Monitoring Cyber Attacks and Analysis of Breaches

Anup S Kumar, N.R. Sathish Kumar, Arun Das, Shubam, S.P. Mani Raj

Abstract--- Analyzing cyber incident data sets is an important method for deepening our understanding of the evolution of the threat situation. In present generation we come to know about many cyber breaches and hacking taking place. In this paper work, we research about the various cyber-attacks and breaches and study the way these attacks are done and find an alternative for the same. We show that rather than by distributing these attacks as because they exhibit autocorrelations, we should model by stochastic process both the hacking breach incident inter-arrival times and breach sizes. We draw a set of cyber securities insights, including that the threat of cyber hacks is indeed getting worse in terms of their frequency.

Index Terms--- Hacking, cyber-attacks, cyber threats, breach prediction, times series, cybersecurity data analytics.

I. INTRODUCTION

An information rupture is a security occurrence in which delicate, ensured or secret information is duplicated, transmitted, saw, stolen or utilized by an individual unapproved to do as such." An information break is the purposeful or accidental arrival of secure or private/classified data to an untrusted domain. Different expressions for this marvel incorporate inadvertent data divulgence, information spill and furthermore information spill. This may incorporate occurrences, for example, robbery or loss of advanced media, for example, PC tapes, hard drives, or smart phones such media whereupon such data is put away decoded, posting such data on the internet or on a PC generally available from the Internet without legitimate data security safeguards, exchange of such data to a framework which isn't totally open yet isn't fittingly or formally authorize for security at the affirmed dimension, for example, decoded email - or exchange of such data to the data frameworks of a conceivably unfriendly office, for example, a contending organization or a remote country, where it might be presented to increasingly serious unscrambling strategies. While mechanical arrangements can solidify digital frameworks against assaults, information breaks keep on being a major issue. This propels us to describe the development of information rupture occurrences. This not exclusively will profound our comprehension of information breaks, yet in addition shed light on different methodologies for relieving the harm, for example, protection. Many trust that protection will be valuable, however the advancement of accurate cyber hazard measurements to control the task of protection rates is past the compass of the present comprehension of information breaks In this paper, we make the accompanying commitments. We shoe that as opposed to by circulating the ruptures we should demonstrate by stochastic procedure both the hacking break occurrence entomb entry times and rupture sizes. We demonstrate that these stochastic procedure models can foresee the between landing times and the rupture sizes. To the best of our knowledge, this is the primary paper appearing stochastic procedures, instead of circulations, ought to be utilized to show these digital danger factors. We demonstrate that the reliance between the episode's entry time and the break sizes can be satisfactorily depicted by a specific copula. This the primary work demonstrating the presence of this reliance and the results of disregarding it. We additionally demonstrate that it is important to consider the reliance while foreseeing entomb entry times and break sizes generally the outcomes are not accurate. We hope the present study will inspire more investigations, which can offer deep insights into alternate risk mitigation approaches. Such insights are useful to insurance companies, government agencies, and regulators because they need to deeply understand the nature of data breach risks. We hope the present study will inspire more investigations, which can offer deep insights into alternate risk mitigation approaches. Such insights are useful to insurance companies, government agencies, and regulators because they need to deeply understand the nature of data breach risks.

II. LITERATURE SURVEY

The nature of the system breaches and the attacks on the system affects the state of operation and working of the system. A system may incur active or passive attack which makes the whole system collapse. When a system is attacked, the data security is breached and all the information contained in the system are hacked or obtained by the hacker in the successful attack. When a system is under attack and if the access to the system is granted, all the potential information will be lost or damaged depending on the intention of the attacker

System States & Cyber-attacks

In order to know the details of the current state of the system, the changes that are made by the cyber attacks must be analysed and the ways in which system has experienced the attack with respective to the changes to the operating system.

