Journal of Science Research

A predictive threat model for efficient management of distributed organized minor network threats

Adeyemo, A. B., Oriola, O. and **Osunade, O.**
Department of Computer Science, University of Ibadan, Ibadan, Nigeria
Corresponding author:

Abstract

Network threats can be classified into major network threats and minor network threats. Minor network threats are the network threats that have little or no negative impacts on information systems. Existing Information Security Management processes have ignored minor network threats because of the perception that they were non-harmful. However, recent studies have shown that organized minor network threats from distributed sources can cause denial of service attacks. This paper presents a predictive threat model for managing distributed organized minor network threats. Sequential Association Mining with multiple actionable attributes was used to extract interesting minor network threats. Attacker and Victim perspectives of intrusion were combined by Belief Theory to improve the rating accuracy. DARPA-sponsored Lincoln Lab Denial of Service and real life Plymouth University Advanced Persistent Threat scenarios of minor network threats were used independently to evaluate the model. The results showed that in both scenarios, distributed organized minor network threats were rated objectively with positive correlation significance. This eventually reduced the number of signature rules and time of detection.

Keywords: Organized distributed minor network threats; predictive threat model; data mining.

Introduction

Organized network threats refer to network threats that are perpetrated in steps. Nowadays,the network threats are explored via web, phone, or cloud in coordinated manner from distributed sources. Examples of such network threats are botnets, worms and Advanced Persistent Threats (APTs). They often involve many simple attacks or complex attack scenario [1] and do inflict more hazards on information systems because they are always targeted. The stages of attack explored by the network threats include preparation, access gaining, privilege escalation, pilfering, track covering, backdoor and denial of service [1]. The denial of service is not a threat but an attack, which disrupts the provision of network, information or asset services either temporarily or permanently.

Snort [2] and the Common Vulnerability Scoring System (CVSS) [3] have proposed both numeric and qualitative schemes for ranking network threats. The consensus is a risk classification, which qualitatively described risk as low, medium and high or threats of low significance and high significance or minor threats and major threats [4]. Porras *et al* [5], Alshubi et al. [6] and Jumaat [7] have all rated preparation and access gaining as *minor network threats* and privilege escalation, pilfering, track covering and backdoor as *major network threats*.

In information security management, major network threats are mitigated at the expense of minor network threats due to high cost of mitigating all of the organized network threats [8]. This act is based on the evidence that major network threats are harmful and belief that minor network threats are not dangerous and could then be accepted. However, an attacker that fails to successfully exploit privilege escalation or any higher stage network threats perpetrate denial of service by

flooding the target at high speed using distributed sources [1]. Therefore, mitigation of distributed organized minor network threats must be emphasized.

According to Ntoukas *et al* [9], Information security management is a continuous and systematic process of identifying, analysing, handling, reporting and monitoring operational risk of an organisation. In the crux of this lies threat modelling, which is: "a systematic, non-provable, internally consistent method of modeling a system, enumerating risks against it, and prioritising them" [10]. It involves steps such as *identification of critical assets, decomposition of the system to be assessed, identification of possible points of attack (vulnerability), identification of threats, categorization and prioritisation of the threats, and mitigation of threats* [11].

There are two methods used for modeling network threats. They include *static threat model* and *predictive threat model.* The static threat model is the commonest method used for modeling threats. The analysis involves associating network threats to predefined categories. Examples include Microsoft STRIDE Model by Hernan *et al* [12], DREAD Model [13] and Snort developed by Caswell and Roesch [2], which is one of the most popular open source security tools. Predictive threat models have been proposed by Porras *et al* [5], Yu *et al* [14], Arnes *et al*[15], Alsubhi *et al* [6], Dondo [16], Haslum [17] and Jumaat [7].

Data mining is the nontrivial extraction of implicit, previously unknown and potentially useful information from databases [18]. Data mining involves the systematic analysis of large data sets using automated methods. Data mining has been applied to the problem of threat prediction. Sequential association mining with a single attributes was applied by Li *et al* [19]. Katipally *et al* [20] also applied data mining techniques to find the patterns of generated alerts by generating Association rules.

The existing works have focused on either organized or simple threats. They have based the prediction on single actionable attributes and minimum support requirements and concentrated on modeling of major network threats, which is unsuitable for the predictive modeling of current distributed organized network threats. Therefore, this paper develops a data mining-based predictive threat model for managing distributed organized minor network threats.

