VGVDJH

Anonymkod/Anonymous code: VGVDJH

TENTAMEN/EXAMINATION

INTROSEC HT2022

Introduktion till informationssäker

Tentamen/Written exam 6 hp/hec

ML470C (SU) 470A AF

Poäng Points	Betyg Grade

torsdag 2023-03-30
13:00-17:00

Markera besvarade frågor med 'X' / Mark answered questions with 'X'													Antal blad
1	2	3	4	5	6	7	8	9	10	11	12		# sheets

Vakt kontrollerat antal blad:

Obs! Denna sida måste ligga överst - This page should be placed in front
Avlägsna tomma blad före inlämningen
Remove empty sheets before handing in the exam
Fyll i samtliga uppgifter på sidhuvudet på varje blad
Please fill in all information in the header on each sheet

[Quiz] Introsec written exam March 30, 2023

Attempt 13:02:12 - 16:59:59

Question 1

Problem 1

If you forget your password for a website and you click [Forgot my password], some website owners send you a new password by email, but some website owners send you your old password by email. Compare the security weaknesses in the two cases. Propose a way to overcome the weaknesses.

People access different websites with different credential details, so it is not uncommon that they might forget or loose their details while accessing a website not commonly used. In such a situation, the wesbsite owner could opt for either of the two scenarios.
In both the above scenarios, if the email of the user is in possession of a hacker or an unwanted intruder, then they would have access to the website credentials simply by receiving th password details. This is a dangerous situation. They would be able to access the website credential details and change the password internally, so the original user would no longer be able to access their login page on the website. This security intrusion could be a result of both the above situations.
However, there is also another pitfall with the second scenario, wherein the website emails the old password to the user. As mentioned above, since users generally access several websites, the chances of them resuing passwords on different websites is highly possible and is a huge security flaw. Once the intruder has access to the old password, not only would they be able to access this website's login page, but they could also attempt the same password for several other websites, and test their luck to enter into other credentials and pages, pages that hold sensitive information. Some people add personal information to the passwords, for example their birthdays or petnames, which means, once the hacker has access to that information they could attempt various combinations of the same and try their luck with every site, with those credentials.
And once they have access into different websites, they would be able to change the password permanently or even change the email address, so that the original user would never have the chance to access those pages again.
One way to overcome these weaknesses is through a form of authentication, where in the subject is first identified and then their identity is approved. Thus, it is performed on what they know that is a password, and what a subject is, biometrics and what they possess, ID cards. Thus every time the sever has to allow access to the user, an identification process has to be carried out, to verify the identity. This could be combatted by using the brute force method, to continue attempting login details.
Another method is through a two-factor authentication method, which is a out-of-band communcation method, an extra addition to the id and password. Here, a one time code is alerted to the user's device, some cases their mobile phone, and after a correct code is entered, access is allowed. This method would require the hacker to have the user's phone, to be able to enter any details. Even when they click on 'forgot password', hence extra security. However, this would require every user to have a valid mobile phone number at the time of account creation.

Question 2

Problem 2

HTTPS (or TLS/SSL) uses PKI (public key infrastructure) and certificates to ensure security. A certificate contains an identity, a public key, and the signatures of CAs (certification authorities). Other fields that may be present include the organization (for example, university, company, or government) to which that identity belongs and perhaps suborganizations (college, department, program, branch, office).
1) Explain what security purpose these fields serve.
2) Describe two uses of certificates.

A certificate is generally used to combat the authenticity issue. It could exist in different forms: Server, Browser and Personal. In authentication process, a certificate is the binding of the public key and the identity of the user and when signed by a certification authority, this would ensure the accuracy of the bind.

