



Intrusion Detection Systems with Live Knowledge System

Byeong Ho Kang
UNIVERSITY OF TASMANIA

05/31/2016
Final Report

DISTRIBUTION A: Distribution approved for public release.

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ IOA
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Executive Services, Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.					
1. REPORT DATE (DD-MM-YYYY) 31-05-2016		2. REPORT TYPE Final		3. DATES COVERED (From - To) 20 May 2015 to 19 May 2016	
4. TITLE AND SUBTITLE Intrusion Detection Systems with Live Knowledge System				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER FA2386-15-1-4061	
				5c. PROGRAM ELEMENT NUMBER 61102F	
6. AUTHOR(S) Byeong Ho Kang				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) UNIVERSITY OF TASMANIA 2 CHURCHILL AVE SANDY BAY, 7005 AU				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AOARD UNIT 45002 APO AP 96338-5002				10. SPONSOR/MONITOR'S ACRONYM(S) AFRL/AFOSR IOA	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) AFRL-AFOSR-JP-TR-2016-0058	
12. DISTRIBUTION/AVAILABILITY STATEMENT A DISTRIBUTION UNLIMITED: PB Public Release					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT Detecting phishing websites has been noted as a complex and dynamic problem area because of the subjective considerations and ambiguities of detection mechanism. Either machine learning technique or human expert system has been applied to acquire and maintain the knowledge for phishing website detection and prediction but neither did work successfully. In this project, we propose novel approach that uses Ripple-down Rule (RDR) to maintain the knowledge from human experts with knowledge base generated by the Induct RDR, which is a machine-learning based RDR algorithm. The performance of proposed model was compared with that of 6 different machine-learning techniques. Our experimental results showed the proposing approach can help to deduct the cost of solving over-generalization and over-fitting problems of machine learning approach.					
15. SUBJECT TERMS Intrusion Detection					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 10	19a. NAME OF RESPONSIBLE PERSON SCHULMAN, MARK
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include area code) 315-225-5880

“Intrusion Detection Systems with Live Knowledge System”

19 May, 2016

Name of Principal Investigators (PI and Co-PIs): Byeong Ho Kang

- e-mail address : Byeong.Kang@utas.edu.au
- Institution : University of Tasmania
- Mailing Address : Private Bag 87 Hobart TAS 7001, Australia
- Phone : +61 (0)3 6226 2919
- Fax : +61 (0)3 6226 1824
-

Period of Performance: 05/20/2015 – 05/19/2016

Abstract:

Detecting phishing websites has been noted as a complex and dynamic problem area because of the subjective considerations and ambiguities of detection mechanism. Either machine learning technique or human expert system has been applied to acquire and maintain the knowledge for phishing website detection and prediction but neither did work successfully. In this project, we propose novel approach that uses Ripple-down Rule (RDR) to maintain the knowledge from human experts with knowledge base generated by the Induct RDR, which is a machine-learning based RDR algorithm. The performance of proposed model was compared with that of 6 different machine-learning techniques. Our experimental results showed the proposing approach can help to deduct the cost of solving over-generalization and over-fitting problems of machine learning approach.

Introduction:

An accelerative growth of Internet-based financing increases online fraudulent activity in which malicious people try to reveal sensitive information of Internet users, also called as phishing. Phishing detection has received great attention but there has only been limited research on a way of overall success due to the nature of problems. The problems of detecting phishing websites are very complex and hard to analyze as technical and social problems are intervened each other. Either machine learning technique or human expert system has been applied to acquire and maintain the knowledge for phishing website detection and prediction while the results do not yet show significant success.

A large number of knowledge-based systems are built for acquiring and maintaining the knowledge for detecting and predicting the phishing website. Phishing website detection knowledge was originally acquired from domain experts. However, acquiring knowledge from an expert in a slow pace cannot meet the demand of the expanding systems since a sophisticated expert system may require an extremely large number of rules. This leads to machine learning based approach as a solution to manage knowledge-based systems.