Materials and methods

The Threat Prediction Model was designed by modifying Li *et al* [19] Sequential Association Mining Algorithm. In addition to time stamp and event name, other actionable attributes such as source IP address and destination IP address were included in creating an event instance. The data mining steps presented in Fayyad *et al* [21] was adapted to develop a predictive analysis model. The threat modelling steps presented in Olzak [11] was adapted to develop a minor network threat modeling. The two models were integrated to formulate a Data Mining based Predictive Threat Model. The framework is presented in Figure 1.

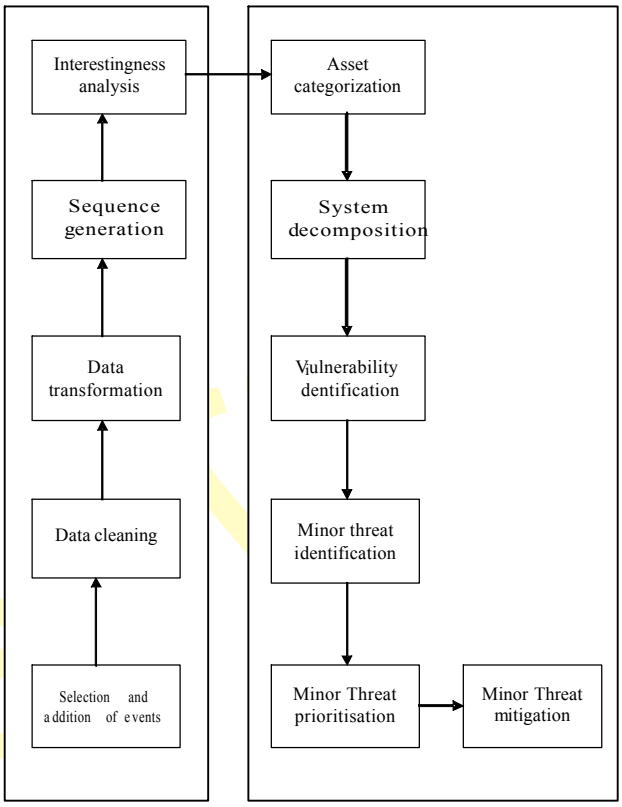


Figure 1. Architecture of the data mining-based predictive threat model.

1. *Selection and addition of events*

The minor network threats are selected from the stored events in each network security management domain. They are merged together.

2. *Data cleaning*

The key actionable attributes such as timestamp, event name, source IP address, destination IP address are selected while other optional attributes such as source port, destination ports, protocols, event id are deleted. The selected attributes are organized into an event table.

3. *Data transformation*

The events are sorted in order of time. The average detection time is chosen as the window size.

4. *Sequence association generation*

The window-size is used to generate candidate sequence. This step is performed by the algorithm below:

Step 1: Set Window size to P, SequenceSize to 1, MaximumSequence Size to L, Sequence to empty.
Step 2: Sort events based on their timestamps.
Step 3: Set the current WindowStep to 1.
Step 4: Set Temp to empty.
Step 5: Add event to Temp.
Step 6: IF Sequence Size is L.
Step 7: Increment WindowStep by 1.
Step 8: EndIF.
Step 9: Else Go to Step 5.
Step 10: Add Temp to Sequence.
Step 11: Return WindowStep, Sequence.

5. *Rule interestingness analysis*

The Rule Interestingness Analysis is used to generate interesting rules. The interesting sequences are the rules with highest occurrence, support and confidence.

Given that $A \rightarrow B$ is an association, A is known as Antecedent and B is known as Consequent. The Support and the Confidence of the Consequent given the Antecedent can be statistically calculated as presented in equations 1 and 2.

$$\text{Support (B)} = \frac{n(A \cap B)}{N} \quad \ldots . 1$$

Where n is the number of records of events in the event table;
n ($A \cap B$) is the number of times A and B occurs together as sequence in the sequence table such that A is antecedent and B is consequent.

$$\text{Confidence (B)} = \frac{n(A \cap B)}{n(A)} \quad \ldots . 2$$

n(A) is the number of times the antecedent A occurs in the sequence table.