1) The various fields of the certificate all serve a purpose. Let's consider the heirarchy of a company: an employee named Mark, would first choose a public key pair, and would publish the public key, in such a way that all the other employees would be able to access this. Several division managers, say Elise, would create her public key pair, and puts the public key with her identity into a message, and the message is then securely transmitted to Mark. Mark would then be able to sign the same by creating a hash value of the received message, and encrypts this woth his private key. When Mark signed the message, he is issuing his certification that the public key, which is Elise's and the identity, also Elise is for the same person, thus the message is called Elise's certificate. In this manner, all of Elise's department managers could also create messages, and would be certified by Elise.
These security fields, such as university, company, branch etc, all help is identifying and creating a hiearchy. This is to emulate the real life, natural hierarchy that exists: wherein a particular officer could vouch for the document or certificate, just like how notary officers can attest the validity of the same in real life, the messages that could be verified by the employees in the bottom leg of the hierarchy, need not interfere with the work of the people at the top of the hierarchy, like CEO or government heads. Since these security fields follow a hierarchy, the trust of the top level is dire. This chain of authenticity is secure as each certificate contains a key that could be used to decrypt the next certificate except for the top most levels. This is also important due to the existence of unscrupulous Certificate Authorities, as several lower level CAs could establish and issues certificates which would appear to be secure, but would not necessarily provide the security.

2) Certificates are utilized to verify the authenticity or validity of the user or a document. As aforementioned, a notary person could attest to the validity or credibility of a signature on a document, similarly, digital certifications could be used by an authorized user, either to verify the credentials of a user or a digital document. For example: university officials could verify digital documents of students and staff. They are also used in the Secure Sockets Layer protocol, which is a protocol to protect the communication between a web server and browser. When the client requests an SSL session, the server responds with its public key certificate, thus client can verify the credentials/authenticity of the server. The client responds with its symmetric session key, which is encrpyted by the server's issued public key. The session key is computed by both the server and the client, and using this key, they switch to the encrypted communication.
They are also used in the extensible authentication protocol (EAP), in the Weak Enryption Protocol (WEP) during the authentication process,

Question 3

Problem 3

Nowadays, more and more private information might be collected and used by third party companies through various apps in mobile phones, such as GPS location, mobile phone number, contact information, camera type etc.
Taking this as an example, discuss the requirements to PETs (Privacy Enhancing Technologies) in data storage, data processing, data transmission, data consumption or provisioning in terms of the privacy properties: anonymity, pseudonymity, unlinkability, unobservability and undetectability.

Privacy Enhancing Technologies are a system of the Information communication and Technology section that helps to protect and ensure privacy by eradicating personal information or prohibiting the unwanted possession of data, while maintaining the functionality of the system. The privacy properties such as anonymity, psuedonymity, unlinkability, unobservability and undetectability must be preserved, in all the steps of the data storage, processing, transmission, data consumption or provisioning. Encryption, Anonymization (which could be differential privacy, k anonymity, onion routing), and psuedonymization (could be masking or tokenization) are examples of PET's.
In the data storage approach, the rule to protect the individual's location when they are stored and the places they visit could be protected by encryption, since it maintains their confidentiality. Unlikability, unobservability and undetectability could be provided in this manner, however, some applications need to gather location details such as Google Maps. Anonymized data could be captured, and anonymization could be maintained. Data minimization should govern the gathering or collection of data.
Similarly, if this extracted information must be used in the data processing phase, it must be encrypted or psuedonymized in a way that it could be traced back to the user.
In data transmission, instead of transmitting plain text, psuedonymized or encrypted/masked information could be sent, by making use of pseudonymization tables. Unlikability, unobservability and undetectability could be provided along with pseudonymity. This includes any sensitive and personal information, like camera type etc, which could be manipulated and masked for data processing.
In data consumption, data minimization should be incorporated and again, instead of sending plain text, psuedonymized/masked data could be sent. The processing should only include the necessary data, as minimum as possible, for example: sensitive infromation like moble phone numbers and contact information should be masked and utilized ONLY when necessary, thus
maintaining Unlikability, unobservability and undetectability and anonymity.

