INTRODUCTION TO CRYPTOGRAPHY

Software Security

CHAPTER 16: EXERCISES FOR PART 3

By Group 4

Submitted to: Mr. Kelemwork

Acknowledgement

We Group four team members would like to express our appreciation for each other for the experience we shared while making this assignment. We are also thankful to Mr. Kelemwork, our Software Security teacher, for giving us with this chance and helping us complete it. The project enables us to know how to import packages, some details about crypto packages and more.

Group Members

Name	ID
Abrham Abayneh	1311576
Abrham Merkuz	1311579
Betelhem Negash	1306870
Bezawit Etsubneh	1306205
Hailemichael Mulugeta	1311614
Samrawit Fikremariam	1308042

Conceptual Exercises

1. List three advantages/disadvantages of using a web of trust model vs. using a certificate authority–based trust model.

Before diving to the question let us see what it means by PKI (public key infrastructure).

What is PKI?

Public Key Infrastructure (PKI) is a security framework that enables secure communication, data integrity, and digital signatures. It allows users, servers, and other devices to securely exchange information over open networks such as the Internet. PKI consists of a public key and a private key. The public key is used to encrypt data and then only the person with the "private key" can decrypt and view it. This ensures high-level security because even if an attacker was able to intercept the encrypted data, they would not be able to read it without having access to the other user's private key. Additionally, PKI can also be used for verifying and authenticating electronic communication or documents using digital signatures.

There are a number of PKI models based on: whether the certificates are issued from one or more central authorities; the trust and revocation mechanisms being employed by the system; the levels of authority and control over the issuance and management of certificates; and whether other parties outside the core organization have a role to play in establishing, issuing, or managing certificates in some way. These are:

1. Certification Authority (CA) Model
2. Hierarchical CA Model
3. Distributed CA Model
4. Bridge CA Model
5. Web of Trust Model
6. Hybrid PKI Model
7. Grid PKI Model
8. Decentralized PKI (DPKI) Model

We are asked about the advantages and disadvantages of using a web of trust model vs. using a

certificate authority–based trust model. But what are those in the first place?

What is Web of Trust model?

The Web of Trust model is a distributed trust system in which users interact to create their own trust relationships. It relies on users to freely share information about other users and verify the authenticity of this information. This system does not have a central body that manages authentication, instead relying on peer-to-peer validation from trusted peers.

There are two types of this model. This are direct and indirect trust model.

A Direct Web of Trust is a trust model in which users must directly trust any transaction that is performed by another user in order for the transaction to be successful. This model relies on these direct connections for all instances of trust, and does not allow for an indirect or third-party system of validation.

Figure 1: direct web of trust

An Indirect Web of Trust uses other people's or entities' ratings to grant permission for transactions to occur. In this type of system, users can form relationships through trust networks and benefit from other people's experiences and opinions about a particular vendor or user.

