An Evaluation of A Country Based Anti-Phishing Approach Using Formal Methods

Abdullah M. Alnajim
Department of Information Technology, College of Computer
Qassim University, Buraydah, Saudi Arabia
najim@qu.edu.sa

Abstract— Phishing is a fraudulent attack that steals confidential information by mimicking a trustworthy entity in a medium of electronic communication. In this paper, research was conducted to evaluate a proposed country-based model to detect phishing attacks using formal methods. SPIN model checker was used to check the absence of deadlocks as well as reachable states. SPIN showed that the model has no error since it did not report "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 equaled to "zero". The aim behind using formal verification is to help checking whether the model is feasible and applicable. This helps deploying the approach model in the real world in order to enhance the country-based phishing countermeasures.

Keywords-Blacklists, Formal Methods, Model Checking, SPIN, e-Commerce Security, Network Proxy, Online Banking Security, Phishing, Saudi Arabia.

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 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 [3]. 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 [3].

There are technical advances that mitigate the problem of Phishing. For instance, security toolbars, such as SpoofStick, TrustBar and SpoofGuard, 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 [4]. In preventing online fraud, Symantec [5] believes that users' awareness is central to helping to change their behaviours 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 [6].

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, research will be conducted to evaluate a proposed country-based model to detect phishing attacks using formal methods. The aim behind that this research uses formal verification is to help checking whether the model is feasible and applicable in order to deploy it 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 [7].

The remainder of the paper is organized as follows. Section two reviews the literature regarding phishing detection methods and shows a country-based anti-phishing approach that was proposed to be deployed in Saudi Arabia. The third section presents the methodology the research follows to evaluate 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.

II. RELATED WORK

A. *Anti-Phishing countermeasures*

Phishing can be performed in different ways. They are as follows [8]:

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 [7]. 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 [9].

To increase the accuracy FP and FN rates, Xiang et. al. [10] 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. [10] 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 [11]. Bo et. al. [11] 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 [12].

Many commercial institutions, such as Microsoft, periodically send email security information to help their customers in protecting their online security [13]. This email provides practical security tips, useful resources and links, and a forum to ask security-related questions.

Microsoft states that the email is suitable for customers to stay up to date on the latest issues and events with:

- Security tips including anti-phishing tips.
- Security critical updates.
- Answers to frequently asked questions (FAQs) on security topics.
- Information about security trials and downloads.
- Tips from security team for home users.

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 [14] 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).

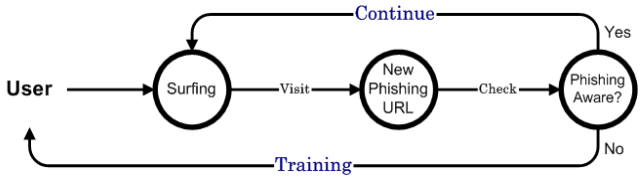

Figure 1. The broad idea of APTIPWD

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 [12]. 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 [14]. 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*".

B. High Level Phishing Detection in Saudi Arabia

Countries around the world follow high level procedures (a country-based) in order to mitigate phishing attacks. Alnajim [15] introduced and analyzed a high level anti-phishing countermeasure implemented in Saudi Arabia (see Figure 2). The Saudi Arabian countermeasure is obviously applied on the Internet traffic within Saudi Arabia. Therefore, it was very important to analyze the countermeasure model against all possible phishing attacks scenarios initiated by or designed to attack users inside and outside Saudi Arabia. The location of the source or the destination of phishing attacks is vital in the analysis of the model because the model works only in Saudi Arabia. Hence, based on the location, the scenarios used in the analysis came across all possible sources of phishing attacks as well as all possible destinations of phishing attacks. Based on the analysis methodology mentioned, Alnajim [15] examined the model and found that the model is effective when phishing websites are reached by users who surf the Internet inside Saudi Arabia whereas it is ineffective in protecting users from falling in phishing when the websites are reached by users who surf the Internet from outside Saudi Arabia.

