

Security Principles

tryhackme.com/room/securityprinciples

Room progress (66%)

5. **Preparing for Error and Exception Handling:** Whenever we build a system, we should take into account that error application, a customer might try to place an order for an out-of-stock item. A database might get overloaded and the systems should be designed to fail safe; for example, if a firewall crashes, it should block all traffic instead of allowing all traffic. Moreover, we should be careful that error messages don't leak information that we consider confidential, such as dumping memory content that contains information related to other customers.

Woop woopl! Your answer is correct

In the following questions, refer to the ISO/IEC 19249 five design principles above. Answer with a number between 1 and 5, depending on the number of the design principle.

Answer the questions below

Which principle are you applying when you turn off an insecure server that is not critical to the business?

2

Correct Answer

Your company hired a new sales representative. Which principle are they applying when they tell you to give them access only to the company products and prices?

1

Correct Answer

While reading the code of an ATM, you noticed a huge chunk of code to handle unexpected situations such as network disconnection and power failure. Which principle are they applying?

5

Correct Answer

Task 7 Zero Trust versus Trust but Verify

tryhackme.com/room/securityprinciples

Room progress (75%)

and intrusion prevention systems.

Woop woopl! Your answer is correct

Zero Trust: This principle treats trust as a vulnerability, and consequently, it caters to insider-related threats. After considering trust as a vulnerability, zero trust tries to eliminate it. It is teaching indirectly, "never trust, always verify." In other words, every entity is considered adversarial until proven otherwise. Zero trust does not grant trust to a device based on its location or ownership. This approach contrasts with older models that would trust internal networks or enterprise-owned devices. Authentication and authorization are required before accessing any resource. As a result, if any breach occurs, the damage would be more contained if a zero trust architecture had been implemented.

Microsegmentation is one of the implementations used for Zero Trust. It refers to the design where a network segment can be as small as a single host. Moreover, communication between segments requires authentication, access control list checks, and other security requirements.

There is a limit to how much we can apply zero trust without negatively impacting a business; however, this does not mean that we should not apply it as long as it is feasible.

Answer the questions below

Make sure you have read the above.

No answer needed

Correct Answer

Task 8 Threat versus Risk

9 Conclusion

tryhackme.com/room/securityprinciples

Room progress (83%)

Sign in

Woop woopl! Your answer is correct

There are three terms that we need to take note of to avoid any confusion.

- **Vulnerability:** Vulnerable means susceptible to attack or damage. In information security, a vulnerability is a weakness.
- **Threat:** A threat is a potential danger associated with this weakness or vulnerability.
- **Risk:** The risk is concerned with the likelihood of a threat actor exploiting a vulnerability and the consequent impact on the business.

Away from information systems, a showroom with doors and windows made of standard glass suffers a weakness, or *vulnerability*, due to the nature of glass. Consequently, there is a *threat* that the glass doors and windows can be broken. The showroom owners should contemplate the *risk*, i.e. the likelihood that a glass door or window gets broken and the resulting impact on the business.

Consider another example directly related to information systems. You work for a hospital that uses a particular database system to store all the medical records. One day, you are following the latest security news, and you learn that the used database system is not only vulnerable but also a proof-of-concept working exploit code has been released; the released exploit code indicates that the threat is real. With this knowledge, you must consider the resulting risk and decide the next steps.

We will cover threats and risks in detail in a separate room.

Answer the questions below

Make sure you have read the above.

No answer needed

✓ Correct Answer

tryhackme.com/room/securityprinciples

Room progress (91%)

Sign in

Woop woopl! Your answer is correct

Finally, the Shared Responsibility Model is worth mentioning, especially with the increased reliance on cloud services. Various aspects are required to ensure proper security. They include hardware, network infrastructure, operating systems, applications, etc. However, customers using cloud services have different access levels depending on the cloud services they use. For example, an Infrastructure as a Service (IaaS) user has complete control (and responsibility) over the operating system.

On the other hand, a Software as a Service (SaaS) user has no direct access to the underlying operating system. Consequently, achieving security in a cloud environment necessitates both the cloud service provider and the user to do their parts. The Shared Responsibility Model is a cloud security framework to ensure that each party is aware of its responsibility.

Having finished the Security Principles room, you may proceed to the Intro to Cryptography room.

Answer the questions below

Make sure you have taken notes of all the key terms and acronyms we covered in this room.

No answer needed

✓ Correct Answer

How likely are you to recommend this room to others?

12345678910

Submit now

 tryhackme.com/room/securityprinciples







You did it! 🇬🇧 Security Principles complete!

Points earned

🔥 56

Completed tasks

📋 9

Room type

👤 Walkthrough


Difficulty


📶 Easv


Streak

🔥 12

 81,327 users are actively learning this week

 tryhackme.com/room/securityprinciples





Room completed (100%)

Finally, the Shared Responsibility Model is worth mentioning, especially with the increased reliance on cloud services. Various aspects are required to ensure proper security. They include hardware, network infrastructure, operating systems, applications, etc. However, customers using cloud services have different access levels depending on the cloud services they use. For example, an Infrastructure as a Service (IaaS) user has complete control (and responsibility) over the operating system.

On the other hand, a Software as a Service (SaaS) user has no direct access to the underlying operating system. Consequently, achieving security in a cloud environment necessitates both the cloud service provider and the user to do their parts. The Shared Responsibility Model is a cloud security framework to ensure that each party is aware of its responsibility.