Question 4

Problem 4

Below are four pairs of concepts/threats/tools. For each pair, define both terms and explain the relationship between them. Then describe how the two terms can be used together to achieve a common goal, for example, to harm or protect one or several security properties, or ensure privacy. Structure each of your answers with the headings “Definition”, “Relationship”, and “Description”. Your answers to each part should show your deep understanding of the concept. The definition,

relationship and description should be described or explained with care; they must not just be copied from the book/documents.
Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem.

1. **Reference monitor and incomplete mediation**
2. **Access control and IDS (Intrusion Detection System)**
3. **TCB (Trusted Computing Base) and memory protection**
4. **Viruses and worms**

1. Reference monitor and incomplete mediation

- **Definition**

A reference monitor is a concept under access control, is an "abstract" machine that mediates the access of all the objects by different subjects. Thus, it is a collection of specifications for a validation protocol, that would enable the execution of different access control operations for different files, documents, objects, memory etc, such as read, write. All the access requests presented by the subjects must pass through this point.

Incomplete Mediation is referred to as the poor checking or verification of input data. And a fundamental principle that falls under security is to minimise, restrict and validate input. Thus in incomplete mediation, a hole in security, is when the user is not required to authenticate themselves. It could be used to send false alerts or mess with the system, as it is due to poor verification.

- **Relationship**

Both of these concepts have to do with access control and the granting of access. Reference monitors are said to be unbypasssable, often illustrated to be a brick wall, that is a trusted security measure. Incomplete mediation would be the worst case scenario of the reference monitor, which is when a subject is not required to authenticate themselves, in order to access different objects, thus bypassing the rules of the reference monitor.

- **Description**

As mentioned earlier, incomplete mediation is when the authentication process has failed to mediate the user's request, reference monitors could be utilized as an additional step, to prevent the user's access until authentication is completed, thus sensitive information like memory and files could be protected until the reference monitor autheorizes the access, thus protecting systems and Operating Systems. Reference monitors would be a way to mitigate incomplete mediation.

2. Access control and IDS (Intrusion Detection System)

- **Definition**

Access control is a mechanism to protect objects, by implementing flexible rules, in a way that policies could be changed easily. This is a control procedure to give selective access to subjects trying to access various locations or objects. The subjects must be authenticated before they are allowed to perform actions on the objects (read, write, modify etc).

An intrusion is referred to as a subject trying to gain access to a system or object, illegally. This could be to collect information from the system to then exploit the vulnerabilities, and in the worst case, could lead to destruction. Thus intrusion detection systems are designed to be able to detect this access, which is unauthorized, identify the possible attacks, not only to the system but also the network, and also check on the running state of the computer. They not only check and monitor access, but also audit for holes and vulnerabilities. Thus preserving the integrity of the system.

- **Relationship**

Since access control is the mechanism that ensures the controlling or monitoring of access requests by different users/subjects onto different objects in the systems, and IDS is a system built in place to recognize and identify the various vulnerabilities, Access control mechanism and IDS could work hand in hand, to detect the access allotted and monitor the system, in case of access control not recognizing or authorizing a subject, the IDS would be able to recognize it.

- **Description**

Operating systems and anti-virus software like Norton could be an example where the two principles could be used to identify any illegal/unauthorized access, and in some scenarios, run prevention techniques.

3. TCB (Trusted Computing Base) and memory protection

- **Definition**

TCB encompases everything in a Operating system that would be beneficial to enforce security policies, thus creating a trusted operating system. This consists of mechanisms from both the hardware and the software, which would implement the security policy of the system. Thus, it should be both good and complete.

When a user is running a program in memory, they must run in a certain portion of the memory, and this portion must be protected against unauthorized access and manipulation. This will not only prohibit external access to the memory but also restrict the user's access to protected memory. This mechanism, to protect the user's memory as well as the rest of the program space, is referred to as memory protection. Thus it is designed to implement sepration as well as sharing.

- **Relationship**

Since TCB is defined as the overall compilation of mechanisms to implement security policies, and is designed to maintain integity, memory protection would be one of the functions of TCB, as it must maintain and monitor the references made to the memory, in order to ensure the integrity and secrecy of the various domains of the memory (code and data).

