ISSN No. 0976-5697

Volume 5, No. 7, September-October 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Artificial Immune System to Protect Social Network

Rajneeshkaur K. Bedi,Oshin Kavdia,Gauri Bhide,Vaidehi Donglikar
Computer Department,MIT College Of Engineering,
Pune,India

***Abstract*—** Social networking web sites are more popular than ever in recent years. The popular usage of these web sites greatly impacts user data privacy and security. Data privacy is owner's right to determine when, how and to what extent their information is provided to outside world. But nowadays many people face the problem of their data being misused by third parties. The goal of an attacker is to obtain knowledge of a significant level to get entry in network. In this case, security has been breached because the privacy of the user had not been safeguarded. This paper intends to give new approach to safeguard user data privacy and security through bio inspired computing wherein inspiration is drawn from the natural world to give better security to user accounts. A social network Intrusion Detection System is proposed to monitor networks for attacks or intrusions and report these intrusions to the root node in order to take corrective action. Immune system techniques, particularly the innate and adaptive immune systems have been studied and an attempt has been made to apply these methods to protect a user within a network. Even though some of these solutions might not seem feasible in today's times, they will provide an alternative way to protect users and may also prove to be better than current solutions in the near future.

***Index terms*-** Social network, Immune system, Data security, Intrusion detection

I. INTRODUCTION

As defined by [1] SNS or social networking site is an online service, platform that focuses on building and reflecting of social networks or social relations among people, who, for example, share interests and/or activities. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. They provide means for users to interact over the Internet. People from all age groups, community, nations with vide variety in education and social differences are the part of SNS. As per the survey conducted by various communities we can conclude that the users on these sites are more than populations of some countries.

Various data is collected on these sites which are broadly classified into categories: private, educational, and professional data. Private data can be name, age, blood groups, relationship, pictures to name a few. Educational and Professional data can be his/her resume, places/institutes where education was acquired, designation of person, current employer company name etc. It is up to the users view point to distinguish as private or public data, as an SNS doesn't provide any hardcore rules to categories the data.

Database level protection techniques are available like, auditing, encryption, backups or network based security like firewall, but they lag in providing protection due to their methodology of protection. First, the methodology is reactive[4]: reaction starts when there is already an intrusion in progress. Many SNSs provide default privacy settings which do not meet the user's requirements and this can be misused by anyone. For example, by default all photos uploaded are public in nature and many times users are unaware of these settings. In case of any misuse or damage done, it comes to light after it takes place. Second, there is no learning mechanism [4] to study and learn about intrusions and provide protection against the same intrusion to the rest of the network. Even if the damage has been taken care of, there isn't any provision of how this intrusion occurred in the user's profile in the first place. There is no provision of keeping such tracking records. Third, there are no preventive measures [4] taken against foreseeable threats that can turn into intrusions based on existing vulnerabilities, which become the cause of zero-day attacks. In an SNS, even though all the protection measures are applied on the database, the vulnerabilities still lie at the hands of the user because he/she has the option of sharing his/her data with others. Therefore no matter how much encryption or firewalls are applied at the database level, once the user decides what matter is going to be public then even these preventive measures cannot stop anyone from accessing the public data. To overcome these problems we are taking inspiration from the human immune system which has got a foolproof method for detecting and doing away with the harmful cells from the body.

II. BACKGROUND KNOWLEDGE

Before going to the artificial immune system let us first understand the biological immune system a little bit with the explanation given in [6] simple for everyone to understand. The biological immune system has multiple levels of defense. The first layer of defense has a simple purpose - prevent pathogens (infectious agents) from entering the body in the first place. This level includes the skin, which is impenetrable to most pathogens, and bodily secretions, such as saliva, which have antibiotic properties. If a pathogen manages to breach these barriers and enter the body, it is next met by the innate immune system. The innate immune system can tell the difference between the self and the foreign - that is, cells that are part of the body and those that are not. Foreign intruders that trigger an immune response are called antigens. The innate immune response involves a multitude of different cellular defenders that can destroy or devour antigens. Some of these defenders, which are called antigen presenting cells (APCs), keep samples of the antigens they consume, and present them to the last, most advanced level of defense - the adaptive immune system, in which the body learns the new attacking virus' properties

and features in the first attack and stimulates the body to produce proteins that will attack the virus if detected in the future.

AIS [6] is a class of computationally intelligent systems inspired by the principles and processes of the immune system in vertebrates. The algorithms typically exploit the immune system's characteristics of learning and memory to solve a problem. The biological immune system is a highly parallel, distributed, and adaptive system. It uses learning, memory, and associative retrieval to solve recognition and classification tasks. In particular, it learns to recognize relevant patterns, remember patterns that have been seen previously, and constructs pattern detectors efficiently. These remarkable information processing abilities of the immune system provide important aspects in the field of computation [7].

