


Bringing British
Education to You
www.nccedu.com

Network Security and
Cryptography

Topic 2:
PKI

V1.0

© NCC Education Limited



Bringing British
Education to You
www.nccedu.com

Network Security and
Cryptography

Topic 2 – Lecture 1:
The Public Key Infrastructure

V1.0

© NCC Education Limited

Scope and Coverage

This topic will cover:

- The Public Key Infrastructure
- Digital Signatures
- Certification Authorities
- Digital Certificates



Bringing British
Education to You
www.nccedu.com

V1.0

© NCC Education Limited


PKI Topic 2 - 2.3

PKI Topic 2 - 2.4

Learning Outcomes

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

- Describe the Public Key Infrastructure
- Explain digital signatures
- Explain the role of Certification Authorities


 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

PKI Topic 2 - 2.5

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


 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

PKI Topic 2 - 2.6

What is PKI?

- **Public Key Infrastructure** (PKI) is a security architecture that has been introduced to provide an increased level of confidence for exchanging information over the Internet.
- It is defined in 2 ways:
 - The method, technology and technique used to create a secure data infrastructure.
 - The use of the public and private key pair to authenticate and for proof of content.


 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

PKI Topic 2 - 2.7

Benefits of PKI


- PKI aims to offer its users the following benefits:
 - Certainty regarding the quality of information transmitted electronically
 - Certainty of the source and destination of such information
 - Assurance of the time and timing of such information
 - Certainty of the privacy of such information
 - Assurance that such information may be used as evidence in a court of law

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.8

Use of PKI


- To support secure information exchange over insecure networks.
 - e.g. the Internet where such features cannot be provided easily
- For information exchange over private networks.
 - e.g. an organisation's internal network
- To securely deliver cryptographic keys.
- To facilitate other cryptographically delivered security services.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.9

How Does PKI Work?


- PKI uses a mathematical technique called public key cryptography.
- A pair of related cryptographic keys are used.
- Verifies the identity of the sender (through signing)
- Ensures privacy (through encryption of data)

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.10

Public Key Cryptography


- Uses a pair of mathematically related cryptographic keys.
- One key is used to encrypt information.
- Only the related key can decrypt that information.
- Knowledge of one key does not allow you to calculate the other.
 - Or it is extremely difficult

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.11

Public Keys and Private Keys


- The public key is made public - it is freely distributed and can be seen by all users.
- A corresponding (and unique) private key is kept secret and is not shared amongst users.
- Your private key enables you to prove that you are who you claim to be.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.12

Asymmetric v Symmetric


Asymmetric	Symmetric
<ul style="list-style-type: none">• Two keys, one each for encrypting and decrypting• Can identify sender or recipient based on encryption/decryption using private key which is known to one entity in the communication	<ul style="list-style-type: none">• Same key for encrypting and decrypting• Cannot be used to identify sender or recipient as all parties involved know the same key

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.13

Public Key Encryption


- When a person wants to send confidential data to a private key holder:
 - They encrypt the data.
 - The data is encrypted using a secret key algorithm (symmetric cryptography) which is much faster than the asymmetric cryptography.
 - A random session key is generated using a symmetric algorithm to encrypt the data.
 - The public key is then used to encrypt that key and both are sent securely to the recipient.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.14

Private Key Decryption

- When a private key holder receives confidential data:
 - If the private key can decrypt the data, the user is certain that the data is meant for him/her but cannot identify the originator.
 - The private key decrypts the session key.
 - The decrypted session key is used to decrypt the actual data.
- This is more secure as the session key has to be decrypted first in order to proceed to the next process of decrypting the data.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.15

Digital Signature


- A **digital signature** is a unique, encrypted numerical value.
- It differs each time it is generated and is used to prove the ownership or copyright of data.
- A hashing algorithm is performed on the document to be signed producing a unique numerical value.
 - This is why it differs each time it is generated
- This is then encrypted using a private cryptographic key and links the result to the document.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.16

Using a Private Key for Signature

- To prove you are the source of data, use a private key to digitally sign it.
- The encrypted value is sent either at the end of the data or as a separate file with the message.
- The corresponding public key may also be sent either on its own or as a certificate.
- This does not prove anonymity as anyone receiving the protected or digitally signed data can easily check the signature, read and process the data.


V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.17

Using a Public Key for Signature - 1

The message receiver can use the correct public key to verify the digital signature as follows:


1. The correct public key is used by the receiver to decrypt the hash value which was calculated by the sender for the data.
2. Then, using the hashing algorithm, the hash value of the data received is calculated.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.18

Using a Public Key for Signature - 2

3. The newly calculated hash value is compared to the hash value calculated by the sender. If the two values are the same, the receiver knows that the data was sent originally by the owner of the private key and the data has not been edited since it was signed.
4. If a public key certificate was sent together with the data, it is then validated with the **Certificate Authority** (CA) that issued the certificate.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.19

Receiving a Document

- You receive a document via email.
- This was digitally signed by the sender by calculating a hash value for the document and encrypting it with their private key.
- You calculate a hash value for the same document and decrypt the encrypted hash value.
 - If the both values are the same, this verifies the sender and that the document has not been edited.
 - If the two values don't match, then the document has been edited or the sender is not who they claim to be.


 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

PKI Topic 2 - 2.20

Summary

- Public Key Cryptography is the encryption & decryption and signing/verification of data.
 - Ensures privacy between sender and receiver of the data by directly preventing unintended disclosure of the data.
 - Identifies the sender of the data by authentication.
 - Ensures that the data has not been modified or tampered with.

 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

 Bringing British Education to You
www.nccedu.com

Network Security and Cryptography

Topic 2 – Lecture 2:
The Public Key Infrastructure

 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

PKI Topic 2 - 2.22

What is a Digital Certificate?

