Security Overview

1. Define computer security.

Computer security is the practice of protecting computer systems, networks, and data from unauthorised access, damage, theft, or disruption, while ensuring the confidentiality, integrity, and availability of information.

2. Can you explain the CIA triad using examples?

The CIA triad stands for Confidentiality, Integrity, and Availability:

- Confidentiality: Ensuring that information is only accessible to authorised users. For example, encrypting sensitive customer data to prevent unauthorised access.
- Integrity: Maintaining the accuracy and trustworthiness of data. For example, using checksums to detect data tampering during transmission.
- Availability: Ensuring that data and systems are available and accessible when needed. For example, implementing redundancy in server infrastructure to minimise downtime.

3. What are the additional two security goals?

The additional two security goals are Accountability and Auditability.

- Accountability: Holding individuals or entities responsible for their actions in the system. For example, logging user activities and actions to trace any unauthorised activities back to specific users.
- Auditability: The ability to review and analyse system activities and events to ensure compliance with security policies. For example, generating audit logs that can be reviewed for security breaches.

4. Define the relationships between basic security concepts.

The relationships between basic security concepts are as follows:

- Assets are protected by safeguarding against vulnerabilities.
- Vulnerabilities are exploited by threat agents, leading to threats.
- Threats, when realised, can result in attacks.
- Attacks can lead to security incidents or breaches.
- Countermeasures are implemented to prevent, detect, or respond to attacks and reduce risk.

5. List and briefly define categories of passive and active network security attacks.

Categories of passive network security attacks include:

- **Release of Message Contents: Attackers eavesdrop on and read unencrypted messages.**
- **Traffic Analysis: Attackers observe patterns in encrypted or unencrypted traffic to deduce content.**

Categories of active network security attacks include:

- **Replay Attack: Attackers capture a valid transmission and retransmit it to gain unauthorised access.**
- **Masquerade: Attackers pretend to be a different entity to gain unauthorised access.**
- **Modification of Messages: Attackers alter messages during transmission.**
- **Denial of Service (DoS): Attackers disrupt normal system operation, making services unavailable.**

6. List and briefly define the fundamental security design principles.

Fundamental security design principles include:

- **Economy of Mechanism: Security mechanisms should be as simple as possible.**
- **Fail-Safe Defaults: Access decisions should be based on permission rather than exclusion.**
- **Complete Mediation: Every access to an object should be checked to ensure permission.**
- **Open Design: Security should not depend on the secrecy of design or implementation.**
- **Separation of Privilege: Multiple privilege attributes are required to access restricted resources.**
- **Least Privilege: Entities should have the least set of privileges necessary to perform tasks.**
- **Least Common Mechanism: Mechanisms for accessing resources should not be shared.**
- **Psychological Acceptability: Security mechanisms should not unduly interfere with user work.**
- **Isolation: Public access, processes, and security mechanisms should be isolated from each other.**
- **Layering: Multiple layers of security should be used to provide defence in depth.**
- **Encapsulation: Internal structure of a system should be hidden.**
- **Modularity: Security functions should be developed as separate modules.**
- **Least Astonishment: Programs should respond in ways least likely to surprise users.**

7. What is an attack surface?

An attack surface consists of the reachable and exploitable vulnerabilities in a system. It encompasses the weaknesses and entry points that an attacker could target to compromise the security of the system.

8. What is a computer security strategy?

A computer security strategy is a comprehensive plan designed to achieve specific security goals and protect an organisation's information assets. It includes defining security policies, implementing security measures, ensuring assurance, and evaluating the effectiveness of security controls.

9. What are the four complementary courses of action in security implementation?

The four complementary courses of action in security implementation are Prevention, Detection, Response, and Recovery:

- Prevention: Measures and controls that aim to prevent security incidents and attacks from occurring in the first place.
- Detection: Techniques and systems that identify and alert on security incidents as they happen or shortly after.
- Response: Actions taken to address and mitigate the impact of a security incident once detected.
- Recovery: Steps and processes to restore systems and data to normal operation after a security incident or disaster.