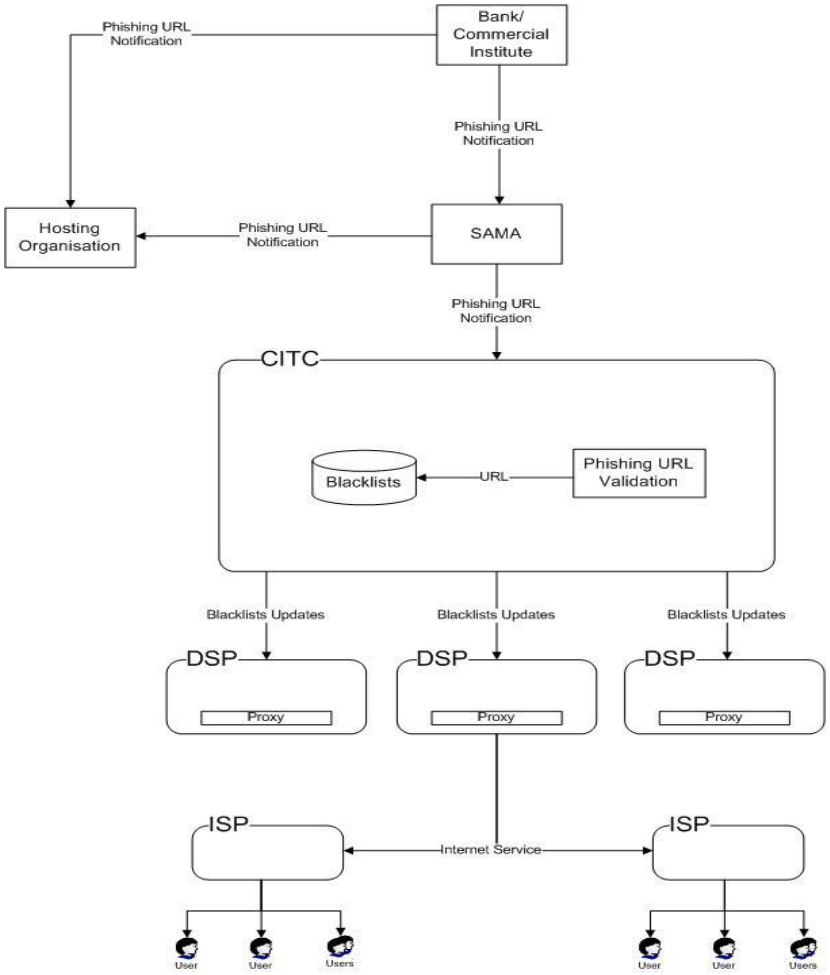

Figure 2. The Anti-Phishing Detection Framework in Saudi Arabia.

C. A Country Based Model Towards Phishing Detection Enhancement

Alnajim [16] then proposed a novel country based model to detect phishing attacks (see Figures 3 and 4). 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 [14] is applied on the current anti-phishing framework implemented in Saudi Arabia [15].

