ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Verifying a Behavior Based Anti-Phishing Approach using Model Checking

Abdullah M. Alnajim

Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia

Abstract: Phishing is a form of electronic identity theft in which social engineering and website spoofing techniques are employed to trick a user into revealing confidential information. In this research, a previously proposed behaviour based anti-phishing approach model is verified using model checking. SPIN model checker is used to check the absence of deadlocks as well as reachable states. SPIN illustrates that there is no error since it does not report "invalid end state" as there is no deadlock in the model. There is also no error and unexecuted codes since as all processes have "zero" unreached states and the trail number equals to "zero". Formal verification using SPIN is applied to help checking whether the model is feasible and applicable. This helps deploying the approach model in the real world in order to enhance phishing countermeasures within LANs.

Keywords: Blacklists, Formal Methods, Model Checking, SPIN, LAN, Network Proxy, Network Security, Phishing, countermeasures.

I. INTRODUCTION

The Internet has become a vital medium of communication in recent years. Security-critical applications (e.g. online banking login page) that are accessed using the Internet are at the risk of Internet fraud. Violations of security in these applications would result in severe consequences, such as financial loss for e-commerce and online banking organizations for individuals. Phishing attack is a criminally fraudulent process of capturing confidential information such as usernames, passwords and credit card details by impersonating a trustworthy entity in an electronic communication [1,2]. The attack is classified as a form of electronic identity theft in which both social engineering and website spoofing techniques are used to trick people into revealing their confidential information [3].

The Anti-Phishing Working Group (APWG) has reported that during the last three months of the 2014 (Quarter 4 (Q4)) only, the number of unique phishing reports submitted to APWG was 197,252 [4]. The report shows that this was an increase of 18 percent from the 163,333 received in Q3 of 2014. APWG also stated that the total number of phishing attacks observed in Q4 was 46,824 which targeted a total of 437 brands. APWG assured that the United States continued to be the top country hosting phishing sites [4].

There are technical advances that mitigate the problem of Phishing. For instance, security toolbars, such as Spoof Stick, Trust Bar and Spoof Guard, can prevent Phishing attacks.

Anti-Phishing training for end users is indispensable to any proposed technical solution. It is suggested that while technical improvements may continue to stop the attacks, end-user training is a key component in phishing attacks mitigation [5]. In preventing online fraud, Symantec [6] believes that users' awareness is central to helping to change their behaviors and thus reduce their mistakes with phishing emails and websites.

Anti-Phishing training will make the end-user aware and it will erect an effective barrier against phishing attempts. Anti-Phishing awareness was shown to have a great positive effect in mitigating the risk of phishing [7].

There are different anti-Phishing training approaches to make users aware of phishing emails and websites and to learn how to avoid them. The most basic approach is publishing guidelines for the Internet users to follow when they go online. These guidelines are referred as tips for users. All the information used in the training approaches is based on tips for users.

In this paper, a behaviour based anti-phishing model is verified using model checking. This research uses formal verification in order to help checking whether the model is feasible to be deployed in the real world.

In this research, there is an assumption that phishing attacks do not use either software to change the host files in users' operating systems or any malicious software, such as a virus, worm or Trojan horse, that runs in users' operating systems. These are called 'Pharming' and 'Malware' and are different from phishing. Phishing is a deceptive attack which aims to take advantage of the way humans interact with computers or interpret messages rather than taking advantage of the technical system vulnerabilities [8].

The remainder of the paper is organized as follows. Section two reviews the literature regarding phishing detection methods and shows behaviour based anti-phishing approach that was proposed in a previous research [9]. The third section presents the methodology the research follows to verify the anti-phishing approach model. The fourth section discusses and analyses the results. The final section concludes the paper and discusses the possible way of future work.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

II. RELATED WORK

A. Anti-Phishing countermeasures

Phishing can be performed in different ways. They are as follows [10]:

1. Email-to-email: this occurs when someone receives an email asking for sensitive information to be replied to the sender email or sent to another email.
2. Email-to-website: this occurs when someone receives an email with embedded web address that leads to a phishing website.
3. Website-to-website: this occurs when a phishing website is reached by clicking on an online advert or through a search engine.
4. Browser-to-website: this occurs when someone misspelled a web address of a legitimate website on a browser and then goes to a phishing website that has a similar address.