Although machine learning technique can acquire knowledge from phishing website data without the help of a domain expert, an abundance of classifier models exist and decision tree based algorithms provide the best performance, over-generalization and over-fitting are still significant problems when sufficient training data are not available in which case there are not

enough patterns that can be found by machine learning. Therefore, large effort usually has to be undertaken to cover those abnormal cases arising from this problem and the cost usually results in repeating reconstruction of the knowledge base.

In order to solve those issues in machine learning and human expert, we assume that combining two different mechanisms of having machine learning and expert system-style knowledge acquisition will optimize knowledge engineering process.

Hence, we focused on developing phishing website detection model by applying Induct RDR approach. The proposed induct RDR (Ripple Down Rules) approach allows to acquire the phishing detection knowledge by machine learning, and maintained by human domain expert.

The main contents of this report consists of submitted publications to the conference [4,5]

Method

In this project, we focused on detecting phishing websites by using the knowledge acquired by machine learning, and maintained by human expert. In order to achieve this goal, we applied Ripple Down Rule based approaches.

In Ripple-down Rules (RDR), its unique knowledge acquisition process solves the problems that lie on knowledge engineering process. RDR is built with rules of hierarchical exceptions. It is a knowledge acquisition and representation technique that allows knowledge of a certain domain to be interpreted as rules. The RDR structure is a finite binary tree where each node can have two distinct branches, which are called except and if-not. Cases are evaluated from the root node of the RDR tree. Each node in the tree is a rule with the form of if α then β (α is the condition and β is the conclusion). When the system encounters an incorrect classification, a new exception rule is added based on experts' judgment with the given case. Therefore, RDR can incrementally develop a relatively accurate knowledge base, provided the domain is fixed and the experts provides the correct judgments.

Since RDR based knowledge base depends on experts' judgment, the correctness of the used language expressed by the expert is the key of developing a good knowledge base. According to Pham and Hoffmann [3], it may cost a long time to classify most of the relevant cases correctly, if the target is linear threshold in the numerical input space. This is because in general an expert is only allowed to use axis-parallel cuts, which is in fact unsuitable to express the knowledge accurately.

The following process describes how to combine human knowledge and machine learning.

1) Generate rules by machine learning via training dataset. (Induct RDR)

Induct RDR allows creating RDR-based knowledge base through machine learning technique. Induct RDR was introduced by Gaines when illustrating a fundamental relation between techniques that transfer existing knowledge from human experts and those that create new expertise through machine learning [2]. He mentioned a sequence of dispersing knowledge partially from the view of a human expert which consists of the following seven stages.

1) Minimal Rules, 2) Adequate Rules, 3) Critical Cases, 4) Source of Cases, 5) Irrelevant Attributes, 6) Incorrect Decisions, 7) Irrelevant Attributes & Incorrect Decisions

The first stage is a complete, minimal set of correct decision rules, so no data is required

for knowledge acquisition since the correct answer is available from the expert. On the contrary, the last stage is a source of data from which the correct answer might be derived with the greatest probability of correct decisions, so the expert has provided little. The stages in the middle from top to bottom show a decrease in existing knowledge though human intervention but an increase in new expertise through machine learning. The main use of existing RDR is close to the top stage. Therefore, Induct RDR which derives rules directly from an extension of Cendrowska's Prism algorithm [3] was made to be close to the bottom. An example of Induct RDR tree is shown in Figure 1. This Induct RDR sums standard binomial distribution as the possibility of selecting correct data at random to measure the correctness of a rule

