Volume 9 ▪ Issue 2 ▪ July 2015

INTERNATIONAL JOURNAL OF SECURITY (IJS)

ISSN : 1985-2320

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF SECURITY (IJS)

VOLUME 9, ISSUE 2, 2015

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-2320

International Journal of Security (IJS) is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJS Journal is a part of CSC Publishers

Computer Science Journals

http://www.cscjournals.org

INTERNATIONAL JOURNAL OF SECURITY (IJS)

Book: Volume 9, Issue 2, July 2015
Publishing Date: 31-07-2015
ISSN (Online): 1985-2320

IJS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2015

EDITORIAL PREFACE

This is the *Second* Issue of Volume *Nine* of The International Journal of Security (IJS). The Journal is published bi-monthly, with papers being peer reviewed to high international standards. The International Journal of Security is not limited to a specific aspect of Security Science but it is devoted to the publication of high quality papers on all division of computer security in general. IJS intends to disseminate knowledge in the various disciplines of the computer security field from theoretical, practical and analytical research to physical implications and theoretical or quantitative discussion intended for academic and industrial progress. In order to position IJS as one of the good journal on Security Science, a group of highly valuable scholars are serving on the editorial board. The International Editorial Board ensures that significant developments in computer security from around the world are reflected in the Journal. Some important topics covers by journal are Access control and audit, Anonymity and pseudonym, Computer forensics, Denial of service, Network forensics etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Started with Volume 9, 2015, IJS appear with more focused issues. Besides normal publications, IJS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

The coverage of the journal includes all new theoretical and experimental findings in the fields of computer security which enhance the knowledge of scientist, industrials, researchers and all those persons who are coupled with computer security field. IJS objective is to publish articles that are not only technically proficient but also contains information and ideas of fresh interest for International readership. IJS aims to handle submissions courteously and promptly. IJS objectives are to promote and extend the use of all methods in the principal disciplines of computer security.

IJS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Security (IJS)

EDITORIAL BOARD

TABLE OF CONTENTS

Volume 9, Issue 2, July 2015

Pages

An Indistinguishability Model for Evaluating Diverse Classes of Phishing Attacks and Quantifying Attack Efficacy

Narasimha Shashidhar *karpoor@shsu.edu*
Department of Computer Science
Sam Houston State University
Huntsville, TX 77384, USA

Lei Chen *lchen@georgiasouthern.edu*
Department of Information Technology
Georgia Southern University
Statesboro, GA 30458, USA

Abstract

Phishing is a growing threat to Internet users and causes billions of dollars in damage every year. While there are a number of research articles that study the tactics, techniques and procedures employed by phishers in the literature, in this paper, we present a theoretical yet practical model to study this menacing threat in a formal manner. While it is common folklore knowledge that a successful phishing attack entails creating messages that are indistinguishable from the natural, expected messages by the intended victim, this concept has not been formalized. Our model attempts to capture a phishing attack in terms of this indistinguishability between the natural and phishing message probability distributions. We view the actions performed by a phisher as an attempt to create messages that are indistinguishable to the victim from that of "*normal*" messages. To the best of our knowledge, this is the first study that places phishing on a concrete theoretical framework and offers a new perspective to analyze this threat. We propose metrics to analyze the success probability of a phishing attack taking into account the input used by a phisher and the work involved in creating deceptive email messages. Finally, we study and apply our model to a new class of phishing attacks called collaborative spear phishing that is gaining momentum. Recent examples include *Operation Woolen-Goldfish* in 2015, *Rocket Kitten* in 2014 and *Epsilon email breach* in 2011. We point out fundamental flaws in the current email-based marketing business model which enables such targeted spear phishing collaborative attacks. In this sense, our study is very timely and presents new and emerging trends in phishing.

Keywords: Phishing, Email Fraud, Data Hiding, Identity Linking, Social Engineering.

