International Journal of Electronics and Communication Engineering.
ISSN 0974-2166 Volume 4, Number 5 (2011), pp. 527-535

http://www.irphouse.com

Study and Analysis for Genetic and Guassian Phishing Detect ion Method

[1]Amrinder Singh and [2]Monika Aggarwal

[1]M.Tech. Regular Student #University Reg. No. 96256881657,
Bhai Gurdas Institute of Engineering and Technology, Sangrur,
Pb. University, Punjab Technical University, Jalandhar, Punjab
[2]Associate Prof.
E-mail: monikaaggarwal76@gmail.com

Abstract

In computing, phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay, PayPal and online banks are common targets. Phishing is typically carried out by email or instant messaging, [1] and often directs users to enter details at a website, although phone contact has also been used.[2] Phishing is an example of social engineering techniques used to fool users.[3] Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical measures.

Keywords: SMTP, AOL, URL, RSA, DNS, DOM, SVM, MIME

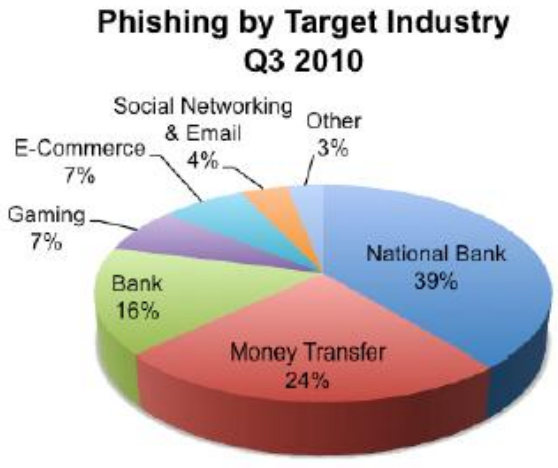
The first recorded mention of the term "phishing" is on the alt.online-service. America-online Usenet newsgroup on January 2, 1996, [4] although the term may have appeared earlier in the print edition of the hacker magazine 2600.[5] A phishing technique was described in detail as early as 1987, in a paper and presentation delivered to the International HP Users Group, Interex.[6] The term phishing is a variant of fishing, [7] probably influenced by phreaking, [8][9] and alludes to the use of increasingly sophisticated baits used in the hope of a "catch" of financial information and passwords. The word may also be linked to leetspeak, in which ph is a common substitution for f.[10].Phishing on AOL was closely associated with the warez community that exchanged pirated software. Those who would later phish on AOL during the 1990s originally used fake, algorithmically generated credit card numbers to create accounts on AOL, which could last weeks or possibly months.

After AOL brought in measures in late 1995 to prevent this, early AOL crackers resorted to phishing for legitimate accounts.[11]

A phisher might pose as an AOL staff member and send an instant message to a potential victim, asking him to reveal his password.[12] In order to lure the victim into giving up sensitive information the message might include imperatives like "verify your account" or "confirm billing information". Once the victim had revealed the password, the attacker could access and use the victim's account for criminal purposes, such as spamming. Both phishing and warezing on AOL generally required custom-written programs, such as AOHell. Phishing became so prevalent on AOL that they added a line on all instant messages stating: "no one working at AOL will ask for your password or billing information".

After 1997, AOL's policy enforcement with respect to phishing and warez became stricter and forced pirated software off AOL servers. AOL simultaneously developed a system to promptly deactivate accounts involved in phishing, often before the victims could respond. The shutting down of the warez scene on AOL caused most phishers to leave the service, and many phishers—often young teens—grew out of the habit.[13]

The capture of AOL account information may have led phishers to misuse credit card information, and to the realization that attacks against online payment systems were feasible. The first known direct attempt against a payment system affected E-gold in June 2001, which was followed up by a "post-911 id check" shortly after the September 11 attacks on the World Trade Center.[14] Both were viewed at the time as failures, but can now be seen as early experiments towards more fruitful attacks against mainstream banks. By 2004, phishing was recognized as a fully industrialized part of the economy of crime: specializations emerged on a global scale that provided components for cash, which were assembled into finished attacks.[15][16]



More recent phishing attempts have targeted the customers of banks and online payment services. E-mails, supposedly from the Internal Revenue Service, have also been used to glean sensitive data from U.S. taxpayers.[17] While the first such

examples were sent indiscriminately in the expectation that some would be received by customers of a given bank or service, recent research has shown that phishers may in principle be able to determine which banks potential victims use, and target bogus emails accordingly.[18] Targeted versions of phishing have been termed spear phishing.[19]

Social networking sites are also a target of phishing, since the personal details in such sites can be used in identity theft;[20] in late 2006 a computer worm took over pages on MySpace and altered links to direct surfers to websites designed to steal login details.[21] Experiments show a success rate of over 70% for phishing attacks on social networks.[22]

Almost half of phishing thefts in 2006 were committed by groups operating through the Russian Business Network based in St. Petersburg[23]

Phishing techniques

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers, such as this example URL, http://www.yourbank.com.example.com/. Another common trick is to make the anchor text for a link appear to be valid, when the link actually goes to the phishers' site, such as http://en.wikipedia.org/wiki/Genuine.