- A digital document that binds your public key to an identity that the issuing **Certification Authority** (CA) is willing to vouch for.
- Users of the popular encryption software **Pretty Good Privacy** (PGP) have the ability to generate their own digital certificates.
- Otherwise you will have to approach a Certification Authority (CA) in order to validate your identity.

* More on this in Topic 4

 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

PKI Topic 2 - 2.23

Digital Certificate Usage

- A digital certificate issued by one of the public CAs will contain information in the key usage field of the certificate.
- This means that the private key may be used for specific purposes such as:
 - digital signatures
 - certificate signing
 - encipher or decipher only
 - key encipherment
 - data encipherment


 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

PKI Topic 2 - 2.24

Checking Usage

- Key usage may be set in the certificate but this does not ensure that the software which uses the public key has done any checks on the content of the certificate.
- Someone receiving a digitally signed document needs to check if the key was authorized for what it has been used for.


 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

PKI Topic 2 - 2.25

Certificate Standards


- The data in a certificate usually conforms to the ITU (IETF) standard X.509.
- Includes information about:
 - the identity of the owner of the corresponding private key
 - the length of the key
 - the algorithm used by the key
 - the associated hashing algorithm
 - dates of validity of the certificate
 - the actions that the key can be used for

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.26

The Components of a PKI


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

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.27

Certification Authority (CA)


- Issues and verifies certificates.
- Takes responsibility for identifying (to a stated extent) the correctness of the identity of the person asking for a certificate to be issued.
- Ensures that the information contained within the certificate is correct and digitally signs it.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.28

CA – Generating Key Pairs


- The CA may generate a public key and a private key for their client.
- Alternatively the person applying for a certificate may generate their own key pair and send a signed request containing their public key to the CA.
 - The person applying for a certificate may prefer to do this to ensure that the private key never leaves their own control.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.29

CA – Issuing Digital Certificates

- The CA will make a variety of checks to prove your identity.
- The CA may state the quality of the checks that were carried out before the certificate was issued.
- Different classes of certificate can be purchased that correspond to the different levels of these checks.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.30

CA –Digital Certificate Classes

- Class 1 certificates can be easily acquired by supplying an email address.
- Class 2 certificates require additional personal information to be supplied.
- Class 3 certificates can only be purchased after detailed checks have been made.
- A 4th class may be used by governments and organisations needing very high levels of checking.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.31

CA – Digital Certificates


- A person may have many certificates issued by many CAs.
- Some applications may insist that you use certificates issued by certain CAs.
- The CA may be:
 - part of your own organisation
 - a company (e.g. a bank or a post office)
 - or an independent entity (e.g. VeriSign)

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.32

CA – Verifying Digital Certificates


- The public key certificate is signed by the CA to prevent its modification or falsification.
- This is used when checking the public key is valid.
- The signature is validated against a list of 'Root CAs' contained within various 'PKI aware' applications such as your browser.
- Certificate validation occurs automatically using the public certificate contained within the root CA list.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.33

Revocation


- There is a system for making it known that certificates are no longer valid (revoked).
- A system of revocation lists has been developed that exists outside the directory/database that stores certificates.
 - It is a list of certificates that are no longer valid.
- Revocation lists may be publicly available as certificates may have been widely distributed.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.34

Registration Authority (RA)


- A **registration authority** is a third-party used by the CA to perform checks on the person or company applying for the certificate to ensure that they are who they claim to be.
- RAs may appear to the requestor of the certificate as CAs but they don't digitally sign the certificate.

V1.0  Bringing British Education to You
www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.35

Certificate Publishing Methods


- PKI systems require the publishing of certificates so that users can find them.
- There are two means of doing this:
 - Publishing it in the equivalent of an electronic telephone directory
 - Sending it to parties who might need it

V1.0  Bringing British Education to You
www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.36

Publishing in Directories


- Directories are databases that are X.500/LDAP compliant.
 - The databases contain certificates in the X.509 format.
 - They provide specific search facilities which are specified in the LDAP standards published by the IETF.
- Directories can be public or remain private:
 - Private directories usually contain confidential data that the owner does not wish to be publicly accessible.
 - Public directories contain information which can be read by anyone with access to them.

V1.0  Bringing British Education to You
www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.37

Publishing in Databases


- Databases can be configured to accept X.509 format certificates.
- This can be done for private systems where search methods do not follow the LDAP structure.
- This method is not used for public directories because it is essentially a proprietary system.

 Bringing British Education to You
www.nccedu.com
V1.0 © NCC Education Limited

PKI Topic 2 - 2.38

Sending to Potential Users


- Certificates can be sent through email so that the recipient can add them to their server or desktop.
- Certificates can also be carried in portable storage media such as:
 - DVDs
 - CDs
 - USB storage devices

 Bringing British Education to You
www.nccedu.com
V1.0 © NCC Education Limited

PKI Topic 2 - 2.39

Certificate Management System


- Systems that manage certificates:
 - publish
 - suspend
 - renew
 - Revoke
- Do not usually delete certificates because they may be required for future legal reasons.
- Typically a CA will run these systems to keep track of their certificates.

 Bringing British Education to You
www.nccedu.com
V1.0 © NCC Education Limited

PKI Topic 2 - 2.40

PKI Aware Applications


- Applications are those that have had a particular CA software supplier's toolkit added to them.
 - enables them to use the supplier's CA and certificates to implement PKI functions.
- These applications have no knowledge base built in to them about what the security requirements really are, or which PKI services are relevant in their delivery.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.41

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>

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

PKI Topic 2 - 2.42

Topic 2 – PKI

Any Questions?

 Bringing British Education to You www.nccedu.com 

V1.0 © NCC Education Limited