Manuscript received February 01, 2019

Anup S Kumar, UG Scholar, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India. (e-mail: anupdx@live.com)

N.R. Sathish Kumar, UG Scholar, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India. (e-mail: sathishkumarnr14@gmail.com)

Arun Das, UG Scholar, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India. (e-mail: nurasad96@gmail.com)

Shubam, UG Scholar, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India. (e-mail: sericsheon@gmail.com)

S.P. Mani Raj, Assistant Professor, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India. (e-mail: spmaniraj@gmail.com)

The purpose and intention of the attacker is to intrude into the system and gain unauthorized access to the system or the information and the resources contained in the system under attack. A malicious code will be sent to the system without the knowledge of the system's owner which can be able to write or transmit the data from the system to the attacker's system through which he can exploit its resources

Contemporary Attacks

These types of attacks are carried out in order to gain elevated or higher access privileges. Through the cotemporary attacks ,the attacker can gain administrative privileges of the system under attack. Any modification, changes that are intended by the attacker can be carried out at once he has access to the administrative privileges of the system. The third type of the cotemporary attack can make the system in operable and isolate the system by flooding the information and data contained in the system .This will make the system unresponsive the administrative privileges. The system will respond to the attacker rather than the owner of the system

Determining the breach probability

By comparing the statistics of the attacks in the past on the system and similar type of attacks across the world and the respective models are taken into account for determining the probability of the attacks across the system .Analyzing the breach probability is an important objective for the system security and protection. It analyses the attacks that succeeded inspite of the different counter measures taken by the system administrator and it assess the risks and threats that are posed by the cyber attacks. If the counter measures are involved during the cyber attack then the overall breach probability will be able to compute the breach probability.

Determining the Access Matrix

We can identify the nature of the access granted to the system to an attacker by listing the attack matrix and the access matrix is determined by coupling with the task of the attack matrix. The privileges that are granted to the attacker are enlisted in the form of matrix and the different types of attacks that are made to breach the security of the system and the combination of the modality is listed in the access matrix

Advanced Persistent Threat

An attack in a network in which a person extracts a network and access important and highly confidential information rather than doing any actual damage to the network or an organization.

III. SECURITY ISSUES

Due to these various breaches and cyber attacks that take place in various systems this has led to a significant financial loss as these hackers stole account information and breach security to relocate money to their account. These threats can range from small losses to an entire information loss. These threats can affect at various levels also like some affect confidentiality of data and others affect the entire system. Many people and organisations are struggling to understand what sought of breach or threat has occurred to their systems and how can they protect their information from such other attacks causing massive losses. There are various types of attackers that attack in different methods. Some such attackers are briefed below.

Bot-network Operators

Bot-network operators are hackers that penetrate into the networks. They do so to take over multiple systems. Like this the whole organisation can be brought down and malicious attacks can be executed. These network services are made available to shady markets and hence can be misused.

Criminal Groups

These group of people or hackers attack the systems for getting financial profits. Different groups use various ways tod a malicious attack and acquire all the confidential information to commit identity theft and online fraud.

Hackers

These group of people breach into systems to challenge or for bragging rights. This requires a good skill or computer knowledge to breach into the systems or securities. They pose a high threat causing massive damage world-wide. Once they understand the algorithm to crack the security of any site then they can do anything they want to the system.

Insiders:

These are the people who are already working inside the organisation. They have all the liberty to access to the system, hence they can easily understand the system and can use it for their own use. They can steal crucial information. The insider threat also includes outsourcing of data and inception of malware into systems.

Phishers

Phishers are groups that use the phishing scheme so that they can steal information for own financial profit. They may also introduce divers' ways as spam in pursuance of their objectives.

IV. WORKING

The main aim of this paper is to find the breach and the frequency of the breach. There are following algorithms for the detection of the breach.

Algorithm for Predicting the VaR_α's of the Hacking Incidents Inter-Arrival Times and the Breach Sizes Separately

Input: Historical incidents inter-arrival times and breach sizes, denoted by $\{(d_{ti}, y_{ti})\}i=1,...,m+n$, where an in-sample $\{(d_{ti}, y_{ti})\}_{i=1,...,m}$ as mentioned above was used for fitting and an out-of-sample $\{(d_{ti}, y_{ti})\}_{i=m+1,...,n}$ is used for evaluation prediction accuracy; α level.