There are technical (e.g. toolbars) and training (e.g. tips) approaches to mitigate phishing. The anti-phishing toolbars are web browser plug-ins that warn users when they reach a suspected phishing site [8]. Anti-phishing tools use two major methods for mitigating phishing sites. The first method is to use heuristics to check the host name and the URL for common spoofing techniques. The second method is to use a blacklist that lists phishing URLs. The heuristics approach is not 100% accurate since it produces low false negatives (FN), i.e. a phishing site is mistakenly judged as legitimate, which implies they do not catch all phishing sites. The heuristics often produce high false positives (FP), i.e. incorrectly identifying a legitimate site as fraudulent. Blacklists have a high level of accuracy because they are constructed by paid experts who verify a reported URL and add it to the blacklists if it is considered as a phishing website [11].

To increase the accuracy FP and FN rates, Xiang et. al. [12] proposed CANTINA+ which is a comprehensive feature-based approach including eight novel features, which exploits the HTML Document Object Model (DOM), search engines and third party services with machine learning techniques to detect phishing. Xiang et. al. [12] designed two filters to help reduce FP. The first is phishing detector that uses hashing to catch highly similar phishing attacks. The second is a login form filter, which directly classifies Web pages with no identified login form as legitimate. CANTINA+ eventually is evaluated and achieved good accuracy rates but yet did not reach a 100 percent accurate FP and TP rates.

The anti-phishing tools always works in a way that receives users' submission of phishing URLs. Usually, they are not fast and efficient enough to find and take down phishing attacks [13]. Bo et. al. [13] propose a hybrid method to discover phishing attacks in an active way based on DNS query logs and known phishing URLs. They analyzed phishing reports from Anti-phishing Alliance of China (APAC) and developed their system to report living phishing URLs automatically to APAC every day. They evaluated the system and reported that it is good complement to traditional anti-phishing tools.

Many financial and commercial, private and government institutions (e.g. eBay and HSBC) have provided anti-phishing training tips for detecting phishing emails and websites. The aim of the tips is to train users to look for phishing clues located in emails and websites to enable them to make better decisions in distinguishing phishing emails and websites. People in general do not read anti-phishing online training materials although some of them are found effective when used [14].

Many commercial institutions, such as Microsoft, periodically send email security information to help their customers in protecting their online security [15]. This email provides practical security tips, useful resources and links, and a forum to ask security-related questions. Theses emails are usually sent in text and HTML formats. The limitation of this approach is that customers who are interested in receiving these emails need to subscribe with the commercial institutions (i.e. anti-phishing emails providers) in order to be included in receiving these emails.

Alnajim and Munro [16] proposed a novel anti-phishing approach that uses training intervention (APTIPWD). The approach helps users to make correct decisions in distinguishing phishing and legitimate websites. It brings information to end-users and helps them immediately after they have made a mistake in order to detect phishing websites by themselves. The new approach also keeps anti-phishing training ongoing process. This means, in all time, once users tries to submit information to phishing website; they will be trained (see Figure 1).

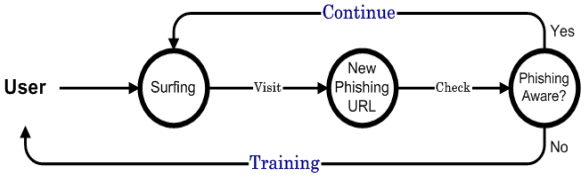

Fig 1. The broad idea of APTIPWD

There are many anti-phishing tips that can be used in the intervention message. The effectiveness of most common users' tips for detecting phishing websites using novel effectiveness criteria was examined [14]. The aim of the tips' effectiveness examination was to find fewer anti-phishing tips that users can focus on to detect phishing attacks by themselves. Therefore, the most effective anti-phishing tip was used [16].