The algorithm to generate interesting minor threats is as follows:

Step 1: Assign MinimumSupport to MinSup, WindowStep to Max.
Step 2: Set WindowStep to 1.
Step 3: Set TempLocation to 0, Temp to empty.
Step 4: While WindowStep< Max.
Step 5: Increment the WindowStep.
Step 6: Add Sequence to Temp.
Step 7: IFTempLocation=! Temp.
Step 8: Increment the TempLocation.
Step 9: Compute the Support (Temp).
Step 10: While Support e" MinSup.
Step 11: Compute the Confidence (Temp).
Step 12: Assign Confidence to Interestingness.
Step 13: Return WindowStep, Sequence, Interestingness.
Step 14: EndWhile.
Step 15: EndIF.

6. *Asset aategorization*

In this work, the operating systems are the assets. The operating systems with the known vulnerabilities are ranked in Category 1, window operating systems are ranked in Category 2 because of their ease of use and popularity while other operating systems are ranked in Category 3.

7. *System decomposition*

Certain information about the victim systems is gathered and some metrics are derived to be used for identification of vulnerability and threat. Attacker and Victim Perspectives of Intrusion of [22] were adapted for the purpose because they are associated with predictive threat modelling.

8. *Vulnerability identification*

Common vulnerability and exposure ID, open source vulnerability databases, and hacking sites information are used to identify the vulnerabilities. Because networks are involved in managing the threat, a policy web of trust is developed to overcome distrust which may result in inaccurate threat measurement. Three actors associated with each administrative domain are identified as determinants in this respect: administrator, communication channel and data source. The following factors determine the trust of each actor: The sum of all the derived-trust variables produce the mass trust.

9. *Minor network threat identification*

Heterogeneous information security sensors generate the minor network threats alerts or events. Because networks are involved in managing the threat, a policy web of trust is developed to overcome distrust which may result in inaccurate threat measurement. Three

actors associated with each administrative domain are identified as determinants in this respect: administrator, communication channel and data source. The following factors determine the trust of each actor: The sum of all the derived trust variables produce the mass trust.

10. *Minor Network Threat Prioritisation*

This involves rating of minor network threats. The following steps are taken to rate the minor network threats:

i. Computation of Belief Value, M(Z) using Dempster-Shafer Function of Rule of Combination

The computation was adapted from Shafer [23] and it is expressed as:

$$M(Z) = \frac{\Sigma A \cap B = z \neq \phi m(A).m(B)}{\Sigma A \cap B \neq \phi m(A).m(B)} \quad \ldots . 3$$

Where A, B, $Z \underline{c}$ Z. m are the mass function. In definite term, the numerator represents the accumulated evidence for the sets A and B, which supports the hypothesis Z and the denominator is the sum of the amount of conflict between the two sets.

ii. *Normalization of the belief value*

The maximum belief values for the criteria are normalized that the sum is equal to 1.

$$\text{Normalized } (P_i) = P_i / \Sigma_{i=1}^{n} P_i \quad \ldots . 4$$

iii. Calculation of the Expected Value for Risk-determination factors' Fusion

This computation was adapted from the Expectation Theory of Ross [24].

The expected value E(X) of objective X is defined as:

$$E(X) = P_1X_1 + P_2X_2 + \ldots + P_kX_k \quad \ldots . 5$$

Since all probabilities p_i add up to one ($p_1 + p_2 + ... + p_k = 1$), the expected value can be viewed as the weighted average, with p_i's being the weights.

$$E(X) = \frac{P_1X_1 + P_2X_2 + \cdots P_kX_k}{P_1 + P_2 + \cdots + P_k} \quad \ldots . 6$$

iv. Estimation of Attack and Victim-based Threat Rating

Attacker-based Threat Rating R_A is the rate of sum of the attacker-centric objective scores with asset criticality rank estimated as:

$$R_A = \frac{\text{Objective Exploitability + Objective Damage + Objective Risk of Exposure}}{\text{Asset Criticality Rank}} \quad \ldots . 7$$

Victim-based Threat Rating R_v is the rate of sum of the victim-centric objective scores with asset criticality rank estimated as:

$$R_V = \frac{\text{Objective Frequency + Objective Severity + Objective Resistance}}{\text{Asset Category Rank}} \quad \ldots . 8$$

vii. Threat Rating:

Threat Rating, R_T is the sum of both Attacker-based Threat Rating and Victim-based Threat Rating computed as:

$$R_T = R_A + R_V \quad \ldots . 9$$

11. *Minor Network Threat Mitigation*

The minor network threats with ratings from 5 and above are mitigated while those below are accepted.

