Bringing British Education to You

www.nccedu.com

Computer Networks

Topic 8:

Security Software

Bringing British Education to You

www.nccedu.com

Computer Networks

Topic 8 – Lecture 1:

Network Security Threats

V1.0

Scope and Coverage

This topic will cover:

- Network security threats
- Security countermeasures
- Security software
- Installing and configuring security software

Learning Outcomes

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

- Understand threats to the security of a network
- Describe a range of security countermeasures
- Install and configure essential software security measures

Tasks of Network Security

Must ensure the network offers:

- Privacy
- Integrity
- Availability

Network Privacy

- Network security should ensure that only authorised users can access network services.
  - Transmitted data cannot be accessed by unauthorised users and/or is unintelligible to unauthorised users.
- There are consequences if privacy is breached.
  - Embarrassment
  - Financial loss
  - Company secrets

Network Integrity

- Network security should ensure that data transmitted on the network:
  - Is not lost
  - Is not modified
  - Is not corrupted

Network Availability

- Network security should ensure that the network is available for use:
  - When needed
  - Providing the required services

Network Security Problems

- Software
- Protocol design
- System configurations
- Actions of people
- Accidents & natural events

Security Threats

- Eavesdropping
- Man-in-the-Middle
- Replay
- Virus
- Trojan
- Worm
- Traffic Analysis
- Physical attacks/damage
- Phishing
- Denial of Service

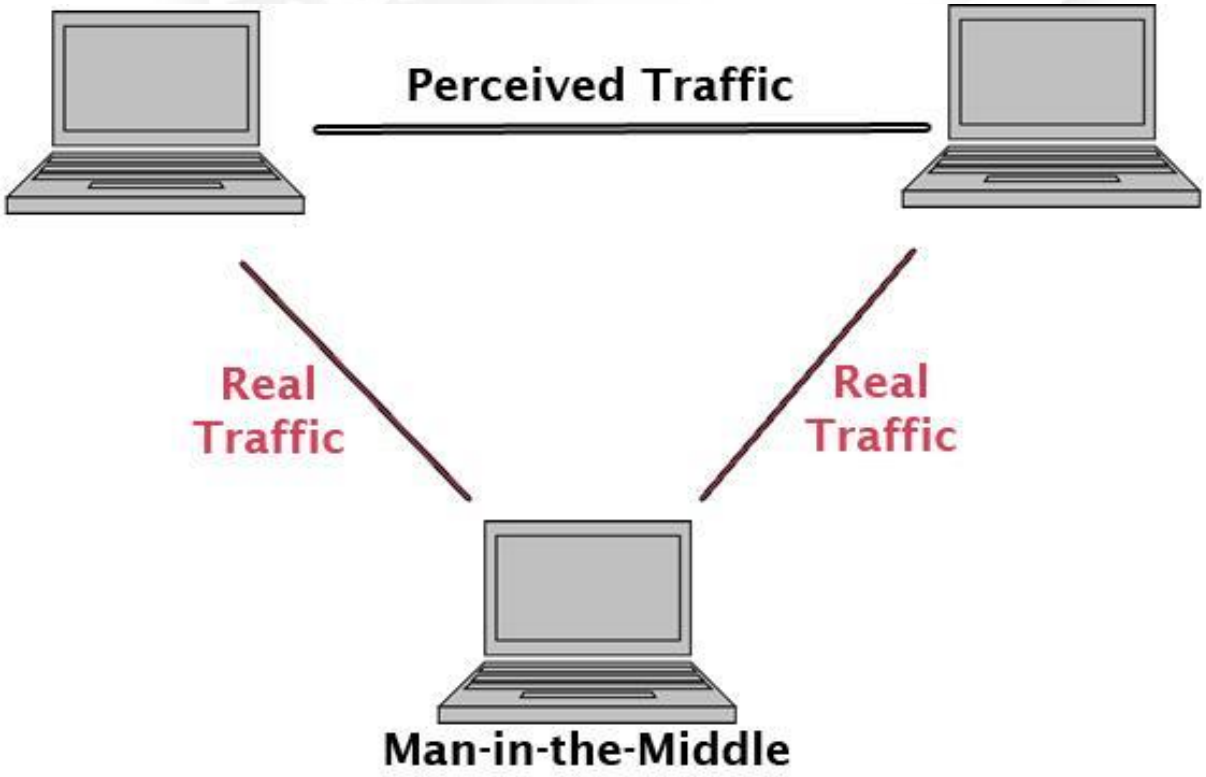
Eavesdropping

- Gaining access to information when not authorised to do so
- Can involve using an authorised user's computer
- Could involve sophisticated approaches to listening into the network
- In wireless networks, the signal can reach outside the physical boundaries of an organisation and be easy to access.

Man-in-the-Middle - 1

- A third party pretends to be one of the parties in a two-way conversation.
- Allows third party to listen to both sides of a conversation
- Can modify information before transmission
- Messages that use a "***store and forward***" transmission method are particularly vulnerable.

