Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

May 22, 2023

Chapter 1 - 3 Review

Question

1.1 Define *computer security*

Computer security is defined as “measures and controls that ensure confidentiality, integrity, and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated” (Stallings & Brown, 2018. p. 2). This to me means that computer security is anything that relates to measuring, controlling, and ensuring the integrity and availability of anything related to technology and its information. For example, configuring an antivirus and firewall are parts of computer security.

When we look at confidentiality there are two parts to it, these parts are data confidentiality and privacy. Data confidentiality means that we are assured that private, or otherwise confidential information is not able to be available or in other ways disclosed to people who are not allowed to access the information (Stallings & Brown, 2018. p. 3). Privacy means that people are able to control and influence the information that is related to them and how and if it is able to be collected and stored as well as whom it is allowed to be stored and collected by (Stallings & Brown, 2018. p. 1.1).

When looking at integrity we have data integrity and system integrity. Data integrity means that information and programs are changed only in a specific and allowed way (Stallings & Brown, 2018. p. 3). System integrity means that we are assuring that a system is performing only its intended functions in a way which it is unimpaired and is free from any deliberate or inadvertent manipulation by people or things which are not allowed to access it (Stallings & Brown, 2018. p. 3).

Availability means that the system is working promptly and that people who are intended and allowed to access it have access to it (Stallings & Brown, 2018. p. 3).

1.3 List and briefly define categories of passive and active network security attacks

There are two primary categories of passive network security attacks. These two categories are the release of message contents, and traffic analysis (Stallings & Brown, 2018. p. 14). Active network security attacks have a few more primary categories. These primary categories are replay attacks, masquerade attacks, the modification of messages, and denial of service (DoS and DDoS) attacks (Stallings & Brown, 2018. p. 14).

Passive attacks are specifically in the nature of eavesdropping, or the monitoring of transmissions and have the goal of obtaining information which is being transmitted (Stallings & Brown, 2018. p. 14). The release of message contents focuses on telephone conversations, electronic mail (email) messages, and transferred files however attackers would likely try to monitor everything which they deem valuable

which may be anything (Stallings & Brown, 2018. p. 14). Traffic analysis attacks are similar to release of message contents, however, they are observing all traffic and try to use it to observe the patterns of messages, such as if an encryption method is put in place, and use it to try to determine the location and identity of the communicating hosts which will help them in guessing the nature of the communications which have occurred and are occurring (Stallings & Brown, 2018. p. 14).

With active attacks, the goal is to involve some sort of modification of data of the creation of false data (Stallings & Brown, 2018. p. 14). With replay attacks, the attacker will passively capture data and use its retransmission to produce an unauthorized effect (Stallings & Brown, 2018. p. 14). With masquerade attacks, the attacker will capture something and then pretend to be it by retransmitting it, for example if someone uses an RFID badge to access a door they can capture the signal if they are close enough and then retransmit it, pretending to be them, and gain access to the locked door (Stallings & Brown, 2018. p. 14). A modification of message attack means that they have taken a legitimate message and then modified it in some way such as delaying or reordering it in order to produce an unauthorized effect (Stallings & Brown, 2018. p. 14). With Denial of Service attacks, as well as Distributed Denial of Service attacks, the primary goal is to inhibit the normal usage and function of communication facilities (Stallings & Brown, 2018. p. 14).

When looking specifically at the categories of these types of attacks we have four primary categories: unauthorized disclosure, deception, disruption, and usurpation (Stallings & Brown, 2018. p. 9 - 11). Unauthorized disclosure consists of: exposure, interception, inference, and intrusion (Stallings & Brown, 2018. p. 9 - 10). Deception

consists of masquerade, falsification, and repudiation (Stallings & Brown, 2018. p. 11). Disruption consists of incapacitation, corruption, and obstruction. Usurpation consists of misappropriation, and misuse (Stallings & Brown, 2018. p. 11). Each of these categories pose different types of threats, unauthorized disclosure is a threat to confidentiality, deception is a threat to the system integrity and data integrity, disruption is a threat to availability and system integrity, and usurpation is a threat to system integrity (Stallings & Brown, 2018. p. 9 - 11).