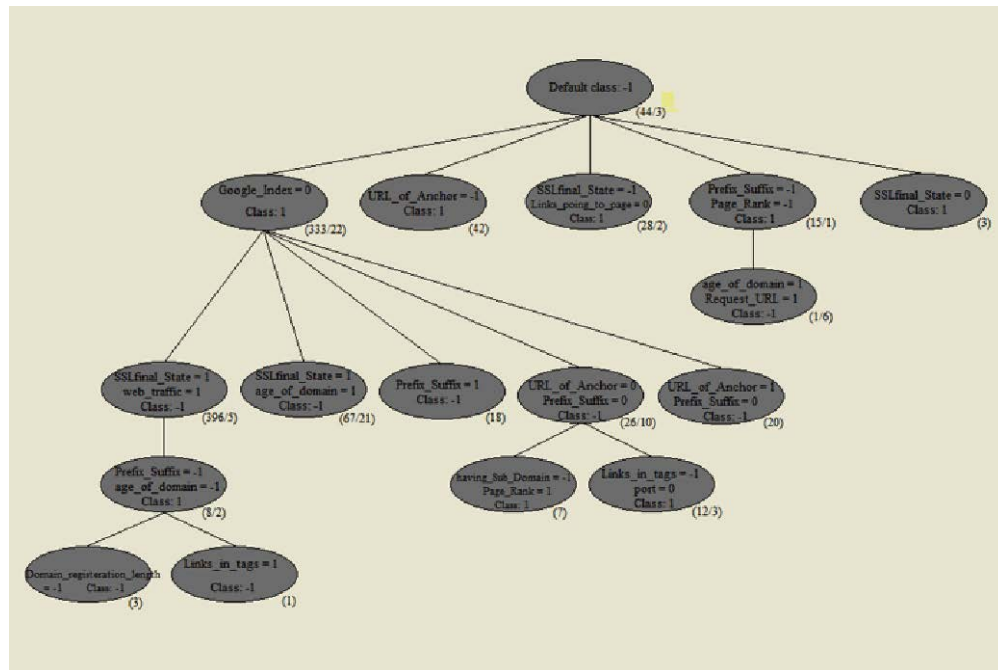


Figure 1 RDR rule tree with induct RDR

2) Find out incorrectly classified data.

Based on the evaluation, we can find the nodes that with poor accuracy. Figure 2 shows a RDR rule tree, where red-circled nodes indicate those nodes with poor prediction of accuracy.