The following features of the immune system are important and can applied in information security systems [4] which we will be focusing in our future work, partially:

- ***a.*** ***Distributed*** **–** The T-cells and B-cells can detect global coordination. In this work we model this feature by having Mobile Agents act as cells in Vulnerability Analysis System (VAS), Intrusion Detection System (IDS) and Intrusion Response System (IRS).
- ***b.*** ***Multi-layered*** **–** The immune system has multiple defense layers, defense in depth.
- ***c.*** ***Diversity*** **–** with diversity, vulnerabilities in one system are less likely to be wide spread. Diversity could be provided by having agents doing a variety of functions; autonomy – the immune system does not require outside maintenance or management.
- ***d.*** ***Adaptability*** **–** the immune system is able to detect and to learn to detect new foreign cells and retains the ability to recognize previously detected foreign cells through immune memory.
- ***e.*** ***Dynamically changing coverage*** **–** The immune system has a limited amount of cells for detection in any moment. There are about 10^{16} foreign cells in the environment where humans spend their lives and these foreign cells must be detect by the limited quantity of detectors of the immune system. The immune system solves this by maintaining a random sample of its detectors that circulates throughout the body.
- ***f.*** ***Identification*** **–** The immune systems marks all the cells that belong to the body as 'self'.

III. RELATED WORK

An approach to use Immune system for IT security is described by [2], where they highlighted techniques to solve two different IT security domain – Database security and Intrusion detection system. More focus is on concept of negative database to ensure the privacy and confidentially of database. Juan Carlos Galeano [8] presented a review of different artificial immune network model, which provides a common notation that allows the comparisons of different models. This helps us to map the keywords for system. How artificial immune system is distinct and effective in useful is well explained by Simon Garrett[9]. The analogy between Natural and Artificial Immune systems using self and non self principle are well stated by Kamran Shafi and H.A. Abbass [10], where focus being place on biologically inspired complex adaptive systems approach for network intrusion detection.

IV. PROPOSED METHOD

The immune system is mapped to the social networking site that we want to protect. The user data (and also his links) will act like the antibodies in the immune system. The intruders in an SNS will play the role of the antigens of the immune system which are to be detected and eliminated. The following algorithm is inspired from the adaptive immune system of the human body. In the method proposed below, when the IDS discovers a new intrusion, it will learn this pattern, i.e. store the pattern in it's memory. The innate equivalent of our IDS will make use of this data to track any similar intrusions in the future

Algorithm

Assumptions:-

a. Each user's ID will be maintained.
b. Every data in a user's profile (pictures, comments, personal info etc) is given an ID. All data of a particular user will be marked as "self" for that user. Any user visiting the "self's" account will be marked as "non-self" and his/her actions will be monitored.
c. All users will have settings either default or set by them by which login can be blocked after 'n' unsuccessful login attempts. Accordingly, the notification will be messaged/mailed to the user thus allowing him to detect if an intrusion has taken place or not.
d. After logging in successfully, a notification is sent.

Before going on to the actual algorithm, it is important to note that the algorithm will work better for a small network of users. In other words, one (or more if necessary) mobile agent will constantly monitor the small network that is allotted to it on the basis of the algorithm proposed below. Depending on the architecture of the SNS, the IDS will be placed in the server/servers and will keep receiving updates about intrusions/possible intrusion that are taking place, much similar to the White Blood Cells that keep monitoring the body for any pathogens. On encountering an attack, the IDS will broadcast this message to other mobile agents to check the spread of the attack.

Data structure used:-**Vulnerability Analysis Table [VAT]**

Table 1. Vulnerability Analysis Table structure

Id_of_accessor	**Freq_Vul_id1**	**Freq_Vul_id2**	**……**	**Freq_Vul_idN**	**Threat**
User_Id#	X_1	X_2	……	X_N	Y

- ***a.*** ***Id_of_accessor***: the id of the user who is accessing the publicly available data (vulnerability)
- ***b.*** ***Freq_vul_id#:*** count of visits to vulnerability by user_Id#
- ***c.*** ***Id#:*** IDs of those data that is vulnerable (eg. Public data)
- ***d.*** ***Danger_rate****:* threat calculated with respect to the threat others are posing to the user.

