ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/224175391

Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks

Conference Paper · August 2010

DOI: 10.1109/CIT.2010.254 · Source: IEEE Xplore

CITATIONS
12

READS
436

3 authors:

Omran Salem
University of Bradford
2 PUBLICATIONS **14** CITATIONS
SEE PROFILE

Mohammed Alamgir Hossain
Anglia Ruskin University
154 PUBLICATIONS **1,397** CITATIONS
SEE PROFILE

Mumtaz Kamala
University of Bradford
37 PUBLICATIONS **179** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

An Intelligent Image-based Colourimetric Test Framework for Diagnosis View project

Conference Paper: E-GOVERNMENT IMPLEMENTATION IN CHAOTIC ENVIRONMENT - LIBYA CASE STUDY View project

All content following this page was uploaded by Mumtaz Kamala on 16 May 2014.

The user has requested enhancement of the downloaded file.

Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks

O. Salem
Department of Computing
University of Bradford
Bradford, UK
O.S.A.Salem@Bradford.ac.uk

A. Hossain
Department of Computing
University of Bradford
Bradford, UK
M.A.Hossain1@Bradford.ac.uk

M. Kamala
Department of Computing
University of Bradford
Bradford, UK
M.A.Kamala@Bradford.ac.uk

***Abstract*— This paper presents a comprehensive literature survey and analysis on Phishing, Vishing and Smishing to exploit the knowledge in implementing an intelligent tool for detection and protection. This is a new social engineering problem which makes our day to day life vulnerable and difficult. This investigation particularly focuses on phishing through email as it has more serious consequences directly related to financial transactions in comparison to the other methods. It is worth mentioning that securing the enormous amount of online transactions is very challenging since several methods are invented daily to breach individual privacy in order to steal their credentials. The cost of these types of attacks exceeds millions of dollars annually. Many tools are proposed to solve this problem; unfortunately, the dilemma still exists. This paper proposes a methodology to develop an intelligent tool and awareness security program to address the risk of this problem.**

***Index Terms*— Security, Phishing, Social Engineering, Intelligent tool, Fuzzy Logic**

I. Introduction

Millions of electronic financial transactions are executed everyday around the world through the internet. Banks, shops and governments offer online account access and online payments [1]. Personal information such as usernames, passwords, credit cards and account numbers are the core of online transaction.

Hackers and curious people are always seeking new methods to breach privacy through vulnerabilities that exist in the World Wide Web's backbone systems. Securing millions of online transactions is becoming more sophisticated as numerous methods are invented every day to breach privacy. Phishing is one of the methods that deceive people into revealing their personal information (i.e. username, password, bank account and credit card number) by using social engineering and technical tools without using the traditional methods such as sniffing, Trojan horses or viruses.

What is phishing?

Anti-phishing work group (APWG) [1] defined phishing as "an attack that uses both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data".

Phishing attacks cost companies and consumers thousands to millions of dollars every year. In addition, the e-business sector loses clients' confidence, which is worth millions. According to APWG's phishing report on February 2007, the number of email phishing attacks increased around 37% in the period between Feb. '06 and Feb. '07. Meanwhile, the unique phishing websites detected by APWG increased by 80% in the same period [2, 3]. Phishing has become a criminal act, categorized as one of the most effective online scams[4].

How phishing works?

The phishing process usually starts with spoofed email influencing people to login to their accounts by using forged WebPages that look like the official webpage of the legitimate service provider, such as a bank or an e-shop[5]. The spoofed emails often look like valid emails because the phishers share the same logos and graphic pictures as the original website [6]. In addition, the scam emails contain deceptive URL addresses linking to a scam website.

Figure 1 shows a scam email that shares the graphic of a bank's website and a deceptive URL linking to a tricky website [6].

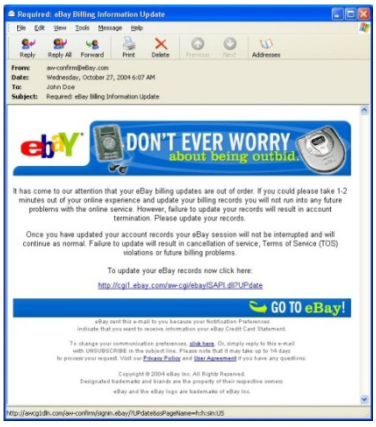

Figure 1: scam email shares graphics with legitimate website

[1] The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types. http://www.antiphishing.org/

By clicking the link, the user will be directed to a false website that looks like the legitimate one. The information is captured as soon as the victim enters the username, password or the credit card number. Therefore, users should not forward unauthenticated emails or click on unusual links in an email or use the search engines to look for online donations and charitable organizations [7].

