REST Journal on Emerging trends in Modelling and Manufacturing
Vol: 5(4), 2019
REST Publisher; ISSN: 2455-4537

Website: http: //restpublisher.com/journals/jemm/

Evaluation of Phishing Websites Using WPM Method

Valecha Deepika Vashdev
SST College of Arts and Commerce, Maharashtra, India
deepikavalecha@sstcollege.edu.in

Abstract

Phishing websites, a new type of malicious software, have proliferated online in recent years, posing a serious threat to data security and online financial services. In this study, we develop and apply an intelligent model for phishing website detection. This study looks at spammers' behavior at the network level, including the IP address ranges that send the most spam, common spamming techniques (such as BGP redirects and bots), the characteristics of each spamming host, and spamming botnets. We simulate a multi-echelon system in which disruptions may arise and various mitigation measures may be assessed at any point to safeguard client service in the event of an interruption. Strategies that make use of the network itself include satisfying demand by purchasing goods or arranging for transportation from a different source or route within the network, as well as keeping strategic inventory balances throughout the network. One of the fastest-growing crimes on the Internet is phishing, a type of online identity theft. The anti-phishing (APA) protocol, which is based on SPEKE a Password Authenticated Key Exchange (PAKE) protocol, is one of many countermeasures and proposals that have been made over the years. This paper demonstrates how the APA protocol is susceptible to malicious server assaults, password compromise impersonation, and intermediate key compromise impersonation. A protocol with improved anti-phishing features, such as mutual authentication and forward secrecy, is also suggested. Large amounts of spatial data may be obtained via satellites, radars, and sensor networks thanks to developments in information technology and innovative approaches. This paper is a weighted product for solving the routing decision problem Model (WPM) used. Every Dynamically assigns weights to criteria This proposed scheme Considers the relevant valuation method for Alexa, Alexa Login, Phish Tank, APWG, and Open Phish. URLs, Extracted, Domains, TLDs, and Logins. Alexa, Alexa Login, Phish Tank, APWG, Open Phish. URLs, Extracted, Domains, TLDs, and Logins. APWG is got the first rank whereas Open Phish has the Lowest rank. **Keywords:** Phishing. Network management, Authentication, Client-Side, Server, Library User Education, WPM Method.

1. INTRODUCTION

A phishing website scam is a relatively recent type of cybercrime when compared to malware attacks. Phishing is a type of internet fraud in which perpetrators use social engineering techniques. Sensitive information (such as passwords, personal identification numbers, and financial account information) can be obtained by tricking people into disclosing it through the use of emails, instant chats, or online adverts that lure users to phishing websites. Security software programs often use a filtering blacklist against recognized domains to guard against phishing websites. However, there is consistently a lag time between website reporting and updates to blacklists. Since phishing websites now only exist for a few hours instead of days, this approach might not work. Several research projects have been completed in recent years on creating intelligent methods for phishing website detection and anti-phishing. This research gives a network-level analysis of spam's (unsolicited commercial email) characteristics. high level of focus The content of spam is meant to be read, but it receives little consideration. network-level spam features that are paid for. The majority of today's spam botnets, according to conventional opinion, are located in Asia, and few studies have attempted to assess some of these traits. Disruptions are a given in the dynamic supply networks of today. The more links there are in the supply chain, the more challenging it is to manage uncertainty both upstream and downstream. In this paper, we concentrate on a company that we know takes into account the risks of supply chain interruptions and various solutions to handle that risk. We simulate how a business can use components of its network to defend against those disturbances. With the help of this multi-echelon model, managers can receive quantitative advice on the best risk-reduction tactics for their network. These quantitative models take into account the network as a whole and enable risk-reduction decisions. Phishing is a risky cyber security tactic that involves impersonating websites and using social engineering to fool Internet users into disclosing sensitive information (such as credit card numbers, PINs, protected passwords, etc.). The most typical method of conducting a phishing attack is by sending thousands of phony emails to online consumers. These emails are made to appear as though they were sent by legitimate businesses with approval. Phishers can steal sensitive information by preying on users' account information, Social Security numbers, and credit card numbers because this is a severe issue. To accomplish this, aspiration first created a phony website that is nearly identical to the real one. Imagine a library where only the librarians are aware of the books that are checked out, as well as the ones that readers have taken from the shelves. Did the reader simply skim the material