COSC362 - Week 1 - Lecture 02 - Security Overview

Tue, Jul 25, 2023 11:49AM • 55:01

SUMMARY KEYWORDS

attack, system, security, talk, attacker, vulnerability, lecture, data, information, threat, confidentiality, password, access, countermeasures, encryption, security policy, means, message, integrity, entity

00:05

All right, I think we'll just add to that sharp 11 again. So cura everyone, welcome to the second class of cost 362 eyes. So I just want to make an announcement before we start. So I got two students who volunteer to be the class rep for this. So I will put the information on to learn after this lecture. So you should be able to contact them from next week. All right. So. So on Tuesday, we talk about the cost structure. We also discussed why cybersecurity is important, and what you can do in cyber. So this lecture, we're gonna give you an overview of what is computer security, and some fundamental concepts in computer security or cybersecurity. So basically, up to this lecture, you should be able to understand some fundamental computer security concepts. And you will be able to discuss different type of security threats and tax, and also the essence, and how they must be dealt with and give some examples of those attacks and threats and SSH. And then we'll talk about some security functional requirements, and followed by the fundamental security design principles. And we'll also talk about attack surfaces. And we'll finally lay out a cybersecurity strategy. Alright, so let's get started. Um, first of all, what is computer security. And so there is an organization is called NIST. So nice represents the National Institute of Standards and Technology is an agency of the United States Department of Commerce. And its mission is to create critical measurement solutions, and also standards, and also promote innovation. So this institution has published a lot of standards and frameworks. And so they have a computer security handbook, it has a definition for computer security. So by definition, computer security is the protection afforded to an automated information system in order to attain the objectives, or preserving the integrity, availability and confidentiality of information system resources. And this resources include all the aspects, including hardware, software, firmware, and data and also telecommunication systems. So here, we're going to extract this three objectives. And we often refer this objectives as CIA triad. So that represents confidentiality, integrity, and availability. So we're going to dive into it. So what is confidentiality? It has two aspects, explained in the textbook. So the first aspect is the data confidentiality. So it assures that confidential information is not disclosed to unauthorized individuals. And there is another aspect, which is privacy, but just from my understanding, I think is a slightly different from confidentiality, so I'll explain it later. But now, the definition of privacy is to assure that individuals control or influence what information related to them may be collected, and stored, and by whom and to whom that information may be disclosed. So you can see the difference here. So data confidentiality, or just confidentiality in general, from my perspective, concern about the data itself, so you just need to keep the data secure. But privacy is, is a broader concept. And it

concerns about the people here. So when you have a data breach, when we say it's a violation of confidentiality, so usually it means that your data is disclosed to an also rise individuals, but just the data itself. But when when we talk about a privacy breach, and is often more than that. So it's occurs when the organization or the individual, either intentionally or accidentally provide an authorized or accidental access to someone's personal information. This is the first dimension and or they just close or alter or lose or destroys someone's personal information. And third dimension is they can also occur if someone is unable to access their personal information due to various reasons it could be their account being hacked. So you can say privacy here is, is a broader concept and is, is fundamentally has some fundamental difference compared with confidentiality. So I think I put the call out the definition here, because a textbook has this two aspect and a confidentiality. But I think later on in this course, when we talk about confidentiality is often just refers to the data confidentiality. All right. Second one is integrity. It has two aspects. One is data integrity, which means it assures that information and programs are changed only in the specified and authorized manner. And the second aspect is system integrity, so ensures the system itself performs its operations as intended. So it's free from deliberate. And, and also Ries manipulation of the system. So once focus on the data and the program, another focus on the system. And last one is availability. So that assures the system works properly, or as attend, as intended, and the service is not denied to authorized users. Alright, so that's the definition. Let's see some examples to help you better understand this. Alright, so the first example is about data confidentiality. Assuming we have Alice, who lives in South Island, and we have Bob who lives in North Island, and they want to communicate with each other. So the internet, right, and then they want to share a secret between each other. Okay, and then we assume that there's also an attacker who is doing eavesdropping. So which means they just monitor the line between these two entities. And the attacker tries to to get the information. They want to know what is the secret about All right, so. So confidentiality means that you have the data that is churned between the parties has not been viewed by a third party, which in this case is the attacker here. Right? So that's the confidentiality. And often, how can you ensure confidentiality, you just use encryption. We'll talk about it in next week's lecture. But so that's the general idea. So I want to introduce just a simple example, as it's called Caesar cipher is one of the oldest cryptography Messrs I so it's a substitution cipher is basically just means you shape the letters. And so you can see we have this is a mechanical tool, and it's called the cipher desk. Um, it has two dials here. So the inner desk, and the outer desk. So if you rotate the desk, and you will be able to, to use the inner disk as a reference for the plane tax. And the outer disk is used for the coded letters. Let's see here. So I got the screenshot. And it has this left shift, you can see, so the outer disk is left shifted by to position here. And we can see the secret here is the total because usually, that party will not know that how much position how many positions you have shipped, they don't know the offset, right. Okay, so here is actually two. And if we have the secret, which is secret, and then you use the inner disk as the plain tags. And then you will find the coda letters in the outer disk. So here as well correspond to U and E will correspond to G, right? So if you just do this, and our message sacred, while being coded as the sequence of letters, we'll talk about this in detail in next week's lecture, but this just gives you an example of like generally how cryptography works. All right, so let's move on. To the next example, which is data integrity.