Man-in-the-Middle - 2



Replay Attack

- Attacker stores a set of messages for later use
- Can include username and password combinations
- Can be an attack on:
  - Privacy
  - Integrity
  - Availability

Virus

- A malicious program that attacks a single computer or a network.
- Often attached to other files
  - Attachments to emails
  - Embedded in image files
  - Now also on mobile phones
- Some are not malicious as they do no real harm but are just created for mischief.

Trojan

- Often a program that appears harmless
- Used to gain unauthorised access to:
  - Networks
  - Files
  - Data
  - Usernames & passwords

Worm

- A worm is a program that can:
  - Reproduce
  - Execute independently
  - Travel across network connections
- A virus is dependent upon the transfer of files between computers to spread.
- A worm can execute completely independently and spread on its own accord through network connections.

Traffic Analysis

- Involves analysing the traffic on the network and identifying important business information, such as:
  - Customers
  - Key personnel
  - General business information

Physical Threats - 1

- May be deliberate or accidental
- Deliberate:
  - Fire
  - Theft
  - Deliberate damage

Physical Threats - 2

- Accidental
  - Earthquake
  - Fire
  - Flood
  - Lightning
  - Power failure
  - Equipment failure

Phishing

- Emails that claim to be from a legitimate organisation
- Intended to fool a recipient into disclosing:
  - Usernames & passwords
  - Bank details
  - PIN numbers
- Often used for fraud by purchasing items or accessing bank accounts

Denial of Service

- An attack on network availability
- Network is flooded with requests
- Service is slowed or completely interrupted
- Can use many sources to flood the network
  - Distributed Denial of Service
- Results in large time delays, loss of customers, etc.
- Costs the targeted organisation money

Bringing British Education to You

www.nccedu.com

Computer Networks

Topic 8 – Lecture 2:

Security Countermeasures

Countermeasures

- Authentication
- Encryption
- Digital signatures
- Anti-virus
- Physical countermeasures
- Firewall
  - Firewalls will be discussed in detail in the next topic

Authentication

- Identifies the person or system attempting to connect to the network
- Determines whether they are allowed to access the network
- Usually involves a challenge or challenges to the user
- The user supplies a response to each challenge
- If correct, they are authenticated

Authentication Methods

- Username and password
- Personal information
- PIN
- Biometrics
- Smart card

Encryption

- Involves changing the information into a form that can only be recognised by the sender and intended recipient
- If the signal is intercepted by a third party, it should be unintelligible.
- The message is manipulated using a cipher or encryption algorithm and deciphered at the receiving end.
- Encryption is a mathematical tool.

Private & Public Keys

- ***Private key encryption*** involves sender and receiver both having the key:
  - Need to distribute the key without unauthorised users having access to it
  - Repeated use of the same key makes it easier to crack.
- ***Public key encryption*** involves two keys:
  - The key used to encrypt is different from the key used to decrypt.
  - The encryption key is made public, hence the name

Digital Signatures - 1

- A digital signature provides assurance to the recipient of a digital document transmitted over a network that:
  - The document comes from the person that claims to have sent it
  - The contents have not been modified since it was sent

Digital Signatures - 2

- Closely related to ***digital certificates*** that are on the Internet
  - A Certificate Authority attests the origins of a website, piece of software, etc.

Using Digital Signatures

- A hashing function is used to create a mathematical summary of the document.
- Sender uses a private key to encrypt the summary
- Recipient calculates the same summary using the same hashing function
- Recipient uses the sender's public key to decrypt the signature
- If the summary calculated by the recipient matches the summary by decoding the signature, then the document is genuine

Virus Protection

- Software protects against viruses, trojans, etc.
- New viruses are continually being created.
- Battle to protect from new viruses **never** ends
- Virus writers, hackers etc. look to exploit vulnerabilities in:
  - Operating systems
  - Software
- Anti-virus software vendors are quick to create updates to match the attackers.

Using Virus Protection

- Install anti-virus software on all networked machines.
- Keep virus definitions up to date.
- Update all software, including operating systems, on networked machines to fix any security holes.
- Educate all users not to open files from non-trusted sources.

Physical Countermeasures

- Physically protecting the network by:
  - Choosing good quality hardware and equipment
  - Having well installed cabling
  - Install fire prevention and detection equipment
  - Keeping wiring & equipment closets locked
  - Preventing unauthorised access to building and rooms
  - Using CCTV etc.
- Have a data back-up and recovery procedure as well

The Security Policy

- Most large organisations have a security policy.
- Focuses attention on the importance of security
- Shows management backing
- Often includes key policies for users:
  - Acceptable use policy
  - Authorisation levels
  - Roles and responsibilities

Acceptable Use Policy

- A set of rules that lay out how the network may be used
- New users should be asked to sign their acceptance of the policy before being provided with network access
- Ideally, this should outline the sanctions on users who break the policy

Authorisation

- Authorisation is the function of specifying access rights to resources for authorised users
- A network should have a policy whereby users are granted access to resources based upon their grade, department, etc.
- This can be done in a number of ways, e.g.
  - Individually
  - Allocating user to a domain and allocating access rights to a domain

