Paradigm Shift in Adaptive Cyber Defense for Securing the Web Data: The Future Ahead

Shishir Kumar Shandilya

School of Data Science & Forecasting, Devi Ahilya University, Indore – MP, India
School of Computing Science & Engineering, VIT Bhopal University, India
E-mail: sksmebackup@gmail.com

Received 05 January 2022; Accepted 06 March 2022;
Publication 18 April 2022

Abstract

Web Applications are becoming more sophisticated to cater the ever-growing demand of data processing and computing. Fast technological advancements in web engineering not only facilitate data intensive and high-performance computing, but also raise serious concerns on security. Cyber threats are also ramping up at the equal pace and attackers are now more organised and equipped with high-end servers. The Data over Web needs to be more authenticated and reliable. Data Provenance-aware methods are capable of identification of data breaches and manipulation through various attacks. They analyse underlying data for the potential threats to ensure protection against various attacks. Cyber Security Practitioners are witnessing severe issues in securing the Web Data and applications as the security risks are growing rapidly due to the sudden eruption in internet usage due to the pandemic in the last few years. People and organisations are relying more on Internet and web applications than ever before. The efforts for securing the web data on such a massive scale is premature to counter the ever-evolving attack attempts. Nature-inspired Cyber Security (NICS) facilitates the development and implementation of robust defensive mechanisms which

Journal of Web Engineering, Vol. 21_4, 1371–1376.
doi: 10.13052/jwe1540-9589.21416

are more adaptive and highly tolerant to online malicious programs. These methods are also capable of dealing with the common algorithmic issues like incompleteness and uncertainty of information and to provide a high-level security mechanism by effectively implementing the bio-inspired methodologies like deception, and camouflage etc. This article will attempt to explore the effectiveness of NICS in web data and application security to provide smart security methods.

Keywords: Web data security, security risks, nature-inspired cyber security, cyber threat analysis.

1 Introduction

Web data since the beginning of world-wide-web has incorporated several types of data sources and it is well-accepted and used by several technologies till date. Machine Learning and Artificial Intelligence treatments are now honing the existing technologies and taking them to another level. Unfortunately, it is true for both the ends as the attackers are also getting undue advantages due to the enormous possibilities with the disruptive techniques. The hackers are gaining access to an organization through an active and smart reconnaissance by implementing the most advanced algorithms on high-performance machines. Above all, they are now more organised and well-coordinated to conduct the attacks on a bigger scale, which makes the web more vulnerable with more risks of compromising data. The conventional signature-based defense methods are getting obsolete as they are failing to serve the prime purpose of privacy and safety. This also leads to interrupt the business continuity in case of a cyber-attack. More adaptive and response-based defensive methods are required to handle these complex security issues.

Nature-inspired methods are implemented in multiple domains and found stable and reliable for multi-objective problems as well. More importantly, the nature-inspired methods are capable to handle the incompleteness, fuzziness and incorrectness of data, which makes them a potential methodology to be used for adaptive cyber defense. Motivated by nature-inspired computing methods, a new concept called Nature-inspired Cyber Security (NICS) is proposed by the researchers, which is targeted to build a behaviour-based defense system by mimicking the behaviour and concepts of natural species. NICS provides a wide range of adaptive defense methods by utilizing the

network data and build a natural resilience phenomenon by structurization and aggregation of available information. Along with this, NICS methods are also capable of implementing self-organization and deception in the proposed security solutions.

2 Related Works

We have proposed a novel network testbed for experimenting with NICS-based security mechanisms with full library support [1]. The testbed can be used to simulate the NICS security in the presence and absence of configured attacks and to compare the proposed mechanism. It can be used to analyse the network behaviour during the active attack based on the various parameters like network devices, load, number and types of clusters and communication protocols. This unified and standard testbed can be used for investigating and benchmarking the best security solution.

Later, we have experimented with NICS-based solution for web attack detection system in addition to the existing Intrusion Detection System [2]. We were successful to generate the adaptive responses of proposed method which is tested and validated on multiple attack scenarios for detecting the suspicious activities. In this work, we have implemented framework of Firefly Optimization method to categorize the malicious activities and to generate the early alerts for Intrusion Detection System.

3 Related Issues and Challenges

With many possibilities, NICS also has several issues and challenges to become a well-established technique. Undoubtedly, NICS offers multiple advantages over conventional defensive mechanism but it is also true that NICS requires a lot of customization, tuning and configuration of processes followed by a rigorous and time-consuming testing and analyse phase, every time when it is being implemented in a new domain. It is mainly because of its behaviour-based mechanism and also as it is relatively new concept. Therefore, NICS is quite typical and cumbersome at its initial stage.

Apart from this, NICS also has following other issues as well, which are required to be catered before expecting the intended results,

3.1 It is often difficult to understand and mimic the exact relationships and processes of nature, and then to implement them for a stable security mechanism [2].

