A Novel Survey on Cloud Security

T. Thirunavukarasu **M. Judith Lucia**

Abstract — **Cloud computing is the delivery of computing services over the internet. Cloud services are capable of allowing individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The model of cloud computing allows access to information and computer resources from anywhere that a network connection is available. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.**

Key Words — **Cyber warfare, Network Centric Warfare, attack graph, distributed firewalls, rule anomalies, zombie explorative attacks.**

I. Introduction

Security is considered one of the most critical aspects in everyday computing and it is no different for cloud computing due to the sensitivity and importance of data stored in the cloud. Cloud computing has several major issues and concerns in areas such as security in data, trust, regulations and performance issues. There is a critical need and urge to store the data, manage effectively, share the resources and analyze massive amounts of complex data to determine the trends in order to improve the quality of healthcare, hence better safe-guard the nation and explore alternative energy. Because of the critical nature of the applications, it is important that clouds be secure. So the security of clouds needs to be safeguarded in the midst of untrusted processes. Hence a survey is necessarily to be taken in different aspects of cloud security.

II. Systematic Mapping Study On Security Threats In Cloud Computing

In this paper [1], a protocol is identified with 661 publications about the subject, where the involvement of security domains is being analyzed. Various types of solutions proposed by the authors are presented and identified that some of those publication were concerned with the compliance of some standard. It is necessary to identify those compliances and reference the respective publications to ease the work of the researcher who wants to explore a specific compliance. Also the Threat is the most explored in literature, in consequence the domains of risk analysis and management and trust model have expressive results. Many combinations of domains related to access control, applied cryptography, data or database protection and privacy are also studied. This reflects in the recent growth of publications that report experiences in solutions for storage and *Bigdata* in the cloud. In this same scenario, Framework and Encryption Scheme are the most used solutions. Regarding compliances, the most present in publications are those indicated by CSA, ISO 27002, ISO 27001 and NIST. For future works, it is necessary to investigate in more detail the obstacles of a given compliance to be inserted in CC scene.

III. Cyber Warfare Simulation To Control Cyber Space

The threats posed by technically sophisticated cyber attacks are increasing. Possessing cyber security will not guarantee victory for a network centric force but the lack of cyber superiority will almost certainly ensure the defeat of a network centric force. While inaccuracy and denial of information are the ancient techniques as warfare itself, technically sophisticated cyber attacks permit, a wide-scale, persistent, and virtually undetectable attack upon the information. The technically sophisticated cyber attack will undermine information, surprise decision-makers, generate confusion among decision makers, forestall situational awareness development, and corrupt decision-making. As a result, systems coupled with architectures that support real-time alteration of cyber defenses using virtual machine and cloud computing environments are needed. The complexity of future cyber systems will continue to increase, as witnessed by the development of inter cloud technologies and "smart grid" technologies for remote control and management of real-world infrastructure, which increases the complexity of cyber attacks, and create new methods for executing cyber attacks.

In this paper [2], the need for cyber warfare training environments for decision-makers has been discussed. As we advance in the use of the NCW (Network Centric Warfare) paradigm for military operations, the network and associated software will become increasingly important and lucrative targets for an adversary and must be prepared to counter their cyber attacks. Therefore, decision-makers and information technology specialists must be trained to be able to recognize and counteract a cyber attack against critical information resources early in the cyber attack. The key to the training is the development of simulation environments that disclose the experience and expertise needed to make effective cyber defense possible in the face of cyber attacks. The future efforts will address the question of simulating complex cyber attacks and cost effective but accurate provisioning of training services. Research targeted at advancement of cyber battle understanding, human behavior modeling and decision-making in NCW and cyber warfare is needed. We must also gain a better understanding of decision-making and situational awareness within large-scale and high-volume data environments that have noise and uncertainty inherent to the data as well as due to cyber attacks.

IV. The Network Level Behavior of Spammers

The network-level behavior of spammers includes IP address ranges that send the most spam, common spamming modes (*e.g.*, BGP route hijacking, bots), how persistent (in time) are the botnet spamming characteristics. This paper [3] answers these questions by analyzing 10 million spam messages that collect data on Internet spam sinkhole, and by correlating these messages with the results of IP-based blacklist lookups, passive TCP Niger printing information, routing information, and botnet command and control traces. The results are small, yet non-negligible, amount of spam is received from IP addresses that correspond to short-lived BGP routes, typically for hijacked addresses. Most spam is received from a few regions of IP address space. It appears that spammers make use of transient bots. These patterns suggest that developing algorithms to identify botnet membership, littering email messages based on network-level properties (which are less variable than an email's contents) and improving the security of the Internet routing infrastructure, may prove extremely effective for combating spam.