10:06

So same here we have Alice and Bob, and they want to communicate with each other. And they want to send a message to each other, and they love this course. All right, and now we have an attacker. So

the attacker want to modify the message, right? So that's a violation of integrity, they just want to alter the message and attended to I hate this course. Alright, so, in this case, data has has been modified in transit. And so as violates integrity, so integrity means that data has not been modified, all right. I is not only interested but just in this example is in transit is also means when the data is stored is at rest or is displayed, it should not be modified in any unauthorized way. And how can we achieve integrity so one way is to have this message or DDoS indication through a hash function. So also talk about this in the next in week three lecture, but just give you had up. So if you have a message here, and you pass it on to the hash function, the hash function will generate a value for you, which is fixed size, and you append this value to the message. And you'll send both the message and value to the, to the sender, and a to the receiver, and the receiver will compute the value by himself. And then it will compare the computed value with the value that is appended to the message and to see whether they're the same or not, because this value is computed based on the message. So if the message has been trained, the value will change. Right. So that's how you do this message authentication. Alright, so next example is availability. I also have Alice and Bob, and they want to communicate, and now the attacker has a different focus. So the attacker wants to do the denial of service, they don't want them to communicate at all. All right, so how can they do that? Often, you will just launch this distributed denial of service attack, where you control many computers in the, in the in the network or on the internet. And they often they're often called bots. And they use this boss to send a lot of traffic to flood the target network. And here you can see, okay, so if they do that, the internet may be down and then they will not be able to communicate. And as I said, this is often called a DDoS attack. So in this case, what is availability is for any information system to serve its purpose. So the information must be available when it's needed. And DDoS attack can happen on different layers in the OSI model. So if you forget what is OSI model, is represents Open Systems Interconnection. It's just a model to represent a universal language for the computers to talk to each other. Alright, so it has seven layers, if you see recall, and sorry, eight or seven layers, and I saw the DDoS attack can happen on these four layers. Usually they will happen in this four layers, like in the application layer, they can do HTTP flooding attack. And on the presentation layer, they could do SSL abuse and transport layer, they could do a SYN floods, and then network layer that could be UDP reflection attacks, but we'll talk about all of them in the lecture about a DoS attacks. So now just give you a heads up, okay. So that's the definition of the CIA. So hopefully remember them. They represent confidentiality, integrity, and availability. We'll have a quiz later on. So make sure you remember them. And so this, the use of the CIA triad, is well established. But as you know, that the cyber landscape is evolving. So some people in the security field saying is not enough to have just the three security objectives. So to introduce additional security goals. So the first one is authenticity. So authenticity is means that being genuine being able to be verified, and trusted and You have confidence in the validity of a transmission or a message, or the message originator, the mesh is the message sender, you can also verify the uses are, who they claim they are. And also each input arriving at the system came from a trusted source. So, let's see an example. Okay, so some of you may have heard of deep fakes, or you may have seen the videos online about just AI generated videos. So you might have seen this before. So this is the CEO of metta, and the former Facebook company. So this is Mark Zuckerberg, and he in this video, he was bragging about having total control of billions of people's stolen data, which is completely false, right. So basically, deep fakes are this synthetic media, and they use AI tools to generate a completely new video. And which portray something that actually did not happen in the reality. So and the main machine learning method used often in generating this videos are called generative neural networks. That could be auto encoders, or, or generative

