RKHDCV

Anonymkod/Anonymous code: RKHDCV

TENTAMEN/EXAMINATION

INTROSEC HT2022

Introduktion till informationssäker

Tentamen/Written exam 6 hp/hec

ML470C (SU) 470A AF

tisdag 2023-08-15
09:00-13:00

Poäng Points	Betyg Grade

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 August 15, 2023

Attempt 09:08 - 12:47:57

Question 1

Problem 1

Suppose Alice and Bob have RSA public keys in a file on a server. They communicate regularly using authenticated confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob. However, she is able to break into the server and alter the file containing Alice's and Bob's public keys.

1. **How should Eve alter that file so that she can read confidential messages sent between Alice and Bob, and forge messages from either?**
2. **How might Alice and/or Bob detect Eve's subversion of the public keys?**

1. Assuming the following procedure is used to establish a secure session:
A encrypts a a symmetric key K with her private key KprivA. This is done to authenticate her a sender since KprivA is not known to Eve it cannot used for impersonation.
Then A uses B's public Key KpubB to encrypt the the whole message. This means only B can decrypt the message "wrapper" with his private key.
B can do the same of course, if he wants to initiate the session.

If public keys are only available on the server have been replaced AND all messages are being intercepted, E could use two new public-private key pairs to insert herself between A and B.
Since the public key must correspond to a private key, but the private key is never known to the other party, E could intercept the message with the encryptade symmetric key, replace that with a new symmetric key, encrypted with her private key and wrapped in B's public key.
B will receive the message and will be able to decipher the wrapper with KprivB and then see the inner encryption and authenticate it (incorrectly) against the CA as coming from A.
Now all messages sent from A will be encrypted by a symmetric key known to E, but not B. E can reencrypt the messages with her own symmetric key she has shared with B and can thusly keep up the appearances that both authenticity and integrity is in place. Likewise, for responses to A, E has the original symmetric key and can impersonate B using the fabricated public key KpubB

2.
If A abd B suspects the public keys have been compromised, they can exchange public or even symmetric keys directly, not through an intermediary server/certificate authority. This however requires that Alice and Bob can identify and authenticate manually and that the communication cannot be intercepted, for instance through a physical meeting or another secure channel consisting of only trusted and verified parties.
They could also keep a hash of eachothers public key to verify whether any tampering has occurred.

Question 2

Problem 2

Nowadays, more and more private information can be collected and used by third party companies through 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 PbD (privacy-by-design) in data storage, data processing, data transmission, data consumption or provisioning.

Privacy by design is the idea that the design process of information system should encompass establishing and upholding privacy thorough the whole life cycle of a system. This means privacy should be addressed early on, and not as an afterthought when designing IS. It also means a focus on prevention and proactivity rather than reactivity and mitigation of incurred damages.
This early on approach also makes it possible to strive for a system that fulfills the requirements of both security and privacy without diminishing one on behalf of the other.
It can be condensed into a number of design principles that should be adhered to, among those are the notions that using privacy as the default setting, meaning the system should be designed and implemented in a way that maximizes information privacy and security.
This idea leads to the practice of limiting the information stored to the minimum amount of information that is necessary, and only for explicitly stated purposes which is actually mentioned in the GDPR guidelines. This idea is in some ways analogous to the notion on need-to-know-basis; if there is more information than strictly necessary, there will always be the risk of misuse/spread of any information and what is not present cannot be spread.
The idea of having a system designed and built from the groun up with privacy as default, together with transparency about the system and the information stored, processed and transmitted should lead acceptance and trust from the users/data subjects and in the end user-centric.

Question 3

Problem 5

Assume no SFTP (Secure File Transfer Protocol) exists. You are asked to define a function analogous to the FTP PUT for transferring files to remote hosts securely. List and explain three security features or mechanisms you would include in your protocol.

End to end encryption for the file transfer ensures both integrity (via hash sums for instance) and confidentialty of the data, and a means for authentication and authorisation, as a form of access control.

Assumption: PUT is the equivalent of "uploading" a file.
1. Establish a secure connection, using authentication and access control. This ensures only authenticated and authorized users can acccess the server side storage location and object(s). It also ensures a separation of users access to objects.
2. Protect the integrity of the data being transmitted.
Hash sums and encryption to verify and avoiding integrity breaches.

3. Protect the confidentiality.
Encryption to prevent interception by unauthorised parties.

4. Ensure the avaialbility of the function throughout the transfer.
Resend/resume functionality based on dropped or altered packets
Reauthentication or some sort of keep alive for the session.

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. **Anonymity and undetectability**
2. **PKI (public key infrastructure) and HTTPS**
3. **Digital signatures and certificates**
4. **The Bell-LaPadula Model (BLP) and Biba model**

1. Anonymity and undetectability

- **Definition**

Anonymity is the idea of being unable to identify an information subject through direct or indirect means with a given information set.
Undetectability is the idea of a third party being unable to tell one user apart from another (from a pool of users using a service)

- **Relationship**

Undetectability can be seen as a goal, or consequence, of utilizing the characteristics of anonymity.