1. INTRODUCTION

Phishing is a sophisticated and rapidly growing social engineering threat aimed at gleaning sensitive information such as user names, passwords and financial information from unsuspecting victims. In this context, victims comprise not only of people, but also corporations and even nation states and leads to billions of dollars in damage each year [1]. The attack campaigns typically involve sending an innocuous looking message to victims in an attempt to deliver malware, glean personally identifiable information or to further a shift in power control, either political or economic [20]. Attacks are typically carried out via standard communication channels such as email or instant messaging by masquerading as legitimate and trustworthy entities. Being a social engineering attack, most studies of this threat have focused on understanding the techniques used by phishers, devising clever strategies to thwart these attacks and the human factors associated with phishing. As of 2015, phishing has become a major vector for cyberattacks employed by several threat groups [14]. As an example, *Rocket Kitten* is a cyber-threat group that actively undermines European and Israeli companies via phishing. In a recent white-paper published by Trend Micro in March 2015 [14], the authors dissect the modus-

operandi of these phishers and conclude that the methods used by these groups are extremely sophisticated in comparison to those in the past. Furthermore, these cyber-attacks are conjectured to be state-sponsored and the academic and industry groups are still exploring the inner workings of these schemes. To address the sophistication and the devious nature of these latest phishing attacks, in this paper, we deviate from the older empirical approach and propose a theoretical yet practical model that captures the interstitial dynamics of this threat. A novel feature of our security model is that it captures the inherent *human* factor and consequently complements the existing empirical study of phishing.

Contributions: Our first contribution in this paper is the development of a theoretical framework for phishing. Our model is also very practical and designed to study a large class of phishing attacks including the non-traditional, but emerging threats such as the Android Market fake banking apps [19]. It is well known that a successful phishing attack entails creating messages that are indistinguishable from the natural, expected messages by the intended victim. Firstly, we formalize this notion in the broadest sense possible to encompass a wide range of attacks. This is important because the rate of growth of phishing attack sophistication does not lend itself to traditional empirical analysis or study. Our model captures the dynamics of phishing in terms of indistinguishability between the natural and phishing message distributions. From the perspective of a phisher, one can view the creation of a phishing message as an attempt to embed a deceptive message within an innocent looking email or instant message. To this end, we treat the problem to be "spiritually" similar to the problem of Steganography. Our motivation stems from the observation that while the goal in Steganography is to create an innocent looking message with a hidden payload without arousing the suspicion of any eavesdropper, a phisher tries to create an "innocent" looking message with a hidden (malicious) payload (such as the GHOLE Malware used by the cyber-threat group Rocket Kitten [14]) without arousing suspicion even from the recipient. We note that our work brings out an elegant, hidden connection between the disparate fields of Steganography and Phishing and we hope that this connection will lead to new and diverse perspectives on phishing detection research.

Secondly, we propose metrics to measure the success probability of a phishing detection algorithm and consequently the success probability of a phishing attempt. We also define the notion of overhead as the ratio of the amount of work done by a phisher to the payoff that s/he receives upon concluding the phishing campaign. This notion of overhead will be useful when we analyze the impact of the Epsilon email breach [16] and the associated payoff for the phishers.

Finally, we describe a new class of phishing attacks, called collaborative spear phishing, an advanced class of spear phishing attacks that may stem from the latest threat posed by the Epsilon email breach [16], Rocket Kitten [14], and Operation Woolen-Goldfish [14] in the recent past. A server breach at the Internet marketing company Epsilon, a unit of Alliance Data Systems Corporation, exposed the names and email addresses of millions of people [22] across different organizations. This breach is being described as the worst of its kind by the media [15], particularly since the breach apparently lasted for months despite warnings of targeted attacks against email service providers. Rocket Kitten is a cyber-threat group (presumed to be state sponsored), that launches targeted spear phishing attacks (Operation Woolen-Goldfish) against Israeli and European companies. Their primary approach is to deliver a malware payload, typically the GHOLE virus onto unsuspecting corporate employees' machines, the latest event occurring in February 2015 [14]. Once the payload has been delivered, and the victim's machines successfully compromised, additional payloads including keyloggers are injected into the infected machine. In this paper, we also point out some of the fundamental flaws in the current email-based marketing business model, which is a by-product of service industrialization. This is an important discussion due to the spate of cyber-attacks and breaches against major businesses such as Home Depot, Target etc. currently. Thus, our study is very timely and presents emerging trends in phishing using new tools and analysis techniques to detect and instrument these events.

2. PRIOR WORK

Phishing is primarily a social engineering attack and has attracted a lot of research interest in this context. Most studies of phishing have focused on understanding the techniques used by phishers, devising clever strategies to thwart these attacks and the human factors associated with this threat.