In the experimental set-up, two distributed organized minor threat data sets were used for the study. The first minor network threat data set was extracted from the publicly available DARPA-sponsored Lincoln Lab Denial of Service version 1.0. This was developed by MIT Lincoln Laboratory's research team in year 2000 and is called DARPA 2000. The second was extracted from the real life Plymouth University Advanced Persistent Threats (APT),and is targeted at exploiting CVE-2012-4681 [25], which is an Oracle Java Vulnerability that affects systems such as MS-Window 12 Server.

The DARPA 2000 minor network threats were distributed over 172.16.112.0/24, 172.16.113.0/24, 172.16.114.0/24 and 172.16.115.0/24 networks and were organized into the following steps:

i. IPsweep of the AFB from a remote site.
ii. Probe of live IP's to look for the sadmind daemon running on Solaris hosts.
iii. Break-in's via the sadmind vulnerability, both successful and unsuccessful on those hosts.

The Plymouth University APTs minor network threats were distributed over 10.1.0.0/27, 10.1.0.32/27, 10.1.0.64/27 and 10.1.0.96/27 networks and were organized into the following steps:

i. Connect to the victims.

ii. Scan the operating systems for exploitable vulnerability.
iii. Attempt to exploit CVE-2012-4681.

Both minor network threats with background traffic are replayed thrice against Suricata and Snort Network Intrusion Detection Systems (which signature rules are emerging threat rule sets). Four network security management domains, 10.1.0.128/27, 10.1.0.160/27, 10.1.0.192/27 and 10.1.0.224/27 each containing snort and suricata network intrusion detection systems, collaborated to model the distributed organized minor network threats.

Results

Tables 1 and 2 present samples of the results of the predictive analysis of DARPA 2000 and Plymouth University APTs respectively. DARPA 2000 minor network threats were 12 while Plymouth University APTs minor network threats were 6. According to Bhattacharya and Ghosh [26], a once successful attack exploit would be exploited by an attacker in the near future; hence only the attack sequences with full support (sequence that occur three times) were chosen to determine the interesting minor network threats.

Tables 3 and 4 present samples of the rating of the predictive threat models for DARPA 2000 minor network threats and Plymouth University APTs' minor network threats. The rating range is between 0 and 12. Non-harmful minor network threats are rated in the range $0 \leq x < 5$ and Harmful minor network threats are rated in the range $5 \leq x \leq 12$. Table 5 presents the Spearman's Correlation Coefficients between our predictive models for DARPA 2000 as well as Plymouth University APTs' minor network threats respectively. The signature rules of harmful minor network threats were enabled for mitigation purposes while the signature rules of non-harmful network threats were disabled. This had an effect on the number of signature rules and the time of detection.

Figure 2 presents charts showing the number of signature rules and time of detection before and after the application of the predictive threat model.

Table 1. Predictive Analysis of DARPA 2000 minor network threats.

S/N	Attack scenario	Exploit	Snort events	Snort events	Source	Destination	Frequency/ support	Confidence
1	C12,41	INFO PING NIX	0	3	172.16.113.50	172.16.113.105	3 times / 0.021897	1
2	C12, 41 =>D12,41	INFO PING BSDtype	0	3	172.16.113.50	172.16.113.105	3 times / 0.0218979	1
3	C12,41, D12,41 => C10,70	INFO PING NIX	0	3	172.16.112.50	172.16.114.169	3 times / 0.021897	1

Table 2. Predictive Analysis of Plymouth University APT minor network threats.

S/N	Attack scenario	Exploit	Snort events	Suricata events	Source	Destination	Frequency/ support	Confidence
1	D2,4	CURRENT_ EVENTS Possible Metasploit Java Exploit	96	70	10.1.0.3	10.1.0.135	3 times /0.02654867	1
2	D2,4=>AN2,11	Trojan MetasploitMeterpretercore_ channel Command Request	1	1	10.1.0.3	10.1.0.197	3 times /0.02654867	1
3	D2,4, AN2,11 => AO2,4	Trojan MetasploitMeterpreterstdapi_Command Request	64	80	10.1.0.3	10.1.0.135	3 times /0.02654867	1

Table 3. Comparison of Rating of Predictive Threat Model, CVSSv2 and Snort for DARPA 2000.