adversarial networks and often referred to as guns. Alright, so if you're interested in deep fakes, you can check the source here, I just got this from, from a online source. So deep fake, can be used to generate this videos. And usually, they are used to mislead the public by spreading this false information. But they can also have malicious purpose. So when I searched deep fake attacks, or like some incidents, I found this news. So an attacker created this voice deep fake. And he used this voice deep fake to scam a CEO of a company. And then, because the CEO of this company did not recognize the voice, is actually the voice of his boss. And he didn't recognize Oh, it's actually not his boss. So he just transferred money to the attacker. So this is the example of identity theft, and it caused a huge financial loss to the company. So yeah, so this is a quite an issue now. And they have several ways to detect this fake a fake video. So if you're interested, you can check it online, how to actually identify this AI generated videos. But that's an example of authenticity. And this happens in the real world. And next one is accountability. So this is the security goal, that generates the requirement for actions of an entity to be traced uniquely to that entity. This means that systems should keep records of their activities. This can help them to permit later forensic analysis to extract evidences of like traces of the attacker, or aid in transaction disputes. So usually, we, it's very hard to build a completely secure system. So that's why we must be able to trace a security breach to a responsible entity. And I also have an example here. So in the cyber world, some companies are doing this cyber strike, attribution. This is basically just to, to find the sources of the attacks, and to find the threat actors that should hold accountability for those attacks. And this is an anti virus company that built this platform, which is to take samples of the of the attacks, and then put into their engine and then we'll be able to identify different categories of the attacks. So that's the general idea of the attribution is to attribute the malicious acts and to be able to punish those malicious threat actors. Alright, so those are the additional two security goals. So now we're gonna move on to some In computer security terminology.

20:06

So first one, we're going to use this terminology across the course. So is better to have a good understanding of them. So the first one is system resource. And we talked about it in the definition before is also can be called asset is enclosed data service or system capability, System equipment, including all the system component like hardware, firmware, software, etc. And also the any facilities that the company use. And then vulnerability, so we're actually going to talk about it quite a lot. So a vulnerability is the flow, or a weakness in a systems design implementation or operation or management that could be exploited by the attacker, and could violate this the system's security policies or violate the, I'm the system's security objectives. So I also have an example here. So sulfur vulnerability is very common vulnerability that can be exploited by the criminals. And often you will need to apply patches to your system. So if you have your mobile phone, you have your laptop, if they ask you to upgrade to apply patches, you probably should do that. Because that's not only about upgrading your, you know, features of your of your systems, also to apply security patches, if there are any loopholes, security holes in your system, and they will use this updates to fix those vulnerabilities. Alright, so next one is security policy. And that just means a set of the rules and practices that specify or regulate how a system organization provides security services, to protect their sensitive data and to protect their systems. I also have an example here, because usually for a company, they would have security policies, which is kind of overarching policy. And they include high level statements to define the organization's security objectives, the goals and requirements. And underneath it, you will have some standards, you can have network security standards, you can have information classification

standard, you can have secure software development standard, and that will always support your policy. And also underneath standard, you also have procedures. So those are step by step instructions on how to carry out a specific task process. And that defines the guidance on how to implement those standards and policies. So there are often like kind of sweet layers here. Alright, so next one, adverse rate or a threat, agent or attacker. So it's often just the entity that tried to attack or is a threat to the system. And threat is a potential for a violation of Security, which exists when there is a circumstance or an a capability or an event that that could breach security and can cause harm. So basically, a sweat, it's a, it's a possible danger that just exist, and that might exploit a vulnerability. And then we have attack. So it's an action or it's an assault on the system security, and often derives from intelligence threat. And it's a deliberate attempt to evade security services and to violate security objectives or prop the policies of a system countermeasure. So when you have an attack, we have an vulnerability and you need to be able to respond to that. So all you need to be able to prevent that. So countermeasure is an action or a device or procedure or technique that reduces read or vulnerability or an attack by either just remove them, removing them or preventing it from happening, or by minimizing the haunting costs, or by discovering and reporting it. And last one is risk. So it's an expectation of loss, expressed as the probability that a particular threat will exploit a vulnerability was a harmful result. All right, so those are all the terminologies and now we're going to see how they are related to each other. Alright, so assuming you are the owner of it, company, you're a CEO of the company, and then you have assets in your company, right. And that could include all different sorts of the resources in your company and you value those assets, you want to protect them. And often the assets will have vulnerabilities and Kobe, just silver runnability, it could be hard work with the people in your company. So you're concerned about this vulnerabilities of the resources or the assets you have. And then you have threat agents. So they try to make any damage, right, or try to abuse try to break into your system to have any harmful results. All right, and then and usually, threat agent will exploit the vulnerability in order to do any damage. And when does happen, so when the threat agent can give rise to the threats to the assets, and then that might increase risk to the assets. And then the owner wants to reduce this risk. So what they can do is they can impose countermeasures to reduce the risk. And those countermeasures are probably defined from the security policy and also their supporting standards, they will just follow that and to protect their system. And the missing part is attack here. So the attack is the thread that is being carried out. And that leads to the violation of the different security objectives. Okay, so in terms of threat agents, that could be a hacker just have some malicious intent, or could be maleeh criminal groups, or it could be insiders that could be disgruntled employees in your company. And that could be terrorists or nation states. And then for the threads. As I said, So threads just exist there. And it could be any malware attacks, or denial of service attacks. So here, Microsoft Haere proposes stride model edges used to, to identify different security issues or threats in the security development lifecycle. So when you design a software or system, you can use this model tool to identify and to mitigate the threats. So if you're interested in that, you could have a look at what are the threats are included in the Microsoft threat model, and it has been widely used and different companies, and when they introduce a new project, so we'll just use the threat modeling to to do some analysis is quite useful to all Alright, so those are the relationships, and I let to further talk about the risk, because you can see that risk is actually the product of three factors. So you have the asset, right, and then the asset has vulnerabilities. And then you have a threat, which is a potential danger. And that can exploit the vulnerability exist on the asset. And then in this case, you would have a risk and being a risk does not mean that being attacked because you may have some countermeasures, and then to prevent the