1.4 List and briefly define the fundamental security design principles

The fundamental security design principles are as follows: economy of mechanism, fail-safe defaults, complete mediation, open design, separation of privilege, least privilege, least common mechanism, psychological acceptability, isolation, encapsulation, modularity, layering, and least astonishment (Stallings & Brown, 2018. P. 17 - 18).

Economy of mechanism – With economy of mechanism, the design of the security measures with both hardware and software should have the goal of being the most simple and small as possible which allows it to be tested and verified thoroughly more easily (Stallings & Brown, 2018. p. 18).

Fail-safe defaults – Fail-safe defaults means that you will have access decisions which are based upon permission rather than exclusion (Stallings & Brown, 2018. p. 18). This, in essence, means that you will default to not having access rather than having excess access (Stallings & Brown, 2018. p. 18).

Complete mediation – Complete mediation means that every access has to be checked against the access control mechanism, in other words systems should not rely on access decisions which are being retrieved from a cache because if it changes and the cache updates it may not necessarily catch this and update itself and just pull from the cache which may result in authorized access (Stallings & Brown, 2018. p. 18).

Open design – Having an open design means that the design of security mechanisms are open rather than secret, such as encryption algorithms but not the encryption keys (Stallings & Brown, 2018. p. 19). This allows for things to be viewed by the open in which it allows them to view and on their own test things to search for vulnerabilities (Stallings & Brown, 2018. p. 19).

Separation of privilege – Separation of privilege means that multiple privilege attributes are required in order to access a restricted source, such as multifactor authentication where you have to get a text or have a randomly generated code every 30 seconds which you can access (Stallings & Brown, 2018. p. 19).

Least privilege – Least privilege is similar to fail-safe defaults where the idea is that the user should only have the minimum amount of privileges needed in order to perform their tasks (Stallings & Brown, 2018. p. 19).

Least common mechanism – Least common mechanism means that the design is supposed to minimize the functions which are being shared by different users which will provide mutual security (Stallings & Brown, 2018. p. 19).

Psychological acceptability – Psychological acceptability means that every security method should not interfere unduly with the work of users, however, it should at

the same time meet the needs of those who authorize access (Stallings & Brown, 2018. p. 19). This also means that security mechanisms should be transparent to the users of the system and introduce minimal obstruction to them while also maintaining a great level of security (Stallings & Brown, 2018. p. 19).

Isolation – Isolation can be applied in a few different ways. The first way is that public access systems, such as a having a demilitarized zone, dmz, should be isolated or cut off or separated from critical resources in order to prevent them from crossing to prevent disclosure and tampering (Stallings & Brown, 2018. p. 20). The second way is that processes and files of users should be isolated from one another except in specific and explicit situations and locations (Stallings & Brown, 2018. p. 20). Thirdly, security mechanisms should be isolated, which means that we try to prevent access to these mechanisms from other things (Stallings & Brown, 2018. p. 20).

Encapsulation – Encapsulation is another form of isolation, it means that a collection of procedures and data objects are of its own and on its own so that the internal structure of the data is only accessible to the procedures of the protected subsystem or encapsulated area (Stallings & Brown, 2018. p. 20).

Modularity – Modularity in security means that the development of security functions are separate, protected modules (Stallings & Brown, 2018. p. 20).

Layering – Layering with security means that there are multiple, overlapping protections approaches which address people and systems (Stallings & Brown, 2018. p. 20).

Least astonishment – Least astonishment means that the system or thing is the least astonishing thing to a user, it is transparent to the user and allows them to be able to understand it easily (Stallings & Brown, 2018. p. 21).

1.5 Explain the difference between an attack surface and an attack tree

An attack surface is only reachable and exploitable vulnerabilities in a system (Stallings & Brown, 2018. p. 21). Some examples of attack surfaces are open ports, services available on the inside of a firewall, the code that processes incoming data such as emails, interfaces such as SQL and web forms, and employees who have access to sensitive information (Stallings & Brown, 2018. p. 21). There are 3 categories of attack surfaces, network attack surface, software attack surface, and human attack surface (Stallings & Brown, 2018. p. 21). The network attack surface is vulnerabilities over an enterprise network, and wide area network (Stallings & Brown, 2018. p. 21). Software attack surfaces are vulnerabilities within applications, utilities, or operating systems (Stallings & Brown, 2018. p. 21). Human attack surfaces are vulnerabilities which are created by personnel or outsiders (Stallings & Brown, 2018. p. 21).

