Threats to computer systems and networks

1.4.1 · Computer systems (Paper 1) · revision notes

The main threats to computer systems and networks: malware, social engineering (including phishing), brute-force attacks, denial of service attacks, data interception and theft, and SQL injection. Questions ask you to identify an attack from a description, explain how it works and its purpose or effect, and discuss threats to an organisation in extended answers.

Key facts

- Malware = software designed to cause harm or gain unauthorised access
- Trojan: disguised as legitimate software. Ransomware: encrypts files, demands payment
- Brute-force attack = trying every possible password
- Data interception = capturing data in transit (e.g. packet sniffing)
- Virus: attaches to files, spreads when they are run. Worm: spreads by itself across networks
- Social engineering = tricking people: phishing, blagging, shouldering
- DoS = flooding a server so genuine users cannot use it; DDoS = from many computers
- SQL injection = SQL code entered into an input box and run by the database

Notes

Malware

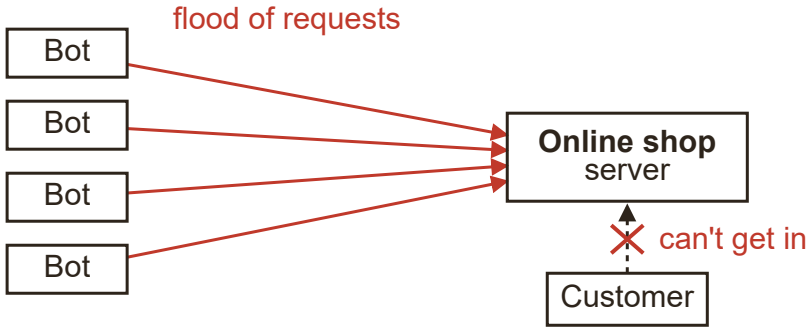
- **Malware** is software written to cause harm to a computer system or to gain unauthorised access to it.
- **Virus**: attaches itself to a file or program and spreads when the infected file is opened or run.
- **Worm**: copies itself and spreads across a network on its own, without the user opening anything.
- **Trojan**: pretends to be useful, legitimate software but secretly does something harmful.
- **Ransomware**: encrypts the victim's files and demands payment for the key. **Spyware** (e.g. a keylogger): secretly records what the user does and sends it to the attacker.

Social engineering

- **Social engineering** means manipulating **people** into giving away information or access. People are often the **weak point** in a system.
- **Phishing**: fake emails, texts or websites that pretend to be from a trusted organisation, to trick users into giving away login or bank details or clicking a harmful link.
- **Blagging**: inventing a believable story, e.g. phoning a worker and pretending to be from IT support to get their password. **Shouldering**: watching someone enter a PIN or password.

Attacks on systems and data

- **Brute-force attack**: automated software tries every possible password (trial and error) until the right one is found, to gain unauthorised access to an account or system.
- **Denial of service (DoS)**: flooding a server with so many requests that genuine users cannot access it. A **distributed** attack (DDoS) uses many computers, often a botnet of infected machines.



DDoS: a botnet floods the server with requests, so genuine users cannot get through

- **Data interception and theft**: data is captured as it travels across a network (e.g. using packet-sniffing software on public Wi-Fi), or stolen from storage or devices. The aim is to steal valuable data such as passwords, card details or personal information.
- **SQL injection**: an attacker types SQL code into an input box on a website. If the input is not checked, the database runs the code, which can reveal, change or delete data, or bypass a login.

How to answer each type of question

Identify the threat from a description 1 mark each **Grade 4**

1. Look for the key idea: 'tricks the user' = phishing or social engineering; 'every password' = brute force; 'floods' = DoS; 'types code into a form' = SQL injection.
2. For malware, look at how it spreads or what it does: attaches to files (virus), spreads by itself (worm), disguised (trojan), locks files for payment (ransomware).

Example. Identify the threat described in each case.
(a) A program copies itself to every computer on a network without anyone opening a file. [1]
(b) A text message pretends to be from a delivery company and asks the user to enter card details on a website. [1]
(c) Software tries millions of different passwords on a user's account. [1]

Model answer.

(a) Worm (1)
(b) Phishing (1)
(c) Brute-force attack (1)

Explain how an attack works and its effect

2 to 4 marks | Grade 5

1. Say what the attacker does.
2. Say what happens to the system or the person.
3. Finish with the effect on users or the organisation.

