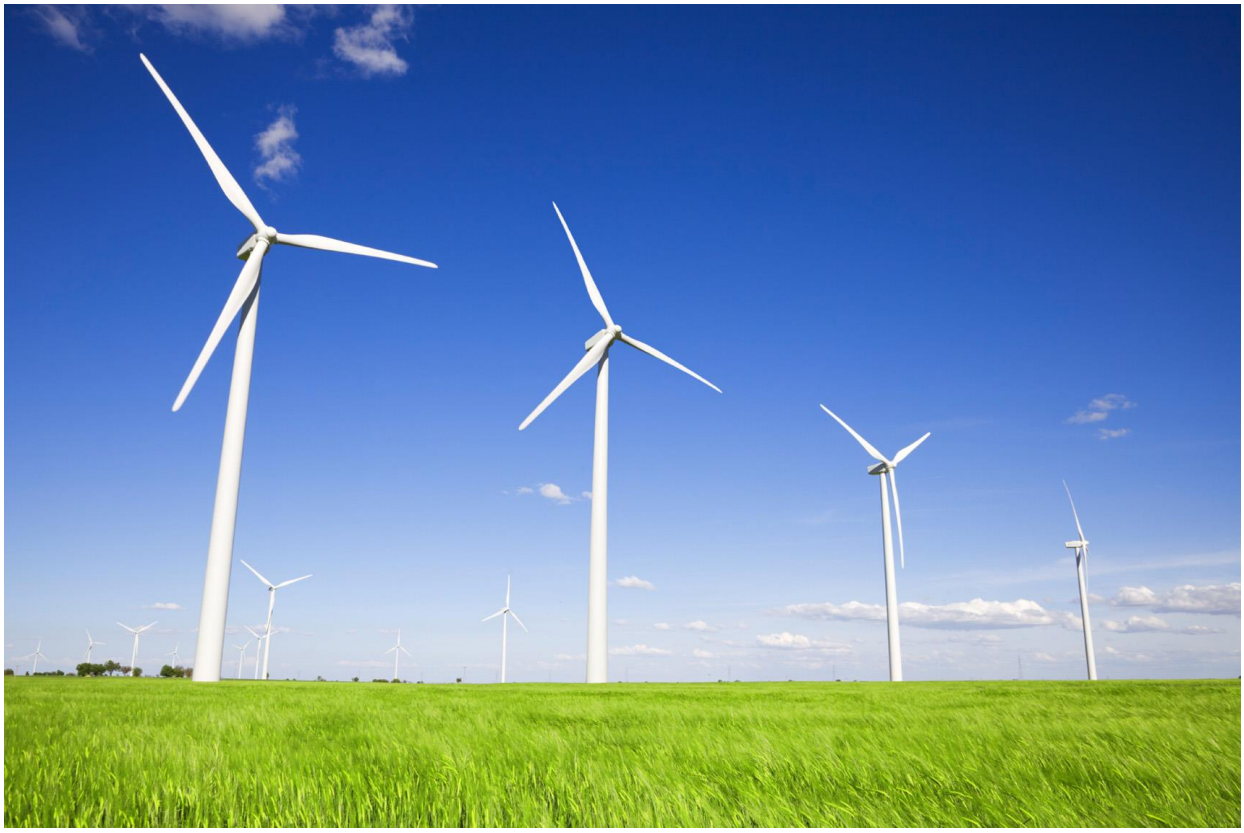
Computer Communication and Networks

(Lecture-09)



DR. KASHIF LAEEQ
PhD (CS), M.Phil. (CS), MCS (CS), M.Sc. (Math)
Member of IACSIT, IEEE, IEEEP, IJSER, ACM Research Group
Professor, Dept. of Computer Science
Federal Urdu University, Karachi

Internet Security

Internet security refers to securing communication over the internet. It includes specific security protocols such as:

- Internet Security Protocol (IPSec)
- Secure Socket Layer (SSL)

Internet Security Protocol (IPSec)

It consists of a set of protocols designed by Internet Engineering Task Force (IETF). It provides security at network level and helps to create authenticated and confidential packets for IP layer.

Secure Socket Layer (SSL)

It is a security protocol developed by Netscape Communications Corporation. It provides security at transport layer. It addresses the following security issues:

- Privacy
- Integrity
- Authentication

Threats

Internet security threats impact the network, data security and other internet connected systems. Cyber criminals have evolved several techniques to threat privacy and integrity of bank accounts, businesses, and organizations.

Following are some of the internet security threats:

- Mobile worms
- Malware
- PC and Mobile ransomware
- Large scale attacks like Stuxnet that attempts to destroy infrastructure.
- Hacking as a Service

- Spam
- Phishing

Email Phishing

Email phishing is an activity of sending emails to a user claiming to be a legitimate enterprise. Its main purpose is to steal sensitive information such as usernames, passwords, and credit card details.

Such emails contains link to websites that are infected with malware and direct the user to enter details at a fake website whose look and feels are same to legitimate one.