after taking a book off the shelf and returning it, as is known to the library staff? Either put it on the shelf or carefully read a few pages. Staff members are aware of which magazines, whose pages were duplicated, and their intended uses if a copier was used to copy them. Employees can better understand how the collection is utilized, what areas need improvement and other things with the use of this information. In brief, the staff can teach patrons how to use the library more effectively. In the world of written texts, this sort of tracking is impossible. Email server engines become overloaded with bandwidth and server storage due to spam messages. Additionally, Phishing mail, a type of spam mail that tries to entice users to divulge personal information and login credentials, is becoming a severe danger to the security of end users. Many mail servers nowadays, including Gmail, Yahoo, and others, use and evaluate various authentication approaches to maintain email content and classify texts using blacklisting and whitelisting. Large towns and cities continue to have an increasing population, which is keeping up with the growth of vehicles. Thus, the daily construction of the existing transportation infrastructure caused by these two developing populations causes serious traffic issues. Similar to how the size of an existing one cannot be changed, traffic jams are nearly always caused by massive automobiles. The fundamental cause of traffic delays is predictability. Road repairs, vehicle accidents, and other things really poor weather conditions Congestion can be blamed on a poor road network in developing nations. Rush hour may also occasionally see constant congestion. Continue driving; delays on the road use up a lot of fuel. Staff and students are reduced to wasting time on buses due to financial losses and environmental damage to the city. Information literacy is quickly becoming a crucial component of user education in university libraries. Despite this, many non-librarians still find it to be an alien concept. Information literacy is essentially distributed throughout the population, according to Virkus. Information specialists like librarians are not well-known in other areas and are neither explicit nor detailed. The phrase "information literacy" was frequently coined to describe the expansion of electronic information. Through cellular and wireless networks, electronic information is accessible wherever the user goes. Young people who enroll in higher education frequently use their newest electronic equipment at home. They discover that "digital technologies are enabling." Fast access to the richest resources throughout the world wherever you are the collection." As a result, people are depending more and more on electronic information. Their situation is hardly unique. Brophy, We are all now distance learners as a result of technological transmission.

2. PHISHING

Because the phishing problem is complex and includes a variety of scenarios, the definition of phishing attacks in the literature is inconsistent. Phishing, for instance, is a false attempt to acquire your personal information that is typically performed by email, according to Phish Tank. Phishing is a type of computer attack that uses electronic communication channels to spread socially engineered messages to people to influence them into taking specific actions that will benefit the attacker. For instance, the action carried out (by the attacker convincing the victim to carry it out) for a PayPal user is providing his/her login information to a bogus website that mimics PayPal. As a by-product, this also suggests that the assault should make the end-user feel as though they must do this step, such as by warning them that their accounts would be suspended if they don't check in to update specific pieces of information. The identification of phishing is a difficult issue. Although security procedures are not computer flaws, this is largely phishing, which is a semantic-based attack that especially targets human vulnerabilities. Phishing spam is a type of unsolicited mass email that might increase the likelihood of phishing assaults, but it differs from the former in that it is primarily used for marketing or product promotion. The topic of this particular survey is phishing. In email phishing, the credentials of genuine users are stolen for fraudulent purposes by phishers via social engineering and impersonation phishing. This study offers a thorough computer analysis of phishing methods and countermeasures. Anti-phishing tools, or failure to provide an integrated overview of research approaches to various phishing techniques, have been the subject of prior studies and taxonomies. The taxonomy proposed in this research, which is multidimensional, sets itself apart from earlier ones by focusing on a single dimension. Furthermore, present taxonomies only include phishing through conventional methods like emails and fake websites.

