

2.2 Physical Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____ **Total: 51 marks**

KEY WORDS piggybacking 尾随（获许可） • tailgating 尾随（未察觉）
• dumpster diving 翻垃圾搜集情报 • card cloning 门禁卡复制 • physical attacks 物理攻击

Objective

Build the skills to answer exam questions on **physical attacks** 物理攻击, physical vulnerabilities, and rating physical risk.

You must be able to:

- name and distinguish the five physical attacks, and say which use social engineering
- name the four kinds of compromise a physical vulnerability can cause
- explain what an adversary achieves with physical access to power, to a room, or to a device's ports
- explain why physical access defeats technical controls
- rate a physical risk high, moderate or low and justify it

1 Worked examples

Study these first. Each one shows the method for a task used later.

- The five physical attacks

Adversaries **often use social engineering** when conducting a physical attack - so several of these are the social-engineering tactics of topic 2.1, applied at a door.

Attack	What happens	Social engineering?
Piggybacking	the adversary manipulates an authorised person into granting them access - they are let in	yes - the person consents
Tailgating	the adversary follows close behind an authorised person through a door	no - the person does not know
Shoulder surfing	the adversary watches a user access sensitive information to use later	no - sometimes aided by a camera or binoculars
Dumpster diving	the adversary searches the target's physical trash for useful information	no
Card cloning	the adversary copies an authorised user's access card	no

Piggybacking versus tailgating is the most-tested pair, and the difference is consent. Piggybacking: “Could you hold the door? My badge is in my other coat.” Tailgating: the adversary simply walks through behind someone carrying boxes, unnoticed.

■ Threats, vulnerabilities and the four compromises

Threats include human adversaries **and natural disasters** - flood, fire, storm - which can physically damage or destroy assets. Do not omit the natural half; it is why a UPS and off-site backups appear as physical controls.

A **vulnerability** is a weakness or flaw that could let an asset be compromised. The four compromises to name:

- unauthorised access to sensitive data or restricted physical spaces
- disruption of services
- theft or destruction of digital or physical resources
- unauthorised modification of data

■ What physical access actually gets an adversary

The access	What follows
Power - damaging fuses, cutting a supply	the device and every service it provides become unavailable
A room holding sensitive information	information can be stolen or copied
A device and its ports	a keylogger or an external drive of malware can be plugged in

■ Why physical risk is rated so heavily

Physical access to a device allows an adversary to bypass many technical controls and layers of security. A firewall does not filter a person standing at the machine, and an access control model does not apply to somebody who has booted the machine another way.

Rating	When
High	sensitive information or systems are exposed in physical spaces that are not sufficiently restricted or monitored
Moderate	a non-critical, non-sensitive part of the organisation is unprotected in a way that could be exploited
Low	the vulnerable asset is of low value and the vulnerability is unlikely to be exploited

2 Practice

2.1 Name the physical attack in each case.

- (a) A visitor asks a staff member to hold the security door because their badge is “in the car”. [1]
- (b) Someone walks through a closing door behind an employee carrying boxes. [1]
- (c) A person photographs a receptionist’s screen from across the lobby. [1]
- (d) Discarded network diagrams are recovered from the bins behind the building. [1]
- (e) An access badge is copied while its owner queues for coffee. [1]

2.2 Explain the difference between **piggybacking** and **tailgating**. [2]

2.3 State the four kinds of compromise a physical vulnerability can cause. [4]

2.4 Explain why natural disasters count as threats in physical security. [2]

2.5 Describe what an adversary achieves in each case.

- (a) They damage the fuses supplying a server room. [2]
- (b) They reach an unattended workstation’s USB ports. [2]
- (c) They enter a filing room holding printed patient records. [2]

2.6 Explain why physical access to a device is so serious, referring to technical controls. [2]

2.7 Rate each risk and justify.

(a) A rack of unlocked servers holding customer financial records stands in an unmonitored corridor. [2]

(b) The staff bicycle shed has a broken lock. [2]

(c) A store room of blank stationery is left unlocked in a building with a staffed reception. [2]

3 Exam-style questions

3.1 An adversary persuades an employee to hold a secure door open for them. This is [1]

- **A** tailgating
- **B** piggybacking
- **C** shoulder surfing
- **D** card cloning

3.2 Dumpster diving is an attack in which an adversary [1]

- **A** copies an access card
- **B** follows an employee through a door
- **C** searches the target's physical trash for useful information
- **D** watches a user type a password

3.3 Physical access to a device is a high-severity risk mainly because it [1]

- **A** is difficult for an adversary to achieve
- **B** allows many technical controls and layers of security to be bypassed
- **C** always destroys the device
- **D** cannot be recorded in any log

3.4 A physical vulnerability is best rated **low** when [1]

- **A** the asset is valuable but the vulnerability is hard to exploit
- **B** the asset is of low value and the vulnerability is unlikely to be exploited
- **C** a non-critical area is left unprotected
- **D** sensitive systems are exposed in an unmonitored space

3.5 A city library runs a public computer area, a staff office reached through a door with a card reader, and a small comms cupboard off the public corridor whose door has been propped open with a chair “because it gets hot”. Staff print borrower records - names, addresses, and fine histories - and recycle drafts in an open bin by the photocopier. One member of staff has twice been asked by a well-dressed stranger to hold the office door.

(a) Identify **three** physical attacks this library is exposed to, naming the specific feature of the scenario that enables each. [6]

(b) Explain what an adversary could achieve inside the propped-open comms cupboard, naming **two** distinct compromises. [4]

(c) The library manager says the borrower drafts are “only paper, not a computer system”. Evaluate this. [3]

(d) Rate the library's overall physical risk and justify it against the criteria. [3]

(e) Recommend **three** controls, each addressing a different attack you named, and say which you would implement first and why. [4]

AP Cybersecurity • 2.2 Physical Vulnerabilities and Attacks

(b) an adversary in the comms cupboard has physical access to network devices and their ports. Two distinct compromises, any two: **disruption of services** by cutting power or unplugging equipment, making the library's systems unavailable; **unauthorised access**

by plugging into a data port or installing a rogue access point, giving a route onto the internal network; **theft or destruction** of the equipment itself. Maximum 4.

(c) The reasoning is **wrong**. The compromise defined by the course is unauthorised access to **sensitive data**, and the format of that data is irrelevant - names, addresses and fine histories are personal data whether printed or stored. Dumpster diving is a named attack precisely because paper is often the easiest route to information that is well protected digitally, and it needs no technical skill at all.

(d) **High**. Sensitive borrower information is exposed in physical spaces that are not sufficiently restricted or monitored - the open recycling bin, the visible screens; and the propped comms cupboard gives physical access to network equipment in a public corridor, which bypasses whatever technical controls the library has.

(e) Three controls, each on a different attack: a shredder or locked confidential-waste bin for borrower drafts; a self-closing lock and ventilation fix so the comms cupboard cannot be propped; an access control vestibule or turnstile, plus security-awareness training so staff are equipped to refuse the door request; privacy screens or repositioned monitors. First: **secure the comms cupboard**, because physical access to network equipment bypasses every technical control at once and the door is currently open to the public. Accept the confidential-waste bin as first if justified by the ongoing, certain exposure of personal data.