Application of the Aho-Corasick algorithm to create a network intrusion detection system

Komil Tashev
Cryptology
Tashkent university of information technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
k.akhmatovich@gmail.com

Agzamova Mokhinabonu
Providing Information security
Tashkent university of information technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
mshagzamova@gmail.com

Axmedova Nozima
Cryptology
Tashkent university of information technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
rrsanobar18@mail.ru

***Abstract*— .....**

.....
..... .

Keywords*— *(max.6)

1. INTRODUCTION

In 2019, Positive Technologies specialists recorded more than 1,500 attacks; this is 19% more than in 2018. In 81% of cyber attacks, the victims were legal entities. At the end of the year, the five most frequently attacked industries included government agencies, industry, medicine, science and education, and the financial industry. [1]

2. RELATED WORKS

Precise Matching. The string matching problem can be simply formulated - for two strings T and P of length m and n, respectively, determine if P occurs in T. Naive or brute force search involves trying to match a pattern using a window size of length n and iterating over each position in T from left to right, resulting in the worst-case complexity O (mn). Boyer-Moore [2] and KMP [3] are two classic singlestring matching algorithms. Both of these algorithms also use a window of size n, but they use a skip or shift table to determine where to look next after each mismatch.

3.1. METHODS (OPTIONAL).

3.2. FORMULATION OF THE PROBLEM (OPTIONAL)

3.3. ALGORITHM FOR SOLVING THE PROBLEM (OPTIONAL)

3.4. RESULTS OF SIMULATION MODELING (OPTIONAL)

3.5. THE OBTAINED RESEARCH RESULTS (optional)

4.1. RESULTS

4.2. DISCUSSION

5. CONCLUSION

ACKNOWLEDGMENTS (OPTIONAL).

PRACTICAL RECOMMENDATIONS (OPTIONAL).

REFERENCES

[1] Current Cyber Threats: Results of 2019 - https://www.ptsecurity.com/ru-ru/research/analytics/cybersecuritythreatscape-2019/

[2] Boyer R.S. and Moore, J.S. (1977). A Fast String Searching Algorithm. Communications of ACM, 20(10), pp.762-772.

[3] Knuth, D.E., Morris, J. and Pratt, V.R. (1977). Fast Pattern Matching in Strings. SIAM Journal on Computing. 6(2), pp.323-350

[4] Horspool, R.N. (1980). Practical fast searching in strings. Software: Practice and Experience. 10(6), pp.501-506.

[5] Baeza-Yates, R. and Gonnet, G.H. (1992). A new approach to text searching. Communications of the ACM , 35(10), pp.74-82.

[6] Dharmapurikar, S., Krishnamurthy, P., Sproull, T. and Lockwood, J.W. (2003). Deep Packet Inspection Using Parallel Bloom Filters. Proceedings 11th Symposium on High Performance Interconnects (HotInterconnects). pp.44-51.

[7] Bloom, B.H. (1970). Space/time trade-offs in hash coding with allowable errors. Commun. ACM. 13(7), pp.422-426.

[8] Song, H. and Lockwood, J.W. (2005b). Multi-pattern Signature Matching for Hardware Network Intrusion Detection Systems. IEEE Global Telecommunications Conference GLOBECOM'05. vol.3, 5 pages.

[9] Zhou, Y. and Wang, X. 2010. Efficient Pattern Matching with Counting Bloom Filter. CIICT2010.

[10] Markatos, E., Antonatos, S., Polychronakis, M. and Anagnostakis, K. (2002). Exclusion-based Signature Matching for Intrusion Detection. In Proceedings of IASTED International Conference on Communications and Computer Networks (CCN 2002);

[11] Tharaka PMK, Wijerathne DMD, Perera N, Vishwajith D, Pasqual A. Runtime rule-reconfigurable high throughput NIPS on FPGA. In: International Conference on Field Programmable Technology (ICFPT); 2017. p. 251–4.