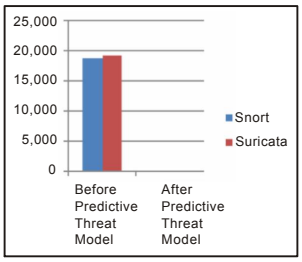
S/N	Threat	CVE_ID	Threat Rating/Category	CVSSV2	Snort Priority
1	Exploit MS_SQL DOS ATTEMPT(08)	CVE:2002-0649	9.8333 / Harmful	8	1
2	NETBIOS NT NULL Session	CVE:2000-0347	4.05556 / Non-harmful	10	2
3	NETBIOS NT NULL Session	CVE:2000-0347	11.16667 / Harmful	10	2

Table 4. Comparison of Rating of Predictive Threat Model, CVSSv2 and Snort for Plymouth University Threats.

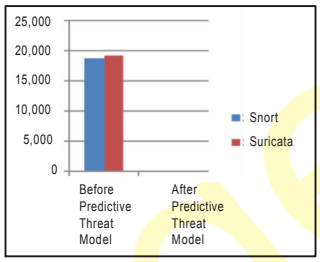
S/N	Threat	CVE_ID	Threat Rating/Category	CVSSV2	Snort Priority
1	CURRENT_EVENTS Possible Metasploit Java Exploit	–	6.5 / Harmful	–	2
2	Trojan Metasploit Meterpretercore_channel Command Request	–	4.0468 / Non-harmful	–	2
3	Trojan Metasploit Meterpreterstdapi_Command Request	–	6.0 / Harmful	–	2

Table 5. Spearman's Correlation Coefficients for DARPA 2000 and Plymouth University APTs Minor Network Threats.

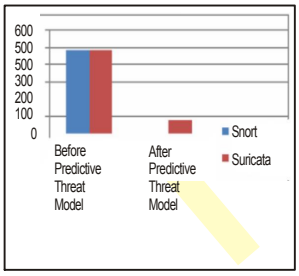
Minor Network Threats	Spearman's Correlation Coefficient	Spearman's Correlation Significance
DARPA 2000	0.5857	Positive Significance
Plymouth University APTs	0.6790	Positive Significance



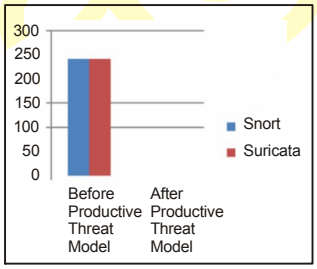
Cost of signature rules for DARPA 2000



Cost of signature rules for Plymouth Univ. APTS



Time of Detection for DARPA 2000



Time of Detection for Plymouth Univ. APTs.

Discussion of results

From results whose samples are presented in Table1, after the interestingness analysis of the DARPA 2000 data sets, eleven sequences of events of twelve steps with aSupport of 0.021897 and Confidence of 1 were selected.Similarly from Table 2, after the interestingness analysis of the Plymouth University APTs data sets, 5 sequences of events of 6 steps with the a Support of 0.02654867 and Confidence of 1 were selected.

Each of the sequence steps occurred three times. This implies that the attackers preferred to use the exploit because it had always lead to success, since an attacker will adhere to the strategy that will give him/her maximum benefit. These conform to the findings of an earlier study that a novice attacker exploits easy-to-use kit Bhattacharya *et al* [26].

The comparison of the attack steps with the original attack description shows that the threat paths reflect to a large extent the attack steps. Different bots were applied at the reconnaissance IPsweep and scanning phases as shown in Step 1 and Step 2. The attack graph shows that after a successful exploit of sadmind vulnerability in a host 172. 16.115.20 in a particular subnet, the attacker pings host 172.16.113.204 in another subnet. This conforms to the description in DARPA [27].