The tip was as follows: "a fake website's address is different from what you are used to, perhaps there are extra characters or words in it or it uses a completely different name or no name at all, just numbers. Check the True URL (Web Address). The true URL of the site can be seen in the page 'Properties' or 'Page Info': While you are on the website and using the mouse Go Right Click then Go 'Properties' or 'Page Info'. If you don't know the real web address for the legitimate organization, you can find it by using a search engine such as Google".

DOI 10.17148/IJARCCE.2015.47102

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

B. A Country Based Model Towards Phishing Detection Enhancement

Alnajim [17] then proposed a novel country based model to detect phishing attacks. The aim is to enhance the phishing countermeasures applied on a country's Internet infrastructure. This is because of that the anti-phishing framework in Saudi Arabia is exposed to users when they fall to phishing attacks and thus enhancing anti-phishing behaviors by training them to detect phishing instead of only blocking phishing websites is proposed. The idea presented by Alnajim and Munro [16] is applied on the current anti-phishing framework implemented in Saudi Arabia [18].

Alnajim [17] new model has advantages and limitations. The advantage is that the model is exposed to phishing victims who are inside the country deployed it (e.g. Saudi Arabia). This enhances the anti-phishing countermeasures deployed nowadays in Saudi Arabia. Whereas a potential drawback could be that it makes the Internet traffic slower. This is because of extra component (i.e. Intervention Server) added to the anti-phishing detection framework in Saudi Arabia.

C. An Automated Analyzer For Users' Anti-Phishing Behaviour Within a LAN

Alnajim [9] also proposed a novel behaviour based anti-phishing approach that is deployed within a Local Area Network (LAN). The approach was a model that automatically and continuously analyzes users behaviours against phishing attacks and then based on the results it decides whether to train them or not against phishing. The aim is to enhance the phishing countermeasures applied on a LAN by making users aware of phishing attacks and how to prevent them.

Organizations, such as universities and companies, have many users to their internal LANs. They use their LANs to do their tasks, access the network resources, use the Internet or communicate with others. They may be exposed to phishing attacks since they are connected to the Internet. Therefore, making users aware of phishing attacks and how to prevent them would enhance the phishing countermeasures. Due to this, this research proposes a model that checks continuously the LAN users' phishing awareness status by automatically analyzing their behaviours against phishing attacks in order to know whether they are phishing unaware users. Based on the results a decision is taken to get them trained against phishing (in case they are unaware) by using the training intervention idea proposed previously [16].

Alnajim [9] stated that there were few technical assumptions that should be stated before presenting the new model. They are as follows:

1. The LAN is connected to the Internet.
2. The LAN resources are controlled. This means that every user should be registered and authorized to use the LAN by an authentication system. Once a user would like to use the LAN, they should authenticate themselves by providing their access credentials (e.g. id and password).
3. Every user has an email address that is linked to his network ID.

The behavior based anti-phishing model has additional components added in order to perform as expected [9]. The new model main component is referred as "Automated Trainer". The Automated Trainer is a framework that includes few subcomponents to perform the task of the model. These subcomponents are as follows:

- An agent named as the User Behavior Analyser' (UBA).
- A database named as the User Awareness Status (UAS).
- A Web Mail Server.
- A server named as the Local Fixed List of Anti-phishing Training Websites Sever (LFLAPTW).

The job of each sub-component mentioned and their interaction with each other (scenario) are described below.