Phishing may be conducted directly through the phone to hunt a victim's personal information. Some phishers pose as employers and call people who have listed themselves on job search websites asking them about the social security number or sensitive information. Another scenario is when someone calls the victim asking him/her to reconfirm the financial information such as the credit card number because of an overdue bill [8].

II. PHISHING TECHNIQUES

Following are five major techniques to accomplish phishing attacks:

1. *Impersonate*

This is a common technique. Simply, the phishing email falsely claims to be from a legitimate business where victims might have an account. The phisher shares the logos and graphics with the original website so that the scam email appears to be an official email asking the user to login to solve certain problems[9]. This type of attack weakens the consumer confidence as it will be difficult for normal users to distinguish between legitimate and fraudulent emails.

2. *Forward Attack*

This is a sophisticated technique where the phisher collects personal information through a scam email that includes harmful code or script. By using an effective anti-virus, this phishing technique becomes ineffective since the anti-virus picks up the code that collects the victim's information [10]. This scenario works when the scammer sends an email containing two text boxes to allow the victim to enter their SSN and the PIN code. After typing the information, the code behind the email transfers the user to the legitimate website after collecting the credentials.

3. Pop-up attack

This technique launches a hostile pop-up in front of the legitimate website asking the victim to login through a secured pop-up window. Once the user logs in to the pop-up, the phisher captures the victim's credentials and forwards him/her to the official website[10]. In this case, the pop-up window works as a man-in-the-middle to collect the information.

4. Voice Phishing

This is a new technique, improved nowadays by phishers. It is believed to be one of the newest breakthroughs in telecommunications[11]; it uses VOIP – Voice Over Internet Protocol - to conduct it.

This technique is called vishing as it uses both voice and phishing to conduct the attack. This kind of attack can be conducted in a variety of ways with only a few minor differences as illustrated in the following two types of vishing attacks:

a) In this first scenario, the victim receives a typical e-mail, like any other traditional phishing scam. They are then asked to provide information over the phone instead of being directed to an Internet site. The victim calls the fraud "customer service" number (a VoIP account, not a real financial institution) providing account numbers, passwords, and other critical information through a series of voice-prompted menus. [11]

b) In another scenario, the victim is contacted over the phone instead of e-mail. When the receiver answers the fraud call, an automated recording message plays, warning the victim about account breaches. The recorded message directs the victim to take an action in order to protect the account. The trick behind this scenario is that the victim receives the call from a spoofed ID number of the financial company.[11]

5. *Mobile Phishing*:

New technology is on the rise; 2006 was evidence of that when phishing attacks shifted from PCs to mobile devices. This attack manipulates mobile phone operators/carriers' SMS by sending text messages to mobile users trying to trick them into following a malicious mobile Internet link[12]. These types of phishing traps are commonly known as Smishing.

III. ANTI-PHISHING SOLUTIONS

Several techniques have been proposed to solve this problem. Unfortunately, this type of problem depends on human awareness. Therefore, the phishing detection algorithm should not be based completely upon user interaction[13]. Since phishing exploits human vulnerabilities rather than software vulnerabilities, education and awareness are the first steps to mitigate the risks of phishing attacks[1, 9].

Three types of solutions can be used to reduce the risk of *phishing attacks:*

1. Anti-phishing Toolbars

Ebay, NetCraft, GeoTrust, EarthLink, CallingID and other vendors offer several toolbars to lessen the risks of phishing attacks. These organizations use different methods to determine the legitimacy of websites such as checking the IP address, combination of heuristics, user ratings, and manual verification [9, 14].

2. Browser Plug-ins

Microsoft has added a new plug-in into IE7 to help users detect phishing websites. It relies on a blacklist hosted by Microsoft. Another tool from SpoofStick is a simple browser extension that helps users detect fake websites. SpoofStick

makes it easier to spot a spoofed website by prominently displaying only the most relevant domain information [15]. The Netscape Navigator 8.1 web browser includes a built-in phishing filter. Firefox 2.0 includes a new feature designed to identify fraudulent websites [9].

