infrastructure

02 Explain digital signatures

03 Explain the role of Certification Authorities

Overview

- This topic provides an overview to the key terms and concepts used in a PKI including:

  - Encryption
  - Public keys
  - Private keys
  - Digital signatures
  - Digital certificates

What is PKI?

PKI (Public Key Infrastructure) is a security architecture that has been aimed at giving a higher degree of trust while transferring information over the Internet.

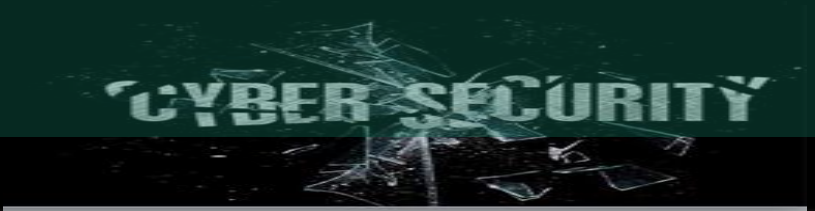
There are two ways to define it:

- The methodology, technology, and mechanism used to build a secure data infrastructure.
- To authenticate and verify content, a public and private key pair is used.

Benefits of PKI

PKI intends to provide the following benefits to its users:

- Assurance of the quality of electronically transmitted information
- Assurance of the source and destination of such information
- Assurance of the time and schedule of such information
- Assurance of the privacy and security of such information
- Assurance that such information may be used as proof in a court of law



Use of PKI

- To improve reliability in transferring information over unsecure networks.
  -ex. Consider the Internet, where such functions are tough to obtain along.
- For the sharing of information through private networks.
  -ex. The internal network of a company.
- To deliver cryptographic keys in a secure way.
- To make other cryptographically provided security services easier to use.

Who Does PKI Works

- Public key cryptography is a mathematical methodology used by PKI.
- A pair of cryptographic keys that are allied are used in.
- Verifies the sender's identity (through signing)
- It protects your privacy (through encryption of data)

Public Key Cryptography

PKI Topic2 – 2.9

- Uses a pair of cryptographic keys that are mathematically correlated.
- Encryption is done using a single key.
- The information can only be decrypted with the corresponding key.
- You can't compute the other key without knowing the first.
  - Alternatively, it is incredibly tough.

Public Keys and Private Keys

- The public key is made public, which means that it is freely shared and visible to all users.
- A related (and unique) private key is kept confidential and not shared among users.
- You can use your private key to verify that you are who you say you are.

Asymmetric vs Symmetric

Asymmetric

- Two keys, one for encryption and one for decryption

- Can identify the sender or receiver based on encryption and decryption using a private key that is only known by one of the participants involved in the communication.

Symmetric

- Encryption and decryption use the same key.

- Since all parties involved in having access to the same key, it cannot be used to identify the sender or receiver.

Public Key Encryption

- When someone intends to transfer confidential information to a private key holder:
  -they encrypt the data.
  - A secret key algorithm (symmetric cryptography) is used to encrypt the data, which is substantially quicker than asymmetric encryption.

  - To encrypt the data, a symmetric method generates a random session key.

  - After that, the public key is used to encrypt the private key, and both are securely transferred to the receiver.

Private Key Decryption

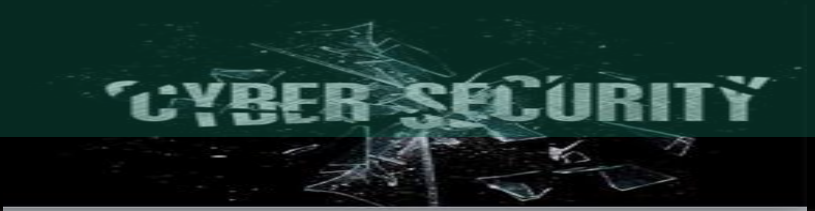
- When an owner of a private key receives secret information:

  -The user knows the material is destined for him/her if the private key can decode it, but the originator cannot be identified.

  -The session key is decrypted using the private key.

  -The real data is decrypted using the decrypted session key.

- This is more secure since firstly, the session key must be encrypted before moving on to the next step of decrypting the data.