From the rating of the predictive threat model for

DARPA 2000 minor network threats (samples are presented in Table 3) the results show that the population of event detected is fairly proportional to the threat rating. This conforms to the general fact in computation that the memory loads affect the performance of instruction processing. Four of the five minor network threats with CVE-ID as well as RPC SADMIND Query with root credentials (a later stage of attacking process), have ratings that are greater or equal to 5, while 6minor network threats have ratings that are below 5. The only minor network threats with CVE-ID that were not rated harmful were reconnaissance events.

In the case of CVSSv2, only 5 threats with CVE_ID were rated harmful while Snort rated them as 1, 2 or 3. The Spearman's correlation coefficient of the ratings of the predictive threat model presented in Table5was 0.5857, which is positively significant. Similarly the rating of the predictive threat model for Plymouth University minor network threats is presented in Table 4. The results show that the population of event detected is fairly proportional to the Threat Rating score and Threat Ranking values. Even though none of the minor network threats had CVE-ID, 5 of the 6 threats had ratings that were greater or equal to 5. In the case of CVSSv2, none of the minor threats were rated because of the absence of CVE-ID, while Snort rated them as 2. The Spearman's correlation coefficient of the ratings of the predictive threat model presented in Table5 was 0.6790, which is positively significant.

The number of signature rules and time of detection, before and after the application of the predictive threat model, for DARPA 2000 and Plymouth University APTs data sets are presented in Figure 2. Before the application of the network threat model 18701 signature rules were enabled for snort and 19082 for suricata network intrusion detection system.

Based on the result of the predictive threat model, where only 5 minor threats were rated as being harmful, only 5 signature rules were enabled, for both the snort and suricata network intrusion detection systems for DARPA 2000 and Plymouth University APTs datasets.

The DARPA 2000 tcpdump was initially detected in an average of 480 seconds against snort and suricata network intrusion detection systems, but after only 5 rules were enabled, they were detected by snort and suricata in 3 seconds and 75 seconds respectively.

The Plymouth University APT tcpdump was also initially detected in average of 240 seconds against snort and suricata network intrusion detection systems, but after only 5 rules were enabled, they were detected by both snort and suricata in 1 second.

Conclusion

Distributed organized minor network threats are new trends of threats that inflict serious damage on critical information systems by causing denial of service attacks. It then requires much attention as the major minor threats. Therefore, the proposed predictive threat model, which combines both Fayyad *et al* [23] data mining model and Olzak [11] threat modelling models is novel. The derived model generates interesting sequential association rules, which combined to form the organized minor threats at confidence of 1. The predictive threat model rates the threats using attacker and victim perspectives of threats, unlike previous works that were based on either attacker or victim variables such as availability of vulnerability, attack severity or frequency. The model produced ratings that are objective (unbiased). This helps to remove the uncertainties in number of signature rules to be enabled during network threat management, which eventually leads to reduction in time of detection. Hence, modelling minor network threats using a data mining-based predictive threat model produces interesting rules, reliable ratings and efficient network threat management. In future, the issue of privacy, interoperation, quality of information sharing among collaborative network threat management domains and the impact of minor network threat modelling on false alarm will be studied.

Acknowledgement

The authors acknowledge the management of the Center for Security, Communications and Networks (England) for approving the use of their networking laboratory for the experiment, and the contributions of Dr Maria Papadaki and Dr B. Ghitta for the attacking experiment.

References

[1] Wang, J. and Zhao, L. 2006. Experimental design for attack scenario traces to validate intrusion detection alert correlation. *WSRC Paper 2006/4-1,* Whartson-SMU Research Centre.

[2] Caswell, B. and Roesch, M. 1998. Snort: The open source network intrusion detection system. Retrieved 10th April, 2014 from http://www.snort.org

[3] CVSS.2014. Common Vulnerability Scoring System version 2 retrieved 4th July, 2014 from http://www.first.org/cvss/cvss-guide.html

[4] Symantec. 2005. Internet Security Threat Report, Volume 17 Retrieved 19th January, 2014 from

www.symantec.com/content

[5] Porras, P.A., Fong, M.W. and Valdes, A. 2002. A mission-impact-based approach to INFOSEC alarm correlation. *Proceedings of the 5th International Symposium Recent Advances in Intrusion Detection, Vol. 2516,* Zurich, Switzerland, pp. 95-114.