3. NETWORK MANAGEMENT

To make meaningful information easily accessible for human network operators, network management systems should make significant volumes of surveillance and measurement data sets available that have been synthesized, filtered, and objectively visualized. The topological network scenes of first-generation network management systems are widely known. To make the setup for topological maps simpler, they provided automatic finding and mapping processes. Network management systems frequently offer time series in addition to topological views to allow users to see how to force measurements have changed over time. Typically, the time scale for these time series ranges from days and weeks to months and years. Only one managed device is covered by a management job. In this instance, a mobile agent is dispatched by the network management station to a controlled device to carry out a certain duty. It can change a managed configuration variable and retrieve the state of a device or managed configuration variable. When the mobile agent is connected to a managed device, it is given access to the management data that is kept there. The mobile agent then carries out the necessary task within the context that has been provided. Before the mobile agent stops itself, the task's outcome is sent back to the network management station via a messaging application. The network management station needs a managed device for the management duty and numerous techniques. By having a network management station send several SNMP requests to managed clients, this scenario expands on the first situation. The managed location's static agent receives instructions from

the node. a tool used to carry out a specific duty. As before, the task can involve changing a number of the controlled device's configuration settings or checking the status of a number of its structure variables.

4. AUTHENTICATION

To help you make the best choice, our method distinguishes between the stated and actual identities on a web page. This domain name serves as the source of the current web page's true identity. When we conduct a keyword search, the claimed identity is obtained from the return search results. Phishing phone scams are impossible to stop. Therefore, fewer password phishing attacks are within the purview of the suggested solution. In other words, if the website is used, our technology can lower the likelihood that password phishing attacks would be successful. However, phishers may target instant messaging services that deliver time passwords to those services and try users' account names and sensitive information. These two attacks go outside the purview of this essay. We also refrain from talking about compromised consumer machines, such as Keyloggers and Root Kids have complete control over how personal computer monitors interact with one another. Attackers collect sensitive information, including usernames and passwords, from the initial user inputs and track it, store it, and transmit it to other parties. Finally, we avoid talking about website compromises when sensitive information on the server can be accessed.

5. CLIENT-SIDE

As was said in the beginning, when offered as a service, the watershed definition Solutions found in the literature require a server. The definition task is not computationally expensive after a watershed. However, because the application is delivered on demand and is accessed by hundreds of users, managing this procedure on the server is not a simple operation. For service providers, it is computationally expensive to calculate each user's requirement. Due to this workload, client-side job delegation to server-side technologies can be handled more efficiently. Full data reporting to the client side has a drawback that can be overcome by encoding the data as an image. lower DEM resolutions, as was already noted. When dealing with the client's hydrological interpretation- Page rather than the server side when data volume is high, it can be stated that client computers are powerful enough to do such work and the algorithm is straightforward to run a given number of times. After encoding, an image can be edited. Future deletions of changed data will be cached during client-side data transfer from the server. These implementations all involve comparable actions and conduct. You can utilize them by integrating them with command-line interfaces or the import of languages, among other planned resources. Inline package Server-side apps accept binary versions of DEM data in addition to the encoded PNG file as input. When the command line provides correct input, the output should be either the generated KML coordinates or the scope water level. Although we don't offer the necessary application interfaces for such an application, it should be noted that these procedures can be further extended to data in which the original text has been encoded.

