Random Password Generation

KIRK SMITH

OLD DOMINION UNIVERSITY

COVA CCI

APRIL 22, 2022

Introduction

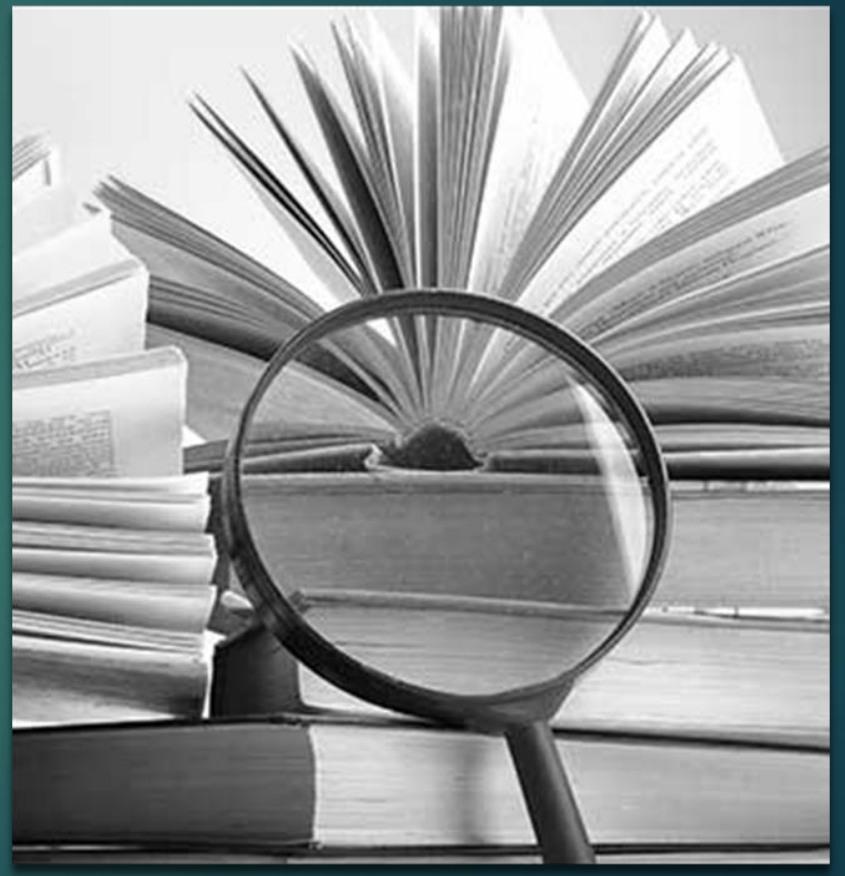
- It is important that we have a very strong definition of random (Smith, 2021).
- Flipping a coin, rolling dice or another independent, unbiased action are all examples of true randomness (Smith, 2021).
- It is important that one applies true randomness to network security.
- Computer issues and Human issues with Randomization

Methods

- "Elementary Information Security Third Edition" by Richard Smith
- Abbie Basile (librarian from ODU)
  - Monarch OneSearch, Science Direct as well as the library guides
  - Discussed 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.
  - Discussed utilizing "" and () in searches.

Literature Review

1. “A comparative study of three random password generators”
2. “A 48-bit pseudo-random generator”
3. “Memristor-based chaotic circuit for pseudo-random sequence generators”
4. “Revisiting the Concrete Security of Goldreich’s Pseudorandom Generator”
5. “The Pseudo-random Code Generator Design Based on FPGA”
6. “A secured trust creation in VANET environment using random password generator”
7. “Assistance in Daily Password Generation Tasks”
8. “Random number generation”



Discussion

- It could be argued that the random generation of passwords are an attempt to protect individuals from themselves.
  - People are biased, and they will choose passwords that are of a limited number of combinations.
  - These biases are exploited through dictionary attacks whereby attackers can retrieve some passwords if they focus on likely passwords.
  - In one instance he success of dictionary attacks by researchers varied from 20 to 35 percent, thus emphasizing the importance that randomness must play in password generation.
- Random Passwords provide strength to network security.
  - Calculations show that randomly generated passwords provide roughly six billion times more combinations versus person generated passwords.
  - 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)

Conclusion

- Random password generation is an important part of network security.
  - Different sources that cover the topic of random password generation were reviewed.
- It is important to know what random means because there are many different definitions of random.
- Random password generation will continue to a part of information security now and into the future.

Citations

Sources

- 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.

Picture Sources

- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQi5yc5VjQmoEJJNT_U30O7043VqSTXtw7hyQ&usqp=CAU
- https://elements-cover-images-0.imgix.net/4452067a-740e-4bae-b81c-bb9f8e972ac4?auto=compress%2Cformat&fit=max&w=632&s=179f69732594f3c5dc283b11f4a800ca
- http://wtgrantfoundation.org/library/uploads/2016/05/research-use-in-policy.jpg
- https://leverageedu.com/blog/wp-content/uploads/2020/03/Types-of-Research-Design.jpg
- https://imageio.forbes.com/specials-images/imageserve/61e875f405571b26080777c7/0x0.jpg?format=jpg&width=1200
- https://d138zd1ktt9iqe.cloudfront.net/media/seo_landing_files/relation-of-billion-with-other-numbers-1618907502.png
- https://www.travelers.com/iw-images/resources/Business/Large/NetworkSecurity_large.jpg