

Bringing British  
Education to You  
[www.nccedu.com](http://www.nccedu.com)

Network Security and  
Cryptography

Topic 5:  
Data Protection

V1.0

© NCC Education Limited

---

---

---

---

---

---

---

---



Bringing British  
Education to You  
[www.nccedu.com](http://www.nccedu.com)

Network Security and  
Cryptography

Topic 5 – Lecture 1:  
Protecting Stored Data

V1.0

© NCC Education Limited

---

---

---

---

---

---


---

---

Scope and Coverage

This topic will cover:

- Overview of data protection
- File encryption technologies
- Disk encryption technologies



Bringing British  
Education to You  
[www.nccedu.com](http://www.nccedu.com)

V1.0

© NCC Education Limited

---

---

---

---

---

---

---


---

Data Protection Topic 5 - 5.4

## Learning Outcomes

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

- Describe disk encryption mechanisms
- Deploy file encryption mechanisms

 Bringing British Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.5

## Why Protect Data?

- Every network is at risk from unauthorised users gaining access to data stored and transmitted on that network
- Outside hackers will try to access your data for illegal purposes or simply to prove that they can
- Internal users may also try to gain unauthorised access to applications and information stored on the network

 Bringing British Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.6

## What Data is of Interest?

- Payment systems
- Research and development information
  - Where a company is trying to develop things that require patents or copyright
- Software that can be downloaded for free rather than paid for
- Commercially sensitive information, such as salary details, marketing plans, etc.
- Information about individuals

 Bringing British Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.7

### How to Respond to Hacking

- Depends upon the nature of the hacking
  - Serious fraud
  - Altering/deleting data
  - Prank
- How long has unauthorised access been going on?
- What is the nature of the data?
- Who knows about the hacking?
- Is there evidence that can be used to trace the hacker or in a legal action?


 Bringing British Education to You  
 www.nccedu.com

V1.0
 © NCC Education Limited

---

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.8

### Preventing Unauthorised Access

- A combination of methods gives the best protection against unauthorised access
- A plan that includes:
  - Staff with key responsibilities
  - Policies for system use
  - Methods for dealing with security breaches
- Technology – software and hardware
- User vigilance – acceptable use policies and training of staff


 Bringing British Education to You  
 www.nccedu.com

V1.0
 © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.9

### A Plan

- The plan should be a tool for managing all of the resources that prevent unauthorised access:
  - Who is responsible for checking log files?
  - How often are tools updated?
  - How often are plans and procedures reviewed?
- Should include details of:
  - Personnel
  - Software
  - Technology


 Bringing British Education to You  
 www.nccedu.com

V1.0
 © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.10

## Technology

- Firewalls
- Intrusion Detection Systems (IDS)
- Virus and content scanners
- Vulnerability assessment
- Patches and hotfixes

V1.0  Bringing British Education to You [www.nccedu.com](http://www.nccedu.com) © NCC Education Limited

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.11

## User Vigilance

- One of the best defences against hacking is an informed, vigilant workforce
- Computer systems are ideal for running repetitive tasks and are ideal at implementing rules that help protect the network
- But people are good at detecting the unusual
- Training staff is a cost-effective means of protecting your network

V1.0  Bringing British Education to You [www.nccedu.com](http://www.nccedu.com) © NCC Education Limited

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.12

## Protecting Your Data

- It is also wise to try and protect your data in the case of a hacker successfully gaining access:
  - Back up data - allows for data recovery in the event that data is deleted or corrupted
  - Have strong access control mechanisms
  - Password protect documents
  - Encrypt files
  - Encrypt disks

V1.0  Bringing British Education to You [www.nccedu.com](http://www.nccedu.com) © NCC Education Limited

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.13

## Data Back-up

- Your planning should include
  - What data is backed up
  - How often data is backed up
- There are many packages that allow for automated back up of data
- Enterprise databases include back-up facilities as part of the DBMS
- Back-up data should be stored securely
  - Data safe
  - Offsite