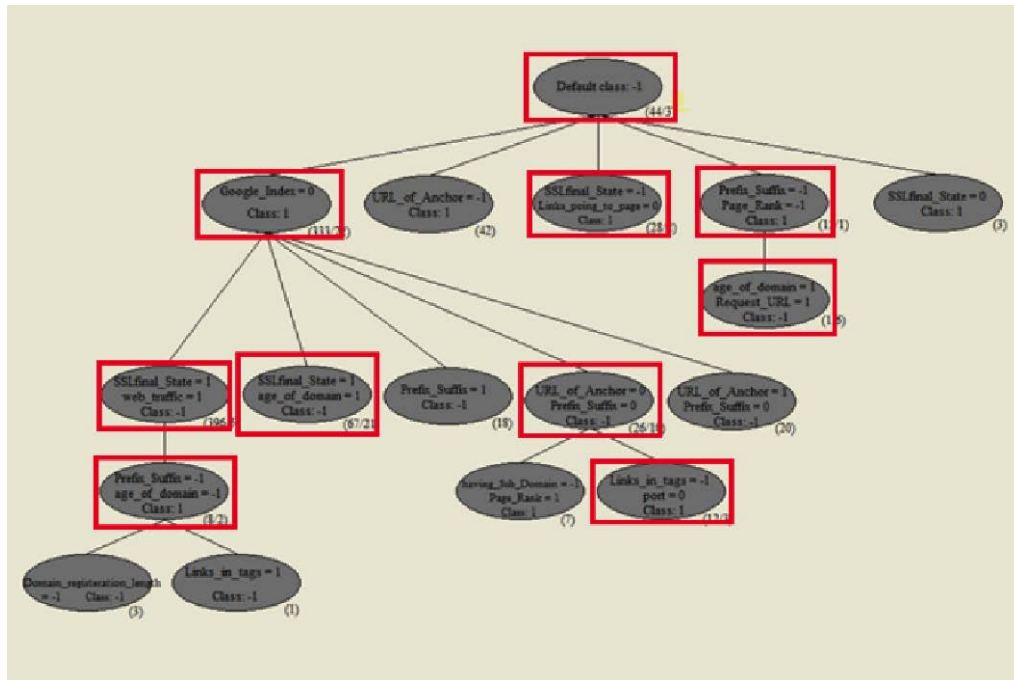


Figure 2 Original RDR rule tree with highlighted nodes to be modified

- 3) Acquire rules from the expert and use those rules (human knowledge) to add exception rules for the machine learning rules where data are incorrectly classified

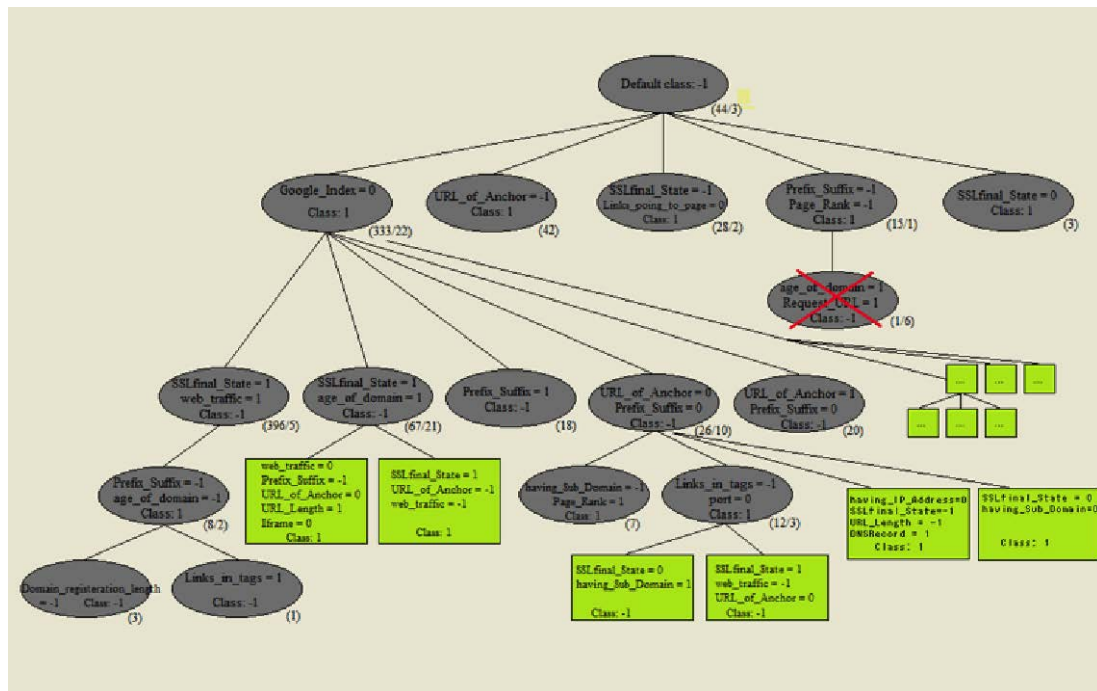
RDR framework supports the function, which enables acquiring the human expert's knowledge based on the current context and adding that knowledge incrementally. The nodes in the above figure should be modified in one of the following ways, 1.Add a new branch to the node, 2.Delete the node, and 3.Delete one of the branches of the node.

Figure 3 describes the result of modified nodes from the original RDR rule tree. Red-coloured 'X' sign represents the stopping rule, and the green-coloured boxes describe the refined rule.

However, when human knowledge is applied to those incorrectly classified data, not all of the knowledge can be applied. There are two reasons for this.

- 1) There are data, which have the same vector of attributes but belong to different classes. This is because the existing attributes are not enough to tell the difference. Therefore, the class which the majority belong to will be decided as the conclusion and it is less possible to correctly classify the minority.
- 2) Some rules applied might affect other correctly classified data. The knowledge created by the expert gives a hint about how these rules affect the whole dataset. If a rule has more incorrectly classified data than correctly classified data, it should not be applied

In this case, all human knowledge is correct and the two problems mentioned above do not apply.