[6] Alsubhi, K., Al-Shaer, E. and Boutaba, R. 2008. Alert prioritisation in intrusion detection systems. Proceedings of the IEEE network operations and management symposium, Salvador, Brazil, pp. 33-40.

[7] Jumaat, A. N. B. 2012. Incident prioritization for intrusion response. University of Plymouth, Unpublished Ph.D. Thesis.

[8] ISO, Retrieved 7th May, 2014 from http://www.iso27001security.com

[9] Ntouskas, T., Pentafronimos, G. and Papastergiou, S. 2011. STORM – Collaborative Security Management Environment. Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication *Lecture Notes. In: Computer Science Volume 6633,* pp. 320-335.

[10] SensePost. 2011. Sense Modelling Threat Modelling. Retrieved 4th April, 2014 from http://www.slideshare.net/sensepost/corporate-threat-modelling

[11] Olzak, T. 2006.A Practical Approach to Threat modelling. Retrieved 4th April, 2014 from www.adventuresinsecurity.com

[12] Hernan, S., Lambert, S., Ostwald, T. and Shostack, A. 2006. Threat modelling: Uncover Security Design Flaws Using the STRIDE Approach. *MSDN Magazine,* November.

[13] Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R. and Murukan, A. 2003. *Improving web application security: threats and countermeasures, threat modelling,* Microsoft Corporation.

[14] Yu, J., Ramana Reddy, Y.V., Selliah, S, and Kankanahalli, S. 2004. A collaborative architecture for intrusion detection systems eith intelligent agents and knowledge-based alert evaluation. computer supported cooperative work in design. The 8th International Conference on Volume 2, pp. 271-276.

[15] Årnes, A., Valeur, F., Vigna, G. and Kemmerer, R. 2006. Using Hidden Markov Models to evaluate the risks of intrusions: system architecture and model validation. *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID),* Hamburg, Germany, pp. 145–164.

[16] Dondo, M. 2009. A fuzzy risk calculations approach for a network vulnerability ranking system. DRDC Ottawa Defence R & D Canada, Ottawa, *Technical Memorandum DRDC Ottawa TM 2007-090.*

[17] Haslum, K. 2010. Real-time network intrusion prevention. Doctoral theses at NTNU, 2010:168.

[18] Zaiane, O. R. 1999. *Principle of knowledge discovery in databases.* University of Alberta, Department of Computer Science, CMPUT690.

[19] Li, Z., Lei, J., Wang, L., and Li D. 2007. A data-mining approach to generating network attack graph for intrusion prediction. *Computer Communications 29.*

[20] Katipally, R., Cui, X. and Yang, L. 2010. Multi stage attack detection system for network administrators using data-mining. CIIIRW '10. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Article No. 51.*

[21] Fayyad, U., Shapiro, G. P., and Smyth, P. 1996. From data-mining to knowledge discovery in databases. AI Magazine, 17(3):37-54, Fall 1996. Retrieved 2nd April, 2014 from http://citeseer.ist.psu.edu/fayyad96from.html

[22] McHugh, J., Christie, A. and Allen, J. 2001. Intrusion Detection1: Implementation and Operational Issues. CROSSTALK. *The Journal of Defense Software Engineering,* Software Engineering Institute, Computer Emergency Response Team/Coordination Centre.

[23] Shafer, G. 1976. *A mathematical theory of evidence.* Princeton University Press.

[24] Ross, S. M. 2007. Expectation of a random variable. *Introduction to Probability Models (9th Ed.).* Academic Press, p. 38.

[25] NVD. 2014. National Vulnerability Databases. https://nvd.nist.gov/vuln/search/results?adv_search=false&form_type=basic&results_type=overview&search_type=all&query=CVE-2012-4681

[26] Bhattacharya, S. and Ghosh, S. K. 2008. A decision model based security risk management approach. Proceedings of the International Multi-Conference of Engineers and Computer Scientists IMECS, Vol. II, 19-21, Hong Kong.

[27] DARPA. 2014. DARPA Intrusion Detection Data Sets. Retrieved 10th April, 2014 from http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html

Journal of Science Research
Volume 15, 2016, ISSN 1119 7333
Citation: Adeyemo, A. B., Oriola, O. and Osunade, O. A predictive threat model for efficient management of distributed organized minor network threats.

Textflow Limited
Ibadan, Nigeria