 Bringing British Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.14

## Access Control Mechanisms

- Access control mechanisms can be used to set access permissions to:
  - groups of network users
  - individual network users
  - other machines on the network
- These mechanisms can set permissions for:
  - Folders
  - Sub-folders
  - Individual files

 Bringing British Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.15

## Password Protecting Documents

- Many software applications allow the user to password protect individual documents
  - Microsoft Office
  - Adobe Acrobat
- Usually not sufficient to deter serious hackers
- Will protect from the casual snooper

 Bringing British Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---

---

---

---

## Encrypting Files


- Most operating systems support file encryption systems
- For example, Encrypting File System (EFS) is a feature of Windows OS
- You can easily store information on your hard disk in an encrypted format
- EFS protects data on the disk - if an EFS file is sent across the network it is not protected

## Encrypting Disks

- There are packages that allow the encryption of an entire disk
- This locks the entire contents of a disk drive or disk partition
- Automatic encryption of data occurs when it is written to the hard disk
- Automatic decryption occurs before being loaded into memory

## Encrypting Disks

- Some packages create invisible folders that act like a hidden disk within a disk
- Other file storage hardware can be encrypted including:
  - Removable USB drives
  - Flash drives, etc.
- Examples include:
  - PGP Whole Disk Encryption from Symantec
  - DriveCrypt from SecuStar



Bringing British  
Education to You  
www.nccedu.com

## Network Security and Cryptography

Topic 5 – Lecture 2:  
File Encryption & Disk Encryption

V1.0 © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.20

## File Encryption

- Also known as folder encryption as files and folders can both be encrypted
- Individual files or individual folders/directories are encrypted by the file system
- Encrypting a file or folder with most operating systems is usually simple
  - Select a checkbox in Windows



Bringing British  
Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.21

## Advantages of File Encryption

- Each file can be encrypted with its own encryption key
- Encrypted files can be managed on a file by file basis
- Public-key cryptography may be used for access control
- Memory only holds the cryptographic keys while the file that is decrypted is open



Bringing British  
Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.22

## General File Management Systems

- Most general purpose file management systems do not usually encrypt the metadata:
  - Directory structure
  - Filename
  - File sizes
  - Timestamps
- Makes the system less secure
  - When files are stored with unencrypted file names, access to the physical disk will show documents stored on the disk but not the contents

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

---

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.23

## Cryptographic File Systems

- Specialised file systems designed specifically for encryption
- Encrypt all data including metadata
- Usually operate on top of existing file systems
  - in a specific directory within a general file system
- Usually offer advanced features
  - Deniable encryption
  - Secure read-only file system permissions
  - Different views of the structure depending on the user

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

---

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.24

## Deniable Encryption

- Allows an encrypted message to be decrypted into several readable plaintexts
  - Depends upon the key used to decrypt the file
- And/or makes it impossible to prove that the original message exists without using the proper encryption key
- Attacker does not know:
  - If the data is encrypted
  - If the file owner can decrypt it

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

---

---

---

---

---

---

---


---



Data Protection Topic 5 - 5.25

## File Encryption with MS Windows

- Available on all recent version of Windows
- Employs the Encrypting File System (EFS)
- Uses a built-in encryption method that uses certificates
- Can protect individual files and/or folders
- To encrypt a file or folder you simply select a check box

V1.0  Bringing British Education to You [www.nccedu.com](http://www.nccedu.com) © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.26

## Encrypting File System

- Employs a combination of asymmetric and symmetric encryption
- User must have an EFS certificate to encrypt a file
  - from a Windows certification authority
  - or self-signed
- EFS files can be opened by:
  - the user who encrypted them
  - a designated recovery agent
  - other authorised user accounts

V1.0  Bringing British Education to You [www.nccedu.com](http://www.nccedu.com) © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.27

## Disk Encryption

- Software or hardware is used to encrypt all data that is written to a disk or disk volume
- It prevents unauthorised access to data storage areas
- Full disk encryption, also known as whole disk encryption, is a term used when everything on a disk is encrypted

V1.0  Bringing British Education to You [www.nccedu.com](http://www.nccedu.com) © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.28