3.2 Troubleshooting of NICS-based defense mechanisms are also difficult and requires dedicated manpower in the organization.
3.3 Management of False Positive alert is also very critical and it may hinder the overall system response.
3.4 Additional cost for training and maintenance.
3.5 Many nature-inspired algorithms are yet to be explored. They may perform better than the experimented ones.

Due to the fore-mentioned issues, NICS is being implemented in parallel with the conventional system or to assist the existing systems. However, the researchers are continuously improving the concept and soon it will be mature enough to handle the entire security mechanism. The potential of NICS is being explored by implementing various nature-inspired algorithms on different types of networks and application domains.

4 The Future Ahead

The organizations are now more focused towards the effective implementation and regulation of information security policies to standardize the threat management issues. The organizations are looking forward to have a more adaptive, automated and intelligent defense system. The NICS can offer many unique functionalities like self-regulation, automatic threat monitoring, cyber deception and even autonomic computing. NICS can also be very useful in achieving Cyber Immunity which is defined as a condition where the cost of attack is to be made way too high than the gain by the attack (Ref. Kaspersky). In near future, the promising defense technologies like AI/ML, Quantum Computing and NICS will transform the current security solutions. These solutions will be more accurate, will be able to learn themself, will have more visualization of entire network. Moreover, the security systems of future would be more reliable and will be able to respond to the attacks while maintaining the business continuity.

5 Conclusions

We have attempted to explore the opportunities with NICS while discussing about some of the related works and future aspects of this highly potential and futuristic security mechanism. However, the full-fledge security solution based only on NICS is yet to be achieved. The future of this methodology looks promising especially when the concept of camouflaging the network

architectures, cyber deception and honeypots is already in place. NICS can be an advantage to achieve an adaptive, self-regulated, and an automatic defense system, especially for the application domains where the operational data is multi-variant, incomplete, or poorly-managed. This editorial article attempts to showcase the potential of NICS and to encourage the readers to research and experiment on this upcoming security technology.

References

[1] SK Shandilya, S Upadhyay, A Kumar, AK Nagar, AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis, Future Generation Computer Systems, Elsevier, 2022

[2] SK Shandilya, Design and Analysis of NICS Based Web Attack Detection for Advanced Intrusion Detection System, Iberoamerican Knowledge Graphs and Semantic Web, Springer, 2021

[3] Gautam, R., Kaur, P. & Sharma, M. A comprehensive review on nature inspired computing algorithms for the diagnosis of chronic disorders in human beings. Prog Artificial Intelligence 8, 401–424, 2019

[4] Michael Warner. Cybersecurity: A pre-history. Intelligence and National Security, 27, 2012

[5] Hong S. Choi M. S. Lee S. J. Kim T. W. Lee S. W. Ha B. N. Lim, I. H. Security protocols against cyber-attacks in the distribution automation system. IEEE Transactions on Power Delivery, 25(1):448–455, 2010

[6] Robert Dewar. The "triptych of cyber security": A classification of active cyber defense. International Conference on Cyber Conflict, CYCON, pages 7–21, 2014

[7] Dewar, Robert, Active Cyber Defense, 2017

[8] Ricardo Neisse, Gary Steri, Igor Nai Fovino, and Gianmarco Baldini. Seckit: A model-based security toolkit for the internet of things. Computers Security, 58, 2015

[9] Neal Wagner, Cem Ş. Sahin, Jaime Pena, and William W. Streilein. Automatic generation of cyber architectures optimized for security, cost, and mission performance: A nature-inspired approach. pages 1–25, 2019

[10] Vajiheh Hajisalem and Shahram Babaie. A hybrid intrusion detection system based on abc-afs algorithm for misuse and anomaly detection. Computer Networks, 136, 02 2018

Biography

Shishir Kumar Shandilya is the Deputy Director of SECURE – Centre of Excellence in Cyber Security and Division Head of Cyber Security and Digital Forensics at VIT Bhopal University. He is working as a Principal Consultant to the Govt. of India for Technology Development and Assessment in Cyber Security. He also holds the position of Executive Director of National Cyber Defense Research Centre, New Delhi. He is a Visiting Researcher at Liverpool Hope University-United Kingdom, a Cambridge University Certified Professional Teacher and Trainer, ACM Distinguished Speaker and a Senior Member of IEEE. He is a NASSCOM Certified Master Trainer for Security Analyst SOC (SSC/Q0909: NVEQF Level 7) and an Academic Advisor to National Cyber Safety and Security Standards, New Delhi. He has received the IDA Teaching Excellence Award for distinctive use of technology in Teaching by Indian Didactics Association, Bangalore (2016) and Young Scientist Award for two consecutive years, 2005 and 2006, by Indian Science Congress and MP Council of Science and Technology. He has seven books published by Springer Nature-Singapore, IGI-USA, River-Denmark and Prentice Hall of India. His recently published book is on Advances in Cyber Security Analytics and Decision Systems by Springer.