Roles and Responsibilities

- A security policy should allocate specific functions to specific job roles.
- Roles should be allocated in such a way that fraud is made difficult.
- Actual roles and responsibilities depend upon:
  - ***Function*** of the organisation
  - ***Size*** of the organisation

Business Continuity

- Network security should also include an analysis of the impact of network failure
- Provision should be made to deal with network failure
  - Mirrors of data and websites
  - Temporary switchboards
- A balance of cost against effects of network failure

Bringing British Education to You

www.nccedu.com

Computer Networks

Topic 8 – Lecture 3:

Security Software

Network Security Software

- Network security software covers many categories including:
  - Intrusion detection software
  - Antivirus software
  - Vulnerability scanners
  - Packet sniffers
  - Firewalls

Intrusion Detection Software (IDS)

- Such software prevents any suspicious software from intruding into a computer system

- Purpose is:
  - To identify possible threats
  - To prepare a report or log about the threats
  - To furnish this report to the security administrator
  - To attempt to stop any loss due to the threat

Antivirus Software

- Really should be called ***anti-malware***
- Prevents malicious software from attacking system
- Most use signatures of viruses that have been designed earlier
- Can prevent suspicious programs from taking control of the computer if they find code similar to code present in its virus directory
- Continuously update their virus database when a new code or virus appears on a network

Vulnerability Scanners

- Computer program that looks for weaknesses in:
  - Computers
  - Computer systems
  - Networks
  - Applications

- Purpose is to assess the vulnerabilities present in one or more targets

Packet Sniffers

- Software or hardware that can intercept and log traffic passing over a digital network or part of a network
- As data streams flow across the network, the sniffer captures each packet and can:
  - decode the packet's raw data
  - show the values of various fields in the packet
  - analyse a packet’s content according to the appropriate specifications.

Firewalls

- A firewall can be implemented both as hardware and software.
- It acts as a filter that permits authorised messages to and from a system whilst blocking unauthorised messages.
- We will examine firewalls in detail in the next topic.

Security Risks

- Threats that lead to a loss in any form to an individual or an organisation
- Such losses may include:
  - Loss of privacy
  - Identity theft
  - Financial loss
  - Negative impact on customer relations
  - Loss or damage of confidential data or information
  - Loss in profitability

Managing Security Risks

- This can be modelled as a three stage process:
  - Identify and analyse security risks
  - Risk assessment
  - Risk management
- Most security risk management systems are designed to comply with ***international standards***

Identify & Analyse Risks

- The purpose of risk identification and analysis is to understand the possible threats that can be used against any possible vulnerability in the security architecture of the organisation.
- Organisations often have multiple layers of security.
- Vulnerability scanners can be used for this purpose.

Risk Assessment

- Identifies problems
- Measures the likelihood of the security threat
- Measures the impact of a security threat
- A combination of ***probability*** of the threat and its ***impact*** determine how important each threat is to an organisation.

Risk Management

- Designing security measures against known and possible threats is time consuming and expensive.
- Most information security risk management systems are designed to comply with international standards.
- These attempt to build safe and sound information transfer methods and environments.
- Continuous updating of these systems makes them expensive and time consuming.

International Standards

- ISO/IEC 27001 Information Security
- Auditable international standard which defines the requirements for an ***Information Security Management System*** (ISMS)
- Designed to ensure the selection of adequate and proportionate security controls
- Helps to protect your information assets and give confidence to customers

Balancing Risks

- Every organisation needs to decide what level of security it needs
- The two extremes are:
  - Total security, difficult to use
  - Total access, not secure
- A policy needs to define how security will be enforced

Spam

- Blocking spam is one of the biggest challenges that organisations face.
- Studies suggest that over 90% of all email traffic is spam.
- Software filters can be deployed to limit the amount of spam.
- Hardware is available for this purpose, known as an anti spam appliance, and is usually operating system independent.

Small Business Security

- There are a number of security features that are ideal for a small to medium sized business:
  - A fairly strong firewall
  - Strong antivirus software and Internet Security Software
  - Use strong passwords and change on a monthly basis
  - When using a wireless connection, use a very strong password
  - Raise awareness about physical security to employees
  - Use tools to monitor the network traffic

College Security

- Extra features are ideal for colleges and schools:
  - A firewall that allows authorised users access from the outside and inside
  - Wireless connections that lead to firewalls
  - Compliance with laws and guidelines on Internet access for children
  - Supervision of network to guarantee updates
  - Constant supervision by teachers, librarians, and administrators to guarantee protection against attacks and also to supervise users

Security Software Vendors

- There are many
- Some software is free
- Some is expensive
- What does the college use?
- Is it the best available?

References

- Price B. (ed) (2003). *Networking Complete,* 3rd edition, Sybex.
- Tanenbaum, A.S. & Weatherall, D.J. (2010). *Computer Networks,* 5th edition, Pearson Education.
- International Organization for Standardization: http://www.iso.org

Topic 8 – Security Software

Any Questions?