What a phishing email may contain?

Following are the symptoms of a phishing email:

Spelling and bad grammar

Most often such emails contain grammatically incorrect text. Ignore such emails, since it can be a spam.

Beware of links in email

Don’t click on any links in suspicious emails.

Threats

Such emails contain threat like “your account will be closed if you didn’t respond to an email message”.

Spoofing popular websites or companies

These emails contain graphics that appear to be connected to legitimate website but they actually are connected to fake websites.

Data Encryption

Encryption is a security method in which information is encoded in such a way that only authorized user can read it. It uses encryption algorithm to generate cipher-text that can only be read if decrypted.

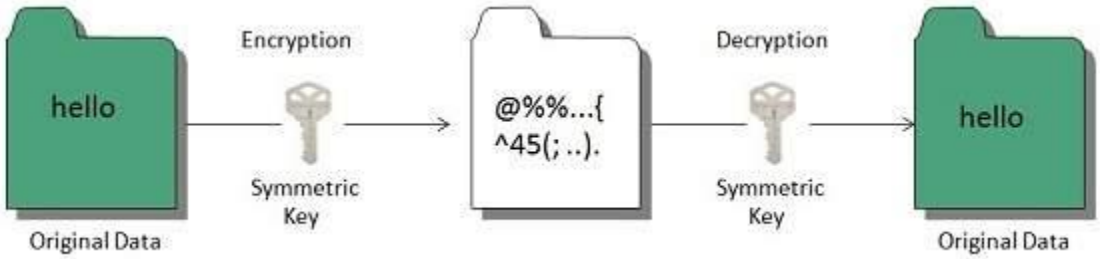
Types of Encryption

There are two types of encryptions schemes as listed below:

- Symmetric Key encryption
- Public Key encryption

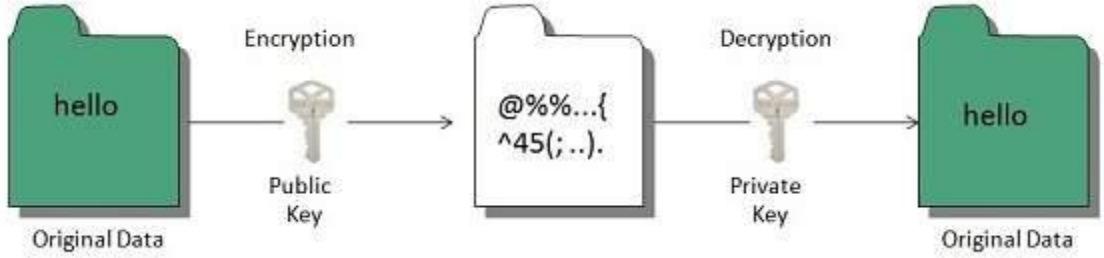
Symmetric Key encryption

- **Symmetric key encryption** algorithm uses same cryptographic keys for both encryption and decryption of cipher text.



Public Key encryption

- **Public key encryption** algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.



Hashing

In terms of security, hashing is a technique used to encrypt data and generate unpredictable hash values. It is the hash function that generates the hash code, which helps to protect the security of transmission from unauthorized users.

Hash function algorithms

Hashing algorithm provides a way to verify that the message received is the same as the message sent. It can take a plain text message as input and then computes a value based on that message.

Key Points

- The length of computed value is much shorter than the original message.
- It is possible that different plain text messages could generate the same value.

Here we will discuss a sample hashing algorithm in which we will multiply the number of a's, e's and h's in the message and will then add the number of o's to this value.

For example, the message is "the combination to the safe is two, seven, thirty-five". The hash of this message, using our simple hashing algorithm is as follows:

$$(2 \times 6 \times 3) + 4 = 40$$

The hash of this message is sent to John with cipher text. After he decrypts the message, he computes its hash value using the agreed upon hashing algorithm. If the hash value sent by Bob doesn't match the hash value of decrypted message, John will know that the message has been altered.

For example, John received a hash value of 17 and decrypted a message Bob has sent as "You are being followed, use backroads, hurry"

He could conclude the message had been altered, this is because the hash value of the message he received is:

$$(3x4x1)+4 = 16$$

This is different from then value 17 that Bob sent.

Digital Signature

Digital signatures allow us to verify the author, date and time of signatures, authenticate the message contents. It also includes authentication function for additional capabilities.

Applications

There are several reasons to implement digital signatures to communications:

Authentication

Digital signatures help to authenticate the sources of messages. For example, if a bank's branch office sends a message to central office, requesting for change in balance of an account. If the central office could not authenticate that message is sent from an authorized source, acting of such request could be a grave mistake.

Integrity

Once the message is signed, any change in the message would invalidate the signature.

Non-repudiation

Non-repudiation is the assurance that someone cannot deny the validity of something. ... In this context, non-repudiation refers to the ability to ensure that a party to a contract or a communication must accept the authenticity of their signature on a document or the sending of a message.

End of Lecture-9