3. *Email-Filters*

Email filters are the most effective solution that can detect spoofed websites, since most victims are directed to spoofed websites from phishing emails[16]. By detecting spoofed emails, the user is more secure, and the solution in this case is categorized as a preventive solution, while the toolbars and browser plug-ins are detective techniques. Ian Fette *(et al)* [13] proposed a simple technique to detect spoofed email called PILFER. The filter works by incorporating features specifically designed to highlight the deceptive methods used to fool users.

IV. PHISHING EMAILS FEATURES

By reading and investigating into a large number of phishing emails, it is noticed that there are many features and tricks that can distinguish legitimate emails from phishing ones; part of these features are hidden from the user and hard to detect, while others are noticed clearly. Based on our analysis of over 600 phishing emails, we can categorize these features into two groups:

1. *Source Code Features (Back End) :*

These tricks and features are hidden to users and can't be detected easily, unless by experts or software tools. Following are some features:

1.1. IP-Based URLs and Non-matching URLs

Phishers attempt to obscure the destination Web site by hiding the URL. This trick conducted by using the IP address instead of using the hostname. An example of an IP address used in a fraudulent website: http://210.16.234.67

In phishing email messages, the link text seen in the email is usually different from the actual link destination. As shown in Figure 2, the email is aiming to pretend linking the user to "https://vault.woodgrove.com/defualt.asp" but as a matter of fact, it links it to "http://203.144.234.138/us/index.html"

Figure 2: Non-Matching URLs

1.2. Contain scripts

Using scripts could help the phishers to hide the destination URL, the JavaScript event "onMouseOver" is used widely by fraudster to show the victim a false URL in the status bar when the mouse moves over the apparent link.[17]

1.3. Number of domains

Since the phishers share images and links with the legitimate website, and forward the victim to the phishing website, it noticed that phishing emails contain multiple domains.

2. *Content Features (Front End) :*

These tricks and features are not hidden to the user, and can be detected easily if the user acquires sufficient training. Following are main features that can be noticed in phishing emails

2.1. Generic salutation

Personalization of salutation increase the trustworthiness, people who are official subscribers should receive personal salutation rather than generic. An example of generic salutation: Dear valued customer, Dear client, etc.

2.2. Security promises, Requires a fast response or "Click Here" link

To gain the trust of the victim, phishers regularly emphasize security issues. They convince users to visit their website, claiming that it is secure and safe.

Phishing emails may claim that the client's account information is out of date, credit card has expired, or the account should be verified as a regular security procedure. The phishers try to collect information as soon as they can before the phishing website is shut down, so they ask the victim for a fast response.

In addition to that, phishers try to trick the victims by using clear hypertext link such as "Click here to login". The phisher wants the user to click this link since it is the most important link in the email. Other links are maintained in the email to keep the genuine "feel", such as the link to the privacy policy, the link to the user agreement, images and logos.

2.3. Links to https:// domains

In order to deceive the victims, phishers used to post links to https:// domains in the front end of the email page, while in the back end it forwards the victim to an unsecure link. This feature is founded just in phishing emails.

V. INTELLIGENT MODEL FOR DETECTION AND PROTECTION

Since phishing is part of social engineering attacks, it is an exploit of a vulnerability in human nature rather than in technology weakness; the solution is a mix of utilizing tools and a rigorous human learning approach to avoid different types of attacks such as email Phishing, Vishing (voice phishing) and Smishing (SMS phishing).

Most of the existing solutions are technical in nature, mainly tools installed on the user's computer to monitor and filter phishing emails. The author(s) suggests that investment in the human element itself as a preventive strategy combined with proper utilization of tools yields better results.

The first step that should be taken into consideration is a proficient security awareness program that can help users to avoid all phishers techniques. Such programs will not stop the effectiveness of the phishing attack, but will reduce it. Awareness programs are usually categorized as proactive solutions, therefore it has more effectiveness and low cost in comparison to reactive solutions.

