St. Vincent Pallotti College of Engineering and Technology

Gavsi Manapur, Wardha Road, Nagpur.

Department of Information Technology

Academic Year: 2014-15

Information Technology

6th Semester

Mini Project

Synopsis

On

INTRUDER IDENTIFICATION SYSTEM

Submitted by

Group: IT-4(a)

Group members:

Nikhil Paonikar

Pratik Khanke

Rohit Ghungrudkar

Samuél Kumar

Under the guidance of:

Mrs. Priti Golar

St. Vincent Pallotti College of Engineering and Technology

Department of Information Technology

Academic year: 2014-15

INTRUDER IDENTIFICATION SYSTEM

1. Abstract

As the digital age takes firm root with the passage of time, our smartphones and tablets grow increasingly important to us. What started out as a simple method of communication, has turned into a warehouse of our digital selves, holding everything from photographs, sensitive text messages, important passwords, crucial financial information and more. As such, the need for protection increases too and security has become one of the top priorities in the digital world.

The old adage "Prevention is better than cure." still holds true in today's digital world. But, sometimes things tend to get out of hand and there's little we can do about it. Like when someone's computer is broken into illegally, there's no definite way to recognize the identity of the suspect.

In information security, intruder identification is the science of detecting intruders behind attacks as unique persons. Here, the identity of the person behind an attack is unveiled by analyzing their computational behavior. This concept is sometimes confused with Intrusion detection (also known as IDS) techniques; detecting the occurrence of an intrusion.

Though conventional methods use computational behavior of intruders, other unconventional approaches might employ getting biometric feedback, implementing decoy interfaces and other discreet traps.

In the undertaken project, the intruder will attempt to log in to the victim's computer. After the first two login attempts will be unsuccessful, access will be intentionally granted to the intruder on the third attempt. The system will take note of this and will then effectuate the designed set of programs put in place by the owner/administrator. Following actions will be carried out by the system:

1. The intruder will be photographed via a connected webcam

2. Keystrokes will be logged.

3. All activity will be logged.

4. Data transfer will be prohibited.

5. All recorded data will be sent to the owner's cloud storage and saved locally as well.

6. Changes made to any program, data will be reverted just before the intruder logs off.

The final outcome of the project may be assimilated with additional features.

2. Minimum Hardware and Software requirements

(a) Hardware
   i. Computer and processor: 1 gigahertz (GHz) or faster x86-bit or x64-bit processor with SSE2
   ii. Memory: 1 GB RAM (32-bit)
   iii. Hard disk: 3.0 GB available disk space
   iv. Display: 1024 x 768 screen resolution
   v. Webcam: Minimum 0.3 Megapixels
   vi. Graphics: Graphics hardware acceleration requires a DirectX 9.0c GPU

(b) Pre-requisite software:
   i. Java Runtime
   ii. Custom scripts/software

(c) Operating system
   i. Windows 7

3. Literature survey

Intrusion Detection: The first step in securing a networked system is to detect the attack. Even if the system cannot prevent the intruder from getting into the system, noticing the intrusion will provide the security officer with valuable information. The Intrusion Detection (ID) can be considered to be the first line of defense for any security system [1].

Honeypots: Lance Spitzner, Founder of Honeypot technology is given the authority of the definition of honeypot as "A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource" [2].Honeypot refers to set of services, an entire operating system or even an entire network that is built to lure and contain the intruder. To collect known and unknown kind of attacks into any organization, honeypot places a significant role.

Honeypot is a security resource whose value lies in being probed, attacked or compromised [3]. Honeypot does not solve a specific security problem; therefore it is not a solution but a general technology which is unique in itself. Honeypot can be involved in various aspects of security such as detection, prevention and information gathering. Honeypot is highly flexible tool with applications in such areas as network forensics and intrusion detection. The motivation gain is to gather the information about the attacker (black-hat community) to learn the tools and techniques used by the attackers.

Keystroke dynamics: The use of keystroke rhythm is a natural choice for computer security. This argument stems from observations that similar neurophysiological factors that make written signatures unique, are also exhibited in a user's typing pattern [4]. When a person types, the latencies between successive keystrokes, keystroke durations, finger placement and applied pressure on the keys can be used to construct a unique signature (i.e., profile) for that individual. For well-known, regularly typed strings, such signatures can be quite consistent. Furthermore, recognition based on typing rhythm is not intrusive, making it quite applicable to computer access security as users will be typing at the keyboard anyway [5].

4. References

[1] Peyman Kabiri and Ali A. Ghorbani,

Research on Intrusion Detection and Response: A Survey
http://www.cs.unb.ca/profs/ghorbani/ali/papers/Journal_paper/IJNS_Survey_05.pdf

[2] Lance Spitzner "Honeypots: Definitions and Value of Honeypots"
http://www.windowsecurity.com/whitepapers/honeypots/Honeypots_Definitions_and_Value_of_Honeypots.html

[3] Iyatiti Mokube, Michele Adams, "Honeypots: Concepts, Approaches, and Challenges" ACM, in ACM-SE 45 Proceedings of the 45th annual southeast regional conference , pp. 321 – 326, North Carolina, 2007.
http://cs.millersville.edu/~csweb/lib/userfiles/honeypot.pdf

[4] R. Joyce, G. Gupta, Identity authorization based on keystroke latencies, Communication. ACM 33 (2) (1990) 168–176.
http://www.cs.cmu.edu/~maxion/courses/JoyceGupta90.pdf

[5] Fabian Monrose, Aviel D. Rubin, Keystroke dynamics as a biometric for authentication http://www1.cs.columbia.edu/~hgs/teaching/security/hw/keystroke.pdf

Roll numbers: (1) 59	Names of students: (1) Nikhil Paonikar
(2) 63	(2) Pratik Khanke
(3) 67	(3) Rohit Ghungrudkar
(4) 69	(4) Samuél Kumar
Signatures: (1)	Date:
(2)	
(3)	
(4)	

Name of the guide :

Signature with date :

Status : Approved / Approved with modification / Not approved

Sign of HOD :

Remarks :

Date :