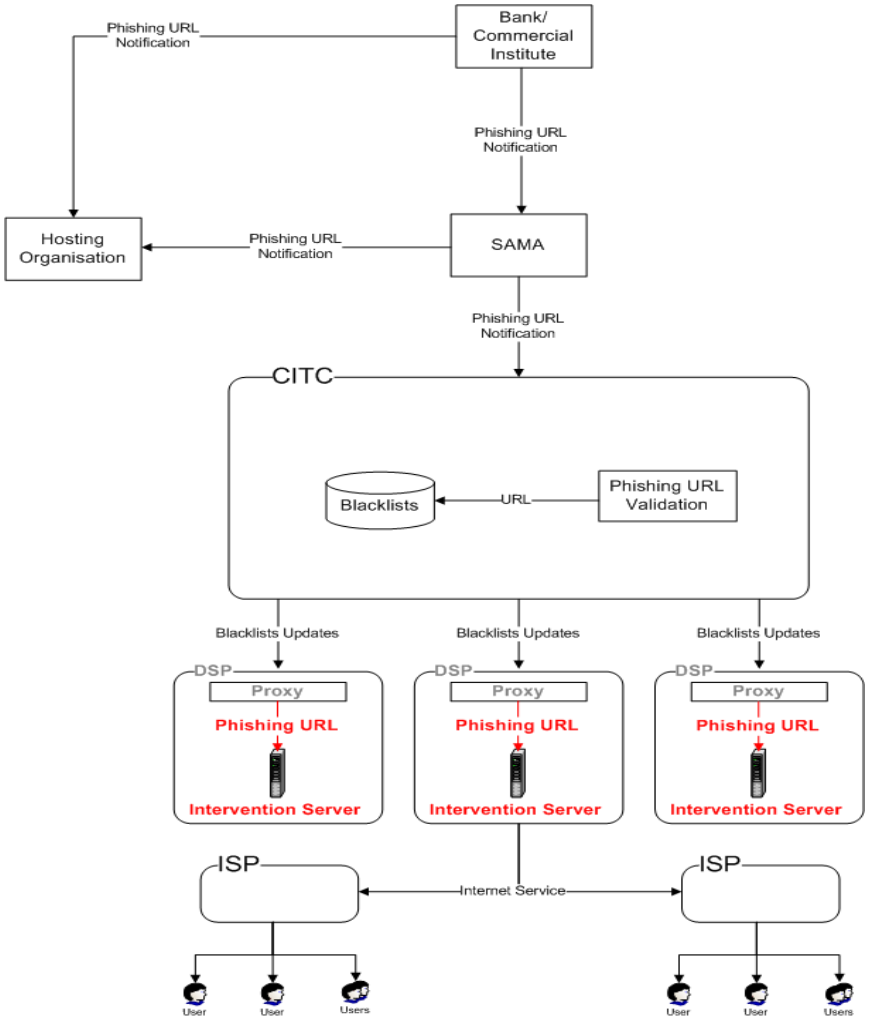

Figure 3. The proposed Intervention Server (in red color)

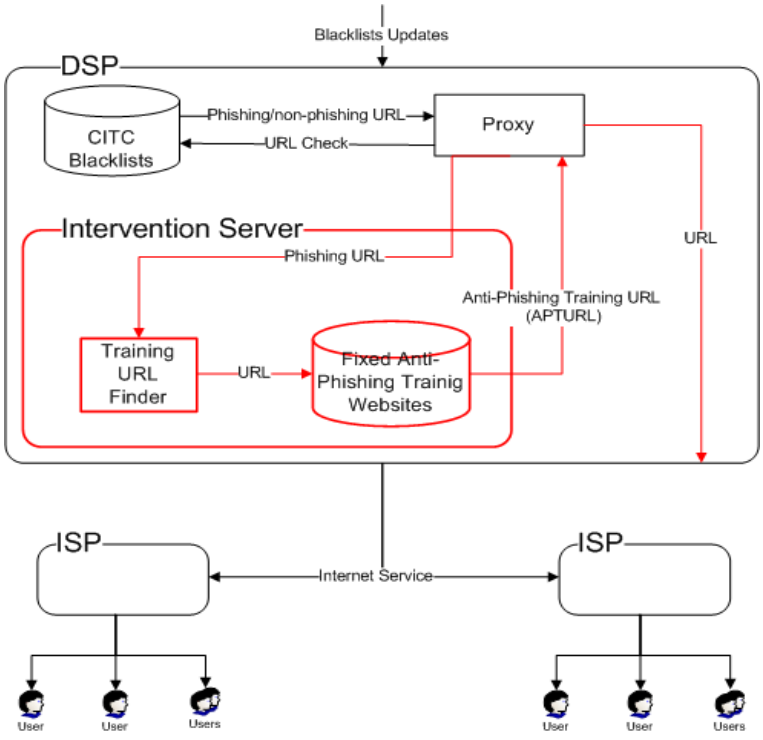

Figure 4. Components of the Proposed Intervention Server (in red color)

The black lists updates come from the Communications and Information Technology Commission (CITC) as an input to Data Service Providers (DSPs). Figure 3 shows that each DSP has got its own proxy. Therefore, if a user requests a URL, the DSP proxy directs the URL to CITC blacklists to check whether the URL is blacklisted or not (see Figure 4). The CITC blacklists replies the results. If the URL is non-phishing, then Proxy responds to it based on the DSP instructions. This case is not the research focus. However, if the URL is a phishing then the Proxy redirects the URL to the Intervention Server (IS). Once the IS receives a notification that a phishing URL is requested, an agent named 'Training URL Finder' (TURLF) connects to a database that include a Fixed Anti-Phishing Training Websites. The IS runs these websites locally.