An old method of spoofing used links containing the '@' symbol, originally intended as a way to include a username and password (contrary to the standard).[24] For example, the link http://www.google.com@members.tripod.com/ might deceive a casual observer into believing that it will open a page on www.google.com, whereas it actually directs the browser to a page on members.tripod.com, using a username of www.google.com: the page opens normally, regardless of the username supplied. Such URLs were disabled in Internet Explorer, [25] while the Mozilla[26] and Opera web browsers opted to present a warning message and give the option of continuing to the site or cancelling.

A further problem with URLs has been found in the handling of Internationalized domain names (IDN) in web browsers, that might allow visually identical web addresses to lead to different, possibly malicious, websites. Despite the publicity surrounding the flaw, known as IDN spoofing[27] or a homograph attack, [28] no known phishing attacks have yet taken advantage of it. Phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise malicious URLs with a trusted domain.[29][30][31]

Filter evasion

Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing emails.[32]

Website forgery

Once the victim visits the website the deception is not over.[33] Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.[34]

An attacker can even use flaws in a trusted website's own scripts against the victim.[35] These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, although it is very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against PayPal.[36]

A Universal Man-in-the-middle Phishing Kit, discovered by RSA Security, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site.[37]

To avoid anti-phishing techniques that scan websites for phishing-related text, phishers have begun to use Flash-based websites. These look much like the real website, but hide the text in a multimedia object.[38]

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts.[39] Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.[40]

An example of a phishing email targeted at PayPal users.In an example PayPal phish (right), spelling mistakes in the email and the presence of an IP address in the link (visible in the tooltip under the yellow box) are both clues that this is a phishing attempt.

Another giveaway is the lack of a personal greeting, although the presence of personal details would not be a guarantee of legitimacy.

Genetic Algorithm Applied to Phishing Detection

Applying genetic algorithm to phishing detection seems to be a promising area. Genetic algorithms can be used to evolve simple rules for preventing phishing attacks. These rules are used to differentiate normal website from anomalous website. These anomalous websites refer to events with probability of phishing attacks. The rules stored in the rule base are usually in the following form:

if { condition } then { act } For the problems we presented above, the condition usually refers to a match between the URL of the current website link in the e-mail and the rules in PADPS (Phishing Attack Detection and Prevention System), which indicates the probability of phishing attack. The act field usually refers to an action defined by the security policy such as reporting an alert to the browser, through the status field. For example, a rule can be defined as:

if
{
The IP address of the URL in the received e-mail finds any match in the Ruleset
}
then
{
Phishing e-mail
}
This rule can be explained as follows: if there exists an IP address of the URL in e-mail and it does not match
the defined Rule Set for White List then the received mail is a phishing mail; so the status is phishing e-mail.
The final goal of applying GA is to generate rules that match only the anomalous URLs of websites. These rules are tested on historical URLs and are used to filter new URLs to find suspicious phishing attacks. In this implementation, data used for GA is a preclassified data set that differentiates normal URLs (websites) from anomalous ones. This data set is gathered using APWG (Anti-Phishing Work Group). The data set is manually classified based on experts' knowledge. It is used for the fitness evaluation during the execution of GA. By starting GA with only a small set of randomly generated rules, we can generate a larger data set that contains rules for PADPS. These rules are "good enough" solutions for GA and can be used for filtering new phishing attack.

Data Representation
In order to fully exploit the suspicious level, we need to examine all fields related with a specific URL in Phishing e-mail.

Example Rule in Ruleset
If (the IP address of the URL in the received e-mail is equal to 209.11.??.??)
Then
Phishing e-mail
End if

Example Chromosome structure for the above-defined rule is (d, 1, 0, b, *, *, *, *). There are eight genes in each chromosome. For simplicity, we have used hexadecimal representation for the IP address. The actual validity of this rule will be examined by matching the historical data set comprised of URLs marked as either phish-mail or not. If the rule is able to find a phishing attack, a bonus will be given to the current chromosome. Otherwise, a penalty will be given to it.

Parameters in Genetic Algorithm
There are many parameters to consider for the application of GA. Each of these parameters heavily influences the effectiveness of the genetic algorithm. We will discuss the methodology and related parameters in the following section.

