International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Survey on Identification of Hacker by Trapping Mechanism

C. Ramprasath
UG Student, Department of Computer Science & Engineering, Easwari Engineering College Tamil Nadu, Chennai

J. Varun
UG Student, Department of Computer Science & Engineering, Easwari Engineering College Tamil Nadu, Chennai

Ms S. SriHeera
Assistant Professor, Department of Computer Science & Engineering, Easwari Engineering College Tamil Nadu, Chennai

ABSTRACT

Advanced persistence threat (APT) attack is to steal data rather than to cause damage to the network or organization. It is one of the initial phases in successful hacking of a system. Here, user's behaviour is analysed based on previous behaviour such as posted data, time of posting, IP address and location of usage of social network. This system includes two processes. The Social network accounts are analysed, tracked and then detected. If the hacker attacks the original user's account, then the system allows the attacker to proceed further until our system captures all the important information about the attacker by directing the hacker to the fake website. The system generates Honeywords based on the user information provided and the original password is converted into another format and stored along with the honeywords. Attacker who knows the E-mail account of original user can easily reset the password of the cloud server. When the attacker tries to login into the purchase portal, he/she is tracked and allowed to do purchase. Server identifies the attacker and sends an alert message to the owner and blocks the attacker from doing transaction from his original account.

Keywords: *Cloud security; Hacker; Honeywords; Sentimental Analysis; Social Networks*

Introduction

Sentimental Analysis:

Sentimental analysis is the process mainly used to predict the emotions based on the content of the text, which may be positive, negative or neutral. It is also known as data mining, deriving the view or attitude of a speaker. Sentimental analysis is mainly based on machine learning where the system classify the emotions and opinions of the humans based on the content, which may be a text or voice. The sentimental analysis predicts the emotions based on the understanding of the opinions and content of the social data given by the user. Sentimental analysis is enormously used because it gives an abstracted view about the public opinions about certain topics or emotions. Social media monitoring tools make that process faster and easier than ever before. The ability or skill to get an understanding about the detailed view of data used in social networks is widely used in lot of enterprises. The changes that have been shown in social media have been similar to that of the changes that have been shown in stock markets. The human language is complex. It's tedious to teach a machine to analyse the various grammatical shades, cultural variations, slang and misspellings that occur in online mentions.

Honeyword

Honeywords are sequence of characters that are generated by humans that look like a password. Honeywords are proposed as part of honeypot, so that any intruder attempting to log in with the password may be assumed to be an attacker. Hackers these days create automata that produce sequence of possible passwords. Some hackers perform a weighted random walk against a PCFG grammar that was trained on

real human generated passwords. In this approach, first a probabilistic context free grammar, (PCFG), is trained on a set of passwords that you want the honeywords to resemble. Next, the honeywords are produced by performing a random walk along the grammar. The (P) in PCFG stands for "probability". This means for each transform in the PCFG a random number is generated, and a transform is chosen based upon that random number and the weighted probability of a transform. For example, if the grammar contains the transform S-> 'word' + '132' and that transform has a probability of 90%, then on average around 90% of the generated honeywords will end with '132'.

Cloud Security

Cloud computing security is a service that includes protecting critical information from theft, data leakage and deletion. One of the benefits of cloud services is that you can operate at scale and remain secure. It proposes how to manage security and different ways of delivering security solutions that address new areas of concern. Cloud security does not change the approach on how to manage security from avoiding to detective and corrective actions. Client requests from the service provider server occurrence and enters most settings and choose the operating system. Then clients determine the size and other settings needed that allows them accessing the cloud and using the applications they requested. After a period, if they needed more space, they enter the accounts in the cloud and increase time in seconds to get over a larger space area.

Literature Survey

[1] The paper proposes a mechanism called Advanced Persistent threats [APT] along with Socialbots. The reconnaissance phase permits the attacker to find an entry gateway into the association leading to the next phases. The main objective is to gain knowledge about the deployment process, creation, and management of the social honeypots, as well as their efficiency and security enhancements.

[2] It uses Openstack in Cloud handling. OpenStack consists of a set of open-source projects which provide a variety of services for an IaaS model. Its five main projects deliver basic functionalities that are required for a cloud infrastructure and mainly produce secured enhancements in cloud

[3] The paper uses COMPA to detect malicious messages before they were posted, avoiding the fake information to spread. Paper applies COMPA to two datasets from popular social networks, Facebook and Twitter, and show that our system would have been able to detect compromised accounts. It also shows that COMPA would have been able to detect four high profile negotiations that affected popular Twitter accounts.

[4] There are mainly four factors related to user authentication: authentication by something user knows (e.g., password), authentication by something user has (e.g., physical token), authentication by something the user is (e.g., biometric authentication) and authentication by someone user knows. Among these four factors of authentication techniques, password-based authentication is widely accepted for its simple login functionality and ease of memorability.

[5] This system speaks about the security intensity of the user passwords. It uses techniques like Chaffing-by-tweaking, Chaffing with “toughnuts”, Chaffing-with-a-password-model for the analysis of the obtained passwords. Also, the security mechanisms like Denial of service attack, brute force attack. To enhance the previous system, a login system with honeychecker is used.

[6] The paper proposes a set of behavioural features of online social networking users that can characterize the activities of the users on social networking sites. The user’s behaviour is characterized into two classes introvertive and extroversive behaviour. The user behaviour is mainly analysed to detect the compromised accounts based on the pattern of the content given by the user.

