Analysis Of Default Passwords In Routers Against Brute-Force Attack

Mohammed Farik, ABM Shawkat Ali

Abstract: Password authentication is the main means of access control on network routers, and router manufacturers provide a default password for initial login to the router. While there has been many publications regarding the minimum requirements of a good password, how widely the manufacturers themselves are adhering to the minimum standards, and whether these passwords can withstand brute-force attack are not widely known. The novelty of this research is that this is the first time default passwords have been analyzed and documented from such a large variety of router models to reveal password strengths or weaknesses against brute-force attacks. Firstly, individual default router password of each model was collected, tabulated, and tested using password strength meter for entropy. Then, descriptive statistical analysis was performed on the tabulated data. The analysis revealed quantitatively how strong or weak default passwords are against brute-force attacks. The results of this research give router security researchers, router manufacturers, router administrators a useful guide on the strengths and weaknesses of passwords that follow similar patterns.

Index Terms: brute-force, default passwords, entropy, router security

1 Introduction

ROUTER manufacturers set default password, which a router administrator is supposed to change during router setup (Fig.1). These default passwords are already known passwords, thus irrespective of their length, cardinality or entropy, they are declared as weak passwords. This is because any password that is known or published is not secure, as it can be easily discovered through various techniques and used for hacking. Hence, router administrators are required to change the known default password of router after initial login. However, for security reasons, the new changed password for *login* (Fig.1) as well as for *wireless security* (Fig.2) are never intentionally revealed or published by router administrator. Thus, if a password cannot be easily cracked by using easier techniques, as the last resort an attacker may use brute-force technique.

1.1 Aim

In this research, we aim to find whether default password of routers can withstand brute-force attacks.

1.2 Novelty

The novelty of this research is that this is the first time default passwords have been analyzed and documented from such a large variety of router models to reveal password strengths or weaknesses.

1.3 Importance

This research provides results that give insight on the strengths or weaknesses of passwords that follow the same patterns as default passwords of routers. IT also identifies some gaps in router security with areas of future work.

- *Mohammed Farik is an Assistant Lecturer in Information Technology in the School of Science and Technology at The University of Fiji, PH-679-6640600. E-mail: mohammedf@unifiji.ac.fj*
- *ABM Shawkat Ali is a Professor in Information Technology in the School of Science and Technology at The University of Fiji*

Fig.1. *Log in to the router*

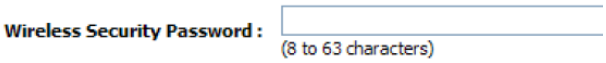

Fig.2. *Password Setup in Wireless Router*

2 Literature Review

2.1 Router

A router is a device that connects multiple networks and routes data packets on a network to their next location so that they can efficiently reach their destination [1]. It uses password authentication for access control and administration of the router. If the password is not secure and strong, hackers can take control of the router and the network by cracking the password.

2.2 Default Password

A default password is a password administered into a router by the router manufacturer for the purpose of initial login and authentication by a buyer or new administrator of a router. Also, a router reverts to the default password if it is reset on the hardware. While default password of a specific router can be collected from the manufacturer's installation manual, there are websites of default passwords of routers freely available on the internet from manufacturers, researchers, or hackers from which passwords can be collected. One such website is routerpasswords.com [2].