TURLF is responsible for recognizing the suitable Anti-Phishing Training URL (APTURL) for the Phishing URL redirected from the Proxy. Thus, the TURLF is assumed that it returns to the Proxy the APTURL dedicated for the website that is being attacked by the phishing URL. Finally, the Proxy sends to the user the dedicated APTURL as a response to the user request initiated in the beginning.

Alnajim [16] 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.

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 [17]. 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 [18]. 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 [19].

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 [20]. The model checker "SPIN" (Simple PROMELA Interpreter) is a general tool for verifying the correctness of distributed software models in an automated fashion [21]. 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 [21].

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 [20]. SPIN checks the properties as the following [22]:

- 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.

Hedge [20] 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 evaluate the proposed country-based model to detect phishing attacks presented in Figures 3 and 4. This research uses formal verification to help checking whether the model is feasible and applicable in order to deploy it in the real world.

III. METHODOLOGY

This paper makes use of formal verification for the anti-phishing model shown in Figures 3 and 4 using SPIN model checker 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. In order to understand the processes, the specification and

description language (SDL) diagram will be built. It shows the procedures, data and behaviours of the model. This helps to build the state diagram of the model.

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 ArgoUML CASE tool. The UML state diagram of the model is expressed into a PROMELA code. This expression is achieved by using Hugo/RT which is a tool that can capture the properties of the model and transfer it as a PROMELA code.