$\mathbf{Y} = (\sum (\text{Relative threat of } x_i)) / N$

(basically the average of threat for each vulnerability)

Where, $i = 1 \ldots N$; N = no. of vulnerabilities

Relative threat of $\mathbf{x_i} = (100 * x_i) / \max(\text{freq\_vul\_id\#})$

Thus, the person with the most views for a particular vulnerability is assumed to have 100% threat to user. For example, consider there are 3 publicly available data in my account that have IDs ID1,ID10 & ID15. Thus, N=3. I have 10 friends in my account totally. Current scenario of my account:-

Table 2. Sample Calculation

Id_of_accessor	Freq_Vul_id1	Freq_Vul_id10	Freq_Vul_id15	Threat
Id1	1	3	0	36.11
Id2	0	4	0	33.33
Id3	2	0	0	22.22
Id4	3	0	1	66.67
Id5	0	1	0	8.3
Id6	2	4	0	55.55

Max(freq_vul_id1) = 3,
Max(freq_vul_id10) = 4,
Max(freq_vul_id15) = 1

Threat calculations for id1:-

Relative threat of public data having id1(freq_vul_id1) =100*1/3=33.33

Relative threat of public data having id10(freq_vul_id10) =100*3/4=75

Relative threat of public data having id15(freq_vul_id15) =100*0/1=0

Threat 'y' for id1 = (33.33+75+0)/ 3=36.11

Likewise, other threats can be calculated.

Whenever an intrusion is detected by user, he will notify to the SNS about it. Even if the attacker hasn't actually tried to break into the a/c but some potential damage has been done to the victim's identity then that should be reported as soon as possible to the SNS so that the following action can be taken.

Taking into consideration the above mentioned assumptions following algorithms will be followed.

A. In case of an intrusion:

a. Look up in VAT for the next highest threat.
b. Match IP of intruder with the IP/IPs of user with the highest threat. If match unsuccessful goto step 1 else goto step 3.
c. Create list of friends that have accessed user account with same id as that of intruder.

a) Add friend with matching id to list.
b) No. of friends= no. of friends – 1
c) If no. of friends ! = 0 then goto step 1

B. In case of damage to identity:

Damage to identity is usually caused due to data that is public. SNS should have provision to allow user to provide the site with data that was used against him/her.

a) Arrange in descending order the column of freq_vul_id# where id# is id of that data that is used against victim and present this list to victim.
b) If more than one data is used, repeat step 1 for all such data.

These algorithms create a list of people (friends) that could have been the cause of the problem. The SNS can make further suggestions to the victim about his/her privacy settings against these people. After studying the list the victim may come to a conclusion about the one/ones who tried to break into/or make malicious use of his account and accordingly report about the result to the SNS. The SNS will then flag that user/users (attacker) and notify to others in the user's network (friends of victim) about the kind of attack and may give them suggestions about their privacy settings against that user. SNS will also make note of pattern of attack for future reference which is similar to the adaptive immune system.

(a). Detecting vulnerabilities:- Detect the possible vulnerabilities in a certain profile. Vulnerabilities, in SNS point of view can be said to be the possible "doorways" through which anyone can gather information about a particular profile; public access to photos, videos, blogs, messages, likes, interests etc. These help a lot in case of social engineering attacks. Therefore, such potential gateways should be noted by the SNS for future use. These vulnerabilities act similar to the pathogens that try to attack the immune system but are detected easily by the T- cells in our body which after some time rupture the pathogenic cells.

(b). Vulnerability Analysis System: Once the SNS makes a note of these vulnerabilities and stores them into a "vulnerability table", it should also monitor and make a note of all those profiles which gain access to these weak points. This step has been inspired by the adaptive immunity [10] of the human body where learning, adaptability and memory are its important characteristics.

(c). Detecting Intrusions And Implementing A Hybrid of IDS and IRS: It is possible that the attacker has gained enough data so as to actually hack into one's profile. He /she will use different password cracking algorithms to guess the user's passwords. Most sites nowadays use captcha to differentiate between an application program and humans. This technique fails because humans can still pass this test and continue with their password guessing. There should be a mechanism so as to notify the real user that an attempt has been made to access his/her account even when offline. Such a message can be sent depending on the count of number of such unsuccessful attempts where the count can be set by the user. In today's times this can be achieved through the use of mobile devices where SNS can notify the person of the attempt by sending him/her the message along and then the person can reply accordingly to the SNS to block the access whatsoever. An email can also be sent simultaneously to the user. In response, the user replies to the SNS to block any accesses to the account for a certain period of time thereby prevent the account from being hacked any further. In terms of Artificial Immune System (AIS) this step can be a hybrid of the Intrusion Detection System (IDS) and Intrusion Response System (IRS).

When we are speaking of detecting intrusions in terms of SNS, a question may arise as to how to detect an intruder. An intruder can be any one of the following:-

i. An unknown person, can be friend of friend.
ii. A known person (friend).
iii. A group (network) of unknown persons, can be friends of friend/s.
iv. A group (network) of known persons (friends)
v. A third party application/s.