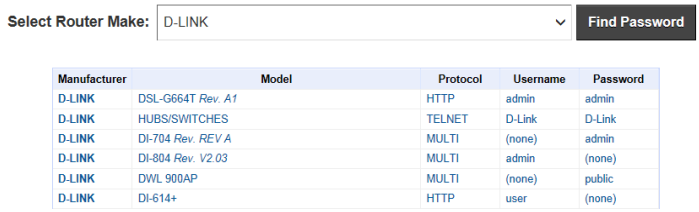

Fig.3. *RouterPasswords.com website*

2.3 Brute-Force Attack Technique

The ready availability of default passwords on the internet for instance makes default passwords insecure for access control on a network router. If the default passwords are not changed by administrators of routers, a router can be easily hacked into by cracking passwords using techniques such as dictionary attack, rainbow table attack, bulk password attack, and others [3]. When these techniques have failed to reveal or crack the password, an attacker then uses brute-force attack technique. Brute force is a computationally intensive technique that generates a series of passwords using character combinations, with which it then tries to crack the router password. It is a method where Maximum-Time-To-Defeat (MTTD) the password is estimated. Maximum-Time-To-Defeat (MTTD) represents the maximum limit of time in which the entire set of combinations of password can be produced by a computer [4]. A successful cracking of password using brute-force attack will take no longer time than this maximum limit of time. How successful the brute force attack will be depends largely on the length of the password set on the router, the character combinations the password is composed of, and the speed of the cracking computer [3].

2.4 Entropy

Entropy is a password's complexity calculated in number of bits. The formula to calculate entropy value for each password is shown in Equation (1) [4].

$$Entropy = \log_2 N^L \quad (1)$$

In Equation (1), N represents password cardinality and L the length. Fig.4 shows possible cardinalities that can be achieved with combinations of upper-case letters (UC), lowercase letters (LC), special characters (O), additional keyboard symbols (S), and decimal numbers (D), and blanks (N) from Fig.5. Password entropy can help calculate number of guesses needed to crack a password. It is not an indicator of the time it will take to crack the password using brute-force attacks with advanced computer technologies. The survivability question is answered using MTTD. Previous research shows that a minimum 8-character password with the cardinality score of 94 equaling an entropy value of 52.4 bits is secure and deemed strong, a reason why wireless security password in routers is supposed to be from 8-63 characters (Fig.2). Table 1 contains our compiled list of criteria for creating a strong password [1], [6], [7].

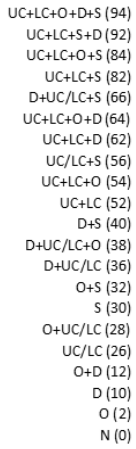

Fig.4. *Possible Cardinalities*

TABLE 1

CRITERIA FOR COMPILING A STRONG PASSWORD

No.	Current Ideal Password Requirements
1	Should be at least 8 character length
2	Should have a cardinality of 94
3	Should equal to at least 52.4 bits entropy
4	Should not reveal any pattern
5	Should be non-dictionary word
6	Should not be information e.g. names, birth-date, etc.
7	Can be built around a passphrase
8	Should not be any known password, e.g. default passwords
9	Should not be a previously used password

Using online websites such as asswordStrengthCalculator.org (Fig.4), administrators can test their passwords for survivability against brute-force attacks [5].

Fig.5 *PasswordStrengthCalculator.org meter*

Fig.5 shows that an 8 character password with a cardinality of 94 has entropy of 52.4 bits and can be cracked by a supercomputer in a time of approximately 0.07 seconds and by a PC & GPU in 20 minutes. This shows that the current

standards of length and entropy are weak and needs improvements.

3 METHODOLOGY

Entire data on routers in RouterPassword.com online database (Fig. 3) is extracted in step 1 and datasheet-1 is created in Excel in step 2. The compiled dataset contained sample size of 1096 instances with five attributes (variables) - manufacturer, model, protocol, username and password. In step 3, PasswordStrengthCalculator.org online meter (Fig.5) is used to test the performance of each password one at a time. The length and cardinality information is entered in the meter, and the meter outputs the entropy and time within which the password can be cracked in step 4. In step 5, test results on additional attributes (variables), the length, cardinality, entropy and time are updated in datasheet-1. Then in step 6, descriptive analyses were performed on datasheet-1 using software tools such as Weka, SPSS, and Excel. In this research, we shall categorize a password as weak if it has entropy<52.4, and strong otherwise. In step 7, the analysis findings are discussed in analysis report-1. A few gaps are then listed down in step 8.