Evaluation function

The evaluation function is one of the most important parameters in genetic algorithm. The proposed implementation differs from the scheme used by, in that the definition on calculations of outcome and fitness is different. The following steps are used to calculate the evaluation function. First the overall outcome is calculated based on whether a field of the URL matches the pre-classified data set, and then multiply the weight of that field. The

Matched value is set to either 1 or 0.

$$\text{outcome} = \sum_{I=1}^{8} \text{Matched} * \text{Weight}_i$$

The order of weight values is used in this function. These orders are categorized according to different fields in an IP address of the URLs. Therefore, all genes in the respective sub-domains of an IP address have the same weight. The actual values can be finely tuned at execution time. This scheme is straightforward and intuitive. These are the most important pieces of information needed to capture a phish-mail. Some URLs are more probable targets for phishing attacks—for example, URLs for Bank domains.

The absolute difference between the outcome of the chromosome and the actual suspicious level is then computed using the following equation. The suspicious level is a threshold that indicates the extent to which two URLs are considered a "match." The actual value of suspicious level reflects observations from historical data.

$$\Delta = | \text{outcome-suspicious level} |$$

Once a mismatch happens, the penalty value iscomputed using the absolute difference. The ranking in the equation indicates whether or not an intrusion is easy to identify.

$$\text{penalty} = (\Delta * \text{ranking})/100$$

The fitness of a chromosome is computed using the above penalty:

$$\text{fitness} = 1\text{-penalty}$$

Obviously, the range of the fitness value is between 0 and 1.

Crossover and Mutation

Traditional genetic algorithms have been used to identify and converge populations of candidate hypotheses to a single global optimum. For this problem, a set of rules is needed as a basis for the PADPS. As mentioned earlier, there is no way to clearly identity whether a hyperlink (URL) in an e-mail is normal or anomalous just using one rule. Multiple rules are needed to identify unrelated anomalies, which mean that several good rules are more effective than a single best rule. Another reason for finding multiple rules is that because there are so many types of hyperlink possibilities, a small set of rules will be far from enough.

Using the genetic algorithm, we need to find local maxima (a set of "good-enough" solutions) as opposed to the global maximum (the best solution) (Sinclair, Pierce, and Matzner 1999). The niching techniques can be used to find multiple local maxima (Miller and Shaw, 1996; see also Sinclair, Pierce, and Matzner 1999)[15]. It

is based on the analogy to nature in that within each environment, there are different subspaces (niches) that can support different types of life.

In a similar manner, genetic algorithm can maintain the diversity of each population in a multimodal domain, which refers to domains requiring the identification of multiple optima. Two basic methods, Crowding and Sharing can be used for niching[15]. The crowding method uses the most similar member for replacements to slow down the population to converge towards a single point in the following generations. The sharing method reduces the fitness of individuals that have highly similar members and forces individuals to evolve to other local maxima that may be less populated.

System Architecture

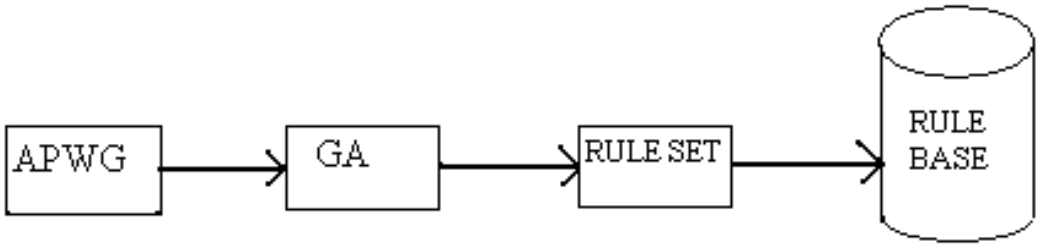


Figure 2.3.2. Architecture of applying GA into PADPS.

The similarity metrics used in these techniques can be phenotype similarity such as the relation between two URLs in this problem. This is more fitful for finding rules used in PADPS. The disadvantage of this approach is that it requires more domain-specific knowledge

Finally comparison of the two methods for effectiveness against phishing based on probability of error has been conducted.