Attack trees differ from attack surfaces in quite a few ways. Attack trees are branching, hierarchical data structures which represent potential techniques for exploiting security vulnerabilities (Stallings & Brown, 2018. p. 22). When looking at an attack tree, the security incident that is the goal of the attacker is the root node of the tree, and the ways in which the attacker is able to access this root node are represented by branches and subnodes of the tree (Stallings & Brown, 2018. p. 22). Each subnode

of a tree are subgoals and each subgoal can have its own subgoals, which is what makes it look like an attack tree because of its root node and branching visuals (Stallings & Brown, 2018. p. 22). Attack trees can also have AND nodes and OR nodes which defines how the branch or node is complete and the objective reaches, AND nodes means that everything much be achieved and the OR node means only 1 of the connected nodes has to be achieved (Stallings & Brown, 2018. p. 22). Attack trees allow the attacker to effectively exploit the information which is available on the attack patterns (Stallings & Brown, 2018. p. 22). Attack nodes can also be good for security analysts to detect and document security attacks in a structured way rather than randomly looking at everything (Stallings & Brown, 2018. p. 22).

2.1 What are the essential ingredients of a symmetric cipher?

A symmetric cipher, or symmetric encryption scheme has five ingredients. These five ingredients are as follows: plaintext, encryption algorithm, secret key, ciphertext, and a decryption algorithm (Stallings & Brown, 2018. p. 32).

Plaintext – Plaintext is the original message or data before it has gone through the encryption algorithm (Stallings & Brown, 2018. p. 32).

Encryption algorithm – The encryption algorithm is what handles substitutions and transformations on the plaintext, in other words it is what encrypts the message or data (Stallings & Brown, 2018. p. 32).

Secret key – The secret key is another input to the encryption algorithm, it uses the secret key in order to perform its substitutions and transformations (Stallings & Brown, 2018. p. 32).

Ciphertext – The ciphertext is the output of the encryption algorithm, it is in an encrypted or scrambled form (Stallings & Brown, 2018. p. 32).

Decryption algorithm – The decryption algorithm, combined with the ciphertext and secret key decrypts the ciphertext and outputs the original message or data in plaintext (Stallings & Brown, 2018. p. 32).

2.2 How many keys are required for two people to communicate via a symmetric cipher?

With symmetric encryption, or a symmetric cipher, the sender and receiver share the same key, so the result is there is a single key required for two people to communicate (Stallings & Brown, 2018. p. 37).

2.3 What are the two principal requirements for the secure use of symmetric encryption?

The two principal requirements for the secure usage of symmetric encryption is having a strong encryption algorithm and that the sender and receiver must both have a copy of the secret key and have been obtained them in a secure way (Stallings & Brown, 2018. p. 32). The idea with symmetric encryption for the first principal

requirement is that that for people who have access to the algorithm, should they gain access to ciphertext, they are unable to decipher the ciphertext or figure out the key, however, this is at a minimal requirement (Stallings & Brown, 2018. p. 32). We would ideally have it so that the third party, should they have already obtained many ciphertexts and plaintexts are still unable to decrypt the ciphertext or discover the key of new ciphers (Stallings & Brown, 2018. p. 32). With the second principal requirement, if a third party obtained the key then it would make the entire communication pointless as they are able to obtain the decrypted plaintext (Stallings & Brown, 2018. p. 32).

3.1 In general terms, what are four means of authenticating a user's identity?

Generally, there are four means of authenticating a user's identity. These four means are: something the individual knows, something the individual possesses, something the individual ism, and something the individual does (Stallings & Brown, 2018. p. 66).

Individual knows – An example of something an individual knows is a password, or a PIN (Stallings & Brown, 2018. p. 66).

Individual possesses – An example of something an individual possesses is an electronic keycard, or a smart card, or a physical key (Stallings & Brown, 2018. p. 66).

Individual is – An example of an individual is includes their fingerprints, retina, and face (Stallings & Brown, 2018. p. 67).

Individual does – An example of an individual does is their voice patterns, handwriting, and typing (Stallings & Brown, 2018. p. 67).