6. SERVER

The organization first determines which traffic zone the car is in using GPS-filtered log location and a matching algorithm for point-to-curve mapping. Yangon, Myanmar, experiences heavy rain In Sheldon, myaynigone, chawdwingone, ad, and 8 miles junction, there may occasionally be traffic, and during rush hour, vehicles are more congested in the evening than in the morning. The next phase is location after determining the current location, when, how frequently, and how continuously learned traffic is heavily based on that past data. Next, the GPS data of the vehicle's behavior are examined. This indicates that when speed is calculated, the time segment frequently crosses the threshold and the distance between sections is close to the farthest door. The algorithm then uses a Bayes classifier to anticipate the present traffic situation after integrating vehicle data and past vital location data. The finished product will be stored in the cloud and used as a training example for traffic detection in the future. Our server-side picture spam filter subsystem will be made available. We initially provide a flowchart for the component, including positive details. A similarity metric caused by sparsity for cluster analysis of spam pictures. The picture spam filter subsystem will be provided by our server side. We initially provide a flowchart for the related system, with positive details. A similarity metric caused by sparsity for cluster analysis of spam pictures.

7. LIBRARY USER EDUCATION

Understanding how to use a big library all throughout their lives, students should be treated well. One goal of higher education is to help students locate reliable knowledge for their own use. Professionals should also stay current and update themselves. It makes sense that a fresh student might feel threatened by a huge academic library. Maybe there wasn't much access to public libraries and schools. Students now have a harder time finding relevant information due to the boom in freshly published material throughout the years. User education initiatives should ease fear and assist new users in navigating the library's mysteries. Although students do not explicitly state a need for instruction, there may be some that would make their search for specific words and sources more effective. Goals should obviously be determined before moving on to strategies and media.

8. WEIGHT PRODUCT METHOD

Weighted Product Model (WPM) is a Well known Multi-Criteria Decision Making (MCDM)/ Multi-Criteria Decision Analysis (MCDA) method. AHP is combined with the Weight Product Method (WPM). The complexity of these methods does not increase with the AHP rate as the number of alternative websites increases. The weight Product Method (WPM) uses linguistic terms that are easy for users to understand and therefore, methods are considered easy to implement. Also, in the case of an evaluation involving several evaluators with no experience in implementation, the Weight Product Method (WPM) seems to be more appropriate. However, the Weight Product Method (WPM) as AHP does To calculate the weights of criteria Does not provide a specific route. Taking all this information into account, AHP can be successfully incorporated with the Weight Product Method (WPM). Weighted Product Method (WPM). WPM is similar to WSM. The main difference is that the Model instead of addition Includes multiplication. Each substitution is By multiplying multiple ratios Compared to others, One for each criterion. to the relative weight of each ration, the corresponding quantity is raised to an equivalent power. Therefore, one-dimensional and In both multidimensional MCDM WPM can be used. These studies discuss UtUV under the Structure of age-specific WPMs. No research has been conducted on UtUV. Considering the UtUV factor Age- and state-specific WPMs Based on the general structure WPM Designed to describe UtUV, Describe the variation in this in degradation rates between different units. The WPM method is most widely used in MCDM One of the methods. then other methods of problem-solving This method is more efficient because it takes less computation time. WPM is simple and easy to use in highly subjective cases. optimal route selection, Web activities like evaluation, production, and selection of project manager WPM is used in many areas. Between WSM and WPM The maximum mean correlation is observed, Also between WPM and TOPSIS Very little correlation is observed. The average of all these coefficients WSM, WPM, ELECTRE, and TOPSIS respectively indicates that there is a strong mean correlation.

Analysis and Discussion

TABLE 1. Phishing Websites

	URLs	Extracted	Domains	TLDs	Logins
Alexa	31163.00	29173.00	9554.00	285.00	2056.00
Alexa Login	4370.00	3992.00	1960.00	117.00	3992.00
Phish Tank	26346.00	20803.00	10813.00	406.00	4999.00
APWG	66929.00	45382.00	7760.00	319.00	2812.00
Open Phish	2249.00	1336.00	710.00	94.00	326.00

Table 1 shows the Phishing Websites. Phishing Websites is alternatives are Alexa, Alexa Login, Phish Tank, APWG, Open Phish. Evaluation Parameter is URLs, Extracted, Domains, TLDs, and Logins.