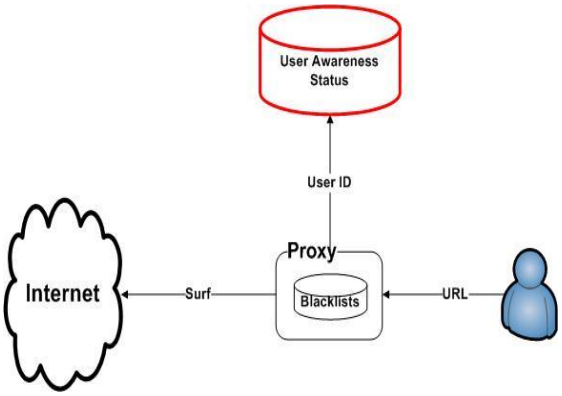

Fig 2. The Proposed User Awareness Status Feed

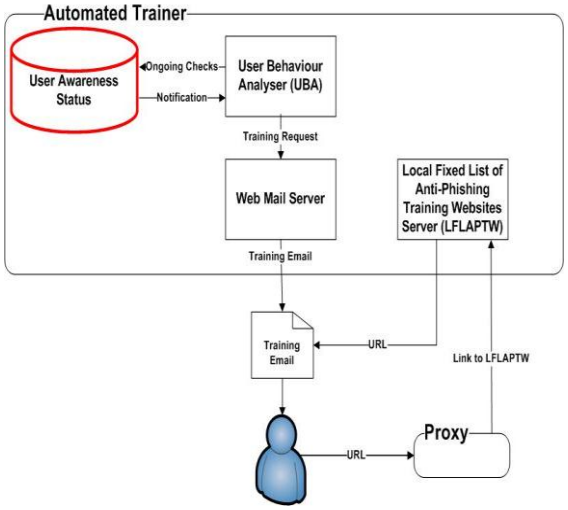

Fig 3. The Proposed Anti-phishing LAN Approach

When a user would like to surf the Internet working from a terminal within a LAN (Local Area Network), they request a URL. The URL is sent to the network proxy. The proxy checks weather the URL is blacklisted or not. Accordingly the proxy accepts –based on a defined policy- the URL

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

and pass it to the Internet zone or rejects it. In case of that a user requests a blacklisted phishing URL the proxy will reject it and then sends the user ID to an Automated Trainer system (described later). The system then changes the user status from 'phishing aware' to 'phishing unaware' in the User Awareness Status (UAS) database (Please see Figure 2). This database is created in order to record users anti-phishing awareness status. All users IDs recorded in the database are 'phishing aware' by default unless a notification comes from the network proxy. This is to ensure that the system is convenient.

Figure 3 shows the proposed anti-phishing LAN approach. The approach is a system called 'Automated Trainer'. This system has a primary component which is referred as 'User Behaviour Analyser' (UBA). The UBA is an agent that performs an ongoing process of analyzing user anti-phishing behaviours within a local network and decides whether users anti-phishing awareness needs to be enhanced or not (see Figure 4). The UBA takes the user status from the UAS database mentioned previously.

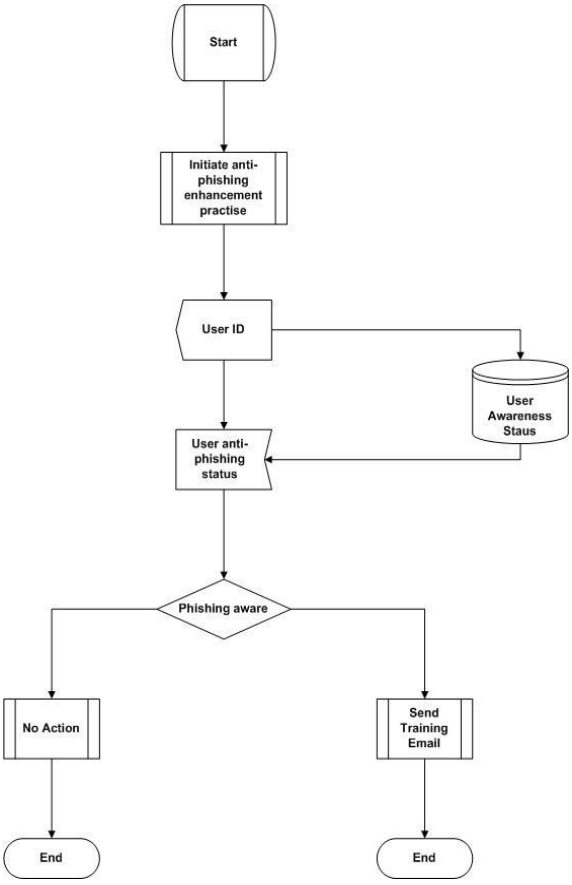

Fig 4. Flowchart of User Behaviour Analyzer (UBA)

The UBA's task is to frequently check the UAS database for users flagged 'phishing unaware'. If it finds phishing unaware users, it initiates a need-for-training request 'training request' and sends it to a Web Mail Server working within the LAN. The UBA sends a packet includes user ID, the textual email content and the fake targeted brand email address.