attack from happening or just to mitigate the impact of the attack. And I have an example here. So let's say you have the your company doesn't have does not have a password policy. It doesn't require you to create a password with certain complexity. So the the administrator so the users in company just create weak passwords like 123456 which is really bad and and then you have threat. So there are different you know, password cracking attacks, they could use dictionary Sir, they could use brute force attack to crack your passwords. So that's the threat here. And if and the risk here is the cyber criminals will gain and authorized access to the sensitive information if they can crack the password of a administrator account so they should be able to they might be able to actually access all the systems in your company.

29:54
And if you don't have any countermeasure this the attack i and may happen, right? But if you ask the employees to create a strong password, or you use multi factor authentication, when they authenticate themselves to the system, then this risk can be reduced. Alright, so those are the relationships of this. No key elements here. Yeah,

30:23
I recently read somewhere that changing sort of passwords from like 12345, to something like has a lot of different characters isn't actually super effective, because it's my advice on my actual encryption of the passwords themselves, because I suppose it'll be a bit better than like brute force, in case something brute forcing it, but in the event that somebody's just breaking encryption, is that sort of, would that really not matter that much?

30:47
Sorry, can you repeat that, like, so? Changing the password?

30:50
Yeah, cuz your countermeasures, create strong passwords, and I assume that will be better. You know, the hackers wouldn't be able to be able to brute force it as easily, but they just write the encryption that sort of throws that entire concept out the windows or not.

31:05
Right? Um, yeah, so training the passwords is not the best way. But it's one way to kind of reduce this kind of attacks that the attacker will be crack your password. So you still want to use a complex password that we'll use. That will take them longer time. But usually the system have this, you know, the number of the limitations, you can try the passwords, and is often three times for company. So they wouldn't actually be able to launch any brute force attack or dictionary search because you have this limitations there. And also if you apply other countermeasures, so just overall, you should be able to reduce the the possibility of attack, but not just, you know, one countermeasure will help you to do to achieve that goal.

31:52
Okay, so So the product of multiple countermeasures.

