Random Password Generation

Kirk Smith

Old Dominion University

April 15, 2022

Introduction:

This paper will discuss the topic of random generation, first by explaining the topic, followed by how the literature review was performed. Then, a literature review will be performed, followed by a discussion of human biases and the strength of random password generation.

When examining the word "random", it is important to understand what that word means. In statistics, the word random means a collection of unbiased and uncorrelated data (Smith, 2021). However, when it comes to security, it is important that we have a very strong definition of random (Smith, 2021). Flipping a coin, rolling dice or another independent, unbiased action are all examples of true randomness (Smith, 2021). It is important that one applies true randomness to network security.

When examining this concept for computers one encounters some specific issues. Computers often use pseudorandom number generator (PRNG), which is a computer process that generates numbers from a procedure (Smith, 2021). PRNGs are not truly random because they are determined by the procedure that generates them (Smith, 2021). As a result, there may be ways to unravel this process in a way that threatens security (Smith, 2021).

When examining for use by humans one encounters separate issues as well. When examining a particular set of characters (52 upper- and lower-case letters, 10 digits, and 32 punctuation symbols) we see that there are 94^8 (or about 6 quadrillion) possible 8-character passwords (Chwan-Hwa Wu, 2016). However, humans are extremely biased, so biased in fact, that they reduce these possibilities down orders of magnitude, reducing the number of

possibilities to about 1 million common passwords (Chwan-Hwa Wu, 2016). As a result, the number of possible passwords is reduced which threatens security.

Methods:

To begin my research, I began by looking through the textbook "Elementary Information Security Third Edition" by Richard Smith. I also looked through the ODU libraries site to examine articles. I also worked with Abbie Basile, a librarian from ODU, who specializes in Engineering, Science, and Mathematics. In our meeting, we discussed the research strategies that I could employ. Some of the resources we discussed were Monarch OneSearch, Science Direct as well as the library guides that ODU has (I examined the one involving computer science).

I also looked through the ACM Digital Library, IEEE Xplore and Computers & Applied Sciences Complete using the keyword of "pseudorandom generator". Some additional discussions that took place involved Bibliography Citation systems (Zotero, End Note, Easy Bib and Pro cite) as well as how to search a database (using certain characters). Additional keywords that were discussed in our meeting were "random generator", "PRG" and "PRNG". Ms. Basile provided me with tips on how to research including starting with a broad search of just 2 or 3 keywords, limiting by language/date, and trying different words in search based on words found in the abstracts, titles, and keywords/subject lists.

Ms. Basile suggested using double quotes around multiple words, common phrases like "random generator" or "computer crime". It was also discussed that words in double quotes will cause the database to search for exactly what one types. She also suggested that if I had synonyms or acronyms to use () parentheses to put them together in a single search. Additionally, she provided me with information on using Interlibrary Loan (ILL).

Literature Review:

The first source that will be discussed is "A comparative study of three random password generators**".** In this study, they focused on systems that employ random passwords and they compared three schemes for generating such random passwords (Michael D. Leonhard, 2007). The first, ALPHANUM, creates sequences of random characters (Michael D. Leonhard, 2007). The second, Diceware, creates lists of words (Michael D. Leonhard, 2007). The last one, Pro-nounce3, creates strings of syllables (Michael D. Leonhard, 2007). The source also suggests improvements for the schemes including generating mnemonic aids for ALPHANUM passwords, removing obscure words in the wordlist for Diceware and adding capital letters/punctuation to the Pronounce3 scheme (to gain entropy) (Michael D. Leonhard, 2007).

The second source, "A 48-bit pseudo-random generator" statistically tested a new 48 psuedo-random number generator for randomness (Kuehn, 1961). It was used to assess its adequacy in Monte Carlo programs (Kuehn, 1961). Statistical tests were applied to half a million generated numbers lying within the interval (0,1) and to three sets of integers obtains from specified bits within the generated numbers (Kuehn, 1961). The study goes on to say that they were able to substantiate the randomness of all numbers except for the set of integers coming from the least significant bits (Kuehn, 1961).

The third source, "Memristor-based chaotic circuit for pseudo-random sequence generators" showed how memristor-based chaotic circuits were exploited for pseudo-random generators (Fernando Corinto, 2016).

The fourth source, "Revisiting the Concrete Security of Goldreich's Pseudorandom Generator" the study looks at Goldreich's pseudorandom generators (Jing Yang, 2021). They

suggest new parameters for achieving 80-bit (128-bit) security with respect to their attacks (Jing Yang, 2021).

The fifth source, “The Pseudo-random Code Generator Design Based on FPGA” they discuss how pseudo-random sequence is widely used in information technology, digital communications, cryptography, automatic control, and other areas (Lan, 2010).

The sixth source, “A secured trust creation in VANET environment using random password generator”, they discuss the network (VANET) that they use (G. Gowtham, 2012). In the article, they also define a random number generator (RNG) as a device designed to generate a sequence of numbers or symbols that lack any pattern, i.e. they will appear random (G. Gowtham, 2012). They describe VANET as an adhoc network that uses moving cars as nodes in a network to create a mobile network (G. Gowtham, 2012). In their proposed work instead of maintaining long records of node details in central trusted authority, they use a password generator to generate a password and then have the parent node distribute them to the child nodes (G. Gowtham, 2012).