[7] The system uses a browser on the network through which the foreground tourists can receive the user registration, login, view merchandise information, browse the site news, etc. with the user registration module, the user login module, the news-browsing module and the product-browsing module. The login users can manage personal information, purchase, view and modify individual orders, review products, initiate complaints etc. with the personal information n management module, the purchasing module, the private order management module, the commodity comments module, and the customer grievance module.

[8] It focuses on spam detection using personal characteristics rather than the reviews as reviews

shall not be trustworthy. This work uses geographical location and the IP address of the device with which he/she is accessing different resources on Internet. In addition, a content analysis method to attack non-reviews using spam dictionary is also proposed.

[9] The paper mainly proposes the strategies to control the eccentricity of the social networking sites based on the behaviour of the context given by the driver nodes. It assumes a set of agents and a set of subjects to be specified. Each agent has a certain level of interest and skill on each subject and both constraints could change when intermingling with other agents.

[10] The datasets are created using various techniques like data collection, labelling, transformation, and sharing. Supervised machine learning algorithm is proposed to obtain the result from the result. But various issues arise in relation to collection bias, imprecise and irreproducible labelling, incomprehensible origin of adjunct datasets, imprecise portrayal of features extraction and data transformation, and finally, complete or partial unavailability of raw and final datasets used to build statistical decision models.

S.No	Title	Author Name	Publication Journals/Date	Algorithm
1.	Data Quality Challenges in Social Spam Research	Nour EI-Mawass and SaadAlaboodi	2017 ACM Journal of Data and Information Quality (JDIQ)	Supervised Learning
2	A Novel User-based Spam Review Detection	Simran Bajaj*, NiharikaGarg and Sandeep Kumar Singh	Information Technology and Quantitative Management (ITQM2017) Elsevier Journal	Spam review detection rule, Non-review detection rule
3	Handling compromised components in an IaaS cloud installation	Aryan TaheriMonfared1* and Martin Gilje Jaatun2	Journal of Cloud Computing: Advances, Systems and Applications, Springer 2016	Cloud computing,OpenStack,Spam detection rule,Queue
4	Towards Improving Storage Cost and Security Features of Honeyword Based Approaches	NileshChakraborty*, SamratMondal	6th International Conference on Advances in Computing & Communications, ICACC 2016	hidden markov chain model,modeling-syntax-approach
5	Achieving Flatness: Selecting the Honeywords from Existing User Passwords	Imran Erguler	IEEE Transactions on Dependable and Secure Computing	Generator Algorithm,Honeychecker
6	Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks	Abigail Paradise, AsafShabtai, Rami Puzis, AviadElyashar, Yuval Elovici, MehranRoshandel, and ChristophPeylo	IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS 2017	Open Source INTelligence (OSINT) tools,HoneyGen

7.	Controllability of social networks and the strategic use of random information	Marco Cremonini and Francesca Casamassima	Computational Social Networks (2017)Springer	Networks metrics and Diffusion metrics.
8.	Design and Implementation of the Online Shopping System	Guoyong Zhao and Zhiyu Zhou	Springer-Verlag Berlin Heidelberg (2012)	Management information system, Model View Controller pattern
9.	Profiling Online Social Behaviors for Compromised Account Detection	XinRuan, Zhenyu Wu, Member, IEEE, Haining Wang, Senior Member, IEEE, and SushilJajodia, Fellow, IEEE	IEEE Transactions on Information Forensics and Security (Volume: 11, Issue: 1, Jan. 2016)	Honeypot accounts,Extroversive and IntroversiveBehavior

Conclusion and Future Enhancements

When it comes to data there must be more security and features so that the confidentiality of the information is preserved. In order to overcome the user's data, the security systems should be enhanced. However, the attacker must be identified to stop further cybercrime. The three parts that are provoked to attacks are hardware, software and data. Among these data is the only part, which is more susceptible to vulnerabilities. So in future, countermeasures must be taken to protect data and a lot of importance must be given to single vulnerabilities.

REFERENCES

1. Abigail Paradise, AsafShabtai, AviadElyashar, ChristophPeylo, MehranRoshandel, Rami Puzis and Yuval Elovici, "Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks", IEEE Transactions on Computational Social Systems (2017)
2. Aryan TaheriMonfared and Martin GiljeJaatun, "Handling Compromised Components in an IaaS Cloud installation", Journal of Cloud Computing (2016 Springer)
3. Christopher Kruegel, GianlucaStringhini, Giovanni Vigna and Manuel Egele ,"Towards Detecting Compromised Accounts on Social Networks",IEEE Transactions on Dependable and Secure Computing (2017)
4. Francesca Casamassima and Marco Cremonini, "Controllability of social networks and the strategic use of random information", Computational Social Networks (2017 Springer)
5. Guoyong Zhao and Zhiyu Zhou, "Design and Implementation of the Online Shopping System", Springer-Verlag Berlin Heidelberg (2012)
6. Haining Wang, SushilJajodia, XinRuan and Zhenyu Wu, "Profiling Online Social Behaviors for Compromised Account Detection", IEEE Transactions on Information Forensics and Security (2016)
7. Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords", IEEE Transactions on Dependable and Secure Computing (2017)
8. Niharika Garg, Sandeep Kumar Singh and Simran Bajaj, "A Novel User-based Spam Review Detection", Information Technology and Quantitative Management (2017 ITQM)
9. Nilesh Chakraborty and Samrat Mondal, "Towards Improving Storage Cost and Security Features of Honeyword Based Approaches",6th International Conference on Advances in Computing & Communications, (2016 ICACC)
10. Nour EI-Mawass and SaadAlaboodi, "Data Quality Challenges in Social Spam Research", (2017 ACM Journal of Data and Information Quality (JDIQ))