Dhamija et al. [4] and Downs et al. [6] studied the factors affecting the success of different malicious strategies used by phishers in an effort to build systems better capable of thwarting phishing attempts. The impact of social networking websites on phishing was studied by Jagatic et al. [10] who found that Internet users may be over four times as likely to become victims if they are solicited by someone appearing to be a known acquaintance. A personality-bias based analysis on the susceptibility of individuals to fall prey to phishing attacks was conducted by Ding et al. [5] and demonstrated that a dictionary based semantic similarity approach to analyzing personality models showed promising results. Some of the strategies devised to thwart phishing attacks mentioned in the literature include: Dynamic Security Skins [3] that allows a remote web server to prove its identity in a way that is easy for a human user to verify and hard for an attacker to spoof; Visual Cryptography and Iris Detection based techniques [17, 12]; Natural language techniques [21]; Detecting phishing emails and websites using machine learning techniques [8]; Web Wallet [24], a browser sidebar which users can use to submit their sensitive information online; password management and website-login innovations [25] and Cantina, a novel, content-based approach to detecting phishing web sites, based on information retrieval and text mining algorithms [27]. Another line of research [26, 23] focuses on the evaluation of anti-phishing tools and their effectiveness.

A graph-theoretic model to analyze the effort expended by a phisher to launch an attack was studied by Jakobsson [11]. A phishing attack was modeled using a graph in which nodes correspond to knowledge and edges captured traversal from one node to another. Edges were associated with costs to reflect the effort of the phisher. This paper also defined a new attack approach called the context aware phishing attack using a method called identity linking - determining the correspondence between identities and email addresses of a victim.

Our model is designed to capture the dynamics of every facet of the phishing threat and not isolated to measuring the effort expended by the phisher. Furthermore, we describe attacks such as collaborative spear phishing that are far more complex than the context aware attack and thus subsumes the earlier attack put forth by Jakobsson [11].

2.1 Notations and Definitions

For a probability distribution *P* with support *X*, we use the notation *P[x]* to denote the probability that P assigns to $x \in X$. A random variable *X* is a function over a sample space Ω, $\mathrm{X} : \Omega \to \mathrm{S}$, for some set *S* and we say that the random variable *X* takes values in the set *S*. The probability distribution on *S* described by the random variable *X* is denoted by P_X.

2.2 Statistical Distance

We use statistical distance as the measure of distance between two random variables and the probability distributions described by these random variables. The statistical distance is the largest possible difference between the probabilities that two probability distributions can assign to the same event. There are several other metrics one could use to measure the distance between two distributions. However, statistical distance is the most widely used and well defined metric as described in the literature. We would like to note that our model does not preclude use of other metrics in this context. Shoup [18] presents a detailed treatment of statistical distance and its properties.

Definition: Let *X* and *Y* be random variables which both take values in a finite set *S* with probability distributions P_X and P_Y. The statistical distance between *X* and *Y* is defined as

$$\Delta[\mathrm{X},\mathrm{Y}] = \frac{1}{2}\sum_{s\in S}\left|P_{X(s)} - P_{Y(s)}\right|.$$

So, two random variables (and the corresponding probability distributions) *X* and *Y* are said to be ϵ-close to each-other if $\Delta|X,Y| < \epsilon$. This notion of ϵ-closeness will be useful to us when we talk about the two distributions – natural messages and phishing messages – being close to each other, thereby capturing the notion of indistinguishability.

3. THE PHISHING MODEL

In this section, we describe our phishing model as depicted by Figure 1. As noted earlier, we build our phishing indistinguishability model on the Steganography security model. In particular, we use the seminal steganography model presented by Cachin [2]. We use the notion of a communication channel to capture email, instant and other means of communication. For the purpose of our discussion here, let us use the example of email communication. Let us consider an individual's email inbox. The phishing problem specifies two message distributions corresponding to the two sources of messages that can find their way to that individual's email inbox: The Natural (*N*) and the Phishing (*P*) message distributions. The two source distributions are shown on the left as two black boxes. Typically, we are unaware of the exact probability distributions associated with these input sources and will treat them as such in our description. The individual's inbox normally receives messages from the Natural distribution (switch is set to *0*) corresponding to the phisher being inactive. The natural distribution is meant to capture the distribution of messages that a person expects to see. When the phisher is active (switch is set to *1*) s/he receives phishing messages. The algorithm used by the phisher operates on some input stream to create the deceptive messages. The Distinguisher algorithm *D* is tasked with being able to distinguish between the messages from these two distributions and essentially protect the user from being phished. Often, the receiver of the email plays the role of the distinguisher *D* although Figure 1 depicts the distinguisher algorithm *D* to be distinct from the receiver. In real life, the receiver along with the software tools, browser toolbar extensions, and spam/phisher filters collectively form the Distinguisher algorithm *D*. The bidirectional arrow between the Distinguisher algorithm *D* and the receiver is meant to signify this relationship between these entities. The arrow out of the receiver pointing to output/action symbolizes the act of clicking on a link or acting upon the instructions in the received message, whether natural or phishing.