The web mail server is configured in a way that it receives the packet from the UBA and sends an anti-phishing Training Email to the user. The email has the sent textual email content and includes a fake URL pretended to be a URL for a genuine website. The fake URL leads to a fake website that is run locally among many websites located in a local server. This server is referred as Local Fixed List of Anti-phishing Training Websites Sever (LFLAPTW). Running these websites locally ensures users confidentiality for their data.

D. Formal Methods and Model Checking

Formal verification is considered as an important topic in the field of formal methods. Formal methods are then considered as mathematical techniques and tools which can be used for the modeling, specification, and verification of systems [19]. All these aspects are concerned with formal behavior description of systems, and to which degrees these systems' reflect the specification.

Formal verification is performed by looking up the state space of the system using model checkers for embracement of the specification properties [20]. If these properties hold, then model checkers mostly return empty file but if there is a violation in a property then a TRAIL file (i.e. the output file of SPIN model checker) or a Counter Example (i.e. the output file of SMV model checker) will be generated to show how the violation has taken place. Model checker can represent the result as a sequence of model states that contain the model variables and their values at that state, which incrementally cause the violation [21].

One way to verify whether a program is correct is to systematically check that the correctness specifications in all possible tracks and that is what model checkers like SPIN are designed to do [22]. The model checker "SPIN" (Simple PROMELA Interpreter) is a general tool for verifying the correctness of distributed software models in an automated fashion [23]. Models to be verified are described in PROMELA (Process Meta Language) codes. Codes in PROMELA are composed of a set of processes. In addition to model checking, SPIN also acts as a simulator, following one possible execution path through the system and presenting the resulting execution trace to the user [23].

SPIN verification is carried out against safety and liveness properties. Safety is a property of reachable states and liveness is a property of sequence of states and absence of deadlocks [22]. SPIN checks the properties as the following [24]:

- Safety property is checked by trying to find a trace leading to the "undesired" thing. If there is not such a trace, the property is satisfied.
- Liveness property is checked by trying to find an infinite loop in which the "good" thing does not happen. If there is not such a loop, the property is satisfied.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Hedge [22] states that the model in PROMELA is simulated using the SPIN tool and checked to verify whether it runs as expected. If the model is ready, then the correctness of the model can be checked. This will be done in two phases namely assertions and linear temporal logic (LTL). Assertions are predicates that are inserted between any two statements in the PROMELA code, to check whether it is evaluated to true or false during simulation. LTL is used to express the properties of the model that depend on the evaluation of a predicate in a sequence of states.

In this paper, research will be conducted to use model checking in order to verify the proposed behaviour based anti-phishing model presented previously by Alnajim [9] and shown in Figure 3. The research in this paper uses formal verification in order to help checking whether the model is feasible to be deployed in the real world within a LAN.

III.METHODOLOGY

This research employs formal verification for the anti-phishing model shown in Figure 3 using SPIN model checker. This is to check for vulnerabilities based on the system components. Each component of the model is considered as a different process. These processes are expressed in PROMELA code (Process or Protocol Meta Language). The PROMELA language is used to write a code that reflects the behavior of the processes mentioned in the state chart diagram of the model. The state chart diagram is shown in Figure 5.

Therefore, the steps taken to perform the formal verification are described as follows. First of all, the anti-phishing model is transferred to UML (Unified Modeling Language) state diagram using Argo UML[1] CASE tool. The UML state diagram of the model is expressed into a PROMELA code. This expression is achieved by using Hugo/RT[2] which is a tool that can capture the properties of the model and transfer them as a PROMELA code.

