Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

July 10, 2023

Chapter 19 & 22 Review

Question

19.1 Describe a classification of computer crime based on the role that the computer plays in the criminal activity

There are three classifications of computer crime which are based on the role that the computer plays in criminal activity. These three classifications are: computers as targets, computers as storage devices, and computers as communications tools (Stallings & Brown, 2018. p. 579 - 580).

Computers as targets – In this classification the crime targets a computer system, they are doing this to acquire information stored on that computer, to control the targeted system without authorization or payment, or to alter the integrity of data or interfere with the availability of the device (Stallings & Brown, 2018. p. 579).

Computers as storage devices – In this classification the crime uses a computer or device in order to store data such as storing passwords, credit cards, or any other type of information (Stallings & Brown, 2018. p. 580).

Computers as communications tools – In this classification the crime uses computers or devices as a communication tool, such as using it to communicate or

assist in the sale of illegal substances or other objects such as weapons (Stallings & Brown, 2018. p. 580).

19.2 Define three types of property

Three types of property are: real property, personal property, and intellectual property (Stallings & Brown, 2018. p. 583).

Real property – Real property consists of land and things which are permanently attached to the land like trees and buildings (Stallings & Brown, 2018. p. 583).

Personal property – Personal property consists of personal effects, moveable property and goods like a car or furniture (Stallings & Brown, 2018. p. 583).

Intellectual property – Intellectual property consists of any intangible asset which consists of human knowledge and ideas like software and data (Stallings & Brown, 2018. p. 583).

19.3 Define three types of intellectual property

Three types of intellectual property are: copyrights, trademarks, and patents (Stallings & Brown, 2018. p. 584 - 585).

Copyrights – Copyrights protect the tangible of fixed expression of an idea, but not the idea itself, there are a few conditions to gain a copyright such as it being an original work and the creator has put the idea into a concrete form such as on paper or

software (Stallings & Brown, 2018. p. 584). Some examples of copyrights are literary works, musical works, and dramatic works (Stallings & Brown, 2018. p. 584).

Patents – Patents are a grant of a property right to the inventor of it (Stallings & Brown, 2018. p. 585). There are three types of patents, utility patents, design patents, and plant patents (Stallings & Brown, 2018. p. 585).

Trademarks – Trademarks are words, names, symbols, or devices used in trade with good which distinguishes it from goods of others (Stallings & Brown, 2018. p. 585).

19.4 What are the basic conditions that must be fulfilled to claim a copyright?

There are two basic conditions which must be fulfilled to claim a copyright. To claim a copyright the proposed work must be original, and the creator has put the original idea into a concrete form like on paper, on software, or in a multimedia form (Stallings & Brown, 2018. p. 584).

19.5 What rights does a copyright confer?

A copyright confers the rights of: reproduction, modification, distribution, public-performance, and public-display (Stallings & Brown, 2018. p. 584).

Reproduction right – This allows the owner to create copies of their work (Stallings & Brown, 2018. p. 584).

Modification right – This allows the owner to modify or create derivatives of their work (Stallings & Brown, 2018. p. 584).

Distribution right – This allows the owner to publicly sell, rent, lease, or lend copies of the work (Stallings & Brown, 2018. p. 584).

Public-performance right – This allows the owner to use it in live performances (Stallings & Brown, 2018. p. 584).

Public display right – This allows the owner to publicly show copies of the work such as in a film (Stallings & Brown, 2018. p. 584).

22.1 List four functions supported by S/MIME

Four functions supported by S/MIME are: enveloped data, signed data, clear-signed data, and signed and enveloped data (Stallings & Brown, 2018. p. 662).

Enveloped data – Enveloped data consists of encrypted content of any type and encrypted-content encryption keys for one or many recipients (Stallings & Brown, 2018. p. 662).

Signed data – Signed data has a digital signature, it takes the message digest of the content and then encrypts that with a private key of the signer, the content plus the key are then encoded using base64 (Stallings & Brown, 2018. p. 662).

Clear-signed data – Clear-signed data uses a digital signature of the content, but only the digital signature is encoded using base64 (Stallings & Brown, 2018. p. 662).

Signed and enveloped data – Signed and enveloped data allow signed-only and encrypted-only entities to be nested, so encrypted data and signed data or clear-signed data may then be encrypted (Stallings & Brown, 2018. p. 662).

22.2 What is radix-64 conversion?

Radix-64 conversion is an encoding technique, it maps arbitrary binary inputs into printery character outputs (Stallings & Brown, 2018. p. Appendix G.). Radix-64 maps each input group of three octets of binary data into four ASCII characters (Stallings & Brown, 2018. Appendix G.). It has four main characteristics, and that is the range of the function is a character set that is universally representable at all sites, the character set consists of 65 printable characters, no control characters are included in the set, and the hyphen character is not used (Stallings & Brown, 2018. Appendix G.).

22.3 Why is radix-64 conversion useful for an e-mail application?

Radix-64 conversion is useful for an email application is because it converts the inputted data into a radix-64 format regardless of the content, even if the input is in ASCII format (Stallings & Brown, 2018. Appendix G.). This means that even if the content is already signed, but not encrypted, it will still apply its encoding technique onto the text (Stallings & Brown, 2018. Appendix G.).

22.4 What is DKIM?

DKIM, or Domain Keys Identified Mail, is an authentication technique which is designed for emails, it allows for it to be transparent to the end-user (Stallings & Brown, 2018. p. 664 - 666). An email is signed by a private key from the administrative domain of where the email originates, the signature is for all content of the email and some headers, at the receiving end the MDA accesses the corresponding public key to verify the signature of the email, authenticating that the message came from where it says it did (Stallings & Brown, 2018. p. 664 - 666).

22.5 What protocols compromise SSL?

SSL is compromised of HTTP, the handshake protocol, the change cipher spec protocol, and the alert protocol (Stallings & Brown, 2018. p. 668).

Problem

22.1 In SSL and TLS, why is there a separate Change Cipher Spec Protocol rather than including a change_cipher_spec message in the Handshake Protocol?

This question can be answered relatively easily as long as you already know about SSL, TLS, and its protocols. There are a couple of primary reasons why the Changer Cipher Spec protocol is separate rather than included in the message in the Handshake Protocol. It technically could be, there is nothing stopping it from doing so, but there are reasons not to do so. The shortened explanation is that since they are separated it allows it to enforce the behavior in the protocols. SSL uses something

called a message which is then encoded over a record, encryption with SSL is then done on individual records, in a single record there can be multiple messages of the same type combined together, however, the Change Cipher Spec message modifies encryption settings and starting a new record after allows the configured settings to be apply after the Cipher Spec message which is needed for security. However, if it were to be implemented differently, it would work if SSL and TLS start new records at the proper time and were allowed to verify the other connection from the peer started the new record too.

References

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Pearson.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

Dalton Murray