Digital Signature

- A digital signature is a numerical value that is unique and encrypted.
- It is used to authenticate the ownership or copyright of data and differs each time it is produced.
- On the document to be signed, a hashing method is used to generate a unique number value.

  -This is why each time it is created, it is unique.
- The result is then encrypted and linked to the document using a private cryptographic key.

Using a Private Key for Signature

- Use a private key to digitally sign data to ensure you are the source.
- The encrypted value is transmitted as a separate file with the message or at the ending of the data.
- The corresponding public key can be delivered separately or as part of a certificate.
- This does not ensure anonymity since anybody who receives protected or digitally signed data can simply validate the signature, read, and process the data.

Using a Public Key for Signature - 1

The message recipient can authenticate the digital signature by using the right public key as follows:

- The receiver uses the right public key to decode the hash value computed by the sender for the data.

- Afterwards, the hash value of the data received is determined, using the hashing algorithm.

Using a Public Key for Signature - 2

- The hash value computed by the sender is compared to the newly generated hash value. If the two values are the same, the receiver knows the data was sent by the original owner of the private key and has not been altered since it was signed.

- If a public key certificate was included with the data, it must be validated with the ***Certificate Authority*** (CA) that issued it.

Receiving a Document

- You receive an email with a document attached.
- The sender digitally signed the document by computing a hash value and encrypting it using their private key.
- For the same document, you compute a hash value and decrypt the encrypted hash value.

  - If both values are the same, the sender has been verified and the document has not been altered.

  - If the two values don't match, the document has been tampered with or the sender isn't who they claim they are.

Summary

- The encryption and decryption of data, and also the signature as well as verification of data, are all covered by public key cryptography.
  - Ensures data privacy between the sender and the recipient by preventing unintentional data exposure.
  - By using authentication, the sender of the data is identified.
  - Ensures that the data hasn't been tampered with or altered.

Break

Topic 2: PKI

Topic 2 – Lecture 2:

The Public Key Infrastructure

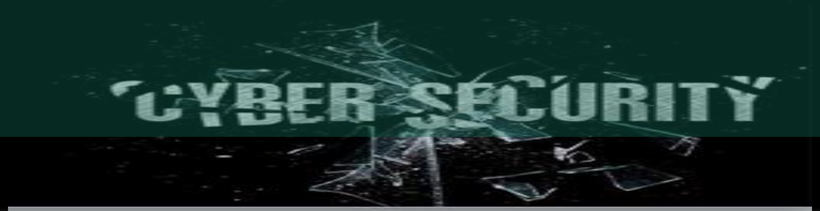
Network Security and Cryptography

What is a Digital Certificate?

- A digital document that associates your public key with an identity that the issuing ***Certification Authority*** (CA) will attest for.

- Users of the widely used encryption program ***Pretty Good Privacy****(PGP) can generate their own digital certificates.

- In another way, you'll have to go to a Certification Authority (CA) to have your identity verified.



Digital Certificate Usage

- In the key usage field of a digital certificate issued by one of the public CAs, there will be information.
- This implies that the private key may be used for a number of specific things, including:

  - Digital signatures

  Signing a certificate

  - Only encipher or decipher

  - Key encipherment

  - Data encipherment

Checking Usage

- Though key usage can be specified in the certificate, this does not guarantee that the software which usage the public key, has performed any verification on the certificate's content.

- When receiving a digitally signed document, the recipient must verify that the key was authorized for the purpose for which it was used.

Certificate Standards

- A certificate's data is normally substantiates with the ITU (IETF) standard X.509.
- It contains information on:

  -the owner of the associated private key's identity,
  -the length of the key,
  -the method or algorithm employed by the key,
  -the hashing methodology used,
  -the certificate's validity dates,
  -the acts that the key can be used for

The Components of a PKI

- Certification Authority (CA)
- Revocation
- Registration Authority (RA)
- Certificate Publishing Methods
- Certificate Management System
- PKI-aware Applications

Certification Authority (CA)

- Certificates are issued and verified.
- Takes responsibility for verifying (to a certain extent) that the identification of the individual requesting a certificate, is correct which need to be issued.
- Assure that the certificate's information is correct before digitally signing it.