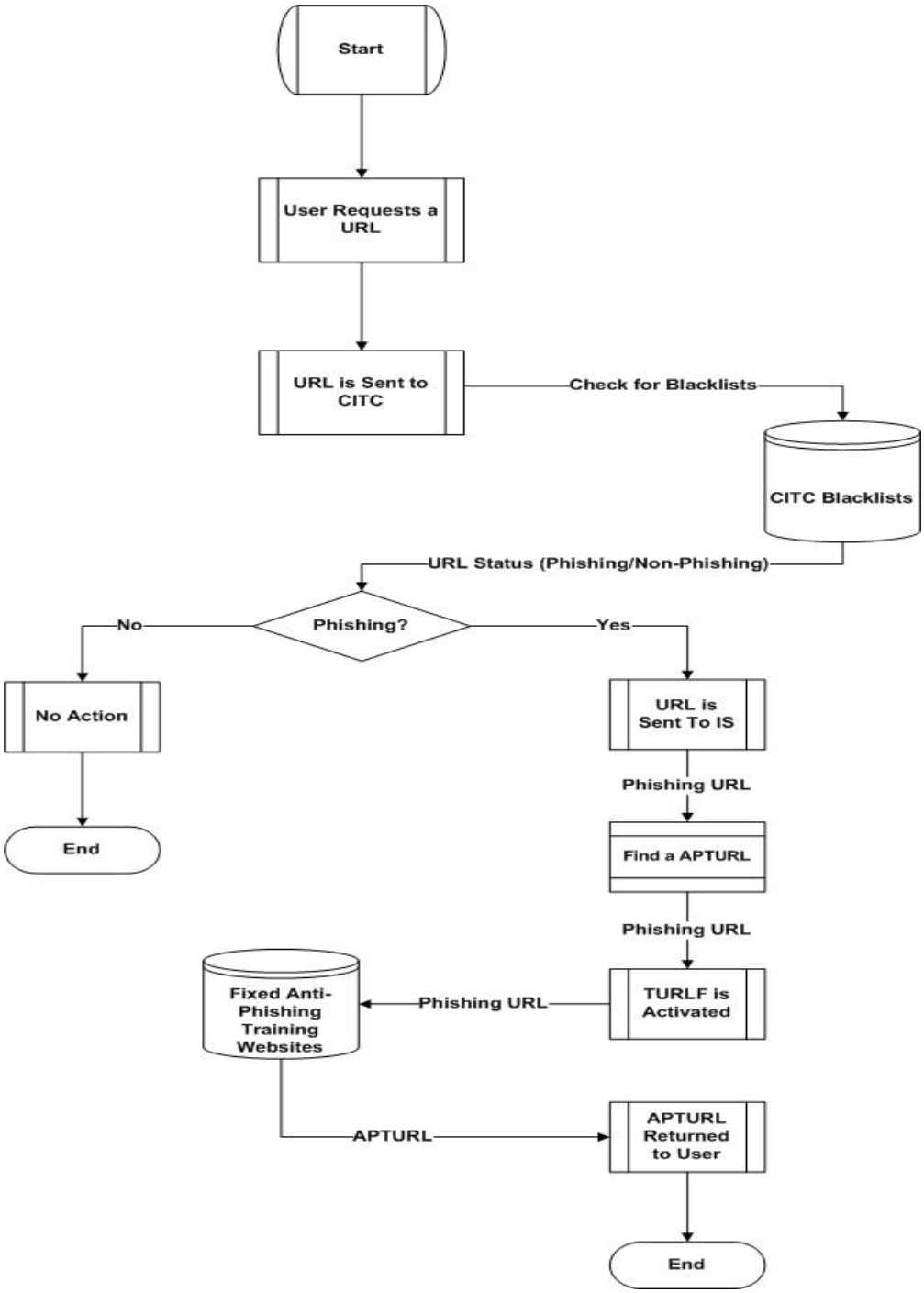

Figure 5. The Model's SDL Diagram

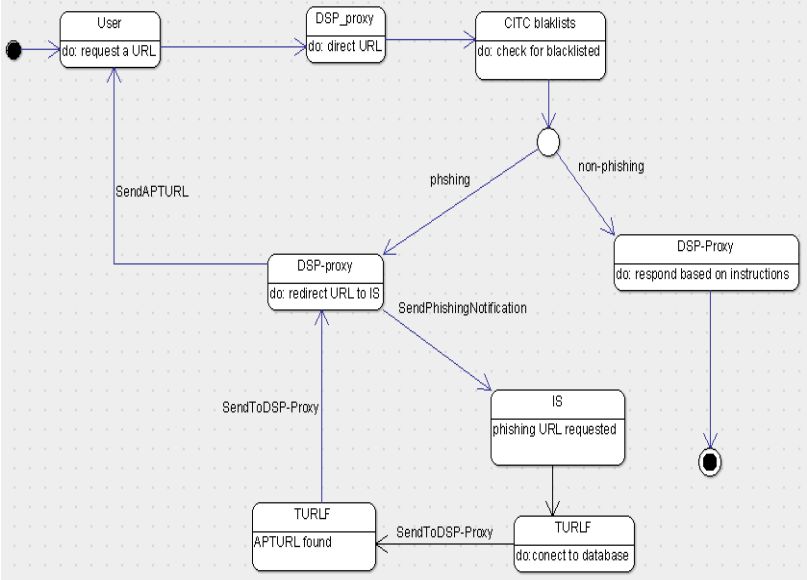

Figure 6. The Model's State Diagram

IV. RESULTS AND DISCUSSION

SPIN model checker is used to check for (1) absence of deadlocks as well as (2) reachable states. Figures 7,8 and 9 present screen shots of the SPIN model checker used. They show the PROMELA code written in the right hand side and the tests results in the right hand side.

Safety, Acceptance and Guided verifications were performed. As shown on Figures 7,8 and 9, 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.