The seventh source, “Assistance in Daily Password Generation Tasks” they discuss their method of password generation (Karola Marky, 2018). They state that they have a deterministic method of password generation, and they utilize a master password as well (Karola Marky, 2018). Additionally, they implement a mobile app and pre-evaluated it (Karola Marky, 2018). They state that their pre-evaluation indicates that their scheme offers good usability (Karola Marky, 2018).

In the eighth source, “Random number generation”, they state that a random number generator is a computer procedure that scrambles the bits of a current digits from a set of

numbers to produce a new one (Marsaglia, 2003). Additionally, they state that it is done in such a way that the result appears to be randomly distributed among the set of possible numbers and independent of the previously generated numbers (Marsaglia, 2003). The article also states that they work well for limited use (when only a few hundred or thousands of numbers are required) (Marsaglia, 2003). However, they state that a random number generator must be chosen carefully if using very fast computers doing Monte Carlo problems (which requires samples of hundreds of millions or billions of numbers) (Marsaglia, 2003).

Discussion:

It could be argued that the random generation of passwords are an attempt to protect individuals from themselves. Individuals often will choose a simple password that contains a word and a number (Michael D. Leonhard, 2007). A similar perspective was echoed in the literature review that stated that people are biased, and they will choose passwords that are of a limited number of combinations (Chwan-Hwa Wu, 2016). These biases are exploited through dictionary attacks whereby attackers can retrieve some passwords if they focus on likely passwords (Smith, 2021). In one situation the success of dictionary attacks by researchers varied from 20 to 35 percent, thus emphasizing the importance that randomness must play in password generation (Smith, 2021).

Additionally, it should be noted that random passwords can provide strength. Calculations show that randomly generated passwords provide roughly six billion times more combinations versus person generated passwords (roughly 6 quadrillion random combinations for randomly generated versus one million for person generated) (Chwan-Hwa Wu, 2016). A modern desktop computer can calculate 100,000 hashes per second and thus it is reasonable to assume that a password generated by a person could be cracked in 10 seconds versus roughly

1902 years for a randomly generated password (Smith, 2021) (Chwan-Hwa Wu, 2016). Such vast differences show the strength of a randomly generated password and the security that it can provide.

Conclusion:

In conclusion, random password generation is an important part of network security. In this paper we reviewed different sources that cover the topic of random password generation. The first topic that was addressed in the review was discussion of different random password generation schemes (Michael D. Leonhard, 2007). The second topic addressed statistically testing a new pseudo random number generator for randomness (Kuehn, 1961). The third topic addressed using a circuit for pseudo-random generators (Fernando Corinto, 2016). The fourth topic was a discussion of improving on a pseudorandom generator (Jing Yang, 2021). The fifth topic explained how pseudorandom sequence is widely used in information security, digital communications, cryptography, automatic control, and other areas (Lan, 2010). The sixth topic addressed the utilization of a random password generator for application on their network (G. Gowtham, 2012). The seventh topic talks about a system that creates random-looking passwords based on stored meta data describing the account, password properties required by the target service and a secret master password (Karola Marky, 2018). The eighth and final topic defined what a random number generator is (Marsaglia, 2003). It should be recognized that additional information of importance regarding this topic exists beyond this review.

It is important to know what random means because there are many different definitions of random. When it comes to security, we need a strong definition of random. Random passwords provide greater possibilities than human- chosen ones as humans generally will choose a limited set of possibilities for a password. As a result of this, attackers can reduce their

search when it comes to search space for a particular password. Random password generation will continue to a part of information security now and into the future.

Citations:

Chwan-Hwa Wu, J. D. (2016). *Introduction to Computer Networks and Cybersecurity.* Boca Raton: CRC Press.

Fernando Corinto, O. V. (2016). Memristor-based chaotic circuit for pseudo-random sequence generators. Lemesos: IEEE.

G. Gowtham, E. S. (2012). A secured trust creation in VANET environment using random password generator. *International Confrence on Computing, Electronics and Electrical Technologies (ICCEET)* . Nagercoil: IEEE.

Jing Yang, Q. G. (2021). Revisiting the Concrete Security of Goldreich's Pseudorandom Generator. *IEEE Transactions on Information Theory* , 1329-1354.

Karola Marky, P. M. (2018). Assistance in Daily Password Generation Tasks . *Proceedings of the 2018 ACM International Joint Confrence and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, (pp. 786-793).

Kuehn, H. G. (1961, August). A 48 bit pseud-random generator.

Lan, L. (2010). The Pseudo-random Code Generator Design Based on FPGA. Yichang: IEEE.

Marsaglia, G. (2003, January). Random number generation.

Michael D. Leonhard, V. V. (2007). A comparative study of three random password generators. *2007 IEEE International Confrence on Electro/Information Technology* (pp. 227-232). IEEE.

Smith, R. E. (2021). *Elementary Information Security Third Edition.* Burlington: Jones & Bartlett Learning.