4 DATA ANALYSIS

The analysis of 1096 instances (records) of router data revealed firstly, the presence of 328 distinct manufacturers (Fig.6). There are 190 (17%) manufacturers that have only one router model in the dataset. The top 10 manufacturers highest numbers of models in descending order belong to 3Com (71 or 6.5%), then HP (67 or 6.1%), and then D-Link (44 or 4%), Lucent (37 or 3.4%), Nortel (32 or 2.9%), Netgear (3.1 or 28%), Cisco (2.8%), Alcatel (22 or 2%), Linksys (21 or 1.9%), and Siemens (20 or 1.8%).

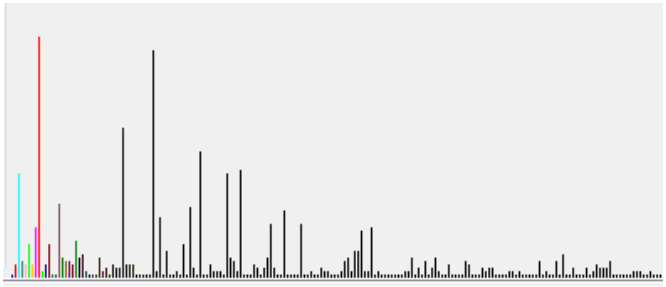

Fig.7 *Distinct Manufacturers*

Secondly, there are 784 distinct models of routers in the 1096 instances. Some manufacturers have multiple same-name models because each uses a different protocol. However, there are instances where different manufacturers use a common name for the model. For example, model name *router* is used by the manufacturers Bay Networks, 3Com, Billion, Verifone, Adtran, Netgear, and RM. Instances such as this has resulted in 673 (61%) unique names for router models in this analysis. Thirdly, there are 49 distinct protocols in the 1096 instances. Out of the 49 distinct protocols 32 (3%) have presence in a single instance. The top 10 protocols in descending order of frequency are Multi (415 or 37.9%), HTTP (278 or 25.4%), Telnet (136 or 12.4%), null (unspecified) (111 or 10.1%), console (57 or 5.2%), SNMP (14 or 1.3%), FTP (11 or 1%), Port 2533 (11 or 1%), Port 7000 (7 or 0.06%), Serial (4 or 0.04%), HTTPS (4), and SSH (4) which altogether makes up 921 or 84 % of instances (excluding null). Fourthly, there are 228 distinct usernames in the 1096 instances, out of which 152 (14%) are unique usernames having only a single occurrence in the dataset. Most Common usernames in descending order of frequency are admin (319 or 29.1%), null, that is n/a, blank, or none (259 or 23.6%), root (62 or 5.6%), Administrator (30 or 2.7%), MGR (23 or 2%), user (15 or 1.4%), tech (13 or 1.3%), sysadm (8 or 0.07%), operator (8), FIELD (8), router (7 or 0.06%), manager (7), login (7), and guest (6 or 0.05%) which altogether makes up 772 or 70% instances. Fifthly, there are 359 distinct passwords have been found to be used for routers in this dataset (Fig.8). However, there were only 259 (24%) unique passwords used. Common default passwords in routers are null, that is login without password (206 or 18.8%), admin (173 or 15.8%), password (66 or 6%), 1234 (32 or 2.9%), epicrouter (18 or 1.6%), 0 (15 or 1.4%), root (11 or 1%), changeme (11), tech (11), access (10 or 0.9%), smcadmin (10), and router (9 or 0.8%).