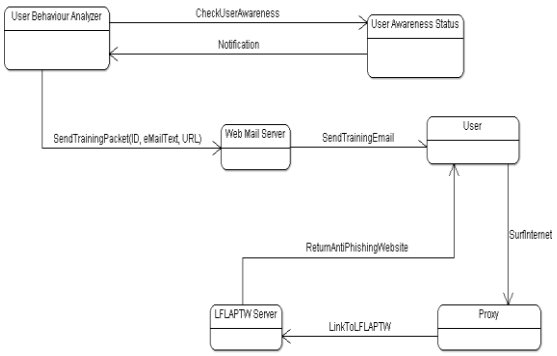

Fig 5. The Model's State Diagram

IV.RESULTS AND DISCUSSION

SPIN model checker is used to check for (1) absence of deadlocks as well as (2) reachable states. Figures 6,7 and 8 present screen shots of the SPIN model checker used. They show the PROMELA code written in the right hand side and the verifications results in the right hand side. This code expresses the flow shown in the state chart diagram of the model presented in Figure 4.

Safety, Acceptance and Interactive verifications were performed. As shown on Figure 6,7 and 8, SPIN did not report "invalid end state" as there is no deadlock in the model. In addition, there is no error and unexecuted codes, as all processes have "zero" unreached states and the trail number equals to "zero" which means that the SPIN analyzer finds no errors in the model.

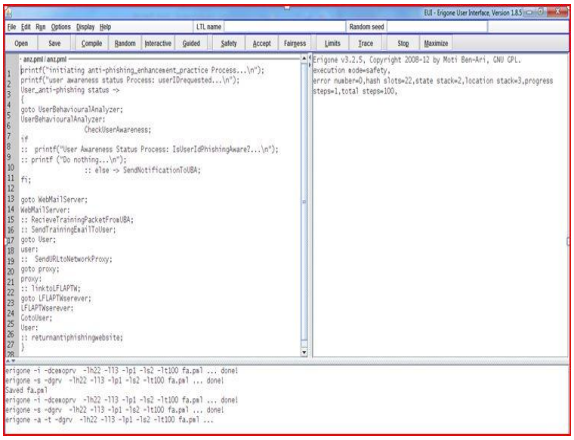

Fig. 6. Safety Test's Results

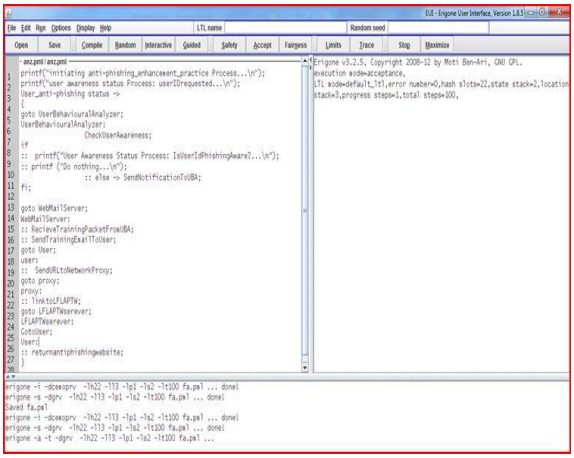

Fig. 7. Acceptance Test's Results

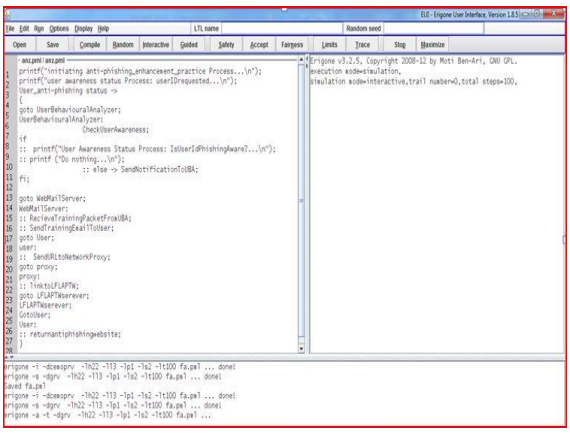

Fig. 8. Interactive Test's Results

DOI 10.17148/IJARCCE.2015.47102

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Having verified the model using SPIN model checker, it is proved that the anti-phishing model shown in Figure 3 has no deadlocks and all its states are reachable. Thus, the model is feasible and applicable. This helps deploying the approach model in the real world in order to enhance the phishing countermeasures applied within a LAN.