Experiment:

Phishing Website Dataset

UCI has published the training dataset that includes important 31 features in detecting and predicting phishing websites. This dataset was collected mainly from PhishTank archive, MillerSmiles archive and Google's searching operators. Although 'there is no agreement in literature on the definitive features that characterize phishing webpages' (UCI Machine Learning Repository n.d.), the features (attributes) of this dataset are understandable and can be easily expressed by human language, which means that it is suitable for a human expert to provide knowledge [1]. The training dataset contains 11063 websites.

- Features/Attributes: having_IP_Address, URL_Length, Shortning_Service, having_At_Symbol, double_slash_redirecting, Prefix_Suffix, having_Sub_Domain, SSLfinal_State, Domain_registration_length, Favicon, port, HTTPS_token, Request_URL, URL_of_Anchor, Links_in_tags, SFH, Submitting_to_email, Abnormal_URL, Redirect,on_mouseover, RightClick,popUpWidnow, Iframe, age_of_domain, DNSRecord, web_traffic, Page_Rank, Google_Index, Links_pointing_to_page, and Statistical_report.
- Class: Phishing/Non-Phishing

Results and Discussion:

In order to evaluate the performance of the proposed model, we tested the performance with six other machine learning techniques by using 10-fold cross validation. The following table describes

No	Evaluation Algorithm
1	LMT (logistic Model Tree) - A learner, Classification trees with logistic regression functions at the leaves
2	SVM (Support Vector Machine)
3	C4.5 DT (Decision Tree)
4	RIPPER (Repeated Incremental Pruning to Produce Error Reduction)
5	One R (Class for building and using a 1R classifier)
6	Induct RDR
7	Induct RDR + Human RDR rule

1. Prediction Accuracy

Compared to other machine learning only model, the combination of Induct RDR (machine learning) and human expert rule achieved much higher accuracy (0.952).

In the case of RDR (machine learning and human rules), the knowledge base is built by Induct RDR before adding human knowledge. Then the test dataset is used to examine this knowledge base to find incorrectly classified data. A simulated expert is used to find correct rules for those incorrectly classified data. In the case of RDR (machine learning only) and C4.5 Decision Tree, they are based on machine learning only so their prediction accuracy is based on predicting the test dataset using the knowledge base acquired from the training dataset.

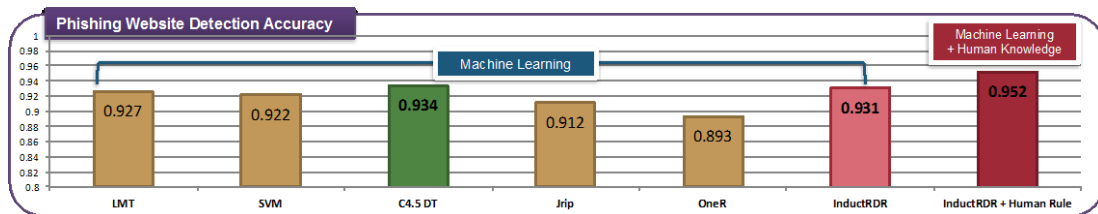


Figure 4 The accuracy of detecting phishing website

It has been found that RDR with machine learning only can achieve 93.1% of prediction accuracy. After adding human rules, the result can be improved up to 95.2%. Although C4.5 Decision Tree had the best prediction accuracy (93.4%), RDR with machine learning and human rules outperforms it eventually. Therefore, it can be concluded that adding human knowledge to the knowledge base created by machine learning does improve the prediction accuracy. Usually prediction accuracy becomes low if there are significant over-generalisation and over-fitting problems. In this case, prediction accuracy has been improved so that it implied that over-generalisation and over-fitting problems have been solved to some extent.