In addition to the awareness development, one can also consider an intelligent system to detect the level of vulnerability, in turn helping to make decisions in regards to phishing attack. This section focuses on a similar scheme of methodology to build an effective and preventive anti-phishing tool:

1. A set of 600 phishing[2] and another 500 non-phishing emails were collected to implement the proposed methodology.
2. All six features discussed in section IV were used to distinguish between legitimate and phishing emails according to their relevance.
3. A VB script was written to extract those features. Initially, the pilot program parses emails on two levels; the content level (front end), which is the body of the email, and the back end, which is the source code. It extracts all discussed features above and then gives the email scores for each feature. The resulting scores are used to assist in further automated phases of assessing whether the email is a phishing trap or not. The implementation of VBA and MS Access 2007 for the backend database.

   An example of the linguistic descriptors used to represent one of the phishing feature indicators (Generic salutation) are as follows:
   - generic salutation (dear customer, dear valued member, etc) – Risk is High
   - Contains the first name (e.g. Dear John) * - Risk is Moderate, because sometimes the first name can be extracted from the prefix part of the user's email.
   - Contains the first name and last name or the customer name (e.g. Dear John Mick) – Risk is Low
4. The first phase of the proposed tool is building a set of fuzzy logic (FL) rules to get an accurate assessment of phishing emails set. These were then utilized to developed FL-based expert system. In brief, FL expert system is a collection of membership functions and rules that are utilized to reason about data [18]. The inference process in FL goes through four steps [19] to achieve the outcome:
   I. **Fuzzification**, the membership function values defined on the input variables is applied to their actual values to determine the degree of truth for each rule premise.
   II. **Inference**, the truth value for the premise of each rule is computed, and applied to the conclusion part of that rule. This results in one fuzzy subset to be assigned to each output variable for each rule.
   III. **Composition**, all of the fuzzy subsets assigned to each output variable are combined together to form a single fuzzy subset for each output variable.
   IV. **Defuzzification** (optional), mainly used when converting the fuzzy output set to a crisp number.

   The rule base system has three input parameters and one output. It contains all "IF-THEN" rules for the proposed tool. The result of building an FL rules for 6 features, each feature has 3 linguistic variables (*Low, Moderate and High*) will need a complicated process of 3^6 rules i.e. 729 rules. This may affect the speed of the proposed tool. Due to the large number of the above rules, the evaluation process is divided into two layers with two groups at the first layer (*Back End* and *Front End group*). The first layer is to rate each group separately. This layer is called the rule based one. Each group has three linguistic variables with a total number of 27 rules. Therefore, 54 rules are built to evaluate the *Back End* and *Front End* groups separately.

   For each group, 3 output fuzzy sets are defined: (*Trusted, Doubtful and Un-Trusted*)

Following is an example of fuzzy rule for *Back End* group risk probability:

IF
IP-Based URLs *is* High *and*
Scripts *is* Low *and*
Multi domain *is* High *and*
Then
The *Back End* group is *Un-Trusted*.

Following is an example of fuzzy rule for *Front End* Group risk probability:

IF
Salutation *is* High *and*
Warning and security *is* Low *and*
Fake *Https* links *is* Low *and*
Then
The *Front End* group is *Trusted*.

[2] The data set of the phishing emails can be obtained from: http://monkey.org/~jose/wiki/doku.php?id=PhishingCorpus

The output of both groups is the input of the second layer which is the rule based two. Finally, a set of 9 rules are built at that layer to evaluate the email for final rate.

Following is the rule based two used for final email rating.

Rule #	Back End Group	Front End Group	Final Evaluation
1	Trusted	Trusted	Safe
2	Trusted	Doubtful	Safe
3	Trusted	Un Trusted	Partially Safe
4	Doubtful	Trusted	Partially Safe
5	Doubtful	Doubtful	Partially Safe
6	Doubtful	Un Trusted	Phishy
7	Un Trusted	Trusted	Partially Safe
8	Un Trusted	Doubtful	Phishy
9	Un Trusted	Un Trusted	Phishy

Table 1: Rule Based 2 for Final Email Evaluation

The three-dimensional plot for rule base 2 is displayed as below:

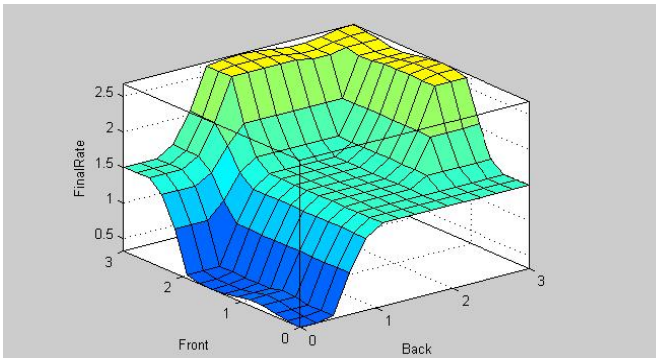

Figure 3: Three-dimensional plots for rule base 2

VI. Experiment and Results

In order to get a clear idea about how phishing works and its effect on victims, each email has been divided into two parts, Front End which is the email body (content part that user usually read) and Back End (which is the source code of the email and hidden to user), first of all the features mentioned in part IV extracted from both front and back ends, then each feature assigned a value of risk (*High, Moderate* or *Low*), by rating the front end; its more easy to deliver the reasons of email risks to user, thus helps prevent users to be victims when they use unprotected environment. Secondly, the output of each group are passed into rule based 2 layer (table 1) to get the final rate of the email. Each email is rated as *Safe, Partially Safe* or *phishy*.

By examining an initial number of healthy and phishing emails, the proposed tool rated 22% of the emails as suspicious phishing emails (*Partially Safe*) and 78% as *Phishy*, while 95% of the healthy emails passed the tools as *Safe* emails with 5% as *Partially Safe* as shown in Figure 4.

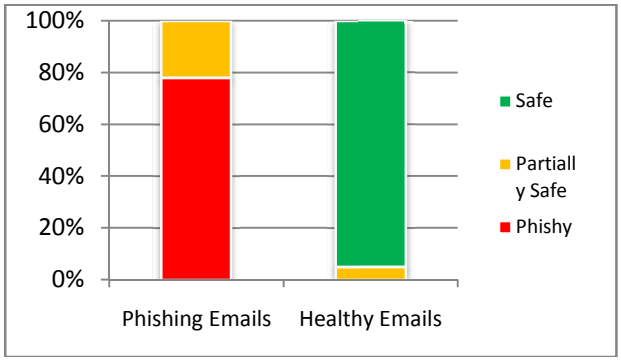

Figure 4: Results of evaluating phishing and healthy emails

In order to improve the accuracy of the proposed tool; the results of our experiments compared with *Microsoft Windows live mail 2009,* which is an existing mail tool that contains anti-Phishing detector. By testing same data set of phishing emails, Microsoft Windows Live Mail 2009 flagged 58% as suspicious phishing emails while 42% were not detected. Figure 5 shows the comparison of the proposed tool and *Microsoft Windows live mail 2009.*

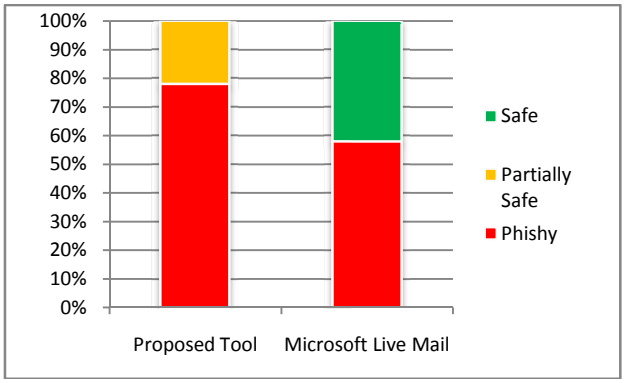

Figure 5: Results of comparison the proposed toll with *Microsoft Windows live mail 2009*

Finally, 94% of the phishing emails founded that they are deceptive users at the front end layer of the incoming email (the readable part of the email), so by implementing a sufficient awareness security program, people will be able detect phishing emails easily, figure 6 shows the results of evaluating the front end vs. the back end.

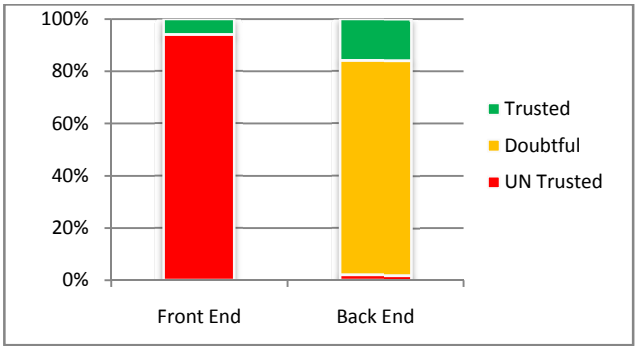

Figure 6: Front End vs. Back End

According to the analysis of the phishing emails, the end user should be awarded against three main features:

1. Since the phisher doesn't have the database of the victims, the user should notice his/her registered name at the salutation line of the incoming email.
2. Asking the user for fast respond and many security promises could be a trick to convince the victim that they are aiming to visit a secure website for a critical issue.
3. Including *"https://"* link on the front end of the email, could be a trick to deceive the user.