Botnets Conventional wisdom suggests that the majority spam on the Internet today is sent by botnets. Collections of machines are acting under one centralized controller. The W32/Bobax (Bobax) worm (of which there are many variants), exploits the DCOM and LSASS vulnerabilities, allows the infected hosts to be used as a mail relay. It attempts to spread itself to other machines affected by the above vulnerabilities over email. Agobot and SDBot are two other bots purported to send spam.

Direct spamming Spammers often purchase upstream connectivity from spam-friendly ISPs which turn a blind eye to the activity. Occasionally, spammers create connectivity and send spam from ISPs that do not condone these ac-problems in these cases, spammers sometimes obtain a pool of dialup IP addresses, send outgoing traffic from the high bandwidth connection, and proxy the reverse traffic through the dialup connection back to the spamming hosts.

BGP spectrum agility This paper exposes a new type of cloaking mechanism –BGP spectrum agility. Whereby spammers briefly announce (often stolen) IP address space from which they send spam and withdraw the routes to that IP address space once the spam is sent, in order to remain untraceable. Although anecdotal evidence has suggested that spammers may use this technique. The study on this paper finds that spammers may be using spectrum agility to complement spamming by other methods. It documents several interesting cases of this activity.

Open relays and proxies Some SMTP servers will allow any client to connect to it for the purposes of sending email. Originally intended for convenience purposes (*e.g.*, to let users send mail from a particular SMTP server while traveling or otherwise in a different network), open relays were readily exploited by spammers because the layer of indirection allowed them to remain untraceable. It would appear that the widespread deployment and use of blacklisting techniques have all advantages but extinguished the use of open relays to send spam.

V. Forgery Properties Of Spam Delivery Paths

It is well known that spammers can forge the header of an email, in particular an attempt to hide the true origin of the email. Despite its critical importance for spam control there has been no study on the forgery behavior of spammers. In this paper [4], the first comprehensive study on the Received header fields of spam emails to investigate the degree of spammers can and do forge the trace information of spam emails has been studied. To ease exposition, in this paper all categories of unwanted emails as spam emails (including, for example, spam, phishing emails, and email based extortion and threats) and senders of these emails as spammers are being referred. The spammers' ability to forge email headers often complicates the spam control efforts and makes it hard to hold accountable the true originators of spam. This presents a great challenge for law enforcement to properly investigate and prosecute email-based criminals. On the other hand, despite its critical importance for spam control and holding accountable the true originators of spam, there has been no systemic study on the forgery behavior of spammers, except anecdotal evidence of spam header forgery. In this paper we provide the first comprehensive study on the forgery behavior of spammers. Given the importance of the trace information carried in the Received: header fields in the investigation of the true origin of a spam email, in this paper effort on the Received: header fields of spam emails to investigate the degree of spammers *can and do* forge the trace information of spam emails are being concentrated.

VI. Wald's Sequential Analysis For Time-Constrained Vision Problems

In computer vision, both classification errors and time to decision making characterize the quality of an algorithmic solution. To formalize such problems in the framework of sequential decision making and derive quasi-optimal time-constrained solutions for three vision problems have been shown in this paper [5]. The methodology is applied to face and interest point detection and to the RANSAC robust estimator. In the interest point application, the output of the Hessian-Laplace detector is approximated by as sequential WaldBoost classifier which is about five times faster than the original with comparable repeatability. A sequential strategy based on Wald's SPRT for evaluation of model quality in RANSAC leads to significant speed-up in geometric matching problems.

This is especially true for applications such as robotics where real-time response is typically required. Time-constrained classification, detection and matching problems can be often formalized in the framework of sequential decision-making. We show how to derive quasi optimal time-constrained solutions for three different vision problems by applying Wald's sequential analysis. In particular, Wald's sequential probability ratio test (SPRT) apply it to the three vision problems:(i) face detection (ii) real-time detection of distinguished regions(interest points) and (iii) establishing correspondences by the RANSAC algorithm with application e.g. In SLAM,3D reconstruction and object recognition. RANSAC (Random Sample Consensus) is a robust estimator that has been used in many computer vision algorithms e.g. for short and wide baseline stereo matching and estimation of structure and motion. In the time-optimal RANSAC, the fastest randomized strategy for hypothesis verification satisfying a constraint on the probability that the returned solution is correct. The optimal strategy is found again with the help of Wald's SPRT test.

VII. An Effective Defense Against Email Spam Laundering

Laundering email spam through open-proxies or compromised PCs is a widely-used trick to conceal real spam sources and reduce the cost of spamming in underground email spam industry. Spammers plague the Internet by exploiting a large number of spam proxies. The facility of deterring spamming activities close to their sources, which would greatly benefit not only email users but also victim ISP's is in great demand. In this paper [6], one salient characteristic of proxy-based spamming activities, namely packet symmetry, by analyzing protocol semantics and timing causality is revealed. Based on the packet symmetry exhibited in spam laundering, a simple and effective technique DBSpam to on-line detect and break spam laundering activities inside a customer network is proposed. DBSpam utilizes a simple statistical method, Sequential Probability Ratio Test, by monitoring the bi-directional traffic passing through a network gateway to detect the occurrence of spam laundering in a timely manner. To balance the goals of promptness and accuracy, a noise-reduction technique in DBSpam, after which the laundering path can be identified more accurately, has been introduced. Then, DBSpam activates its spam suppressing mechanism to break the spam laundering.