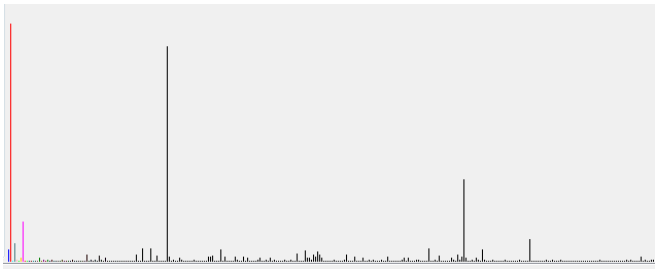

Fig.8 *Distinct Passwords*

Sixthly, the frequency distribution of default router password lengths shows all default passwords lengths in the study are between 0 and 19 characters, with a mean of 4.96 characters (Fig.9). Out of the 1096 default passwords, 18.6% (about 200) are of length 0 meaning 'no password is required'. The most common password length is 5 making up 21.5% of all default router passwords. The pie chart shows that only 23% of default router 1096 passwords are greater than or equal to 8 characters (Fig.10). Here, 77% of the router models have not adhered to the secure password lengths requirement of at least 8 characters as per literature search requirements. Table 2 shows the mean, standard deviation and other descriptive statistics on the length, cardinality, and entropy of default passwords.

TABLE 2
DESCRIPTIVE STATISTICS ON LENGTH, CARDINALITY, ENTROPY

		Length	Cardinality	Entropy
N	Valid	1096	1096	1096
	Missing	0	0	0
Mean		4.96	22.50	23.62
Std. Error of Mean		.092	.428	.471
Median		5.00	26.00	23.50
Mode		5	26	0
Std. Deviation		3.058	14.177	15.609
Variance		9.349	200.974	243.649
Skewness		-.095	.331	.260
Std. Error of Skewness		.074	.074	.074
Range		19	82	108
Minimum		0	0	0
Maximum		19	82	108
Percentiles	25	4.00	10.00	13.50
	50	5.00	26.00	23.50
	75	7.00	26.00	34.20

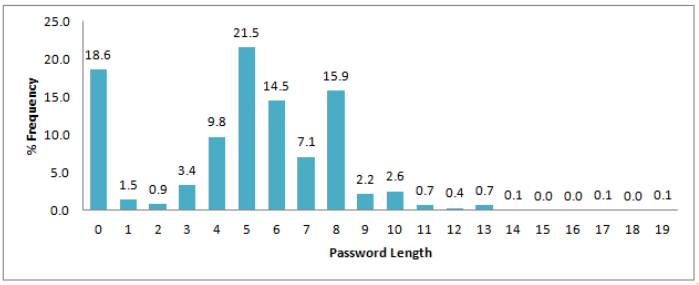

Fig.9 *Distribution of password lengths*

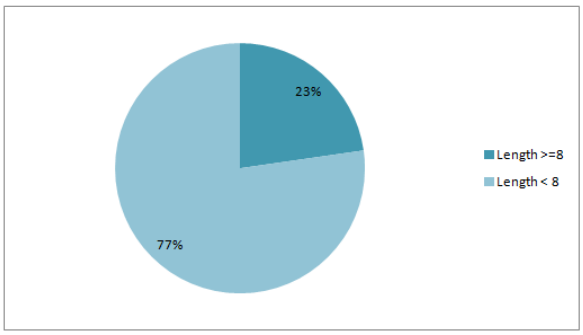

Fig.10 *Length Classes*

Seventhly, the analysis revealed that router's default passwords only belong to 10 distinct cardinalities out of 21 cardinalities (Fig.11). The minimum password cardinality in the dataset is 0, maximum is 82, and mean is 22.5. As expected, there is a high occurrence (18.6% or 205) cardinality of 0 as a result of length of 0 characters (blank or null). About 6.7% (10) passwords were solely composed of decimal digits; while 63.8% (699) default passwords were composed of either uppercase or lower case alphabets. There were no passwords that were composed of the ideal cardinality score of 94.

