An Approach towards Data Security

Neha Tyagi[1], Vishal Tyagi[2], Runjhun Saxena[3], Harsh Tyagi[4], Nikita[5]

Assistant Professor, Department of Computer Science and Engineering, G.L. Bajaj Institute of Technology and Management, Greater Noida, Uttar Pradesh, India[1]

Students (B.Tech.), Department of Computer Science and Engineering, G.L. Bajaj Institute of Technology and Management, Greater Noida, Uttar Pradesh, India[2345]

***Abstract*-The modern day world runs on data and thus, security of data is an integral part of present day work life. Data pilfering is something that almost all of us have faced. In the face of these threats, it becomes absolutely essential to protect our data, both at the host ends as well as in transit. Also to effectively prevent pilferage attempts, one needs to know the user who is actively involved in such a scenario, in case we need to block him or track him for further such attempts. For this purpose, we propose a system that seamlessly binds the security aspects as well as keeping tabs upon the users who are attempting to access data not meant for them.**

***Keywords*- data, security, intrusion detection**

1. Introduction

With the ushering of globalization and rapid modernization of organizations resulting in growth of economy, protection of information from malicious entities is gaining importance with each passing day. It is becoming absolutely necessary to ensure the safety of data, not only at the senders end, but also while the data is in transit and even at the receivers end. At the same time, one must also know the perpetrators in order to censure or block the same for preventing future attacks on the integrity of data. By definition, an all encompassing security infrastructure must provide a robust mechanism for securing the data, flagging the perpetrators as well as taking necessary steps to prevent the attack as well as providing remedy in case the same attack happens in the future. Although many products exist in the market which provides such services but there is a dearth of products which provide all of these services blended into a single package. Owing to these factors, it would be of great viability to have a system which provides all round security of data. Also, the cost of such a product will become a matter of paramount importance since a viable product must have an optimum Return on Investment.

In the next section, we would discuss a couple of approaches to detect erring users and discuss their negative aspects.

2. Review

In (Denning,1987), a model of a real time intrusion-detection expert system capable of detecting break-ins, penetrations and other forms of computer attack is described. She proposes the need to build a user-profile based on the types and variations in the system usage statistics and then comparing the same with the present trends in order to detect anomalous behavior. The research paper basis the system security on the fact that any attacker when exploiting the system vulnerabilities will have to deviate from its general pattern of usage and thereby amounting to an anomalous behavior. Such a methodology may help prevent attacks by illegitimate users as well as by legitimate users who try to go beyond their brief. The user profiles can be built by taking into cognizance factors such as activity name, period of usage, time between audits of usage, thresholds, exception patterns and the like.

But the most basic back draw of this system is that it does not take into account the variables such as assigning the system to any new user or variations in workload etc., or other such factors. The exception patterns would have to be updated frequently if the work is of diverse nature. Also, defining the threshold value, which would ultimately be required for testing abnormality, is a paradox since predicting future trends is in itself filled with anomalies.

In (Boer & Pels, 2005), the authors propose that an intrusion occurring on a host system can be detected in four different manners as,

- File system monitoring
- Log file analysis
- Connection analysis
- Kernel-based intrusion detection

The authors have also listed out the ways in which one can beat the detection techniques as given :

File system monitoring technique can be evaded by removing the usable data from the file and padding it with bogus data, removing traces from log files, abusing hash collisions etc.

Log file analysis technique can be evaded by gaining root privileges, encoding the access attempts in a format which is different than the one recognized by the system, defining the thresholds which helps make distinction between errors and user forgetfulness etc.

Connection analysis technique can be evaded by using unsupported protocols, using a large pool of ip's, performing slow or unsupported port scans such that the connection analyzer is not tripped, denial of service attacks etc.

Kernel-based intrusion detection can be evaded by masquerading the program to jump to C library and performing system calls from that location, as this won't trip the IDS. Another way to beat this technique would be to use multiple processes in attack instead of a single process.

Although these efforts may help in detection and prevention of unauthorized attempts being made at a system, they do not provide for measures that help in ensuring the integrity of the data itself. It may even happen that the attacker is successful at evading the detection systems but the system should not let him access any meaningful information from the data which he might have been able to capture. This is the root of our proposed model which is explained in the next section.

3. Proposed Model

The proposed security model is intended to work on a closed network existing in an organization such that the IP address of the system connected in the network remains fixed. The user when registering for the services provides his details such as name, user name, contact, email id, password, and a profile picture for easy recognition. In our model, the profile picture has been made a mandatory feature without which the system would not accept the registration. The system automatically stores the user's IP and MAC address into the database. The MAC is stored since it provides the administrator with a unique signature to determine the origins of the traffic.

But merely submitting the data by the user does not amount to acceptance into the system. After the user submits his details, the same are forwarded to the system administrator for review. It is within his purview to either accept or reject a particular user. Once the user has been rejected, he would not be able to access the system and thus, would be unable to avail the services. Also, once a user has been rejected, he would have to apply again, providing the same details, if he wants to be considered in the future.