- **Description**

Memory protection is a subdvison or a task of the TCB, thus is any malicious or illegal

manipulation or access request to the memory is presented, the TCB would monitor the request, and thus not only ensure that the memory is protected and not tampered with, but also maintain the integrity of the system, thus creating a fortress structure. This could be ecnompassed into a security kernel, which would consist of all the security policies.

4. Viruses and worms

- **Definition**

A virus is a program that has the capacity to replicate itself, and then passes on malicious code to other clean (undisturbed) programs and infects them. It is created for malicious purposes, all for infecting other programs. They can be spread be emails, but could also exist in either transient (runs until the life of the host exists) or resident form (leeches on and behaves as a stand-alone program).
Worms are identified as bots that can spread several copies of itself through the network. It is a malware, and can do harm or just continue spreading. Could be used to alert the creator of any new development or connection.

- **Relationship**

Both viruses and worms use applications, however, a worm's primary operation mode is through networks, whereas a virus would be able to spread through any available medium (generally copied files, programs or data files). Worms also sends copies that could act as stand-alone programs, however, viruses have to attach/embed onto programs.

- **Description**

They could be utilized to create botnets, which is a large network of bots, they could infect several computers, which could further be sold and used for the denial of service attacks, sending spams through emails and also cryptomining.

Question 5

Problem 5

Attackers may make use of weaknesses in all the layers of the OSI 7-layer reference model.
1) Name an attack on each of
   a) Layer 2 (Data link layer)
   b) Layer 3 (Network layer)
   c) Layer 7 (Application layer)
2) Explain why and how the attacks can happen.
3) Describe a countermeasure for each of these attacks.

1) Interceptions could occur at any level, Attacks that target the various layers could be:
a) On the second layer: Data link -To obtain information being transmitted, eavesdropping and snooping, data corruption
b) On third layer: network layer - Sequencing attack, that is an error in the order of data, i.e., packet 1 arrives after packet 2. Substitution attack, where the packets could be replaced by others (data manipulation). Man in the middle attack.
c) On seventh layer: application layer - Where the data is formatted and delivered in a total unit, Replay attacks could affect it.
2) Sequencing attacks are quite common since the data units would be routed based on the routing information available, if the router discovers a certain node is busy, then it is sent to another route. Eg: Packet 1 is sent, and the most optimal route via node found is C. If the router receives information that node C is no longer optimal, the it is sent via Node D, in a way that packet 1 arrives after packet 2. Congestion and network interference, could also play a factor.
Substitution attcks could take place when adjacent cables or interference known as crosstalk is created. An attacker could introduce this attack by splicing a piece of information from one communication to another. Man in the middle in an interception attack where the data is modified and exploited.
Since packet filters only notice the header of the packet, the data inside could be manipulated and this could cause damage.
Replay attacks are when useful data are reused through interception, generally when data is resued without any changes made to the data itself. Thus, unsuspecting damage.
3) Link to link encryption could be used to protect the message when it is being transmitted from one node to another´, in such a way to hide the message from outside intruders, and header and trailer information is also appended to the block before it is encrypted. Onion routing could also be used to prevent eavesdropping. and prevents an attacker from learning the content, source or any additional information.
Packet filtering gateways could be used as a firewall to Networking protocols such as TCP, could be a countermeasure, to provide server authentication, and encryption could be a solid solution, since the entire message is covered which means the attacker would not be able to identify the message, find it difficult to splice, or creating an integrity check.
Secure sockets layer SSL, could also be incorporated at level 4, since it operated between different applications like browsers.
Application proxy, such as the file transfer protocol (FTP) is a firewall that would be applied on the seventh layer, such that the layer only receives requests to act properly. Sequencing number could be used to counter replay attacks, as it is unique to the recipient, and end to end encryption could be introduced, and only data portion is encrypted and masked, since the headers are not as sensitive.

[Assignment] Fx-2

Nothing submitted

[Assignment] Fx-5

Nothing submitted