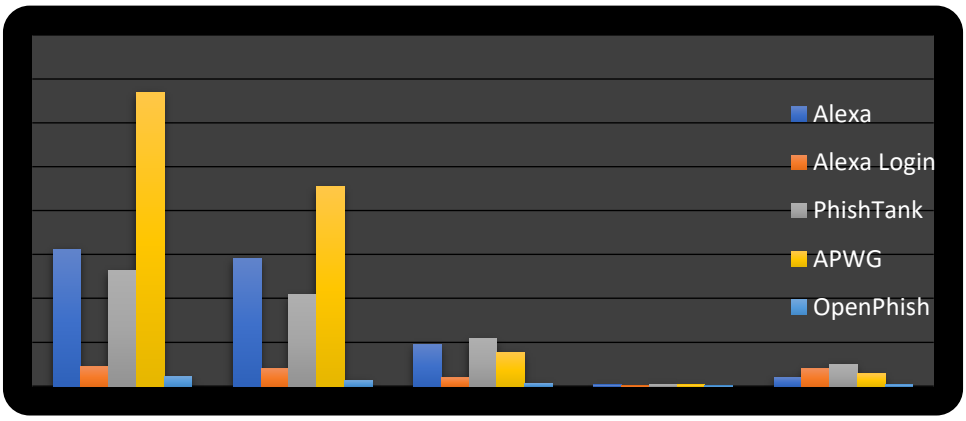

FIGURE 1. Phishing Websites

Figure 1 shows the Phishing Websites. Phishing Websites is alternatives are Alexa, Alexa Login, Phish Tank, APWG, Open Phish. Evaluation Parameter is URLs, Extracted, Domains, TLDs, and Logins.

TABLE 2. Performance Value

	Performance value				
Alexa	0.46561	0.64283	0.88357	0.70197	0.41128
Alexa Login	0.06529	0.08796	0.18126	0.28818	0.79856
Phish Tank	0.39364	0.45840	1.00000	1.00000	1.00000

APWG	1.00000	1.00000	0.71765	0.78571	0.56251
Open Phish	0.03360	0.02944	0.06566	0.23153	0.06521

Table 2 shows the performance value of Phishing Websites for using weight product method.

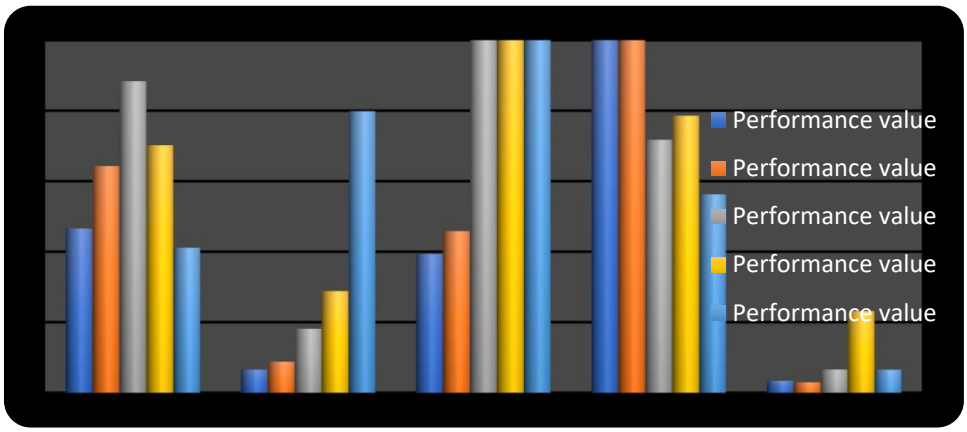

FIGURE 2. Performance Value

Figure 2 shows the performance value of Phishing Websites for using weight product method.

TABLE 3. Weight

Weight				
0.25	0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25	0.25

Table 3 Shows the Phishing Websites weights are same.

TABLE 4. Weighted normalized decision matrix.