31:55

Yes, definitely. Yeah. All right. Good question. All right. Any questions so far? All right. Okay, let's continue. So there are a lot of network security attacks. So that's why we just try to categorize them in terms of this network attacks. So there are passive attacks, which means that the attacker just tried to learn something from your system, or just try to make use of the information. And often they just eavesdrop or they just monitor your system. So there are two types. One is release of the message contents. If you don't have encryption, and you just send plant tags to each other, then the attacker will be able to just guess what is there. So the technique here could be just encrypt your message. And another type is traffic analysis. So this means that even if you have encryption, the attacker can still use some tools to observe the patterns of this messages. So they can still kind of deduce the content of the message. And they also have active attack, which means the attacker tries to just alter the system resources, or fact their operation. And there are four categories here. So one is replay attack, where the attacker just capture a valid transmission, just retransmitted. And then we also have Masquerade. So that is to what entity pretend to be another entity at modification, messages, we already talked about it. And just to modify the message, some portion of it didn't have a service, that's just to prevent the normal use or management of any systems or facilities. And then the attack can be also categorized by on the origin of the attackers, it could be initiated by the entity inside of the security perimeter. That's what I said it could be just a disgruntled employee. Or it could be initiated from outside the perimeter, there'll be an external attack. So the first category is based on the actions. The second category is based on the origin of the attack. All right, security functional requirements. So so nice, as I said, has a lot of standards and they have published something about security functional requirements, and there are 17 of them. So I don't expect you to remember all of them just in this lecture. So we'll use it as a reference page basically. So because in this class, you will learn different technical measures. We may also touch on some management controls and procedures like a risk assessment. So after this course At the end of the semester, we'll go back here and to see how many controls and measures we have learned. But now we'll just use it as a reference page. Okay, so fundamental security design principles. All right. So this principles are used to guide the development of protection mechanisms, and there are 13 of them. And so we'll just quickly talk about it one by one, and then we'll have a quiz to test your knowledge on that. So, first one is economy of McCarthyism is about security mechanism should be as simple as possible, because the more complex system is the more vulnerability you introduce. And then simple system is also simple systems also easy to test and validate. Secondly, failsafe defaults. So, that means access decisions should be based on permission rather than exclusion. And that's how most file system works here, they have access controllers, and they just grant you access based on your role. And then complete mediation that means every access to the object should be checked to ensure they are allowed. So, this means that you should validate the access rights whenever there is the access request, open design is the security of a mechanism should not depend upon secrecy of his design or implementation. So we can use encryption algorithm as an example. So, you will, you will want the algorithms to be open to the public and many experts will be able to kind of validate and examine your algorithms, but you you will need to keep the keys which are the impose of your algorithms secret, but the design of the algorithm should be open and separation of privilege, that means multiple privilege attributes are required to achieve access to a restricted resource. An example could be often you have multiple people to approve an action before it can be completed. This just prevents from prevents any one person from having too many controls over sensitive information or the system. And the least privilege means that entities should be given the least set of privileges needed to

perform a task. Um, the next one least common mechanism. So the mechanisms should I use to access resources should not be should not be shared. Um, and the next one is psychological acceptability. This means that security mechanism should not interfere unduly with the work of the users. So that just means that you should not add any actual burden to the user. Even if you add that should be minimal and reasonable that you have this balance between this user acceptance and the security complexity. Isolation three aspects. So public access should be isolated from the critical resources. And second one is the use of processes and file which should be isolated between each other. And certainly security mechanism should also be isolated from preventing, you know, and also risk access to this mechanisms. And number 10. Larry is super important in terms of the defense, so you want to use multiple layers of protection approaches in your system. Because if one layer has been breached, you'll still have multiple layers. At the behind. And this too, we'll talk about together there's more related to this object oriented programming concepts in terms of encapsulation and modularity. So encapsulation is is a specific form of isolation and to hide the internal structure of your system. And modularity is about developing the security functions as separate modules and also use of a modular architecture for your design. Okay, so last one least astonishment. So the program should always respond in a way that is least likely to start Finish user. All right. So I know there are a lot of concepts. And so we're going to have a quiz very quickly. So if you could if you could log into this website so we're gonna start the quiz

40:28
so this time is going to be quick. I'll just be five questions and each question you have 30 seconds to answer that just to test whatever remember from from the first pie from the previous part of the lecture. So this is a pink coat all right, I've seen students popping up

41:02
right, so we're gonna get started

41:11
alright, so I hope everyone has login. Okay, so let's get started

41:31
first question, which one of this is not the three pillars of security in this a trap? So we talked about it multiple times? You have 30 seconds to answer that.

41:48
Alright, so that's an easy one.

41:59
All right. Yeah. So should be the third one, which is accountability, as we said, this additional security goal introduced later on. Okay, so is it should be confidentiality, integrity, and availability. Second one, okay. Nice. So I don't always niche. Okay. Well done. Second one. So LS download is a software that appears to be legitimate, but actually contains malicious code. Okay, so this software contains malicious code, which principle has been breached or violated?