V. CONCLUSION

In this research, a previously proposed behaviour based anti-phishing approach model was verified using model checking. The aim behind using formal verification is to help checking whether the model is feasible and applicable in order to deploy it in the real world.

The verified model was presented by Alnajim [9] and shown in Figure 3. SPIN model checker was used to check for vulnerabilities based on the system components. SPIN checked the absence of deadlocks as well as reachable states. The model's processes were expressed in PROMELA code. This expression was achieved by using Hugo/RT that captures the properties of the model's state diagram and transfers it into a PROMELA code.

Safety, Acceptance and Interactive verifications were performed. SPIN showed that there was no "invalid end state" as there was no deadlock in the model. There was also no error and unexecuted codes since as all processes had "zero" unreached states and the trail number equalled to "zero". This means that the SPIN analyzer found no errors in the model.

All in all, it is proved that the anti-phishing model proposed and shown in Figure 3 has no deadlocks and all its states are reachable. Thus, the model is feasible and applicable. This helps deploying the approach model in the real world in order to enhance the phishing countermeasures applied within a LAN.

A possible direction of future work could be trying to apply the model in a 'real' environment. This will return a valuable real time evaluation for the approach effectiveness against phishing attacks.

VI. ACKNOWLEDGMENT

The author would like to thank **Dr. Hazem Alrawashdeh** for his appreciated cooperation in helping the author installing and running the software package of SPIN model checker with its required software tools.

REFERENCES

[1] The National Consumers League Projects (2015), "Phishing". Available Online: http://www.fraud.org/scams/internet-fraud/phishing, last access on 15/5/2015.

[2] G. K. Tak, N. Badge, P. Manwatkar, A. Ranganathan, S. Tapaswi, "Asynchronous Anti Phishing Image Captcha approach towards Phishing". Proc. the 2nd International Future Computer and Communication (ICFCC), Wuhan, IEEE Press, 2010, pp. V3-694 - V3-698.

[3] M. Aburrous, M. A. Hossain, K. Dahal, F. Thabtah, "Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies". International Journal of Cognitive Computation, vol. 2 issue. 3, New York, USA: Springer, 2010, pp. 242-253.

[4] Anti-Phishing Working Group APWG (2015). Phishing Activity Trends Report, 4th Quarter 2014. Available: http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf, last access on 26 June 2015.

[5] S. A. Robila and J. W. Ragucci, "Don't be a Phish: Steps in User Education". Proc. 11th annual SIGCSE conference on innovation and technology in computer science education. New York: ACM Press, 2006, pp. 237 – 241.

[6] Symantec (2004). Mitigating Online Fraud: Customer Confidence, Brand Protection, and Loss Minimization. Available: http://www.antiphishing.org/sponsors_technical_papers/symantec_online_fraud.pdf, last access on 21/3/2007.

[7] A. Alnajim and M. Munro, "Effects of Technical Abilities and Phishing Knowledge on Phishing Websites Detection". Proc. the IASTED International Conference on Software Engineering (SE 2009), Innsbruck, Austria, ACTA Press, 2009, pp. 120-125.

[8] J. S. Downs, M. B. Holbrook and L. F. Cranor, "Decision strategies and susceptibility to phishing". Proc. the 2nd symposium on usable privacy and security. New York, USA: ACM Press, 2006, pp. 79 – 90.

[9] A. Alnajim, 2015. "An Automated Analyzer for Users' Anti-Phishing Behaviour within a LAN". International Journal of Soft Computing and Engineering (IJSCE), vol. 5 issue. 3, India: BEIESP, 2015, pp. 115 – 119.

[10] A. Alnajim, and M. Munro, "An Approach to the Implementation of the Anti-Phishing Tool for Phishing Websites Detection". Proc. International Conference on Intelligent Networking and Collaborative Systems (INCoS). Barcelona, Spain: IEEE Press, 2009, pp. 105 - 112.

[11] Y. Zhang, J. I. Hong and L. F. Cranor, "Cantina: a content-based approach to detecting phishing web sites". Proc. 16th international conference on WWW. New York: ACM Press, 2007, pp. 639 – 648.