While it may be easy to detect (1), (3) and (5), it becomes relatively difficult to tell whether (2) or (4) are going to cause trouble or not. This is similar to the negative

selection mechanism of the immune system. The purpose of negative selection [5] is to provide tolerance for self cells. It deals with the immune system's ability to detect unknown antigens while not reacting to the self cells. During the generation of T-cells, receptors are made through a pseudo-random genetic rearrangement process. Then, they undergo a censoring process in the thymus, called the negative selection. There, T-cells that react against self-proteins are destroyed; thus, only those that do not bind to self-proteins are allowed to leave the thymus. These matured T-cells then circulate throughout the body to perform immunological functions and protect the body against foreign antigens. In a social network, self cells would be the users whose data is to be protected and non-self cells will be the one which will cause harm to the users. Though the non-self cells are dealt with in the early stages in the immune system, in the case of SNS these (users) prove to be harmful after a while. In that case applying the direct logic would be difficult because of the delay in the formation of the "non-self cells" in a social network. But this problem can be tackled if the SNS keeps a track in the from of flags on all users in the form of text mining(to detect what kind of vocabulary is used), frequency of access to each other's data and also how much data is being forwarded to users outside the network. Then when an internal attack has taken place it becomes easy to track down the approach of the attack.

(d). Tracing the cause of attack:

The next step is to trace the cause of the login attempt if it was or was not successful. There should be a provision for the user to report to the SNS of such an event. The SNS should then make use of the "vulnerability table" and make a detailed study called the Post Intrusion Vulnerability Analysis of all those profiles which tried to make use of accessible data and thus try to track down the intruder and the method in which he/she made an unauthorized access. Even though the intruder may not have been identified, the SNS can record the method of attack. This is similar to the adaptive or dynamic nature of the immune system where the cells evolve themselves into better weapons by memorizing the architecture and pattern of attack of the most recent pathogens.

(e). Notifying the social network group:

Once the method has been guessed or identified the SNS can notify it to the user and can also give suggestions about the changes in his/her privacy settings so as to prevent future attacks.

As the immune system notifies other white blood cells (WBC) about the attack, so will the SNS notify others that are linked to the profile which had undergone the attack. This will prevent further intrusion into those profiles that are already related or "friends" with the person whose account had been misused.

V. CONCLUSION

The motive of the method is to give the best and the most effective security measures to the user data even if the user has not taken much care of the privacy settings. But as discussed there are the advantages and the disadvantages to the method because of certain assumptions that are being made. The method will be more effective if the user makes his privacy settings more stringent in nature thereby giving very little to his data to only a limited number of users. It is hoped that that the loopholes of this methods are overcome by the advancing technology and that this method becomes more robust in nature in the near future.

VI. REFERENCES

[1] http://en.wikipedia.org/wiki/Social_networking_service

[2] Thomas Stibor, Claudia Eckert, Jonathan Timmis (2006). Artificial Immune Systems for IT-Security (Künstliche Immunsysteme für IT-Sicherheit) it - Information Technology: Vol. 48, Issue 3, pp. 168-173.

[3] Michael Meisel_,a,Vasileios Pappasb, Lixia Zhanga, "A Taxonomy of Biologically Inspired Research in Computer Networking", Journal of Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 54,no.6, April 2010, pp. 901-916.

[4] Muhammad Awais Shibli, Jeffy Mwakalinga and Sead Muftic, "MagicNET: The Human Immune System and Network Security System" IJCSNS International Journal of Computer Science and Network Security, vol. 9, no.1, January 2009, pp. 87-94.

[5] U.Aickelin, and D. Dasgupta Artificial Immune Systems, Book by Edmund K. Burke (Editor), Graham Kendall (Editor), "Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques , Chapter 13.

[6] http://en.wikipedia.org/wiki/Artificial_immune_system

[7] http://ais.cs.memphis.edu/

[8] Juan Carlos Galeano, Angelica Veloza-Suan, Fabio A.Gonzalez, "A comparative Analysis of Artificial Immune Network Models", In Proceedings of 2005 Conference on Genetic and Evolutionary Computation, 25-29, June 2005, Washington, DC, USA, pp. 361-368.

[9] Simon Garrett, "How do we Evaluate Artificial Immune Systems?", Journal of Evolutionary Computation, vol 13, no.2, June 2005, pp.145-178.

[10] Kamran Shafi and H.A. Abbass, "Biologically-inspired Complex Adaptive Systems approaches to Network Intrusion Detection", Elsevier Information Security Technical Report, vol. 12, no. 4, 2007, pp.209-217.

Short Bio Data for the Authors

First Author – Rajneeshkaur K. Bedi, HOD Of Computer Department, MIT College of Engineering, Pune, rajnibedi16@gmail.com.

Second Author – Oshin Kavdia, Computer Department, MIT College of Engineering, Pune, oshin.kavdia@gmail.com

Third Author – Gauri Bhide, Computer Department, MIT College of Engineering, Pune, gauri.bhide91@gmail.com

Correspondence Author – Vaidehi Donglikar, Computer Department, MIT College of Engineering, Pune getvaidehi@gmail.com.