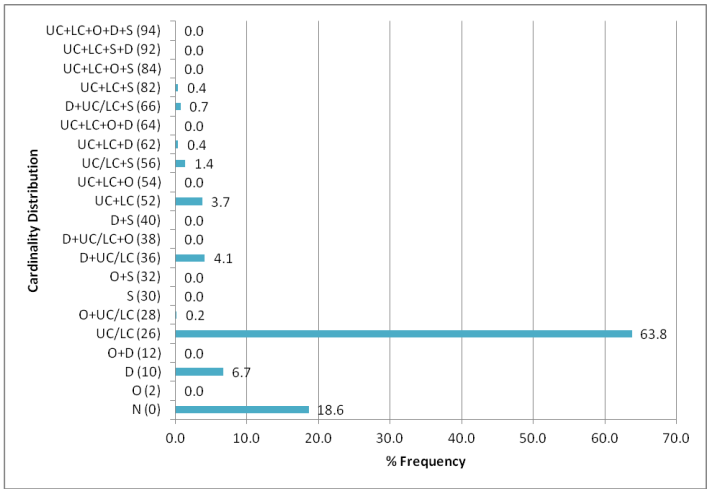

Fig.11 *Distribution of password cardinality*

Eighthly, the 359 distinct passwords in the study belonged to one of 56 distinct entropies as seen in the frequency distribution (Fig.12). 18 of these 56 entropies were unique. Furthermore, the minimum entropy is 0; maximum is 108.3 mean is 23.62, and the standard deviation is 15.609. Moreover, as seen in the pie chart (Fig.13), 97% of the current router passwords is below 52.4 bit entropy as opposed to requirements stated in literature review.

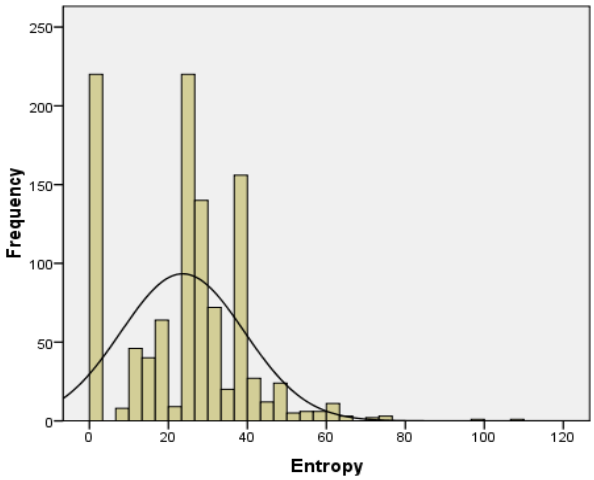

Fig.12 *Distribution of password entropy*

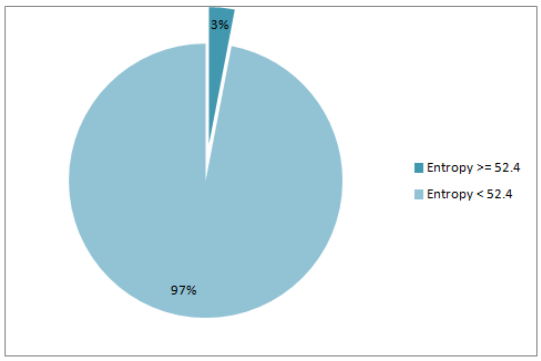

Fig.13 *Entropy Classes*

Entropy of default passwords in routers can be mathematically represented by the linear Equation (2) as shown in Fig.14.