3.2 List and briefly describe the principal threats to the secrecy of passwords

The principal threats to the secrecy of passwords are as follows: offline dictionary attacks, specific account attacks, popular password attacks, password guessing against a single user, workstation hijacking, exploiting user mistakes, exploiting multiple password use, and electronic monitoring (Stallings & Brown, 2018. p. 70).

Offline dictionary attack – It is possible for an attacker to gain access to a system's password file, they are then able to use an offline dictionary, which is frequently just a text file or a file in CSV format which is simply an extremely long list of passwords, words, and character combinations which they can then compare to the hashes found in the system's password file (Stallings & Brown, 2018. p. 70). If there is a match, they can then use the password to gain access to the system (Stallings & Brown, 2018. p. 70 - 71).

Specific account attack – With a specific account attack the attacker will target a specific account by submitting lots of password guesses until the password is discovered or they are unable to continue guessing by means of a set amount of password attempts (Stallings & Brown, 2018. p. 71).

Popular password attack – A popular password attack is similar to a offline dictionary attack where they use a large file of popular passwords and try them against a large range of usernames (Stallings & Brown, 2018. p. 71).

Password guessing against a single user – With password guessing against a single user there are many ways to do it, however, they will target a single user, similar to the specific account attack, and attempt to gain knowledge about the user and password to try to guess the username and password correctly (Stallings & Brown, 2018. p. 71).

Workstation hijacking – With workstation hijacking the attacker will wait until a logged in user leaves the workstation unattended and then use it to perform unauthorized activities (Stallings & Brown, 2018. p. 71).

Exploiting user mistakes – With exploiting user mistakes, the attacker will try to find mistakes the user makes such as writing their password on a sticky note and then using it to access the account (Stallings & Brown, 2018. p. 71).

Exploiting multiple password use – With exploiting multiple password use, many people use the same password for all of their accounts, they are able to find one password to their other accounts and then use it to gain access to every account (Stallings & Brown, 2018. p. 71).

Electronic monitoring – With electronic monitoring, the attacker is able to monitor the network to try to find communicated passwords in order to gain access (Stallings & Brown, 2018. p. 71).

3.3 What are two common techniques used to protect a password file?

One common technique used to protect a password file is through the usage of a salt value (Stallings & Brown, 2018. p. 72). With using a salt value, a new password is entered into the system, the user then is able to select or gets assigned a password, and the password is combined with a fix-length salt value (Stallings & Brown, 2018. p. 72). The hashed password is then stored within the passwords file, the plaintext copy of the salt value is also stored with the password file (Stallings & Brown, 2018. p. 72). When trying to log in with a salt value, the user provides their username and password, the operating system then uses the username to index the password file and retrieve the salt value with is used to decrypt the password along with the user's password (Stallings & Brown, 2018. p. 72). Using a salt value helps prevent duplicate passwords from being visible in the password file, increases the difficulty of dictionary attacks, and it makes it nearly impossible to figure out if the person uses the password on multiple systems (Stallings & Brown, 2018. p. 73).

Another way to protect a password file is through the usage of password file access control (Stallings & Brown, 2018. p. 77). This means that the attacker is denied access to the password file unless they have access to a privileged user account along with a whatever else is set to be on the password file such as needing an additional password along with the privileged user's credentials (Stallings & Brown, 2018. p. 77). It is also important to use a shadow password file, meaning that the usernames are kept separate from the password file (Stallings & Brown, 2018. p. 77).

Problem

3.1 Explain the suitability or unsuitability of the following passwords:

Today's base level requirement for passwords are as follows:

12 characters long

Minimum of 1 capital letter

Minimum of 1 lower case letter

Minimum of 1 number or punctuation

No spaces

Cannot be based upon your name, username or id, or on words found any any dictionary

Cannot be based on simple repeating patterns

(https://www.uic.edu/apps/strong-password/)

I will run each password through two checkers. The first one is more basic and only looks at characters themselves and does not look if it contains names, locations, or anything intelligent, https://www.uic.edu/apps/strong-password/. The second one is more advanced and looks at more things such as common names, locations, brute force attack time, and if it already exists in a couple of dictionaries. The brute force also is purely a brute force time and not checking if it exists already in any dictionary which would significantly cut down times.

a. YK 334

Unsuitable. This password simply does not have enough characters or complexity in order to make it meet today's base level requirement for passwords.