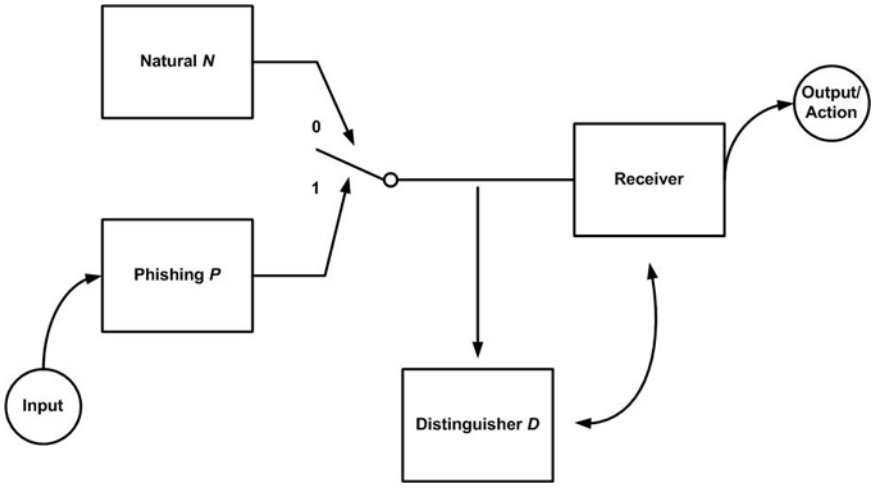

FIGURE 1: The Phishing Model.

3.1 Evaluating the Success of a Phishing Attempt

The success of a phishing attempt is measured by the intended victim's ability to distinguish between "natural" and "phishing" messages over the communication channel. To characterize

natural communication we need to define and formalize the communication channel. We follow the standard terminology used in the literature to define communication channels [9]. We let $E = e_1, e_2, \ldots, e_s$ denote an alphabet and treat the communication channel as a family of random variables $I = \{I_h\}_{h \in E^*}$. These channel distributions model a *history-dependent* notion of channel data that captures the notion of real-life communication. As an example, if *E* were to represent the set of the "email alphabet" and $h \in E^*$, the history of emails received by a person thus far, then I_h represents the random variable that captures the probability distribution of the person's email inbox at that point in time. In our model, we have captured the history dependence of communication and an individual's expectance to "see" a message in his inbox.

In evaluating the success of a phishing attempt, we need to take into consideration the amount of randomness present in a person's email inbox. We use *min-entropy* as the measure of this randomness. The min-entropy of a random variable *X*, taking values in a set *V*, is the quantity

$$H_\infty(X) \triangleq min_{\mathrm{v} \in \mathrm{V}} (-\log \Pr[X = v]).$$

We say that a communication channel (such as an email inbox) has min-entropy δ if for all $h \in E^*$, $H_\infty(I_h) > \delta$. We would like an individual's inbox, for all histories, to have some non-zero randomness, i.e, $\delta > 0$. This randomness parameter is designed to capture the diversity of the messages present in a person's inbox. As an example, if someone were to receive only *one* particular kind of email, then there is no randomness present in this communication scheme. The study of phishing on such a communication channel is not as interesting since the success probability of a phishing attempt in this situation is very small. Observe that the metric min-entropy is designed to capture the worst-case entropy inherent in a distribution. Naturally, other measures of entropy can also be applied to our model as well.