1. for i =m+1,⋯,n do
2. Estimate the $LACD_1$ model of the incidents inter-arrival times based on $\{d_s|s =1,……,i -1\}$, and predict the conditional mean
   i =exp(ω+a1 log(i−1)+b1 log(i−1));

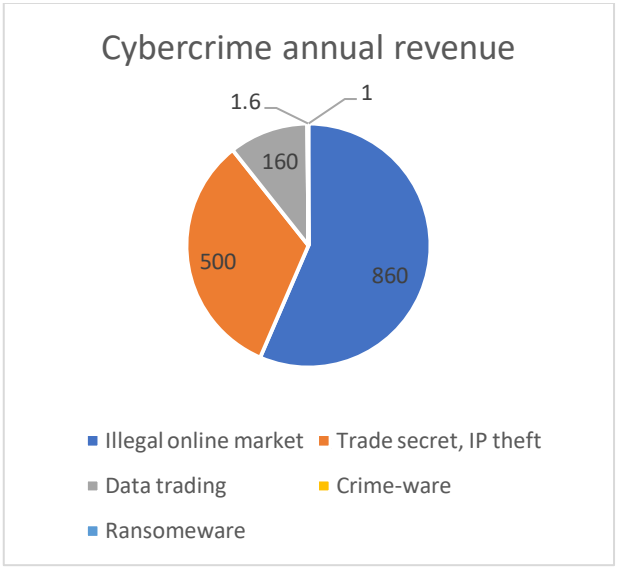
3. Estimate the ARMA-GARCH of log-transformed size, and predict the next mean μ_i and standard error σ_i;
4. Select a suitable Copula using the bivariate residuals from the previous models based on AIC;
5. Based on the estimated copula, simulate 10000 2-dimensional copula samples $(u^{(k)}_1,i,u^{(k)}\ 2,i)$
   k =1,...,10000;
6. For the incidents inter-arrival times, convert the simulated dependent samples $u_1^{(k)}$ into the $z^{(k)}$,i's by using the inverse of the estimated generalized gamma distribution,
   k =1,...,10000;
7. For the breach sizes, convert the simulated dependent samples $u^{(k)}$,i's into the $z_2^{(k)}$,i's by using the inverse of the estimated mixed extreme value distribution,
   k =1,...,10000;
8. Compute the predicted 10000 2-dimensional breach data $d_i^{(k)}$,$y_i^{(k)}$,
   k =1,...,10000
9. Compute the VaR_α's ,$d^{(i)}$ for the incidents inter-arrival times and VaR_α's ,$y^{(i)}$ for the log-transformed breach sizes based on the simulated breach data.
10. if $d_i^{(k)}$>VaR_α's ,$d^{(i)}$ then
11. A violation to the incidents inter-arrival time occurs;
12. end if
13. if $y_i^{(k)}$>VaR_α's ,$y^{(i)}$; then
14. A violation to the breach size occurs;
15. **end if**
16. end for

Output: Numbers of violations

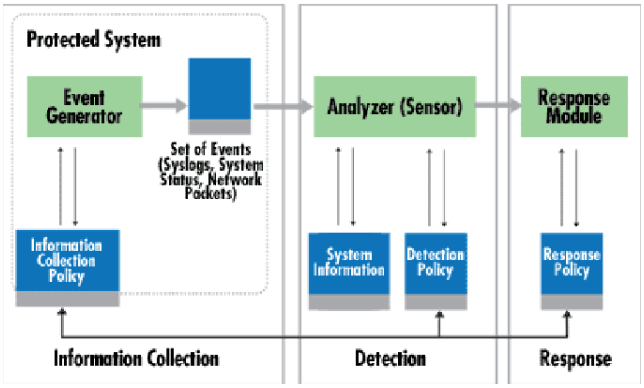
Interarrival times and breach sizes.

