Subject : Computer Network Security
Class : BCA/MCA
Semester : VI
Name of the Paper: Computer Network Security
Topic : Digital Signature
Keywords : Digital Signature, Authentication, Security

Created by:-
Vineet Kumar Singh
Assistant Professor
Department of Computer Application (BCA)
Jagatpur Post Graduate College, Jagatpur Varanasi
E-mail ID: vineet.jpgc@gmail.com

1

SELF DECLARATION

"The content is exclusively meant for academic purpose and for enhancing teaching and learning. Any other use for economic/commercial purpose is strictly prohibited. The users of the content shall not distribute-disseminate are share it with any one else and its use is restricted to advancement of individual knowledge. The information provided in this e-content is authentic and best as per my knowledge"

By:-
Vineet Kumar Singh
Assistant Professor
Department of Computer Application (BCA)
Jagatpur Post Graduate College, Jagatpur Varanasi
E-mail ID: vineet.jpgc@gmail.com

2

Objectives

- To learn about the Digital Signature.
- To study need of digital signature authentication.
- To learn about type of digital signature.
- Learn about the digital signature and verification etc.

3

Course Outline

In continuation of earlier study about the digital signature we are able to learn about the following points:

- Introduction of digital signature.
- Type of digital signature
- Digital signature and verification
- Application of digital signature
- Advantage and disadvantage of digital signature

4

Introduction of Digital Signature

- A digital signature is an electronic signature that can be used to authenticate the identity of sender of a massage or a signer of a document and to ensure that the original content of a massage or document that has been sent is unchanged.
- Digital signature are easily transportable, cannot be imitated by someone else and can be automatically time-stamped.
- A digital signature can be used with any kind of message, whatever it is encrypted or not, simply the receiver can be sure of the sender's identity.
- A digital certificate contains the digital signature of the certificate issuing authority so that any one can verify that the certificate is real.

A digital signature scheme typically consist of three algorithms which are as follows:

5

- **1.** A key generation algorithm that select a private key uniformly at random from a set of possible private key. The algorithm output the private key and a corresponding public key.
- **2.** A signature algorithm which given a message and a private keys, produce a signature.
- **3.** A signature verifying algorithm which given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

6

Digital Signature Authentication Need

- **1.** Nobody should be able to calculate it from the message.
- **2.** People should be able to check and make sure that it's correct.
- **3.** Nobody should be able to change the document and calculate what the changed signature would be.
- **4.** Nobody able to find another document that will produce the same function output.

7

Type of Digital Signatures

Two useful type of digital signatures are clearsigned documents and detached signature. Both type of signatures incorporate the same security of authenticity, without requiring your recipient to decrypt your entire message.

- **1. Clearsigned Message:** In a clearsigned message, your signature appear as a text block within the content of your letter.
- **2. Detached Signature:** A detached signature is sent as a separate file with your correspondence.

8

Digital Signature and Verification

A digital signature is a mechanism by which a message is authenticated i.e. proving that a message is effectively from a given sender, much like a signature on a paper document. For digital signature, another technique called hashing are used that produces a message digest that is a small and unique of the complete message. The main reasons for producing a message digest are:

- The message integrity being sent is preserved; any message alteration will immediately be detected.
- The digital signature will be applied to the digest, which is usually considerable smaller than the message itself; and
- Hashing algorithm are much faster than any encryption algorithms (symmetric or asymmetric).

9

Applications of Digital Signature

Because the DSA authentication both the identity of signer and the integrity of the signed information, it can be used in a variety of applications which are as following:

- 1. Electronic Mail System
- 2. Legal System
- 3. Electronic Fund Transfer System (EFT)
- 4. Electronic Data Interchanged (EDI)
- 5. Electronic Bidding
- 6. Distribution of Software
- 7. Database Applications

10

Advantages of Digital Signature

Below the some common reasons for applying a digital signature to communications:

- **1. Authentication:** Digital signature can be used to authenticate the source of message When ownership of a digital signature is bound to a specific user, a valid signature show the message was send by that user. For example, a bank branch send a requesting change in the balance of an account .
- **2. Integrity:** It means message is not altered during the transmission between sender and receiver. Encryption hides the content of message, it may be possible to change an encrypted message without understanding it. Any changes in the message after signature will invalidate the signature.

Disadvantages of Digital Signature

Below the some common reasons for applying a digital signature to communications:

- 1. **Association of Digital Signature and Trusted Time Stamping :** The signer might have include the a time stamp with the signature or document it self might have date mentioned on it.

- **2. Non-Repudiation :** The repudiation refers to ay act of disclaiming responsibility for a message. A non-repudiation requires the existence of a Public-Key Interface (PKI) which is complex to establish and operate.

12

Related Questions:

1. Describe the computer limitations.
2. Explain the use of computer.
3. Explain the generation of computer in brief.

References:

1. Sanjay Kumar, Lalit Kumar & Akhilesh Singh, Computer Network Security, Thakur Publication, Lucknow.

2. William Stallings , Cryptography and Network Security, Third Edition.

THANK YOU

15