VII. Conclusion

This paper presents an investigation into the social engineering issues and technical aspects of detection and protection of phishing, vishing and smishing. A detail literature survey is used to provide an analysis of different context of vulnerability of the users and to demonstrate the existing state of technology. Particular attention has been given to email phishing as it is considered one of the most common attacks on individual vulnerability. It is clearly demonstrated that by determining the main differences between the legitimate emails and the phishing, one can reduce the risk of this type of attack. In addition, a fuzzy logic based intelligent expert system has been explored to evaluate the suitability for real-time detection and protection. A new approach of dividing phishing e-mails into layers and groups is used. This has helped to simplify implementing fuzzy rules in a speedy and efficient way by rating each group individually, in order to increase the awareness level of the users, the tool will be provided with a clarification screen, to illustrate the reasons behind the phishing rate, which will help to protect them when they receive such emails at a non-secured environment.

VIII. References

1. Larcom, G. and A.J. Elbirt, *Gone phishing.* Technology and Society Magazine, IEEE, 2006. **25**(3): p. 52.
2. APWG, *Phishing Activity Trends, Report for the Month of February, 2007*.
3. Wenyin, L., et al., *An antiphishing strategy based on visual similarity assessment.* IEEE Internet Computing, 2006. **10**(2): p. 58.
4. Brooks, J., *Anti-Phishing Best Practices: Keys to Aggressively and Effectively Protecting Your Organization from Phishing Attacks.* 2006, Cyveillance
5. Engin, K. and K. Christopher, *Protecting Users Against Phishing Attacks with AntiPhish*, in *Proceedings of the 29th Annual International Computer Software and Applications Conference (COMPSAC'05) Volume 1 - Volume 01*. 2005, IEEE Computer Society.
6. Microsoft, C. *Recognize phishing scams and fraudulent e-mails*. http://www.microsoft.com/athome/security/email/phishing.mspx (accessed on 26/09/2009)
7. Tzer-Shyong, C., J. Fuh-Gwo, and L. Yu-Chia. *Hacking Tricks Toward Security on Network Environments*. 2006.
8. *How phishing works?* http://www.phishinginfo.org/how.html (accessed on 28/09/2009)
9. Yue Zhang, S.E., Lorrie Cranor, and Jason Hong. *Phinding Phish Evaluating Anti-Phishing Tools*. in *14th Annual Network & Distributed System Security Symposium (NDSS 2007)*. San Diego, CA.
10. James, L., *Phishing Exposed*. Oct 2005, Syngress
11. FBI, *Something Vishy, Be Aware of a New Online Scam* 2007.
12. Shah, J., *Online Crime Migrates to Mobile Phones.* Sage, April 2007. **1**(2).
13. Ian Fette, N.S., Anthony Tomasic, *learning to detect phishing emails*. June 2006, Carnegie Mellon University Technical Report CMU-ISRI-06-112. .
14. ebay corporation, 2007 http://pages.ebay.com/ebay_toolbar/. (accessed on 28/09/2009)
15. *What is SpoofStick?* http://www.spoofstick.com/ (accessed on 30/09/2009)
16. Liu, W., et al., *Phishing Webpage Detection*, in *Proceedings of the Eighth International Conference on Document Analysis and Recognition*. 2005, IEEE Computer Society.
17. Christine E. Drake, J.J.O., and Eugene J. Koontz *Anatomy of a Phishing Email* 2004, MailFrontier, Inc.
18. J. Buckley and D. Tucker. Second generation fuzzy expert system. *Fuzzy Sets and Systems*, 31:271{284, 1989.
19. Earl Cox, 2001, FL and Measures of Certainty in E-Commerce Expert System. Article. Scianta Intelligence, Chapel Hill.

View publication stats