42:50
Okay. Right, okay. So most obviously, the answer them correctly. So its integrity because the program has been modified, right. So when we say the program has been modified, there's a data integrity issue. All right. So once students like to bray Trove availability, while here, Alice should still be able to use the software, but just the malicious code, maybe so in some malicious payload, or the some part of the program is doing some malicious activities at the background. So Alice should be still should still be able to use a cell phone but just but just the program has been has modified but sometimes when you have the molester call in the cell phone, you may not be able to use it. That's definitely affect reliability. But for this question, is a breach of integrity. Okay, so next one. All right. Nice. So we have another person now the top of the ranking. Okay. So which principles dice the default access? Right? should be no access. Alright, so we talked about 13 principles. Not sure if you still remember them.

44:34
Okay, so is actually the second one fell safety false. Yeah, so you can check the definition of the others just to review the other principles. So we'll quickly go to the next one. All right, so KD is doing very well. All right. First one, have true or false question. The security of a mechanism should depend on the secrecy of its design. or implementations, we talked about it just now. You should be able to choose the right answer.

45:12
All right, yes, it should be false. Because as we said, like encryption algorithm, you want it to be open to the public. And you want the experts reviewed them, but you do want to make the key secure. So the design should be, should be open, rather than keeping secret. Okay, last one. All right, cool. So Unix sudo is a command that allows a user to apply administrative rights temporarily to perform a privilege task is to elevate your rise temporarily. So which principle does it follow? So you want to give the users minimum rights?

46:16
All right, there's the there's a spread of the answers. That's actually the least privilege principle. And sometime you can be confused between this separation of privilege principle and least privilege. So separation means that multiple people share this privilege. Right? But then this one is the least privilege, just one user, you just give them temporary administrative rights. All right. So this is so we can see who is on the top of okay. So the first one

47:00
okay. All right, so let's go back to the lecture, we have three minutes.

47:18
So we're probably just gonna talk about attack surface, and we'll just end here. So attack surface is, consists of reachable and exploitable vulnerabilities. So that's the linkage was the vulnerability we talked about. And there are different types of vulnerabilities. As I said, that could be weak password, that could be some web web application that face the public Internet. And they are vulnerable to the attacks, that could be your employee, right. And they have access to the sensitive information, but they can be vulnerable to social engineering attacks. So they can be different vulnerabilities in your system,

and that form the attack surface. And so often, you divide attack surfaces by three groups. So you have network attack surface. So basically, that's the vulnerabilities in your network. And then you have your network or your devices, or that could be your protocols. And then we also have a software attack surface, that could be just the vulnerabilities in your operating system, or the applications running on the operating system. And then we also have human attack surface, you may have heard about it like human is the weakest link in security, and which is true, a lot of attacks, actually, because the phishing attacks, and then the just allow the attackers have the access to the system. So that's just basically the vulnerability created by the human that could be social engineering, or they just simply make mistake in the system configuration. All right, since we may just try to finish this. So the last concept here is just computer security strategy. So a strategy is often a special plan that is made to achieve a market position and to reach the organizational goals. So it has several elements that can support you to create your computer security strategy. And the first step is to have your security policy. Right. So that's the high level statements and to specify your security goals, objectives and requirements. And second one, you implement those requirements. So that's called Security implementation. And there are different categories of the actions we'll talk about in the next slide. And the third one is assurance. So um, Do you often deal with the question about does the security system design Mace is requirement. So it gives you a degree of confidence that all of these measures actually work. And then last one is evaluation. So we have this process of testing the controls, and examining the computer system was a certain criteria. Okay, so in terms of the security implementation, this is the last slide of this lecture. So we have four categories. And it's super important because kind of relate to the assignment. So we have prevention, detection, response and recovery. So prevention means you prevent the attack from happening, and you just block, you prevent it. So the attacker wouldn't be even be able to come into your system to penetrate into your system. So you can do encryption of the data, you can have access control, to the encryption keys, and to prevent the attacks on any transmitted data or data at rest. And then you can also detect the attack, that's super important. Because some attacks will be able to penetrate into your system, right. And once you detect them, you need to be able to respond to the attack. So you want to help the attack and prevent further damage. And then if there is any damage, you do want to recover from the attack. So you meant to backup, you may try to reload the credit copy of the data and restore your system operations. So that's basically the recovery. Alright, so that's all about the course actually, I wanted to talk about the assignment. But I think we'll just do the first thing in the next lecture. So make sure you have a read of this assignment specification and make sure you understand the requirement and bring the questions to the lecture next time. And also we're going to start the computer labs from next week. So hopefully you will be there and to get all the help from the from the tutors. Alright, so thank you