$$y = 0.0469x – 2.0834 \quad (2)$$

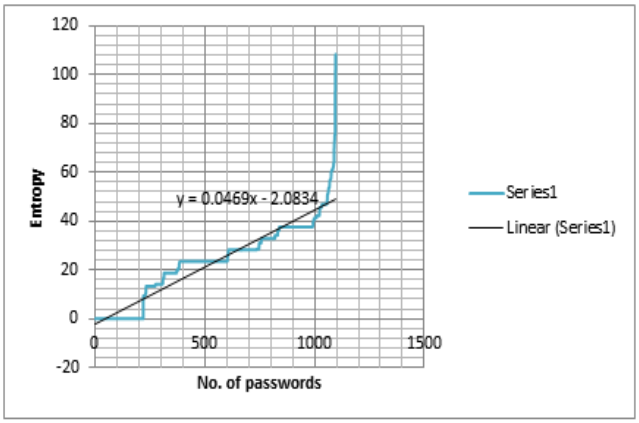

Fig.14 *Linear Regression graph on Entropies of Router Default Passwords*

Ninthly, Fig.15 shows the number of default passwords in router that can be successfully brute-force hacked within the stated time-frames. This means that of the 1096 passwords, 1057 or about 96.4% can be cracked within 32 seconds, 11 within 45 minutes, 8 within 17 hours, 14 within 39 days, and 7 will take more than 20 years.

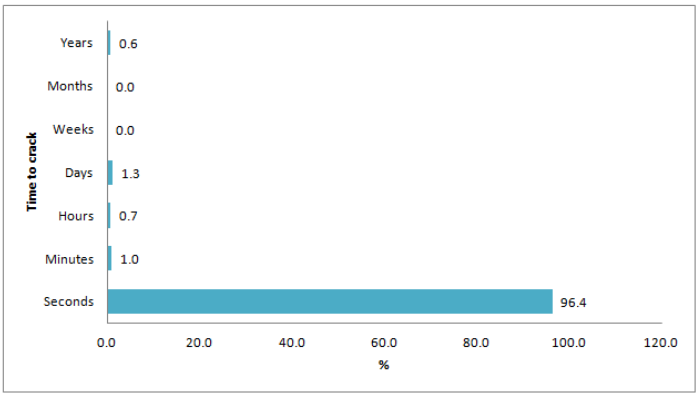

Fig.14 *Distribution of no. of passwords with time needed to crack*

5 Gaps and Future Work

Default router passwords can now be confirmed as of weak strength against brute-force attacks techniques also. Hence, default passwords should not be mimicked when entering new passwords on routers. It would be better if there are some built-in software mechanisms in routers that not only tests a password for entropy but also only allows entry of strong passwords for both router login and wireless security. This research showed that only 23% of the default passwords were 8 or more characters in length, none had a cardinality of 94, and only 3% met the 52.4 bits entropy benchmark. However, looking at the distribution on the time needed to successfully crack password using brute-force attack techniques, it can be seen that using the current bench marks, only 7/1096 or 0.0064% passwords can be declared safe as they will require years to crack. Hence, we believe that the length of the passwords should be increased from 8 to at least 12 characters with a cardinality of 94.

6 Conclusions

This research shows that router manufacturers have themselves failed to adhere to password standards. This has led to default passwords being weak against brute-force attacks, and they should not be used as a model for creating new passwords by router administrators. This is because they do not use the current minimum requirements of character length, cardinality, and entropy. It can be further implied that it is time to now set up a higher benchmark for minimum length and cardinality of password to a minimum of 12 characters and 94 cardinality respectively.

References

[1] D. Morley and C. S. Parker, Understanding Computers: Today and Tomorrow, 14th ed., Boston: Course Technology- Cengage Learning, 2013, p. 352.

[2] "RouterPasswords," [Online]. Available: http://www.routerpasswords.com. [Accessed 10 April 2014].

[3] "Understanding Password attacks," [Online]. Available: http://passwordstrengthcalculator.org/understand.php. [Accessed 10 April 2014].

[4] "Interpreting the Calculation," [Online]. Available: http://passwordstrengthcalculator.org/interpret.php. [Accessed 10 April 2014].

[5] "Estimate password strength and survivability," [Online]. Available:http://passwordstrengthcalculator.org/index.php. [Accessed 10 April 2014].

[6] "Create Effective Passwords," [Online]. Available: http://passwordstrengthcalculator.org/understand.php. [Accessed 10 April 2014].

[7] "ASCII chart," [Online]. Available: http://lookuptables.com. [Accessed 10 April 2014].