CA – Generating Key Pairs

- For their customer, the CA may generate a public key and a private key.

- Alternately, the individual requesting a certificate can create their own key pair and transmit a signed request to the CA that includes their public key.

  -The individual asking for the certificate may prefer to do so in order to keep control of the private key.

CA – Issuing Digital Certificates

- To verify your identification, the CA will run a series of checks.
- The CA may comment on the quality of the checks performed prior to the certificate's issuance.
- Certificates of various classes can be acquired to correspond to the various stages of these checks.

CA –Digital Certificate Classes

- By providing an email address is enough, that is required to obtain a Class 1 certificate.
- Additional personal information is required for Class 2 certifications.
- Class 3 certification may only be bought after thorough inspections.
- Governments and organizations that require extremely high levels of verification may employ as 4th class.

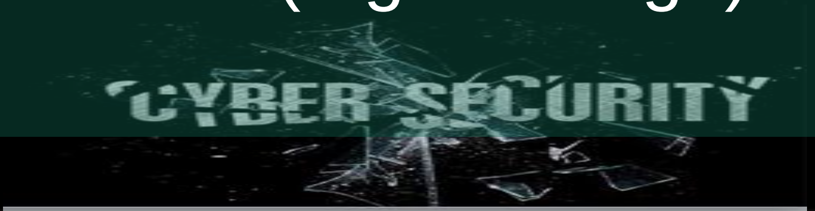
CA – Digital Certificates

- A individual person may have several certificates from several CAs.
- Several applications may want you to access certificates issued by specific CAs.
- The CA perhaps:

  - a component of your own firm,

  -a holding company (such as a bank or a post office),

  -a separate business (e.g. VeriSign)



CA – Verifying Digital Certificates

- The CA signs the public key certificate to prevent it from being altered or falsified.
- This is used to verify the validity of the public key.
- The signature is validated to a list of 'Root CAs' contains a number of 'PKI aware' applications, including your browser.
- The public certificate contained in the root CA list is used to validate certificates automatically.

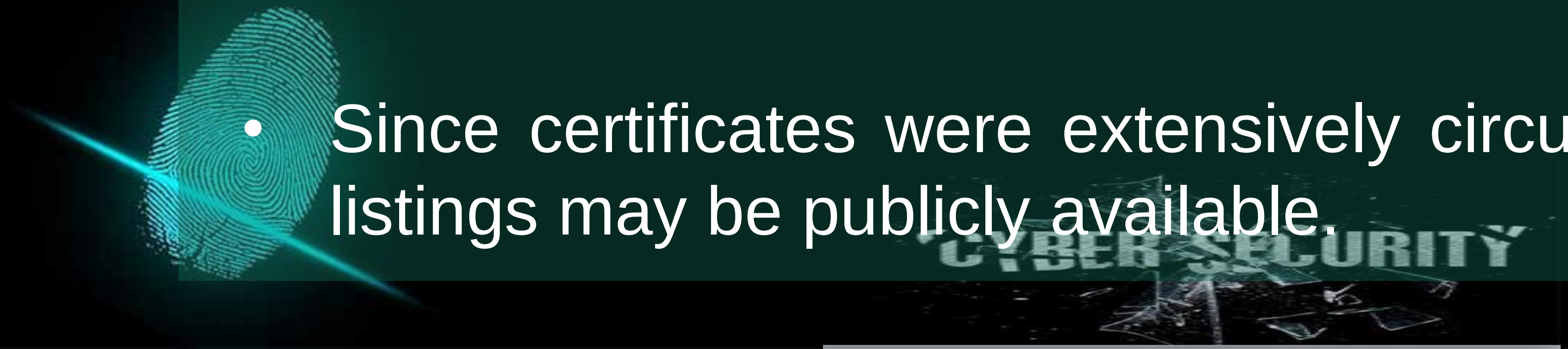
Revocation

- There is a mechanism in place for notifying people when their certificates are no longer valid (revoked).

- Outside of the directory/database that contains certificates, a system of revocation lists has been devised.

  -It's a list of certificates that aren't valid anymore.

- Since certificates were extensively circulated, revocation listings may be publicly available.