Once the administrator approves a particular user, he can login to the service by providing his email address and password submitted at the time of registration. Once the login is authenticated by verifying the details provided and matching the MAC and IP addresses of the user with those stored in the database, the user can avail the services which include encryption/decryption, sharing of files and updating of profile.

The enciphering/deciphering service uses Advanced Encryption Standard (AES) algorithm. The AES algorithm implemented here uses a 128-bit key alongside a 128-bit block size. We propose AES since a symmetric key encryption works faster as compared to a public key encryption.

If the user wants to share his file with his peers, he can choose to do so by selecting the file to be shared and providing the email id of the peer with whom it is to be shared. The user will be able to share both the encrypted as well as non-encrypted data. The only constraint here is that the friend, with whom the data needs to be shared, should also be a registered user of the system. Any and all data shared will appear in the download section of the respective user's account.

When the user receives a shared file, he can view the file in the download section and can simply click on the link provided to initiate the download process. The actual shared file will only be downloaded onto the accesses' system if his ID matches the one provided by the sender. Since the MAC address of a workstation is unchangeable, we can run a trace for it when matching the email ID of the person who is attempting to access the data with the registered MAC of the person to whom it was actually addressed.

In case the ID of the person trying to access the data does not match with the ID of the user for which the data was intended, then an empty file will be downloaded onto his system and his IP would be flagged for the administrator for review. Also, an email would be sent to both the administrator and the originator of the data as soon as the intrusion attempt occurs and is detected. This is done so as to enable them to take preventive measures in real-time.

The shared files will be hosted on a local cloud server and will be downloaded from the same.

There is the provision of an administrator who will accept or reject the user's signing up for the service. He can view the IP addresses of the intruders and reject such user's from all future access. He can review the details of the user's that have been accepted into the system as well as those who have been rejected. The rejected user's list has been provided so that the administrator can review new entrants with the ones who have been rejected earlier. This will help in pruning out the defaulters who may try to sign up using different credentials.

4. Future Scope

The system can be upgraded to use a bigger block and key size AES algorithm such as the 192 and 256-bit variants for considerable improvements in the security infrastructure.

Also, commonly available open-source intrusion detection tools can be blended into the model for providing enhanced detection capabilities. Such services can be used to track down intrusion attempts of varying characteristics.

The system can be made to detect intrusions at both the host's end as well as in the network.

An expert system capable of retaliating against intrusion attempts can be deployed which will make the process a whole lot automated. This will help in reducing the workload of the administrator as well providing real-time security.

We can also incorporate public key cryptography into the proposed model to make it much more secure than symmetric key cryptography proposed by us in the given model. Thus we would be able to create a separate secure transmission link for each communication between the sender and receiver. Although adding public key cryptography will result in slower encryption/decryption speeds, but it will help in improving the security and availability of data.

5. Conclusion

The current security services lack the ability to function in a multi-dimensional operating environment. This is a big issue since the users operate both at the host level and at the network simultaneously.