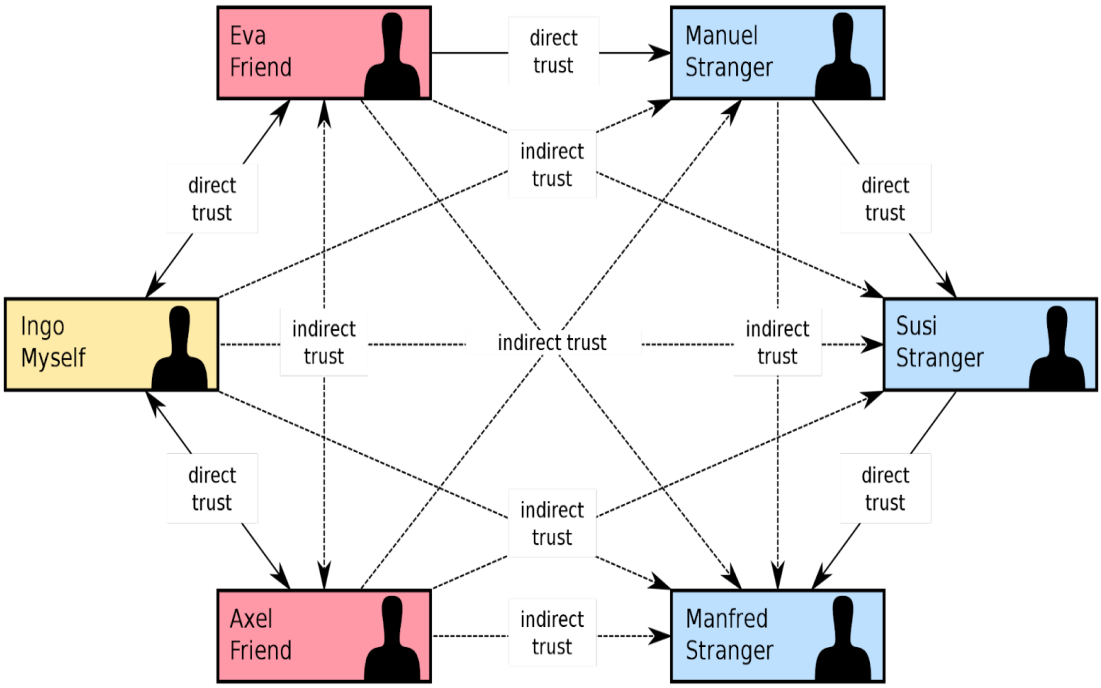

Figure 2: Indirect and direct web of trust

Advantages of web trust model

1. More flexibility as users may add or remove people from the network without having to contact a central authority.

2. Lower cost due to reduced infrastructure requirements and no need for ongoing payments to a centralized certificate authority.

3. People participate voluntarily, allowing them to decline if they don't feel comfortable with the security measures in place.

What are the disadvantages of web trust model?

1. Users must evaluate the validity of other users' certificates, making it difficult to guarantee correctness and accuracy in the verification process.

2. Security can be compromised by fraudsters or malicious actors who might get included into networks through false identities or forged credentials.

3. It is time-consuming, as each user has to perform steps manually that otherwise could have been completed automatically by touching a single button when working with trusted certificate authorities (CA).

What is certificate authority-based trust model?

A Certificate Authority-based Trust Model is a type of trust model that relies upon the assurance provided by digital certificates issued by an independent third-party Certificate Authority (CA). A CA is responsible for verifying the identity of certificate applicants, issuing digital certificates for those applicants and periodically validating their authenticity. Digital certificates can be used to facilitate secured communications between two parties without the need for manual validation. The trustworthiness of a Certificate Authority is based on its reputation, security protocols, audit requirements, and customer service.

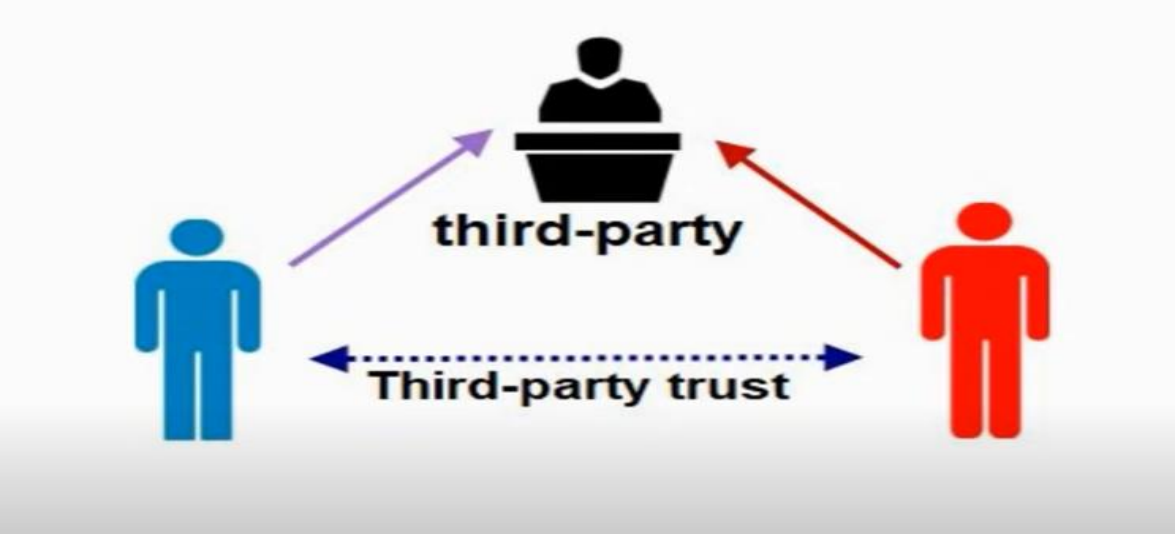

Figure 3: certificate authority-based model

Advantages of certificate authority-based trust model

1. Establishes trust beyond just individual hosts.

2. Establishes industry standard protocols for verified identities.

3. Ensures secure and efficient communication within the network.

4. Requires one time authentication, making it easier to manage authentication procedures in large networks.

5. Provides scalability and eliminates manual security checks of each host connection change.

6. Supports multiple cryptography algorithms as well as digital signature implementations to ensure data integrity and protect against malicious activities.

7. Reduced costs associated with identity verification processes due to its centralized nature and automated procedures for confirmation and authorization requests.