In addition to the good accuracy of phishing website detection, the proposed approach in this project allows human experts to incrementally add and maintain the knowledge in the knowledge base with no rebuilding or initialization process.

2. Cost

Solving over-generalisation and over-fitting problems in machine learning is usually accompanied with adding new data cases to the existing data cases to enrich the patterns. The existing knowledge base is abandoned and a new knowledge base is constructed. The amount of knowledge can be quantified as the numbers of nodes and conditions in a knowledge base, so the cost of solving the problems can be quantified as how many nodes

and conditions are reconstructed. This is the case of machine learning. For the case of adding human knowledge, the cost is how many nodes and conditions are added to the original knowledge base.

The following table summarises the result of reconstructed or increased nodes and conditions after solving over-generalization and over-fitting problems. By applying human knowledge, the increased ratio of nodes for improving 1% of accuracy is 33.54%, much smaller than those of RDR (machine learning only) and C4.5 Decision Tree (111.80% and 99.92% respectively). Similarly the increased ratio of conditions for improving 1% of accuracy is 69.41%, much smaller than those of RDR (machine learning only) and C4.5 Decision Tree (193.45% and 195.49% respectively). As mentioned above, the reason that pure machine learning models cost much is because they abandon the existing knowledge base and create a new one every single time that it encounters a new data case which cannot be explained by the existing knowledge base.

Table 1 Cost Evaluation Result of Knowledge Increased

Models	RDR (machine learning and human rules)	RDR (machine learning only)	J48
Number of nodes original	16	16	28
Number of conditions original	26	26	73
Number of nodes after solving the stated problems	27	77	80
Number of conditions after solving the stated problems	63	119	210
Improved ratio of predication accuracy	2.05%	3.41%	0.96%
Increased ratio of nodes	68.75%	381.25%	185.71%
Increased ratio of conditions	142.30%	340.74%	187.67%
Increased ratio of nodes per 1% of accuracy improvement	33.54%	111.80%	193.45%
Increased ratio of conditions per 1% of accuracy improvement	69.41%	99.92%	195.49%

Therefore, it can be concluded that the reconstructed or increased ratio of knowledge base is much smaller by combining human knowledge and machine learning than those approaches based on machine learning only.

Reference:

- [1] Mohammad RM, Thabtah F, McCluskey L. Predicting phishing websites based on self-structuring neural network. Neural Computing and Applications. 2014 Aug 1;25(2):443-58.
- [2] B. R. Gaines and P. Compton, "Induction of ripple-down rules applied to modeling large databases," in Journal of Intelligent Information Systems, vol. 5, no. 3, 1995, pp. 211-228.
- [3] Pham, S.B. and A. Hoffmann, A new approach for scientific citation classification using cue phrases, in AI 2003: Advances in Artificial Intelligence. 2003, Springer. p. 759-771

- [4] Chung, H, Chen, R, Han SC, and BH Kang “Combining RDR-based Machine Learning Approach and Human Expert Knowledge for Phishing Prediction”, 14th Pacific Rim International Conference on Artificial Intelligence, 2016 (Accepted)
- [5] Han, SC and BH Kang, “Modification of Induct RDR for Intrusion Detection System”. International Journal of Reliable Information and Assurance (IJRIA) 2016 (Submitted)

List of Publications and Significant Collaborations that resulted from your AOARD supported project:

e) manuscripts submitted but not yet published

Chung, Hyunsuk, Renjie Chen, Soyeon Caren Han, and Byeong Ho Kang. (2016, Accepted). “Combining RDR-based Machine Learning Approach and Human Expert Knowledge for Phishing Prediction”, 14th Pacific Rim International Conference on Artificial Intelligence

Han, Soyeon Caren and Byeong Ho Kang. (2016, Submitted). “Modification of Induct RDR for Intrusion Detection System”, International Journal of Reliable Information and Assurance (IJRIA)

Attachments: Publications a), b) and c) listed above if possible.