	Weighted normalized decision matrix				
Alexa	0.82605	0.89541	0.96953	0.91533	0.80082
Alexa Login	0.50549	0.54460	0.65250	0.73268	0.94532
Phish Tank	0.79209	0.82283	1.00000	1.00000	1.00000
APWG	1.00000	1.00000	0.92040	0.94149	0.86603
Open Phish	0.42815	0.41422	0.50621	0.69367	0.50534

Table 4 the weighted normalized result matrix is presented in Table 4 for WPM method is presented in to Phishing Websites.

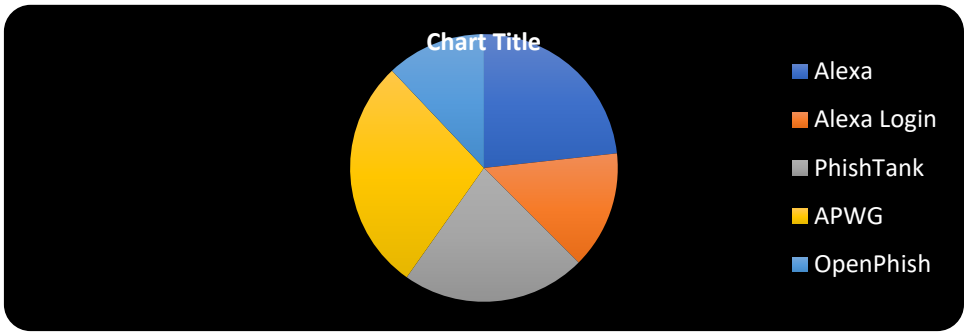

FIGURE 3. Weighted normalized decision matrix

Figure 3 the weighted normalized result matrix is presented in Table 4 for WPM method is presented in to Phishing Websites.

TABLE 5. Preference Score and Rank

	Preference Score	Rank

Alexa	0.52566	3
Alexa Login	0.12441	4
Phish Tank	0.65176	2
APWG	0.75046	1
Open Phish	0.03147	5

Table 5 shows the Result of Final Preference score and Rank of WPM for Phishing Websites. Preference score APWG is showing the highest value for preference score and Open Phish is showing the lowest value.

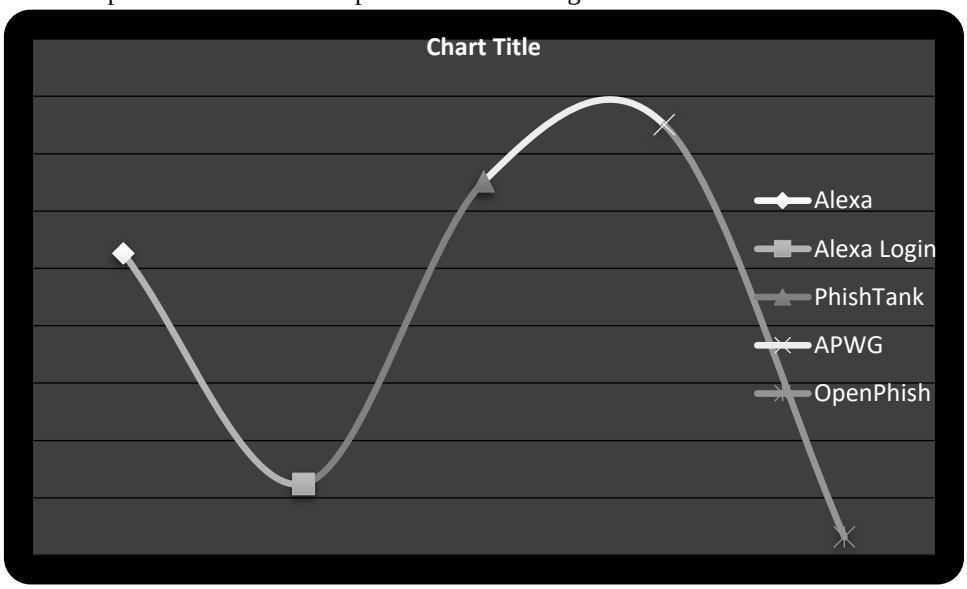

FIGURE 4. Preference Score

Figure 4 shows the Result of Final Preference score and Rank of WPM for Phishing Websites. Preference score APWG is showing the highest value for preference score and Open Phish is showing the lowest value.