## Full Disk Encryption

- Everything written to a disk is encrypted, including data and bootable OS partitions
- Some systems still leave the master boot record (MBR) unencrypted
  - This means there is a part of the disk that remains unencrypted
- There are hardware disk encryption systems that can encrypt the MBR and therefore really do encrypt the whole disk

V1.0  Bringing British Education to You [www.nccedu.com](http://www.nccedu.com) © NCC Education Limited

---

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.29

## Disk Encryption Keys

- Often the same key is used for encrypting the whole disk
- Some solutions use different keys for encrypting different partitions
  - This is a more secure solution

V1.0  Bringing British Education to You [www.nccedu.com](http://www.nccedu.com) © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.30

## Advantages of Disk Encryption

- Disk encryption has some advantages over file encryption
- Temporary files are also encrypted
- All individual files are automatically encrypted
- Data is made unusable by destroying the cryptographic keys
  - This essentially destroys the data as it cannot be read
  - In highly secure applications, the data should be wiped using a suitable tool

V1.0  Bringing British Education to You [www.nccedu.com](http://www.nccedu.com) © NCC Education Limited

---

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.31

## Disk Encryption Tools

- There are many tools with a variety of features
- Hardware-based tools residing within a storage device (self-encrypting drives) have no impact on system performance
  - As the encryption key is stored on the device it is not open to OS virus infections
- External hardware tools are generally faster and more secure than software tools

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

---

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.32

## Losing the Password

- It is essential to have a password recovery system
  - User may leave the organisation
  - User may simply forget the password
- Important in any large organisation using disk encryption to protect data
  - Multiple users
- Require a simple yet secure way to recover any "lost" passwords

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

---

---

---

---

---

---

---

---

Data Protection Topic 5 - 5.33

## Challenge/Response

- System challenges user and requires correct response
- Allow passwords to be recovered
- Advantages:
  - No need to store recovery encryption key
  - No need to exchange secret data during recovery
  - Not open to sniffing attacks
- Can be used remotely without the need for a network connection

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

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.34

## Booting with Full Disk Encryption

- When the whole boot disk is encrypted the blocks storing the OS are also encrypted
- This means some decryption is required before the OS can boot
- Many solutions have a small and secure pre-boot OS that allows for authentication before the full OS is launched
- Requires some external key to launch the full OS

 Bringing British Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.35

## External Keys

- A range of external key types are available for pre-boot authentication including:
  - Username/password
  - Smartcard and PIN
  - Biometric authentication methods:
    - Fingerprint
    - Iris scan
  - Dongle
    - Dongle must be kept safe and not lost
  - Use a combination of methods

 Bringing British Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

---

---

---


---

---

Data Protection Topic 5 - 5.36

## References

- Scambrey, J., McClure, S. and Kurtz, J. (2001). *Hacking Exposed: Network Security Secrets & Solutions*, 2<sup>nd</sup> Edition. McGraw Hill.
- Cobb, C. (2004). *Cryptography for Dummies*. John Wiley & Sons.

 Bringing British Education to You  
www.nccedu.com

V1.0 © NCC Education Limited

---

---

---

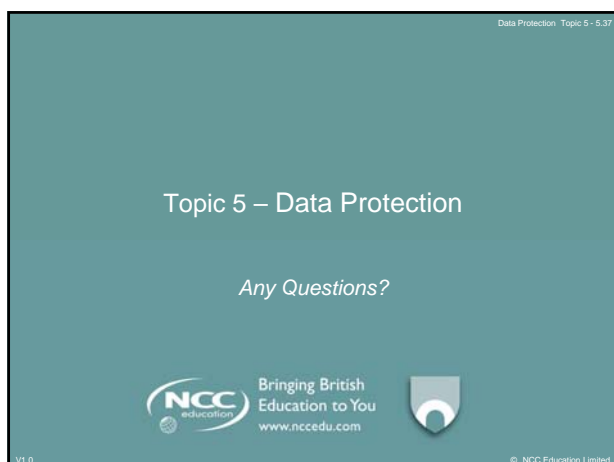
---

---

---

---

---



---

---

---

---

---

---