Having finished the Security Principles room, you may proceed to the Intro to Cryptography room.

Answer the questions below


Make sure you have taken notes of all the key terms and acronyms we covered in this room.

No answer needed

✓ Correct Answer

 Thank you!

Your feedback helps us improve our content! We appreciate the time you took to share your thoughts!



✓ Close

tryhackme.com/room/securityprinciples


Sign in

TryHackMe

DashboardLearnPracticeCompete

Go Premium11

Cyber Security 101 > Build Your Cyber Security Career > Security Principles



Security Principles


Learn about the security triad and common security models and principles.

90 min1,86,597

Save Room

3974 Recommend

Options



Room progress (0%)

Task 1 Introduction

Security has become a buzzword; every company wants to claim its product or service is secure. But is it?

Before we start discussing the different security principles, it is vital to know the adversary against whom we are protecting our assets. Are you trying to stop a toddler from accessing your laptop? Or are you trying to protect a laptop that contains technical designs worth millions of dollars? Using the exact protection mechanisms against toddlers and industrial espionage actors would be ludicrous. Consequently, knowing our adversary is a must so we can learn about their attacks and start implementing appropriate security controls.

tryhackme.com/room/securityprinciples

Sign in

TryHackMe

DashboardLearnPracticeCompete

Go Premium12

Room progress (0%)

Woop woopl Your answer is correct

No answer needed


Correct Answer

Task 2 CIA

12Your streak has increased! You're closer to your next badge of 30 days. Keep up the amazing work!

tryhackme.com/room/securityprinciples

Room progress (8%)



Before we can describe something as *secure*, we need to consider better what makes up security. When you want to judge the security of a system, you need to think in terms of the security triad: confidentiality, integrity, and availability (CIA).

- **Confidentiality** ensures that only the intended persons or recipients can access the data.
- **Integrity** aims to ensure that the data cannot be altered; moreover, we can detect any alteration if it occurs.
- **Availability** aims to ensure that the system or service is available when needed.

Me

Time: 00s Question: 1/5

You went to cash out a cheque, and the bank teller made you wait for five minutes as they

Instructions

In security principle, choose options for safeguarding information. Ensure confidentiality, integrity, and system availability.

Continue

Confidentiality Integrity Availability

C I A

Security Principles 1

tryhackme.com/room/securityprinciples

Room progress (8%)

3. Integrity
4. Authenticity
5. Confidentiality
6. Possession

We have already covered four of the above six elements. Let's discuss the remaining two elements:

- **Utility:** Utility focuses on the usefulness of the information. For instance, a user might have lost the decryption key to access a laptop with encrypted storage. Although the user still has the laptop with its disk(s) intact, they cannot access them. In other words, although still available, the information is in a form that is not useful, i.e., of no utility.
- **Possession:** This security element requires that we protect the information from unauthorized taking, copying, or controlling. For instance, an adversary might take a backup drive, meaning we lose possession of the information as long as they have the drive. Alternatively, the adversary might succeed in encrypting our data using ransomware; this also leads to the loss of possession of the data.

Answer the questions below

Click on "View Site" and answer the five questions. What is the flag that you obtained at the end?

THM{CIA_TRIAD}

✓ Correct Answer

Hint

Woop woopl Your answer is correct

Task 3 DAD

Task 4 Fundamental Concepts of Security Models

tryhackme.com/room/securityprinciples

Room progress (25%)

be able to function properly. They can go back to paper temporarily; however, the patient records won't be available

Protecting against disclosure, alteration, and destruction/denial is of utter significance. This protection is equivalent to w

Protecting confidentiality and integrity to an extreme can restrict availability, and increasing availability to an extreme can result in losing confidentiality and integrity. Good security principles implementation requires a balance between the three.

Answer the questions below

The attacker managed to gain access to customer records and dumped them online. What is this attack?

Disclosure

✓ Correct Answer

A group of attackers were able to locate both the main and the backup power supply systems and switch them off. As a result, the whole network was shut down. What is this attack?

Destruction/Denial

✓ Correct Answer

Task 4 ○ Fundamental Concepts of Security Models

Task 5 ○ Defence-in-Depth

Task 6 ○ ISO/IEC 15546

tryhackme.com/room/securityprinciples

Room progress (33%)

Sign in

We covered only three security models. The reader can explore many additional security models. Examples include:

- Brewer and Nash model
- Goguen-Meseguer model
- Sutherland model
- Graham-Denning model
- Harrison-Ruzzo-Ullman model

Answer the questions below

Click on "View Site" and answer the four questions. What is the flag that you obtained at the end?

THM{SECURITY_MODELS}

✓ Correct Answer

Task 5

Defence-in-Depth

Task 6


ISO/IEC 19249

Zero Trust versus Trust but Verify

tryhackme.com/room/securityprinciples

Room progress (41%)

Sign in



Defence-in-Depth refers to creating a security system of multiple levels; hence it is also called Multi-Level Security.

Consider the following analogy: you have a locked drawer where you keep your important documents and pricey stuff. The drawer is locked; however, do you want this drawer lock to be the only thing standing between a thief and your expensive items? If we think of multi-level security, we would prefer that the drawer be locked, the relevant room be locked, the main door of the apartment be locked, the building gate be locked, and you might even want to throw in a few security cameras along the way. Although these multiple levels of security cannot stop every thief, they would block most of them and slow down the others.

Answer the questions below

Make sure you have read the above.

No answer needed

✓ Correct Answer

Task 6

ISO/IEC 19249