Registration Authority (RA)

- The CA uses a ***registration authority*** to perform verification on the individual or entity applying for the certificate to confirm that they are who they state they are.

- Although RAs appear to the certificate requestor as CAs, they do not digitally sign the certificate.

Certificate Publishing Methods

- Certificates must be published in PKI systems so that users may discover them.
- There are two ways to accomplish this:

  -It will be published in the electronic version of a telephone directory.

  -Sending it to those who may require it

Publishing in Directories

- X.500/LDAP compliance directories are databases.

  -The certificates in the databases are in the X.509 format.

  -They give certain search capabilities that are described in the IETF's LDAP standards.

- Directories can be public or stay private:
  - Private directories generally include sensitive information that the owner does not want to be publicly disclosed.
  - Anyone with access to a public directory can read the information contained inside.

Publishing in Databases

- Databases can be configured to accept certificates in the X.509 format.
- This can be done for private systems that don't use the LDAP structure for their search techniques.
- As it's essentially a proprietary system, this technology is not utilized for public directories.

Sending to Potential Users

- Certificates can be sent through email and then installed on the recipient's server or PC.

- Certificates can also be kept on portable storage devices like:
  - DVDs
  - CDs
  - USB storage devices

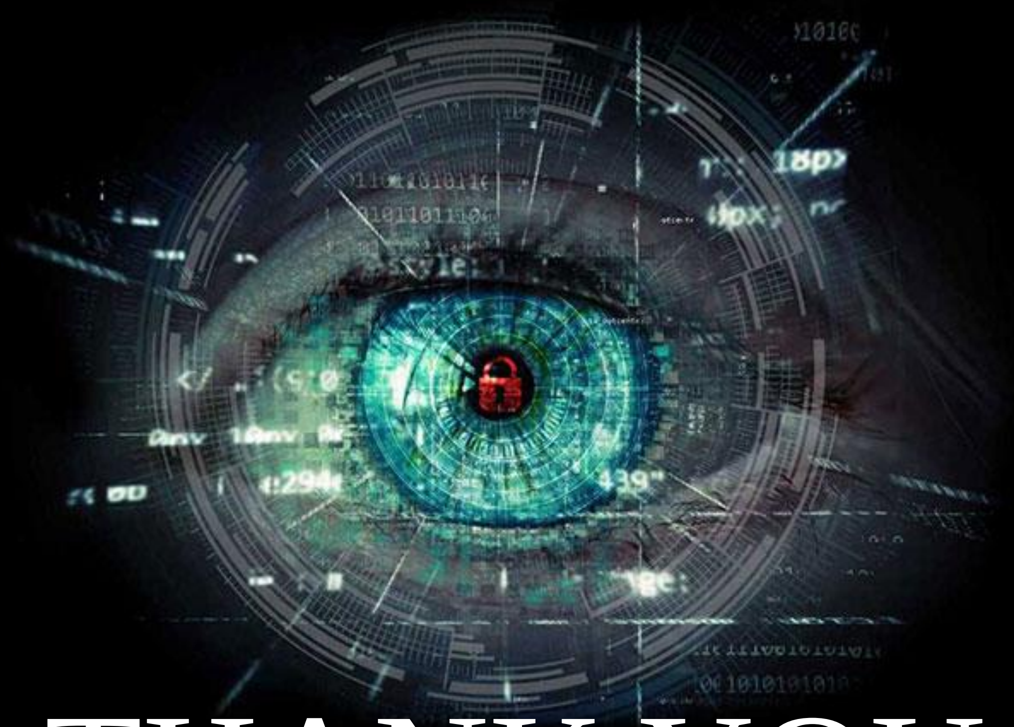
Certificate Management System

- Certificate management systems
  - Publish
  - Suspend
  - Renew
  - Revoke
- Certificates should not normally be deleted since they may be necessary for legal reasons in the future.
- These systems are often administered by a CA to maintain track of their certifications.

References

- Stallings, W. (2010). Cryptography and Network Security: Principles and Practice. Pearson Education.

- Network Working Group (1999). Internet X.509 Public Key Infrastructure [Available Online] http://www.ietf.org/rfc/rfc2459.txt



THANK YOU

Any Question?

Topic2 – PKI