Let us now discuss the success probability of the Distinguisher algorithm *D* in being able to detect a phishing message. Let us overload the notation and let *P* denote the phishing algorithm as well as the distribution of the phishing messages produced by it. We now define the *advantage* of the Distinguisher *D* over the phishing algorithm *P* as:

$$Adv_D^P(m) = \left| \Pr[D(m) = success] - \frac{1}{2} \right|, \qquad (1)$$

where *m* is the message to be distinguished and *D(m) = success* is the event that the Distinguisher *D* was successful in identifying a phishing message. Observe that any Distinguisher algorithm has an advantage of ½ in being able to detect a phishing message by merely flipping a fair coin. Hence, we need to look at the absolute value of the difference between the success probability of *D* from ½.

An alternative definition for the *advantage* of the Distinguisher *D* over the phishing algorithm *P* is obtained from the observation that the *total variation distance* between two probability measures *N* and *P* is the largest possible difference between the probabilities that these two probability distributions can assign to the same event, in particular to the event *D(m) = success*.

$$Adv_D^P(m) = \frac{1}{2} \sum_{m \in M} |N(m) - P(m)|, \qquad (2)$$

where *N* and *P* are the natural and the phishing message distributions respectively and represents the messages in the message set *M* (the user's inbox). Our model captures phishing in terms of this indistinguishability between the natural and phishing message distributions.

We can now define the capacity *C* of an individual to shield him/her from a phishing attack as:

$$C = \max_D \{Adv_D^P(m)\}, \qquad (3)$$

this maximum taken over all Distinguisher algorithms *D* available at the individual's disposal. This definition is meant to capture the different software tools such as browser toolbars, add-ons and other installed tools using any techniques that one might use to defend against phishing.

We now derive the measure for evaluating the success probability S_P of a phishing attempt *P* as:

$$S_p = 1 - C. \qquad (4)$$

We say that a user is $(\epsilon, \delta) - secure$ from a phishing attack if for all his email-inboxes with min-entropy δ, we have $S_P < \epsilon$. The *overhead* of a phisher is judged by the relation between the amount of *work* done by a phisher and the corresponding *payoff*. We adopt the ratio $o = w/p$ as a measure for overhead. Obviously, if the payoff is high and the work done is low, then the overhead is low. This measure is useful in comparing the damage caused by different phishing attacks.

In this paragraph, we discuss the different parameters that contribute towards the *work* done by a phisher. Drake et al., present an anatomy of a phishing email where they enumerate the different tricks used by phishers in an attempt to create deceptive messages that are indistinguishable from the original messages [7]. The most important (and expensive to acquire) of these parameters are the personally identifiable information (*PII*) such as name, email address, the final four digits of an account number, year of expiration etc. The other costs associated with work are technical in nature, i.e., creating similar sounding domain names such as tax-revenue.com, ebaybuyerprotection.com, creating emails that appear to come from legitimate "From:" email address, designing the structure and content of the email, creating a plausible premise, using JavaScript event handlers, redirection, etc. We define work to comprise essentially of two main parts – work done in collecting personally identifiable information, *PII* and the technical work, i.e, $w = w_{PII} + w_t$.

4. COLLABORATIVE SPEAR PHISHING

In this section, we discuss an emerging, new class of phishing attacks, that we call collaborative spear phishing. We wish to shed light on this new class of phishing attacks that may become popular as a result of the latest server breach at the email marketing giant Epsilon [16] and other breaches on major U.S. retailers. This attack is an advanced class of spear phishing that a phisher may develop using collaborative filtering techniques described below. In April 2011, a server breach at the Internet marketing company Epsilon, a unit of Alliance Data Systems Corporation, exposed the names and email addresses of millions of people [16]. While a complete list of all the companies affected by the breach is not yet known, roughly 50 companies are said to be on that list, including Best Buy, Citibank, Disney, JPMorgan Chase, The Home Shopping Network, Hilton, Marriott and the College Board. This breach is being described as the worst of its kind by the media [15]. Such attacks have already started becoming prevalent as was observed recently in the attack campaigns launched by Rocket Kitten in 2014 and 2015 [14].

Collaborative filtering is the process of filtering for information or patterns using techniques involving collaboration among multiple data sources. Commonly used to infer purchase statistics by implementing recommendation algorithms for item recommendation by Amazon and other online retailers, this technique can now be used to launch highly advanced phishing attacks. While any breach that leaks personally identifiable information is a blessing to phishers, this particular breach at Epsilon is much more so. In the context of this breach, a phisher might now try to infer potential accounts that an individual may have with organizations using information that he already possesses. Furthermore, it gives a plausible premise that a phisher may use to hide his tracks. Observe that the breach at Epsilon leaked much more information than just personally identifiable information – It leaked the relationships that an individual has with different organizations. The phisher is able to observe that a particular account is affiliated with a number of organizations and hence is able to filter for more information than s/he could otherwise.