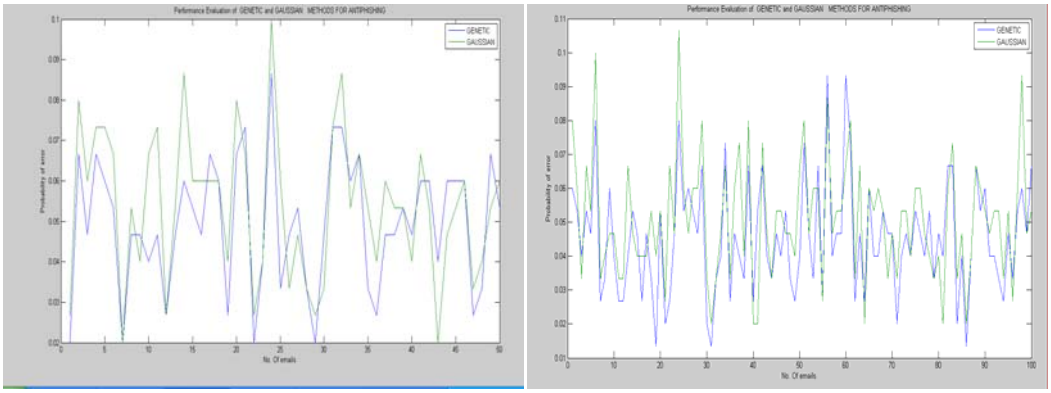
Guassian Method : In machine learning, support vector machines and Gaussian processes are said to implement transductive inference, since outputs for new cases are computed without constructing an explicit model. In contrast, supervised learning is an example of inductive reasoning. Supervised learning methods such as neural networks and classification trees construct an explicit model from observed examples, and then outputs for new cases are computed from the model.

The use of support vector machines for transductive inference was originated by Vladimir Vapnik. According to Vapnik, as a motivating principle for machine learning, transduction is preferable to induction since induction requires the solution of a more general problem (inferring an unobserved model) before solving a more specific problem (computing outputs for new cases). Transductive inference is especially useful in problems for which there are many examples, but few examples have labels. For example, in web page categorization problems, there are many web pages, but few web pages have known categories (as assigned by a human expert).

Bayesian inference yields another interpretation of transduction. In Bayesian inference, transduction is the computation the posterior probability of new cases given previous, observed cases. The dependence on a predictive model is removed by averaging (integrating) over all models considered possible, weighting each model by its posterior probability given the observed cases. --- similar to supervised learning, but does not explicitly construct a function: instead, tries to predict new outputs based on training inputs, training outputs, and new inputs.

Experiments

In the first iteration 50 email messages were generated and classified according to Genetic mean and Gaussian mean method. The plot shows the variation of probability of error. It can be seen that the maximum POE is almost 0.93 in the case of Gaussian mean method and mostly the POE of the Genetic mean method is generally less than the Gaussian mean method. However at some instances the POE of Genetic mean method is more is at the 25th and 35th email message.



In the this iteration 100 email messages were generated and classified according to Genetic mean and Gaussian mean method. The plot shows the variation of probability of error. It can be seen that the maximum POE is almost 0.117 in the case of Gaussian mean method and mostly the POE of the Genetic mean method is generally less than the Gaussian mean method. However at some instances the POE of Genetic mean method is more is at the 30th and 70th email message.

Conclusion

It can be seen from the above iterations that most of times Genetic method gives better performance and the POE is less as compared to Gaussian method. Still a few times the Gaussian mean method in less POE but these instances are rare.

So it can be concluded that in fighting cyber crime the method of Genetic method is better in classifying email messages as Phishing emails that the Gaussian method.

References

[1] J.shreeram, M.subam, P.shanthi, K.manjula. Sastra University Kumbakanam "Anti phishing detection of phishing attacks using genetic algorithm".Retrieved on October 8, 2010
[2] Microsoft Corporation. What is social engineering?. Retrieved on August 22, 2007.
[3] "phish, v." OED Online, March 2006, Oxford University Press.. Oxford English Dictionary Online. Retrieved on August 9, 2006.
[4] Ollmann, Gunter. The Phishing Guide: Understanding and Preventing Phishing Attacks. Technical Info. Retrieved on July 10, 2006.
[5] Felix, Jerry and Hauck, Chris (September 1987). "System Security: A Hacker's Perspective". 1987 Interex Proceedings 1: 6.
[6] Spam Slayer: Do You Speak Spam?. PCWorld.com. Retrieved on August 16, 2006.
[7] "phishing, n." OED Online, March 2006, Oxford University Press.. Oxford English Dictionary Online. Retrieved on August 9, 2006.
[8] Phishing. Language Log, September 22, 2004. Retrieved on August 9, 2006.
[9] Mitchell, Anthony. "A Leet Primer", TechNewsWorld, July 12, 2005.
[10] Phishing. Word Spy. Retrieved on September 28, 2006.
[11] Stutz, Michael. "AOL: A Cracker's Paradise?", Wired News, January 29, 1998.
[12] History of AOL Warez.
[13] GP4.3 - Growth and Fraud - Case #3 - Phishing. Financial Cryptography (December 30, 2005).