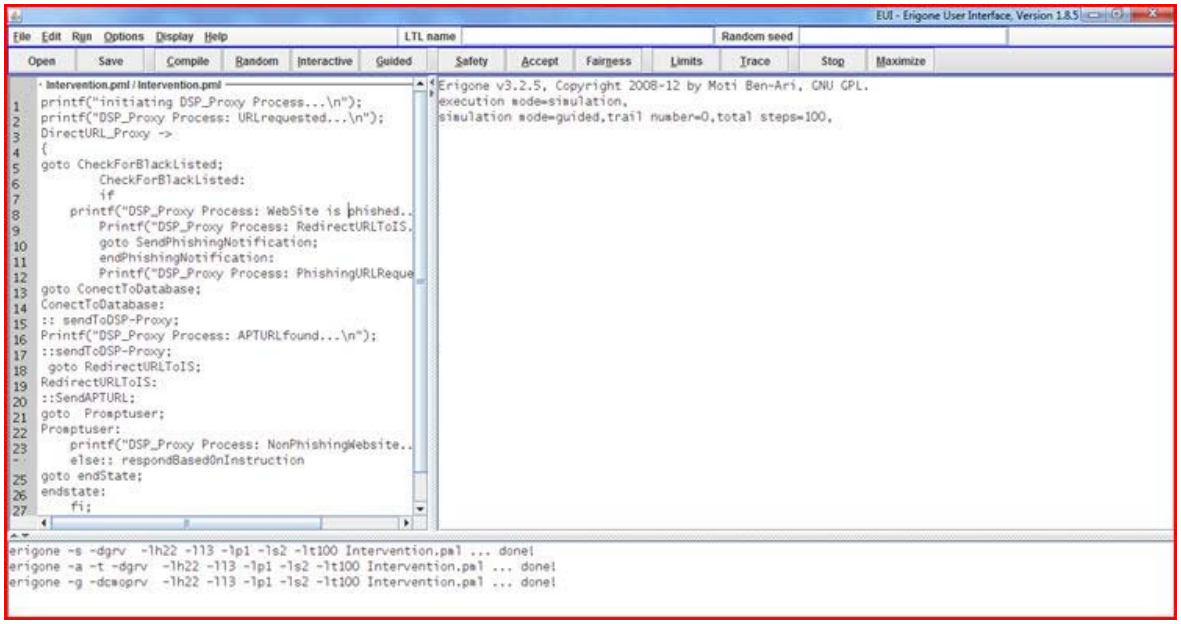

Figure 7. Guided Test's Results

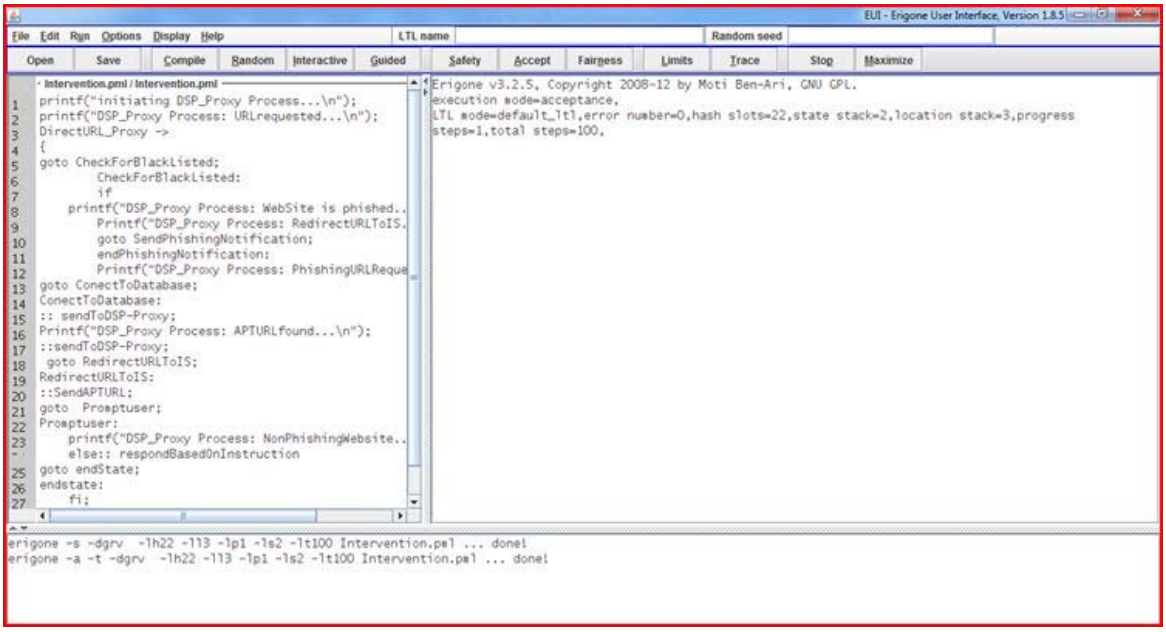

Figure 8. Acceptance Test's Results

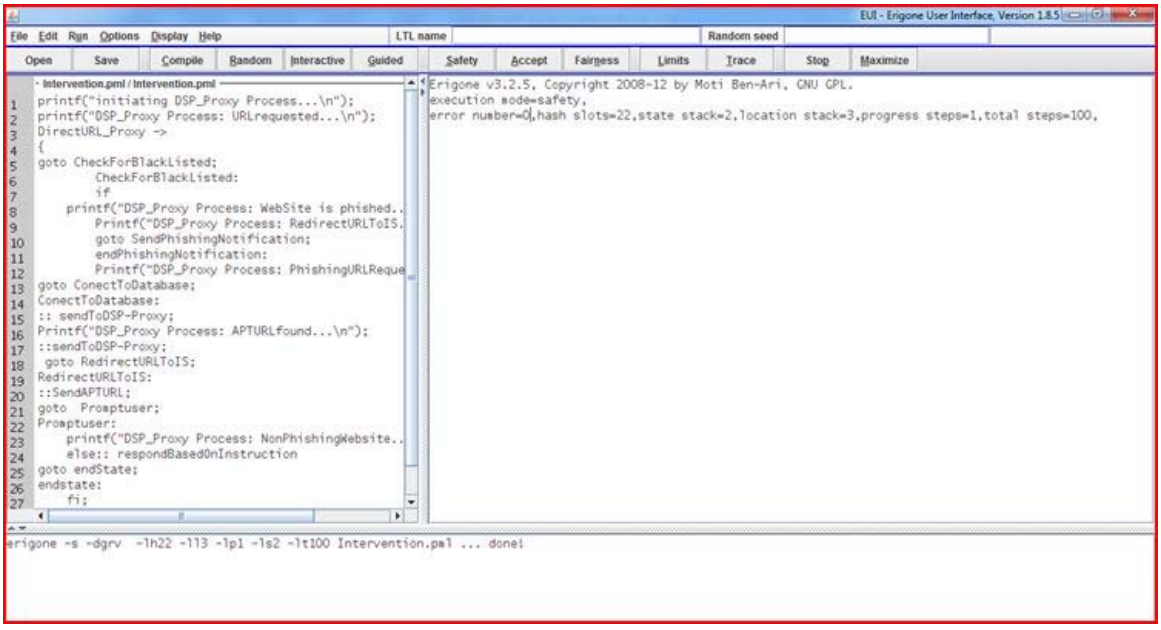

Figure 9. Safety Test's Results

Having verified the model using SPIN model checker, it is proved that the anti-phishing model proposed and shown in Figures 3 and 4 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 on Saudi Arabia Internet infrastructure.

V. CONCLUSION

In this paper, research was conducted to evaluate a proposed country-based model to detect phishing attacks using formal methods. 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 proposed country-based model was previously discussed [16] and shown in Figures 3 and 4. The model verification was based on model checking. 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 as a PROMELA code.

Using SPIN model checker, Safety, Acceptance and Guided verifications were performed. Having verified the model, SPIN did not report "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 equaled to “zero”. This means that the SPIN analyzer found no errors in the model.

In conclusion, it is proved that the anti-phishing model proposed and shown in Figures 3 and 4 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 on Saudi Arabia Internet infrastructure.

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] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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
[12] 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.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] Wing J. M., “A specifier’s introduction to formal methods,” Computer, vol. 23, issue. 9, 1990, pp. 8–23.
[18] 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.
[19] 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 Interaction”. IEEE Transactions On Human-Machine Systems, vol. 44, issue. 5, New York, IEEE Press, 2014, pp. 561-575.
[20] 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.
[21] Mordechai Ben-Ari, Principles of the Spin Model Checker. New York, USA: Springer, 2008.
[22] 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.

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.