[12] G. Xiang, J. Hong, C. P. Rose, L. Cranor, "CANTINA+: A Feature-Rich Machine Learning Framework for Detecting Phishing Web Sites". ACM Transactions on Information and System Security (TISSEC), vol. 14 issue. 2, New York, ACM Press, 2011, Article No. 21.

[13] H. Bo, W. Wei, W. Liming, G. Guanggang, X. Yali, L. Xiaodong, M. Wei, "A Hybrid System to Find&Fight Phishing Attacks Actively". IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology. Lyon, IEEE Computer Society, 2011, pp. 506-509

[14] A. Alnajim and M. Munro, "An Evaluation of Users' Tips Effectiveness for Phishing Websites Detection". Proc. 3rd IEEE International Conference on Digital Information Management ICDIM, London, IEEE Press, 2008, pp. 63-68.

[15] Microsoft Corporation. (2007). Microsoft Security for Home Computer Users Newsletter. Available: http://www.microsoft.com/protect/secnews/default.mspx, last access on 16 March 2007.

[16] A. Alnajim and M. Munro, "An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection". Proc. 6th IEEE International Conference on Information Technology - New Generations (ITNG). Las Vegas, IEEE Computer Society, 2009, pp. 405-410.

[17] A. Alnajim, 2015. "A Country Based Model Towards Phishing Detection Enhancement". International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 5 issue. 1, 2015, pp. 52 – 57.

[18] A. Alnajim, "High Level Anti-Phishing Countermeasure: A Case Study". Proc. The The World Congress on Internet Security (WorldCIS-2011), London, UK, IEEE Press, 2011, pp. 139 – 144.

[19] Wing J. M., "A specifier's introduction to formal methods," Computer, vol. 23, issue. 9, 1990, pp. 8–23.

[20] A. Aziz, F. Balarin, S. T. Cheng, R. Hojati, T. Kam, S. C. Krishnan, R. K. Ranjan, T. R. Shiple, V. Singhal, S. Tasiran, H-Y. Wang, R. K. Brayton, A. L. Sangiovanni-Vincentelli, "HSIS: A BDD-based environment for formal verification". Proc The 31st Design Automation Conefernce. San Diego, USA: IEEE Press, 1994, pp. 454-459.

[21] M. L. Bolton, N. Jimenez, M. M. van Paassen, M. Trujillo "Automatically Generating Specification Properties From Task Models for the Formal Verification of Human–Automation

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Interaction". IEEE Transactions On Human-Machine Systems, vol. 44, issue. 5, New York, IEEE Press, 2014, pp. 561-575.

[22] M. S. Hegde, J. HK, S. Singh, "Modelling And Verification Of Extensible Authentication Protocol Using Spin Model Checker". International Journal of Network Security & Its Applications (IJNSA), vol.4, issue. 6, SCIRP, China, 2012, pp. 81-98.

[23] Mordechai Ben-Ari, Principles of the Spin Model Checker. New York, USA: Springer, 2008.

[24] E. A. Strunk, M. A. Aiello, J. C. Knight. "A Survey of Tools for Model Checking and Model-Based Development". 2006, Available Online: http://www.cs.virginia.edu/~eas9d/papers/CS-TR-2006-17.pdf, last accessed on 30 May 2015.

BIOGRAPHY

Dr. Abdullah M. Alnajim is an information security and academic consultant. He is also a faculty in the Information Technology Department, college of Computer at Qassim University, Saudi Arabia. Dr. Abdullah Alnajim had BSc in Computer Science from King Saud University in Saudi Arabia in 2002. Dr. Alnajim had MSc in Internet and Distributed Systems from Durham University in the United Kingdom in 2005. Dr. Alnajim had a Ph.D from the Department of Computer Science at Durham University in 2009. His Ph.D thesis was entitled as 'Fighting Internet Fraud: Anti-Phishing Effectiveness for Phishing Websites Detection'. Dr. Alnajim's research interests involve Internet security and frauds that encounter web applications especially online banking and e-commerce applications. He has published several scientific papers in international journals and conferences.