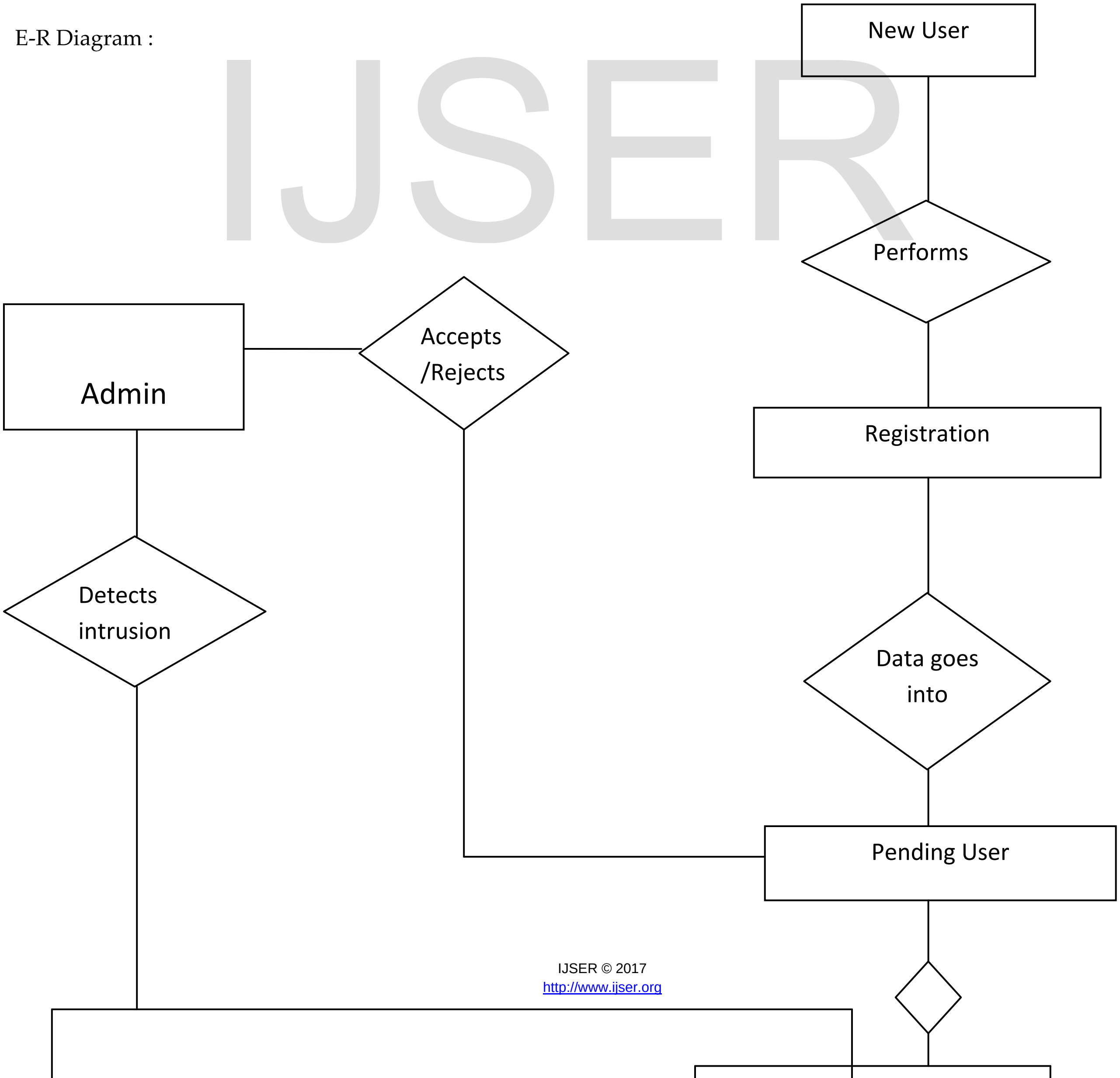
The technological innovations have been borne out of specific needs of the users. Thus, it would be unfair to categorize the security systems as weak and non-capable for providing total and complete security in a single package.

A robust future security infrastructure will use biometrics for access control, bigger key sizes for better encryption, and have better capabilities of generating alarms, display alarms, clear alarms, and also provide context-sensitive online help. It will also have a database mechanism and also have tools for effective data management. These tools will allow a security management staff to analyze the data as desired.

Consequently, when these flaws have been realized, would we move on to enhance the security of the infrastructure as a whole and not just the individual components. This will help provide the highest levels of security round-the-clock.

Finally, it can also be expected that in the future, security solutions would be customized for each individual user according to their needs. There would not be a single product, but rather an integrated system with its components ready to be added and replaced as and when needed.

E-R Diagram :


New User
Performs
Registration
Data goes into
Pending User
Admin
Accepts /Rejects
Detects intrusion

6. . REFERENCES

[1] Host-based Intrusion Detection Systems (Pieter de Boer & Martin Pels) – February 4, 2005

[2] An Intrusion-Detection Model (Dorothy E. Denning) – February 1987

[3]Advanced Intrusion Detection Environment (AIDE) , http://sourceforge.net/projects/aide/

[4] Linux Intrusion Detection System , http://www.lids.org/

[5] SecurityFocus: Intrusion Detection, Theory and Practice ,David Elson, 2000

[6] Intrusion detection system based on process behavior rating , T. Pluskal , 2004 , http://plusik.pohoda.cz/thesis/thesis.pdf

[7] Evading non-executable stackprotections , R. Wojtczuk , 1998 , http://community.core-sdi.com/ juliano/non-exec-stack-problems.htm

[8] Anomaly detection library and articles , http://www.cs.ucsb.edu/ rsg/libAnomaly/

[9] D. E. Denning and P. G. Neumann, "Requirements and model for IDES-A real-time intrusion detection system," Comput. Sci. Lab, SRI International, Menlo Park, CA, Tech. Rep., 1985.

[10] IBM Corp., System Management Facilities, 1st ed., Rep. BC28-0706, 1977.

[11] UNIX Programmer's Manual, Dep. Elec. Eng. and Comput. Sci., Univ. California, Berkeley, 4.2 Berkeley Software Distribution ed., 1983.

[12] AIDE Manual , http://www.cs.tut.fi/ rammer/aide/manual.html

[13] The MD5 Message-Digest Algorithm , http://www.ietf.org/rfc/rfc1321.txt

[14] SNORT, The Open Source Network Intrusion Detection System , http://www.snort.org/

[15] US Secure Hash Algorithm 1(SHA1) , http://www.ietf.org/rfc/rfc3174.txt