International Journal of Scientific Research in Computer Science and Engineering
Vol.5, Issue.4, pp.60-62, August (2017)

Review Paper

E-ISSN: 2320-7639

Study and Overview of Anti-Trespasser

Jayendra S Jadhav

Computer Engineering Department, Lokmanya Tilak College of Engineering, Mumbai University, India

Corresponding Author: jayendra071985@gmail.com

Available online at: www.isroset.org

Received 10th Jun 2017, Revised 16th Jul 2017, Accepted 12th Aug 2017, Online 30th Aug 2017

Abstract - In current scenario, security systems remain generic with limited authentication abilities. Existence of such security methods for primary purpose is legitimate. With the growing technology and emergence of malicious people around, it may be possible to break barriers. Safety of one's precious data is primary concern. This project proposes a security mechanism to enhance the level of security for every individual. The application tries to leverage individual's presence to be a key to access virtual area. The system requires mobile device with Bluetooth functionality, which is coupled with principle device that you need to secure. The Project aims to tightly couple security mechanism with the operating system allowing it to take final steps to maintain privacy of data

Keywords - *Bluetooth; Piconet; Ad hoc; Trespasser;Mobile;*

I. INTRODUCTION

Data and personal information is extremely pivotal to every individual. This data can be stored at multiple instances and time. There can also be a scenario of manipulating multiple devices or network through single device if it is administrator. Such workstations and servers have privilege to manage massive number of devices. Also clustered cloud computers who manage cloud drives, exclusive machines with confidential data can be accessed, if not secured properly.[1]

Presently, world follows generic security mechanisms. Project drafts a prelude of using human proximity as a key parameter to access a particular area. The introduction of human existence in proximity of device prohibits another individual to trespass the area. This security mechanism can be used for physical access to a particular area also. Many applications of such mechanisms can be explored in future, example: applying it for exclusive application or accessing confidential matters. The ability to couple up with the operating system and manipulate it becomes objective of proposed system.

Project proposes a security mechanism to enhance the level of security for every individual. The application tries to leverage individual presence to be a key to access virtual area. System aims to sustain the integrity of pivotal data. This system requires mobile device with Bluetooth functionality, which is coupled with principle device that you need to secure. Project aims to tightly couple security mechanism with the operating system allowing it to take final steps to maintain privacy of data. Individuality of person is difficult to replicate hence such system has higher amount of success ratio. Occurrence of such security mechanism perhaps produces shielded ecosystem for every individual.

The given architecture signifies overall behavior of "Anti-Trespasser". In real time, the architecture of application interacts with operating system of principle devices. This gives application an authority over operating system to manipulate it. Whole framework works as an ad- hoc wireless network. [1]

The architecture constitutes of two Bluetooth oriented devices capable of establishing a small "piconet". The framework of "Anti-Trespasser" works only if paired device and active device match during authentication. Once identification of device with active state is confirmed, the application takes suitable action selected by user in options.

The core idea of application is use human presence as a key to provide access to utilities. This presence of Bluetooth device acts as a fundamental to provide principle device consciousness about human presence.

II. LITERATURE SURVEY

2.1 Securing Computer Folders using Bluetooth

Security of the computer files and folders have been core issue ever since the advent of the windows. Passwords were then introduced to solve this issue but they themselves lend a host of disadvantages. In present day, the increasing reliance on computer systems has led to the dependence on confidential security measures. Various methods used to identify a user are Digital signature, Challenge-Response, Biometrics, IPSec (Internet Protocol Security), Single-Sign On and Password. Password has become one of the most ubiquitous modern day security tools and is very commonly used for authentication. These passwords are string of characters used for authentication or user access. [2]

Biometrics on the other hand requires the assumption of unrealistic preconditions for performance gain. Access control systems require time-trusted and reliable personal recognition. To overcome the problems faced by these processes individually, there can be a combination of two or more security processes. Two-factor authentication has ameliorated security in authentication systems.[3]

Proposed prototype with Bluetooth functionality has primary factor to rectify the presence of mobile device. Such systems can also be used for advance level security purpose. By deploying architecture

of above manner, there can an effort to enhance the measures of safety and integrity of one's data. Advance wireless technology with effective high level languages can produce top end utility applications.