Password YK 334

☐ Hide password

Complexity Weak

Score

Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	6	+ 24
Uppercase letters	Cond/Incr	+((len-n)*2)	2	+ 8
Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	2	0

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	0	0
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	2	- 3
Consecutive uppercase letters	Flat	-(n*2)	1	- 2
Consecutive lowercase letters	Flat	-(n*2)	0	0
Consecutive numbers	Flat	-(n*2)	2	- 4
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional Exceeds minimum standards. Additional bonuses are applied.

Sufficient Meets minimum standards. Additional bonuses are applied.

Warning Advisory against employing bad practices. Overall score is reduced.

Failure Does not meet the minimum standards. Overall score is reduced.

TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 16 minutes
Fast Desktop PC	About 4 minutes
GPU	About 2 minutes
Fast GPU	49 seconds
Parallel GPUs	5 seconds
Medium size botnet	0 seconds

Dictionary attack check

'YK ' + '334' is not a safe word combination. The word is composed of two components: 1) 'YK ' is a dictionary word. 2) The string '334' follows the pattern [dictionary word][one or two digits].

Your password is:	Not safe!

b. mfmitm (for “my favorite movie is tender mercies)

Unsuitable. This password does not meet base level requirements for passwords, and has repeating characters.

Password mfmitm

☐ Hide password

Complexity Very Weak

Score

Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	6	+ 24
Uppercase letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	6	0
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	1	0

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	6	- 6
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	3	- 2
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	5	- 10
Consecutive numbers	Flat	-(n*2)	0	0
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional Exceeds minimum standards. Additional bonuses are applied.

Sufficient Meets minimum standards. Additional bonuses are applied.

Warning Advisory against employing bad practices. Overall score is reduced.

Failure Does not meet the minimum standards. Overall score is reduced.

TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	3 seconds
Fast Desktop PC	1 second
GPU	0 seconds
Fast GPU	0 seconds
Parallel GPUs	0 seconds
Medium size botnet	0 seconds

Dictionary attack check

'mfm' + 'itm' is not a safe word combination. The word is composed of two components: 1) 'mfm' is a dictionary word. 2) 'itm' is a dictionary word.

Your password is:	Not safe!

c. Natalie1

Unsuitable. This password does not meet base level requirements for passwords and contains a name.

Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	8	+ 32
Uppercase letters	Cond/Incr	+((len-n)*2)	1	+ 14
Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 4
Numbers	Cond	+(n*4)	1	+ 4
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	4	+ 8

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	0	0
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	2	- 1
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	5	- 10
Consecutive numbers	Flat	-(n*2)	0	0
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional Exceeds minimum standards. Additional bonuses are applied.

Sufficient Meets minimum standards. Additional bonuses are applied.

Warning Advisory against employing bad practices. Overall score is reduced.

Failure Does not meet the minimum standards. Overall score is reduced.

TOP 10000 password	YES	**Password is one of the most frequently used passwords.**

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 25 days
Fast Desktop PC	About 6 days
GPU	About 3 days
Fast GPU	About 1 day
Parallel GPUs	About 3 hours
Medium size botnet	2 seconds

Dictionary attack check

The string 'Natalie1' follows the pattern [dictionary word][one or two digits].

Your password is:	Not safe!

d. Washington

Unsuitable. This password does not contain base level requirements for passwords and contains a common location.

Password Washignton

☐ Hide password

Complexity Weak

Score

Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	10	+ 40
Uppercase letters	Cond/Incr	+((len-n)*2)	1	+ 18
Lowercase Letters	Cond/Incr	+((len-n)*2)	9	+ 2
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	3	0

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	10	- 10
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	2	- 1
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	8	- 16
Consecutive numbers	Flat	-(n*2)	0	0
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional Exceeds minimum standards. Additional bonuses are applied.

Sufficient Meets minimum standards. Additional bonuses are applied.

Warning Advisory against employing bad practices. Overall score is reduced.

Failure Does not meet the minimum standards. Overall score is reduced.

TOP 10000 password	YES	Password is one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 46 years
Fast Desktop PC	About 12 years
GPU	About 5 years
Fast GPU	About 2 years
Parallel GPUs	About 3 months
Medium size botnet	About 24 minutes

Dictionary attack check

'Washington' is a dictionary word.

Your password is:	Not safe!

e. Aristotle

Unsuitable. This password does not contain base level requirements for passwords and contains a name.