As a quick example, we use a very simple Item-to-Item recommendation algorithm to illustrate this attack. The table below captures Alice, Bob and Emily's relationship with three organizations. A *Yes* in the table below corresponds to the affirmative knowledge that a phisher has obtained (Using the Epsilon database, Retailer breaches or otherwise) about an individual's relationship with that organization and *No* (no knowledge) corresponds to the lack of this knowledge.

Name	Best Buy	Citibank	JPMorgan Chase
Alice	Yes	No	Yes
Bob	No	Yes	Yes
Emily	No	Yes	No

TABLE 1: Collaborative Phishing.

The cosine between Best Buy and Citibank is obtained by:

$$\frac{(1,0,0)\cdot(0,1,1)}{\|(1,0,0)\|\|(0,1,1)\|}=0\ .$$

The cosine between Best Buy and JPMorgan Chase is obtained by:

$$\frac{(1,0,0)\cdot(1,1,0)}{\|(1,0,0)\|\|(1,1,0)\|}=\frac{1}{\sqrt[2]{2}}.$$

The cosine between Citibank and JPMorgan Chase is obtained by:

$$\frac{(0,1,1)\cdot(1,1,0)}{\|(0,1,1)\|\|(1,1,0)\|}=\frac{1}{2}\ .$$

Hence, a phisher armed with the knowledge that a particular individual who has an account with Best Buy can make an educated guess that h/she may possibly have an account with JPMorgan Chase as well. This makes good sense because many Best Buy Credit accounts are indeed handled by JPMorgan Chase. While we have used a very elementary algorithm for the sake of exposition, a motivated phisher could use an elaborate collaborative filtering algorithm such as Slope One [13] to improve the success of this attack. While the context-aware attack proposed by Jakobsson [11] uses the concept of identity-linking to launch phishing attacks, our proposed attack is not only context-aware but also is capable of extrapolating for information that the phishers don't yet have.

In this paragraph, we point out some of the fundamental flaws in the current email-based marketing business model, which we believe is a by-product of service industrialization - treating services as an industrial process. By placing the personally identifiable information of millions of customers under the control of one organization, such as Epsilon, the *overhead* for the phisher is dramatically reduced – The work is diminished and the payoff is maximized. Furthermore, the phishers can now send targeted emails to their victims thereby making sure that these emails are out of the hands of the phishing research community. They can also ensure guaranteed delivery of their phishing emails by spoofing the correct "From" email addresses that most people have saved in their address books. Gary Warner [22] has an elaborate discussion of such targeted phishing attacks and we have already started seeing such sophisticated attacks [14].

5. CONCLUSION

Our primary goal in this paper was to present a treatment of phishing in a formal theoretical framework. Our model captures the dynamics of phishing in terms of indistinguishability between the natural and phishing message distributions. We propose metrics to analyze the success probability of a phishing attack which takes into account the input parameters used by a phisher and the associated work involved to create deceptive email messages. Finally, we present a new class of phishing attacks, called collaborative spear phishing which is an advanced class of spear phishing that may stem from the latest threat posed by the Epsilon email breach and other retailer breaches in the recent past. We also point out some of the fundamental flaws in the current email-based marketing business model, which is a by-product of service industrialization. In this sense, our study is very timely and presents new and emerging trends in phishing. We hope that our model will help shed some more light on the threats posed by phishing.

6. REFERENCES

[1] Anti-Phishing Working Group. "Phishing activity trends report". In *APWG Global Response to Cybercrime*, http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf, March 2014. Retrieved 2 April, 2015.

[2] Christian Cachin. "An information-theoretic model for steganography". In Information Hiding, pages 306–318. Springer, 1998.

[3] Rachna Dhamija and J Doug Tygar. "The battle against phishing: Dynamic security skins". In Proceedings of the 2005 symposium on Usable privacy and security, pages 77–88. ACM, 2005.