The implement a prototype of DBSpam based on libpcap, and validate its efficacy through both theoretical analyses and trace-based experiments. To break this spam laundering, we propose a simple and effective mechanism, called DBSpam, which detects and blocks spam proxies' activities inside a customer network and further traces the corresponding spam sources outside the network. DBSpam is designed to be placed at a network vantage point such as the edge router or gateway that connects a customer network to the Internet. The customer network could be a regional broadband (cable or DSL) customer network, a regional dialup network, or a campus network. It detects ongoing proxy-based spamming by monitoring bidirectional traffic. Due to the protocol semantics of SMTP and timing causality, the behavior of proxy-based spamming demonstrates the characteristics of connection correlation and packet symmetry. Utilizing this unique spam laundering behavior, it is easy to identify the suspicious TCP connections involved in spam laundering. Then, trace the spam sources behind the spam proxies, and block the spam traffic. Based on libpcap, we implement a prototype of DBSpam and evaluate its effectiveness against email spam laundering through theoretical analyses and trace-based experiments.

First, DBSpam pushes the defense line towards spam sources. DBSpam enables an ISP (Internet Service Provider) to on-line detect spam laundering activities and spam proxies inside its customer networks. The quick responsiveness of DBSpam offers the ISP an opportunity to suppress laundering activities and quarantine the identified spam proxies.

Second, DBSpam has no need to scan message contents, and has very few assumptions about the connections between a spammer and its proxies. DB Spam works even if (1) these connections are encrypted and the message contents are compressed; and (2) a spammer uses proxy chains inside the monitored network.

CONCLUSION

With cloud computing, the necessary action needs to take place to the interface between service suppliers and multiple groups of service consumers. Although cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the internet, there is much to be cautious about its issues in security. There are various emerging technologies at a rapid rate, each with technological advancements and with the potential of making human lives' easier. In this paper, the considerations and challenges in key security which are currently faced in Cloud computing are highlighted. Cloud computing has the potential ability to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

REFERENCES

[1] Carlo Marcelo Revoredo da Silva,Jose Lutiano Costa da Silva, Ricardo Batista Rodrigues, Leandro Marques do Nascimento, Vinicius Cardaso Garcia, "Systematic Mapping Study on Security threats in Cloud Computing", International Journal of Computer Science and Information Security(IJCSIS), Vol. 11, No. 3, March 2013.

[2] Martin R. Stytz, Ph.D. Sheila B. Banks, Ph.D., "Cyber Warfare Simulation to prepare to control cyber space".

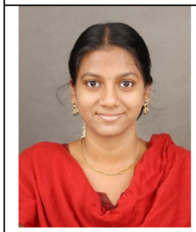
[3] Anirudh Ramachandran and Nick Feamster, College of Computing, Georgia Tech, "Understanding the Network-Level Behavior of Spammers", SIGCOMM'06 ACM, Pisa, Italy, 2006.

[4] Fernando Sanchez, Zhenhai Duan, Yingfei Dong , Florida State University "Understanding Forgery Properties Of Spam Delivery Paths" , Seventh annual Collaboration, Electronic messaging, Anti-Abuse and spam Conference July 13-14, 2010, Redmund, Washington, US.

[5] Jiri Matas, Jan Sochman, "Wald's Sequential Analysis For Time-constrained Vision Problems" , Springer US, Unifying Perspectives in Computational and Robot Vision Volume 8, 2008, pp 57-77.

[6] Mengjun Xie, Heng Yin, Haining Wang, Department of Computer Science, The College of William and Mary, Williamsburg, VA 23187, "An Effective Defense Against Email Spam Laundering", CCS'06 ACM , Alexandria, Virginia, USA, 2006.

AUTHOR'S PROFILE

	T.THIRUNAVUKARASU He received the M.E degree in the specialization of computer Science Engineering from Sona College of Technology, Salem on 2010 under Anna University Coimbatore. Now he is Working as a Assistant Professor, Department of Information Technology in SNS College of Technology, Coimbatore-35.
	**M.JUDITH LUCIA** She received the B.E degree in the specialization of Computer Science Engineering from Velammal College of Engineering and Technology under Anna University. Now she is currently pursuing post graduation (M.E) in Department of Information Technology, SNS College of Technology, Coimbatore-35.