Insight suggests that we model the hacking breach incidents inter-arrival times with an autoregressive conditional mean (ACD) model, which was originally introduced to model the evolution of the inter-arrival time, or duration, between stock transactions and later extended to model duration processes

V. GLOBAL MARKET ANALYSIS



Crime	Annual Revenues
Illegal online markets	$860 Billion
Trade secret, IP theft	$500 Billion
Data Trading	$160 Billion
Crime-ware	$1.6 Billion
Ransomware	$1 Billion
Total cybercrime Revenues	$1.5 Trillion



Architecture Diagram

As shown in the above figure firstly an event (such as establishment of network connection occurs) then a set of these events are passed through the analyzer. The analyzer then uses the system information and the specified detection policy to analyze the event, on the basis of this analysis a response is generated via response module which uses response policy to generate the response. In case a potential threat is detected the system alerts the user by notifying them saying threats found.

VI. CONCLUSION

The widespread of ordinary data breaches around the world demonstrates how real the danger of critical infrastructure attack As the hackers increase in terms of sophistication and technical expertise, and as the critical information infrastructure becomes more massive and intricate, it is more vulnerable to attack. We can treat them like an act of terrorism which justifies action under the Internal Security Act. If we take this path, we must be prepared of the consequences. What is more compelling is the need to strengthen the security of the CII itself. As illustrated in this article, a multi-prong action is required; one that involves a mixture of technology, competency of manpower, prudence and effective legal framework. At this end, it is note-worthy that there are few areas emerged from this initial study that can be made an agenda of future direction. Firstly, from the technical perspective, there is a need to assess new methods that threaten the security of critical information infrastructure. Secondly, from the perspective of law and policy, governments need to ensure that each sector identified as critical infrastructure should be properly protected both by legal and policy instruments. Further research is required to analyse the comprehensive legal landscape that aim to protect the critical information infrastructure, involving all enabling laws from all sectors.

FUTURE SCOPE

The internet is not safe without the proper knowledge of it's working. The study on cyber hacking breaches and various attacks helps the server to maintain the quality of the service provided to the customers. It will also make sure that the data on a server or on a PC is safe. The sooner the breach is detected; we can cease further damage to the data or we can avoid data compromising. The frequency of the attack can be derived from the inter arrival time and this allows us to find what the hacker wants to derive from the server.

The future of internet is not safe at all, the amount of hackers everyday is rising. So the study and algorithms helps us to understand and avoid the misuse of data to the unknown.

REFERENCES

1. P. R. Clearinghouse. Privacy Rights Clearinghouse's Chronology of Data Breaches. Accessed: Nov. 2017. [Online]. Available:https://www.privacyrights.org/data-breaches
2. ITR Center. Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout. Accessed: Nov. 2017. [Online]. Available: http://www.idtheftcenter.org/ 2016databreaches.html
3. Leigh and L. Harding, Wikileaks: Inside Julian Assange"s war on secrecy. US: Guardian Books, 2011.
4. Ming-Chien Yang and Ming-Hour Yang April(2012),"RIHT: A Novel Hybrid IP Scheme," IEEE Transactions on Information Forensics and Security vol. 7
5. C. Gong and K. Sarac, "Toward a practical packet marking approach for IP traceback," Int. J. Network Security, Mar. 2009.
6. Baumgärtner L., Strack C., Hoßbach B., Seidemann M., Seeger B., and Freisleben B. (2015)., "Complex event processing for reactive security monitoring in virtualized computer systems", In Proceedings of the 9th ACM International Conference on Distributed Event-Based Systems (DEBS '15). ACM, New York, NY, USA, 22-33.
7. Seymour E. Goodman and Herbert S. Lin, editors. Toward a Saferand More Secure Cyberspace. National Academies Press, 2007
8. D. Howard and K. Prince, Security 2020: Reduce security risks this decade. US: Wiley, 2010.
9. Dmitrieva, "Stealing information: Application of a criminal anti theft statute to leaks of confidential government information," 55 Fla. L. Rev. 1043.