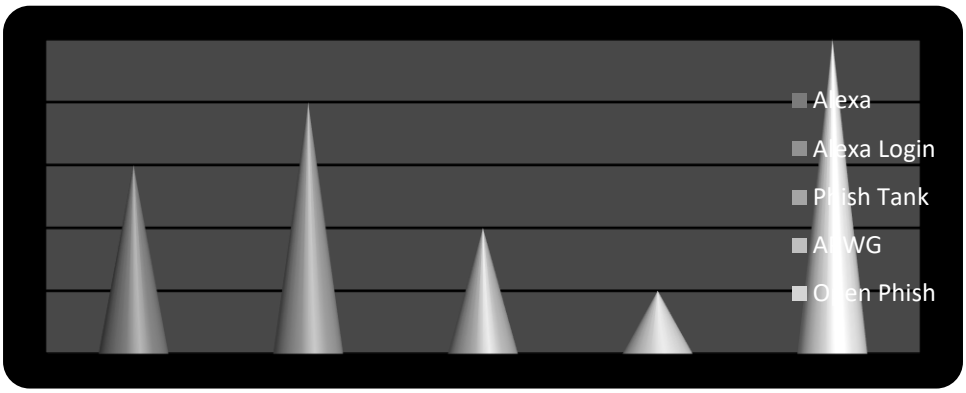

FIGURE 5. Shown the Rank

Figure 5 Shows the Ranking of Phishing Websites. APWG is got the first rank whereas is the Open Phish the Lowest rank.

9. CONCLUSION

Network administrators hate having to permit more complex network administration tasks as the configuration of computer networks changes. That network is challenging to operate for two key reasons:

• Constantly changing network status

• Device-specific low-level network configuration

Sophisticated networking techniques The framework does not let network operators disclose network policies based on higher-level objectives or automatically configure network policies in response to low-level networking events. Networking presents a means to exploit summary level for network architecture, developing languages, and network controllers because software is constrained. It constantly and frequently switches to network mode on its own. Procera is an event-driven network SDN-based control architecture that we built and implemented to streamline many parts of network operations and management. Implement and enact a reactive network policy by using the four control domains available to network operators: time, data application, authentication status, and traffic flow. Our language-based high-level configuration is Reactive functional programming.

REFERENCES

1 Ramachandran, Anirudh, and Nick Feamster. "Understanding the network-level behavior of spammers." In *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 291-302. 2006.

2 François, Jérôme, Issam Aib, and Raouf Boutaba. "FireCol: a collaborative protection network for the detection of flooding DDoS attacks." *IEEE/ACM Transactions on networking* 20, no. 6 (2012): 1828-1841.

3 Schmitt, Amanda J. "Strategies for customer service level protection under multi-echelon supply chain disruption risk." *Transportation Research Part B: Methodological* 45, no. 8 (2011): 1266-1283.

4 Klovdahl, Alden S. "Social network research and human subjects protection: Towards more effective infectious disease control." *Social Networks* 27, no. 2 (2005): 119-137.

5 Sifalakis, Manolis, Stefan Schmid, and David Hutchison. "Network address hopping: a mechanism to enhance data protection for packet communications." In *IEEE International Conference on Communications, 2005. ICC 2005. 2005*, vol. 3, pp. 1518-1523. IEEE, 2005.

6 Jain, Ankit Kumar, and Brij B. Gupta. "Two-level authentication approach to protect from phishing attacks in real time." *Journal of Ambient Intelligence and Humanized Computing* 9, no. 6 (2018): 1783-1796.

