Cryptography and Network Security

An Introduction

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	24 June 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Aim
- Introduction
- Background
- Definitions
  - Computer Security
  - Personnel Security
  - Network Security
- Internet security
- Summary
- Test your understanding
- References

Aim

- To understand the principles of encryption algorithms, conventional and public key cryptography.
- To have a detailed knowledge about authentication, hash functions and application level security mechanisms.

Agenda

- Aim
- Introduction
- Background
- Definitions
  - Computer Security
  - Personnel Security
  - Network Security
- Internet security
- Summary
- Test your understanding
- References

Introduction

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—The Art of War, Sun Tzu

Agenda

- Aim
- Introduction
- Background
- Definitions
  - Computer Security
  - Personnel Security
  - Network Security
- Internet security
- Summary
- Test your understanding
- References

Background

- Information Security requirements have changed in recent times
- traditionally provided by physical and administrative mechanisms
- computer user requires automated tools to protect files and other stored information
- use of networks and communications links requires measures to protect data during transmission

Agenda

- Aim
- Introduction
- Background
- Definitions
  - Computer Security
  - Personnel Security
  - Network Security
- Internet security
- Summary
- Test your understanding
- References

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Agenda

- Aim
- Introduction
- Background
- Definitions
  - Computer Security
  - Personnel Security
  - Network Security
- Internet security
- Summary
- Test your understanding
- References

Internet security

- our focus is on **Internet Security**
- consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information

Agenda

- Aim
- Introduction
- Background
- Definitions
  - Computer Security
  - Personnel Security
  - Network Security
- Internet security
- Summary
- Test your understanding
- References

Summary

- Today's lecture provides a general overview of the cryptography and network security.
- Next class we will discuss the network security services and mechanisms, and of the types of attacks they are designed for.

Test your understanding

1. Define computer security.
2. What is network security?

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.