- **Description**

In order to achieve undetectability, one could utilize the properties for anonymity by making sure the potential users are anonymous but also share a number of characteristics,making them unique in a statistical sense but from an identification point of view they should be indistinguishable.
Anonymity can however be threatened given additional information. In order to control that threat, one could implemetn various countermeasures or policies governing the storage and accumulation of data as well as methods to ensure an apporopriate granularity of the the information for agiven contect/research area.
An example is the K anonymity approach. Which is implemented in order to ensure

that one specific individual from a larger dataset cannot be identified based on the information given. Instead, the set and data should be constructed in a way that any given person should have at least K other possible candidates with the same level of matching score for identification purposes

2. PKI (public key infrastructure) and HTTPS

- **Definition**

Public key infrastructure is a framework for distributing trusted and authenticated public keys for assymetric encryption.
HTTPS is the secure version of hyper text transfer protocol

- **Relationship**

HTTP uses SSL to create a secure session using a public key.
Public keys are distributed by PKI

- **Description**

When using https-url:s the browser initiates a request for a secure session using the SSL protocol. The server provides a public key certificate for authentication purposes and upon autentication, the browser/client sends a symmetric key using the servers public key.
The PKI is a a framework for providing public key distribution and traceability via trusted certificate authorities.

3. Digital signatures and certificates

- **Definition**

Digital signatures are the digital counterpart to signatures, which is a file that provides a proof of identification and the authenticity and consent of the signer as well as some sort of tamperproof.
Certificates are used to authenticate the identity of some entity.
This is done through linking a public key and its owners identity in a certificate

- **Relationship**

Digital signatures are autenticated through linking a public key and its owners identity in a certificate. This is done by a trusted certificate authority.

- **Description**

Digital signatures are often used in financial transactions or in other (digital) scenarios where you need to identify/authenticate yourself as well as indicate consent.
Certificates are used to issue and ensure the trust of digital signatures, often through certificate authorities that can be seen as root level and widely accepted as trusted organisations.
There exists different types of digital certificates, with different solutions to linking of authentication signatures.
The idea of Digital signatures harkens back to the signatures or seals used throughout

history. It is a token that implies authenticity and approval and assumes unforgeability (nontampering) It is bound to a file through an public encryption key which forms the certificate.

4. The Bell-LaPadula Model (BLP) and Biba model

- **Definition**

Bell - LaPadula Model is a model that specifies the enforcement of policies concerning the preservation of information confidentiality
Biba is another security model, focused on the preservation of information integrity

- **Relationship**

Both models were proposed with military classification levels of information as the basis of how to (and not to) treat information flowing from one hierarchical classification level to another.
The Bell -LaPadula model is used in scenarios where the main objective is to keep confidentiality intact, the so called "need-to-know", whereas the Biba model's goal is to not compromise the integrity of the information. That is, the "correctness" of the data is more important than who is able to access it. This lends the Biba model more suited to business practices rather than strict military intelligence.

- **Description**

The Bell - LaPadula models governs the information flow in a hierarchical classification going from unclassified (lowest) to top secret (highest) classification scheme. The main rule is that on any given level a person with that given security clearance is only allowed to write reports on the same or higher classification levels and only to read reports on the same or lower classification levels
This ensures that no information with higher classification can leak to a lower classification level, and thusly confidentiality is preserved,

The Biba model, on the other hand, is based on the notion of data integrity/quality, as in how trustworthy, accurate and precise the information is governs its classification level with the least trusted data on the lowest level and the most accurate and verified information on the top levels.
The policy enforced in Biba's model is therefore read up, write down, ensuring no information of lower quality can contaminate more accurate and/or trusted information.
I am not entirely sure how these characteristics should be measured or weighed against eachother.
Information "sensitivity" as in BLP's confidentiality and "trustworthiness" as in Biba's sense of integrity model are not necessarily diametrically opposed, however. Some information can be both highly accurate and highly sensitive. Like supply routes and schedules, or the exact (business) plans of an adversary/competitor. On the other hand, one could come across highly sensitive, but unverified information. resulting in potentially high value if it can be verified. I therefore do not think they should be treated as mutually exclusive.

Question 5

Problem 5

A noted computer security expert has said that without integrity, no system can provide confidentiality.

1. **Assume the system provides no integrity controls. Do you agree with the noted computer security expert? Justify your answer.**
2. **Now suppose the system has no confidentiality controls. Can this system provide integrity without confidentiality? Again, justify your answer.**

Part of a previous question was about the Bell-LaPadula and Biba models.
Examining these two models, it seems to me that one could come across a situation with any combination of high/low confidentiality or integrity for information.
However, these models are not representative of a complete system, wherein both the confidentiality and the integrity of the information
as well as information needed for authentication and access control of users are needed.
If there are no integrity controls for autentication and access control mechanisms, then that information could be altered with the consequence of breach of confidentiality. My answer is therefore that I agree with the expert.

On the other hand, a completely open system wrt confidentiality (everyone has access to everything) could still have integrity controls due to the ability for anyone to access and checking the information.
One such (utopian) system could be an open research (or learning) system where everyone could read and contribute to resarch topics on a non profit basis.
Such systems are however, susceptible to attacks and bad faith actors who may seek to disrupt the system.

[Assignment] Fx-2

Nothing submitted

[Assignment] Fx-5

Nothing submitted

[Assignment] Fx-3

Nothing submitted

[Assignment] Fx-1

Nothing submitted