[4] Rachna Dhamija, J Doug Tygar, and Marti Hearst. "Why phishing works". In Proceedings of the SIGCHI conference on Human Factors in computing systems, pages 581–590. ACM, 2006.

[5] Ke Ding, Nicholas Pantic, You Lu, Sukanya Manna, Mohammad Husain, et al. "Towards building a word similarity dictionary for personality bias classification of phishing email contents". In Semantic Computing (ICSC), IEEE International Conference on, pages 252–259. IEEE, 2015.

[6] Julie S Downs, Mandy B Holbrook, and Lorrie Faith Cranor. "Decision strategies and susceptibility to phishing". In Proceedings of the second symposium on Usable privacy and security, pages 79–90. ACM, 2006.

[7] Christine E Drake, Jonathan J Oliver, and Eugene J Koontz. "Anatomy of a phishing email". In CEAS, 2004.

[8] Ian Fette, Norman Sadeh, and Anthony Tomasic. "Learning to detect phishing emails". In Proceedings of the 16th international conference on World Wide Web, pg 649–656. ACM, 2007.

[9] Nicholas Hopper, Luis von Ahn, and John Langford. "Provably secure steganography". IEEE Transactions on Computers, (5):662–676, 2008.

[10]Tom N Jagatic, Nathaniel A Johnson, Markus Jakobsson, and Filippo Menczer. "Social phishing". Communications of the ACM, 50(10):94–100, 2007.

[11] Markus Jakobsson. "Modeling and preventing phishing attacks". In Financial Cryptography, volume 5. Citeseer, 2005.

[12] Anjali Jose and S Vinoth Lakshmi. "Web security using visual cryptography against phishing". Middle-East Journal of Scientific Research, 20(12):2626–2632, 2014.

[13] Daniel Lemire and Anna Maclachlan. “Slope one predictors for online rating-based collaborative filtering”. In SDM, volume 5, pages 1–5. SIAM, 2005.

[14] Trend Micro. “Rocket kitten showing its claws: Operation woolen-goldfish and the ghole campaign”. In Trend Micro Security Intelligence Reports, Retrieved 8 April, 2015. http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing, March 2015.

[15] ABC News News/Technology. “Epsilon email breach: What you should know”. In Epsilon email breach, Retrieved 12 Mar, 2014. http://abcnews.go.com/Technology/epsilon-email-breach/story?id=13291589, 2011.

[16] Mathew J. Schwartz. “Epsilon fell to spear-phishing attack”. In Information Week, Retrieved 15 Mar, 2014. http://www.darkreading.com/attacks-and-breaches/epsilon-fell-to-spear-phishing-attack/d/d-id/1097119?, 2011.

[17] Saranya Shaji et al. “Anti phishing approach using visual cryptography and iris recognition”. IJRCCT, 3(3):088–092, 2014.

[18] Victor Shoup. A computational introduction to number theory and algebra. Cambridge University Press, 2009.

[19] SlashDot. “Malicious app in android market”. In The epsilon phishing model, Retrieved Mar 12,2014. http://mobile.slashdot.org/-story/10/01/10/2036222/Malicious-App-In-Android-Market.

[20] RSA Fraud Report Team. “Phishing kits - the same wolf, just a different sheep’s clothing”. In RSA Monthly Online Fraud Report, EMC, pages Retrieved 8 April, 2015. http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012013.pdf, February 2013.

[21] Rakesh Verma, Narasimha Shashidhar, and Nabil Hossain. “Detecting phishing emails the natural language way”. In Computer Security–ESORICS 2012, pages 824–841. Springer, 2012.

[22] Gary Warner. “Cybercrime and doing time. In The epsilon phishing model”, Retrieved 12 Mar, 2014. http://garwarner.blogspot.com/2011/04/epsilon-phishing-model.html, 2011.

[23] Min Wu, Robert C Miller, and Simson L Garfinkel. “Do security toolbars actually prevent phishing attacks?” In Proceedings of the SIGCHI conference on Human Factors in computing systems, pages 601–610. ACM, 2006.

[24] Min Wu, Robert C Miller, and Greg Little. “Web wallet: preventing phishing attacks by revealing user intentions”. In Proceedings of the second symposium on Usable privacy and security, pages 102–113. ACM, 2006.

[25] Ka-Ping Yee and Kragen Sitaker. “Passpet: convenient password management and phishing protection”. In Proceedings of the second symposium on Usable privacy and security, pages 32–43. ACM, 2006.