Example. Explain how a denial of service (DoS) attack would affect an online shop. [3]

Model answer. The attacker floods the shop's web server with a huge number of requests (1). The server becomes overloaded and cannot respond to them all (1), so genuine customers cannot use the website and the shop loses sales (1).

Explain the concept of SQL injection

2 to 3 marks | Grade 7

1. Say where it happens: an input box on a website, such as a login form.
2. Say what is entered: SQL code instead of normal data.
3. Say what happens: the input is not checked, so the database runs the code, revealing, changing or deleting data.

Example. A website's login page puts whatever the user types into this SQL statement:

```
SELECT * FROM Users WHERE Username = 'name' AND Password = 'pass'
```

Explain how an attacker could use SQL injection on this page. [3]

Model answer. The attacker types SQL code into the username or password box instead of normal data (1). The website adds the typed text straight into its SQL statement without checking it (1), so the database runs the attacker's code, e.g. a condition that is always true, which could log them in without a valid password or reveal other users' data (1).

8-mark: discuss the threats to an organisation

8 marks (marked in levels) **Grade 8**

1. Choose several different threats that fit the organisation.
2. For each, explain how it could happen there and what its impact would be.
3. Include the human weak point as well as technical attacks.
4. End with a judgement, e.g. which threat is the greatest risk and why.

Example. An online company sells concert tickets through its website. Customers create accounts and pay by card. Discuss the threats to the company's systems and the impact each could have. [8]

Model answer.

A denial of service attack could flood the website with requests when tickets for a popular concert go on sale, so genuine customers cannot buy tickets and the company loses sales and its reputation.

If the website's forms do not check their input, SQL injection could be used to reveal customers' names, addresses and account details from the database. A brute-force attack could break into customer accounts that have weak passwords.

Card details could be intercepted as they travel across the Internet if they are not encrypted. Staff are also a weak point: a phishing email could trick an employee into giving away their login, and ransomware in an email attachment could encrypt the company's files and stop ticket sales completely.

The impact goes beyond lost sales: a breach of customers' personal data breaks the Data Protection Act 2018, which could lead to a large fine, and customers may stop trusting the company.

Conclusion: attacks on the website (DoS and SQL injection) are the greatest risk, because the whole business depends on it.

Top band (6–8 marks): explains several different threats, how each could happen to this company and its impact, with a supported judgement.

Don’t lose marks

- Calling all malware a 'virus'. Name the correct type.
- Saying a DoS attack steals data. Its aim is to stop a service working.
- Describing phishing as hacking into a computer. It tricks a person.
- Saying SQL injection 'hacks the website'. Say that SQL code is entered into an input box and run by the database.

More tips

Memory tricks

- A Virus needs a Victim to open it; a Worm Wanders by itself; a Trojan Tricks you into installing it (like the wooden horse).
- Brute force is a burglar trying every key on a huge keyring, one after another.
- SQL injection = 'code in the box': whenever you see a web form and a database, think SQL injection.

Exam technique

- When asked to 'explain' a threat, give what happens AND its effect on the organisation.
- Use the scenario: a website with a login form points to SQL injection or brute force; an office full of staff points to phishing and shouldering.
- If the question also asks about prevention, pair each threat with a suitable method (see 1.4.2).

What each grade needs

What you need to be able to do, from the first marks up to the top grade.

Grade 3 — **Name the main threats to computer systems**
Malware, social engineering, brute-force attacks, denial of service, data interception and theft, SQL injection.

Grade 4 — **Identify an attack from a description**
E.g. flooding a server with requests so users cannot reach it is a denial of service attack.

Grade 5 — **Describe the main types of malware**
Virus, worm, trojan, ransomware and spyware, and how each one spreads or causes harm.

Grade 5 — **Explain how phishing and social engineering work**
They trick people into giving away information or access, by exploiting trust, fear or urgency.

Grade 6 — **Explain why people are the weak point**
People can be tricked, choose weak passwords or be careless, and technical defences cannot stop this.

Grade 7 — **Explain the concept of SQL injection**
SQL code typed into an input box is run by the database, e.g. to bypass a login or reveal data.

Grade 8 — **Discuss threats and their impact on organisations**
Explain how several attacks could happen to the organisation described and what their effects would be.

Free notes, Full packs, practice papers and mock exams at chhetriacademy.com. Written for this site; not taken from past papers. Stuck? 1-to-1 tutoring with a free 30-minute trial lesson.