Password Aristotle

☐ Hide password

Complexity Weak

Score

Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	9	+ 36
Uppercase letters	Cond/Incr	+((len-n)*2)	1	+ 16
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 2
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	3	0

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	9	- 9
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	2	- 1
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	7	- 14
Consecutive numbers	Flat	-(n*2)	0	0
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional Exceeds minimum standards. Additional bonuses are applied.

Sufficient Meets minimum standards. Additional bonuses are applied.

Warning Advisory against employing bad practices. Overall score is reduced.

Failure Does not meet the minimum standards. Overall score is reduced.

TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 11 months
Fast Desktop PC	About 3 months
GPU	About 1 month
Fast GPU	About 16 days
Parallel GPUs	About 2 days
Medium size botnet	28 seconds

Dictionary attack check

'Aristotle' is a dictionary word.

Your password is:	Not safe!

f. tv9stove

Unsuitable. This password also does not meet base level requirements for a password, despite being very slightly more complex it does not meet length requirements, capital requirements, special character/punctuation requirements.

Password	tv9stove
	☐ Hide password
Complexity	Weak
Score	

Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	8	+ 32
Uppercase letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 2
Numbers	Cond	+(n*4)	1	+ 4
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	1	+ 2
Requirements	Flat	+(n*2)	3	0

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	0	0
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	4	- 1
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	5	- 10
Consecutive numbers	Flat	-(n*2)	0	0
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional Exceeds minimum standards. Additional bonuses are applied.

Sufficient Meets minimum standards. Additional bonuses are applied.

Warning Advisory against employing bad practices. Overall score is reduced.

Failure Does not meet the minimum standards. Overall score is reduced.

TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 8 hours
Fast Desktop PC	About 2 hours
GPU	About 47 minutes
Fast GPU	About 24 minutes
Parallel GPUs	About 2 minutes
Medium size botnet	0 seconds

Dictionary attack check

'tv9' + 'stove' is not a safe word combination. The word is composed of two components: 1) The string 'tv9' follows the pattern [dictionary word][one or two digits]. 2) 'stove' is a dictionary word.

Your password is:	Not safe!

g. 12345678

Unsuitable. This password does not meet the base level of requirements for a password and contains a set of counting numbers which are incredibly common.

Password 12345678

☐ Hide password

Complexity Very Weak

Score

Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	8	+ 32
Uppercase letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
Numbers	Cond	+(n*4)	8	0
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	6	+ 12
Requirements	Flat	+(n*2)	2	0

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	0	0
Numbers only	Flat	-n	8	- 8
Repeat Characters (case insensitive)	Comp	-	0	0
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	0	0
Consecutive numbers	Flat	-(n*2)	7	- 14
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	6	- 18
Sequential symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional Exceeds minimum standards. Additional bonuses are applied.

Sufficient Meets minimum standards. Additional bonuses are applied.

Warning Advisory against employing bad practices. Overall score is reduced.

Failure Does not meet the minimum standards. Overall score is reduced.

TOP 10000 password	YES	Password is one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	1 second
Fast Desktop PC	0 seconds
GPU	0 seconds
Fast GPU	0 seconds
Parallel GPUs	0 seconds
Medium size botnet	0 seconds

Dictionary attack check

'12345678' is a dictionary word.

Your password is:	Not safe!

h. dribgib

Unsuitable. This password also does not meet the base level requirements for passwords such as length, and otherwise basic levels of complexity.

Password dribgib

☐ Hide password

Complexity Very Weak

Score

Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	7	+ 28
Uppercase letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	0
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	1	0

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	7	- 7
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	4	- 2
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	6	- 12
Consecutive numbers	Flat	-(n*2)	0	0
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional Exceeds minimum standards. Additional bonuses are applied.

Sufficient Meets minimum standards. Additional bonuses are applied.

Warning Advisory against employing bad practices. Overall score is reduced.

Failure Does not meet the minimum standards. Overall score is reduced.

TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 1 minute
Fast Desktop PC	20 seconds
GPU	8 seconds
Fast GPU	4 seconds
Parallel GPUs	0 seconds
Medium size botnet	0 seconds

Dictionary attack check

The word 'dribgib' is reverse of the dictionary word 'bigbird'.

Your password is:	Not safe!

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