[26] Yue Zhang, Serge Egelman, Lorrie Cranor, and Jason Hong. “Phinding phish: Evaluating anti-phishing tools”. ISOC, 2006.

[27] Yue Zhang, Jason I Hong, and Lorrie F Cranor. “Cantina: a content-based approach to detecting phishing web sites”. In Proceedings of the 16th international conference on World Wide Web, pages 639–648. ACM, 2007.

INSTRUCTIONS TO CONTRIBUTORS

Information Security is an important aspect of protecting the information society from a wide variety of threats. The International Journal of Security (IJS) presents publications and research that builds on computer security and cryptography and also reaches out to other branches of the information sciences. Our aim is to provide research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems.

IJS provides a platform to computer security experts, practitioners, executives, information security managers, academics, security consultants and graduate students to publish original, innovative and time-critical articles and other information describing research and good practices of important technical work in information security, whether theoretical, applicable, or related to implementation. It is also a platform for the sharing of ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community. We welcome contributions towards the precise understanding of security policies through modeling, as well as the design and analysis of mechanisms for enforcing them, and the architectural principles of software and hardware system implementing them.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Started with Volume 9, 2015, IJS will appear with more focused issues. Besides normal publications, IJS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJS LIST OF TOPICS

The realm of International Journal of Security (IJS) extends, but not limited, to the following:

- Anonymity
- Attacks, security mechanisms, and security service
- Authorisation
- Cellular/wireless/mobile/satellite networks securi
- Public key cryptography and key management
- Cryptography and cryptanalysis
- Data integrity issues
- Database security
- Denial of service attacks and countermeasures
- Design or analysis of security protocols
- Distributed and parallel systems security
- Anonymity and pseudonymity
- Code security, including mobile code security
- Biometrics
- Authentication
- Confidentiality, privacy, integrity, authenticatio
- Data confidentiality issues
- Data recovery
- Denial of service
- Dependability and reliability
- Distributed access control
- Electronic commerce

- Formal security analyses
- Information flow
- Intellectual property protection
- Key management
- Network and Internet security
- Network security performance evaluation
- Peer-to-peer security
- Privacy protection
- Revocation of malicious parties
- Secure location determination
- Secure routing protocols
- Security in ad hoc networks
- Security in communications
- Security in distributed systems
- Security in e-mail
- Security in integrated networks
- Security in internet and WWW
- Security in mobile IP
- Security in peer-to-peer networks
- Security in sensor networks
- Security in wired and wireless integrated networks
- Security in wireless communications
- Security in wireless LANs (IEEE 802.11 WLAN, WiFi,
- Security in wireless PANs (Bluetooth and IEEE 802.
- Security specification techniques
- Tradeoff analysis between performance and security
- Viruses worms and other malicious code
- Fraudulent usage
- Information hiding and watermarking
- Intrusion detection
- Multicast security
- Network forensics
- Non-repudiation
- Prevention of traffic analysis
- Computer forensics
- Risk assessment and management
- Secure PHY/MAC/routing protocols
- Security group communications
- Security in cellular networks (2G, 2.5G, 3G, B3G,
- Security in content-delivery networks
- Security in domain name service
- Security in high-speed networks
- Security in integrated wireless networks
- Security in IP networks
- Security in optical systems and networks
- Security in satellite networks
- Security in VoIP
- Security in Wired Networks
- Security in wireless internet
- Security in wireless MANs (IEEE 802.16 and WiMAX)
- Security policies
- Security standards
- Trust establishment
- WLAN and Bluetooth security

CALL FOR PAPERS

Volume: 9 - **Issue:** 3

i. Submission Deadline : August 31, 2015 **ii. Author Notification:** September 30, 2015

iii. Issue Publication: October 2015

CONTACT INFORMATION

Computer Science Journals Sdn BhD

B-5-8 Plaza Mont Kiara, Mont Kiara

50480, Kuala Lumpur, MALAYSIA

Phone: 006 03 6204 5627

Fax: 006 03 6204 5628

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2015
COMPUTER SCIENCE JOURNALS SDN BHD
B-5-8 PLAZA MONT KIARA
MONT KIARA
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6204 5627
FAX: 006 03 6204 5628
EMAIL: cscpress@cscjournals.org