Disadvantages of certificate authority-based trust model?

1. Complex system which requires technical knowledge in order to properly implement and maintain the network's trust management systems securely across all participants on the network .

2. Reliance on a single central entity like Certificate Authority means that if it is compromised or fails, then the entire system would be impaired or ineffective as resulting trust may no longer be verifiable or accurate .

3. Restricted control for users over their preferred method of authentication since requests must go through an external third-party provider like a Certificate Authority, which can add additional latency in verifying identities before authenticity is established .

4. The initial cost of implementing such a system may be significant depending on the scale of the network it is applied to.

2. State how you can use symmetric encryption to achieve (a) authentication, (b) confidentiality, and (c) message integrity.

Let us first discuss about symmetric encryption. It is a type of encryption where only one key is used to both encrypt and decrypt the data. It is also known as private-key encryption, because the same key is used for both operations. Unlike asymmetric encryption (also known as public-key encryption), symmetric encryption algorithms are much faster, which makes them more suitable for encrypting large amounts of data.

Now let us see how we can use symmetric encryption to achieve authentication, confidentiality and message integrity.

How can we achieve authentication using symmetric encryption?

Symmetric encryption, also referred to as secret key encryption, is an encryption scheme that uses the same key for both encrypting and decrypting data. It is a form of data security used to protect digital information by allowing only authorized users to access the encrypted information. It is one of the most widely used methods for authentication and can be used in a host of different applications. For example, symmetric encryption can be used to authenticate messages between two parties over the internet, or to protect sensitive documents such as credit card numbers.

In order to achieve authentication using symmetric encryption, firstly both parties (i.e., sender and receiver) must agree on a shared secret key and should be exchanged between them through secure means like through physically with each other or by transporting it via insecure channels with proper protection like SSL/TLS/VAULT. This is done so that the key is known only by both parties but not anyone else. Once the key has been agreed upon, either party can use this secret key to encrypt messages they

wish to send, ensuring that only those who have agreed upon this same shared secret will be able to decipher it properly later.

When transmitting messages securely over the Internet using symmetric encryption, both parties must ensure that their communication channel is secure from outside interference or interception by malicious actors. To do this, each message consisting of plaintext must then be encrypted using a public-key cryptographic algorithm such as AES or Triple DES before being sent across the channel; after which it must then again be decrypted at its destination using a separate private-key algorithm. As long as no third-party individual knows either party's private keys (or indeed even accesses them), then this provides 'proof' of authenticity for each message transmitted – since only its intended recipient will receive it in an intelligible form suitable for further processing – thereby providing effective authentication.

How can we achieve confidentiality using symmetric encryption?

In symmetric-key encryption, a single key is used to encode (encrypt) and decode (decrypt) the data. This means that for the data to remain confidential it needs to be kept secret from viewers or attackers in order to maintain its security. To use symmetric encryption, two parties must first exchange keys through a secure channel. Both parties must have copies of the same key in order for encryption and decryption to occur correctly.

Once the key has been exchanged, both parties can use it simultaneously in different computer systems or devices both senders and receivers can then encrypt their messages using this shared key, which allows them to communicate securely while their messages remain confidential. In addition, they can even digitally sign their messages to ensure that tampering or frauds will not occur during the transmission process. Symmetric encryption also helps reduce computational resources since only one shared key needs to be managed rather than two distinct keys for separate users for each communication session.

An example of how symmetric encryption can be used to achieve confidentiality is when sending sensitive information over the internet. For example, if two people wanted to securely exchange financial information using email, they could do so using symmetric encryption. The data would be encrypted using the key and sent over a secure connection in order to maintain confidentiality.

How can we achieve message integrity using symmetric encryption?

Message integrity guarantee the validity of a message, ensuring that it has not been altered since it was sent by its original author. This can help protect against man-in-the-middle attacks and other malicious alterations of data. This can be achieved by combining two cryptographic primitives: Message Authentication Code (MAC) and Encryption.

A Message Authentication Code is a short block of code that is generated through a hash algorithm with a secret key as input. The MAC protects the integrity of the message, ensuring it hasn't been modified from its original form.

Encryption is the process of transforming plaintext into an unreadable form or ciphertext, which cannot be read until it has been decrypted with the proper secret key. When symmetric encryption is used, both the sender and recipient need to possess the same secret key in order to decipher the message.

By using symmetric encryption in combination with a MAC, both parties can verify that any messages they have exchanged have not been tampered with prior to arriving at its destination. Additionally, since only someone who possesses the same secret key can decrypt it, data confidentiality is also maintained.

We have already illustrated all this in the programming task that is given for us.