2.2. Study of Various Systems

1) Finger Print Detection System

Finger printing or finger-scanning technologies is the oldest of the biometric sciences and utilizes distinctive features of the fingerprint to identify or verify the identity of individuals. Finger-scan technology is the most commonly deployed biometric technology, used in a broad range of physical access and logical access applications. All fingerprints have unique characteristics and patterns.[6]

2) Retina-scan Technology

The last biometric technology to discuss is retinal scanning. Retina-scan technology makes use of the retina, which is the surface on the back of the eye that processes light entering through the pupil. Retinal Scan technology is based on the blood vessel pattern in the retina of the eye.[6]

The principle behind the technology is that the blood vessels at the retina provide a unique pattern, which may be used as a tamper-proof personal identifier. Since infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue, it is used to illuminate the eye retina. Analysis of the enhanced retinal blood vessel image then takes place to find characteristic patterns.

3) Facial-Scan Method

Facial-Scan Technology Another biometric scan technology is facial recognition. This technology is considered a natural means of biometric identification since the ability to distinguish among individual appearances is possessed by humans. Facial scan systems can range from software-only solutions that process images processed through existing closed-circuit television cameras to full fledged acquisition and processing systems, including cameras, workstations, and backend processors. With facial recognition technology, a digital video camera image is used to analyze facial characteristics such as the distance between eyes, mouth or nose. [6]

2.3 Motivation

Existing System with generic security measures wouldn't have proximity protection system. Hence, there is a requirement of application like Anti-Trespasser which provides additional layer of safety to structures. After enabling "Anti –Trespasser", security mechanisms of system get enhanced. Application existing with two modules of securing folders or logging off machine can be selected by user according to preference.

III. SYSTEM OVERVIEW

3.1 Objectives

Objective of a project defines the goal it wants to achieve. There can be multiple motives which are needed to be addressed. Objective defines proper aim in a structured pattern.

- To develop a secured ecosystem for everyone's personal device
- To sustain the integrity of data via proximity protection.
- To provide authenticated security measures to user's confidential matter.
- The system focuses to privatize important data, essential for individual

The primary objective of system is to provide authenticated security measures to user's confidential matter. System aims to sustain the integrity of pivotal data. The primary focus of application is to privatize important data essential for individual. To generate such ecosystem for everyone's personal device, proposed application which tries leverage of human presence.

To achieve such ecosystem we rely on proximity protection. To provide authenticated security measures to user's confidential matter. The system focuses to privatize important essential for individual. The application has functionality of locking down system folder or shutting the device as a counter measure.

3.2 System Architecture

Architecture showcases overall structure of Anti-Trespasser. To procure resultant scenario two Bluetooth oriented devices interact with each other. Principle device exist with the Anti-Trespasser. Here, Anti Trespasser gets information about the active state of mobile device.

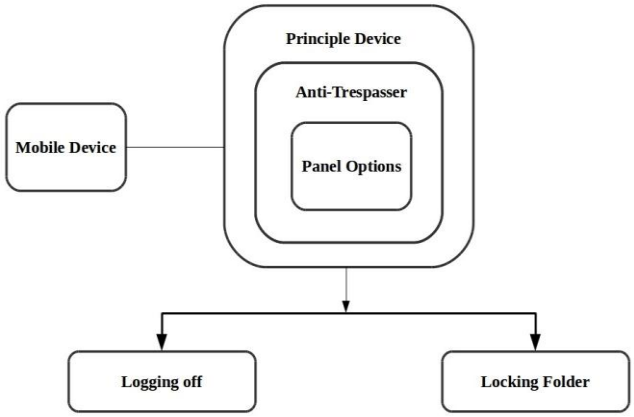

Fig. 1 Anti- Trespasser Architecture

Panel Option lets you decide which function user need to include. Panel option is interior of the anti-trespasser. This device has two function:-Logging off and locking off. Accordingly it will choice the function in the range of user. System will react according to option user have selected.