7 Saeed, Maryam, and Hadi Shahriar Shahhoseini. "APPMA-An anti-phishing protocol with mutual authentication." In *The IEEE symposium on Computers and Communications*, pp. 308-313. IEEE, 2010.

8 Huang, Chun-Ying, Shang-Pin Ma, and Kuan-Ta Chen. "Using one-time passwords to prevent password phishing attacks." *Journal of Network and Computer Applications* 34, no. 4 (2011): 1292-1301.

9 Sit, Muhammed, Yusuf Sermet, and Ibrahim Demir. "Optimized watershed delineation library for server-side and client-side web applications." *Open Geospatial Data, Software and Standards* 4, no. 1 (2019): 1-10.

10 Garrido, Alejandra, Sergio Firmenich, Gustavo Rossi, Julian Grigera, Nuria Medina-Medina, and Ivana Harari. "Personalized web accessibility using client-side refactoring." *IEEE Internet Computing* 17, no. 4 (2012): 58-66.

11 Fenstermacher, Kurt D., and Mark Ginsburg. "Mining client-side activity for personalization." In *Proceedings Fourth IEEE International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS 2002)*, pp. 205-212. IEEE, 2002.

12 Sharma, Amit Kumar, and Renuka Yadav. "Spam mails filtering using different classifiers with feature selection and reduction technique." In *2015 Fifth International Conference on Communication Systems and Network Technologies*, pp. 1089-1093. IEEE, 2015.

13 Aung, Swe Swe, and Thinn Thu Naing. "Naïve Bayes classifier based traffic prediction system on cloud infrastructure." In *2015 6th International Conference on Intelligent Systems, Modelling and Simulation*, pp. 193-198. IEEE, 2015.

14 Gao, Yan, Alok Choudhary, and Gang Hua. "A comprehensive approach to image spam detection: from server to client solution." *IEEE Transactions on Information Forensics and Security* 5, no. 4 (2010): 826-836.

15 Chen, Kuan-nien, and Pei-chun Lin. "Information literacy in university library user education." In *Aslib proceedings*. Emerald Group Publishing Limited, 2011.

16 Patterson, Charles D., and Donna W. Howell. "Library user education: Assessing the attitudes of those who teach." *RQ* (1990): 513-524.

17 Khonji, Mahmoud, Youssef Iraqi, and Andrew Jones. "Phishing detection: a literature survey." *IEEE Communications Surveys & Tutorials* 15, no. 4 (2013): 2091-2121.

18 Aleroud, Ahmed, and Lina Zhou. "Phishing environments, techniques, and countermeasures: A survey." *Computers & Security* 68 (2017): 160-196.

19 Aarikka-Stenroos, Leena, and Paavo Ritala. "Network management in the era of ecosystems: Systematic review and management framework." *Industrial Marketing Management* 67 (2017): 23-36.

20 Kim, Hyojoon, and Nick Feamster. "Improving network management with software defined networking." *IEEE Communications Magazine* 51, no. 2 (2013): 114-119.

21 Hood, Christopher, and Guy Peters. "The middle aging of new public management: into the age of paradox?." *Journal of public administration research and theory* 14, no. 3 (2004): 267-282.

22 Pras, Aiko, Jurgen Schonwalder, Mark Burgess, Olivier Festor, Gregorio Martinez Perez, Rolf Stadler, and Burkhard Stiller. "Key research challenges in network management." *IEEE communications magazine* 45, no. 10 (2007): 104-110.
23 To, Huy Hoang, Shonali Krishnaswamy, and Bala Srinivasan. "Mobile agents for network management: when and when not!." In *Proceedings of the 2005 ACM symposium on Applied computing*, pp. 47-53. 2005.
24 Suleiman, Shammasi Ali. "User education programs in academic libraries: the experience of the International Islamic University Malaysia students." *Library Philosophy and Practice* 139 (2012).