3.3 Methodology

Methodology is a system of methods used in a particular area of study or activity. It states the methods, architecture as well as models we use to achieve results.

A] Algorithm for folder locking

Step 1: Pair your mobile phone with targeted device.
Step 2: Store data in targeted folder.
Step 3: Enable Anti –Trespasser.
Step 4: If Authenticated paired mobile device in Range of principle device then, Folder gets publicly accessible.
Step 5: ELSE,Folder goes protected/private.

B] Algorithm for Logging off function

Step 1: Pair your mobile phone with targeted device.

Step 2: Enable logging off option.
Step 3: Enable Anti –Trespasser.
Step 4: If Authenticated paired mobile device in Range of principle device then, Do Nothing.
Step 5: ELSE,Initialize Logging off.

3.4 Advantages

- Anti-Trespasser shields ones most important data with efficiency.
- This system uses one's own presence with Bluetooth enabled device to be the key to access data.
- System provides integrity and authorization to important matters.
- It provides a secured ecosystem.

IV. CONCLUSION AND FUTURE SCOPE

Optimization of Application is the primary concern. Anti-Trespasser creates MANET via Bluetooth functionality which renders filtering of active devices. Once the application preferences are set, for example- option of logging off or folder locking, it takes a while to scan for device and take suitable action. This speed of taking action requires a countdown for activating the functionality. This countdown can be neglected in future to activate result. This makes application quicker and better. Implementation of such project can also be accomplished through Wi-Fi Hot-spots which perhaps can result in more contemporary design.

REFERENCES

[1] Esteban Alcorn, Bluetooth Architecture Overview", Microsoft Windows Embedded Compact 7, Published: March 2011, https://www.ieee.org/documents/ieeecitationref.pdf
[2] S.K. Kenue and J.F. Greenleaf, "Limited angle multifrequency diffiaction tomography," IEEE Trans. Sonics Ultrason., vol. SU-29, no. 6, pp. 213-2 17, July 1982. www.techterms.com/definition/manet
[3] C. Brusaw, C. Aired, and W. Oliu, Handbook of Technical Writing, 3rd ed. New York: St. Martin's Press, 1987. [Online]. Retrieved on- December 2016 Available: http://softsprogrammer.blogspot.com/2014/04/lock-folder
[4] G. J. Broadhead, "Style in technical and scientific writing." In M.G. Moran and D. Joumet, eds. Research in Technical Communication. A Bibliographic Sourcebook, pp. 379-401. Westport. CT: Greenwood Press, 1985.
[5] M. M. Botvinnik, Computers in Chess: Solving Inexact Search Problems. Translated by A. Brown, Berlin: Springer-Verlap, 1984. http://www.cs.wustl.edu/~jain/cis788-97/ftp/ip_security
[6] Smart Handheld Group, Hewlett-Packard Company, Bluetooth Technology Overview[Online]. Retrieved on: October 2016 Available:(http://inpressco.com/wp-content/uploads/2015/02/Paper71397-400.pdf)
[7] Securing Computer Folders using Bluetoothand Rijndael Encryption [Online].Retrieved on - December 2016 Available: (http://inpressco.com/wp-content/uploads/2015/02/Paper71397-400.pdf)
[8] Securing ComputerDeviceUsing Bluetoothtechnology, Retrieved on- December 2016, [Online]. Available: (http://www.ijecs.in/issue/v4-i4/60%20ijecs.pdf)
[9] Wankhade S.B., Damani A.G., Desai S.J., Khanapure A .V., "*An Innovative Approach to File Security using Bluetooth*", Mumbai, Maharashtra, IJSET, Vol. 02, Issue No. 5, pp:417-223

