www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11426-11429

Securing Computer Device Using Bluetooth technology and One-Time Password

Mrs Aruna Gawde, Sanchit Jain[a] ,Mohsin Masani[b], Sahil Deliwala[a,b,]

[b]*Mohsin Masani, Mumbai 400053, India*

[a]Sanchit Jain, Mumbai , India

Abstract

Securing your Computer/Laptop and its vital data is the most important concern for everybody in today's life. We want to secure our device when we are not using it, or might be we are not in the proximity of it. Many a times, it happens that our device password is known by people close to us. They can use this password to login secretly, and steal/change some vital data.

Hence, securing our systems, when we are not in its proximity is an important task. To do so, we have to have some lock on our system by which only we could be able to open it. A solution to this is to have additional password in order with the normal Windows password on login. This will be a one-time password and will change on every login. This will act as an additional protection for the system. Also, using the Bluetooth technology we will maintain the user authentication and communication to track the authenticated user.

Keywords: Securing, Passwords, Protection, Proximity, One-time password, Bluetooth.

1. Introduction

Protecting data has been our primary concern for the computer users all over the world. In today's time people are entrusted with very sensitive data i.e. of personal and organizational use. Windows authentication policies provide securities to a limited extent. However, these policies do not ensure guarantee of personal and organizational security. Windows authentications policies can be broken down easily and cracked easily by the hackers. Hence it does not ensure a full proof security to the users. Windows does not provide any other security mechanism other than this.

About 30% of the user's passwords are easy to guess and appear in the hacker's dictionary. Using difficult user passwords can also create a problem of remembering them. Hence people will start writing their passwords on notes, keeping them in desk drawers, etc. which will lead to more problems. People generally choose passwords related to themselves. So other people close to a user can guess the password.

We now need some other security mechanism(s) to ensure our security. This additional security layer must provide us automated services when we are not in the proximity of the laptop/computer device.

2. Review of Literature:

2.1. Present System:

2.1.1. Windows Authentication Policies and its Drawbacks:

Windows uses simple login authentication process for the authentication of valid users. But this login validation and authentication process is not so strong. User passwords are easily cracked by hackers as the passwords are generally user specific and related to users. The passwords kept by the users are easy to remember passwords and not so strong. These policies are often broken down by hackers to gain system access and update content of user files.

2.1.2. User Passwords:

Generally, users tend to keep same password for multiple accounts. Also, the frequency of changing the passwords is also very less. Hence is becomes very easy of a person knowing password for one account to get access to another account. This becomes a major drawback for users and a benefit for the intruders.

2.2. Other Paper Solutions.

A solution proposed by Pharaoh Chaka, Hilton Chikwiriro, Clive Nyasondo, in paper - Improving the windows password policies using the mobile Bluetooth and rijndael encryption, IJCSMC vol.3 issue 3, 2014, proposes to secure laptop/computer device using Bluetooth proximity detection and locking the device when mobile device is not in proximity of the laptop. Also it further states to encrypt the full computer data using rijndael algorithm.

The drawback with this proposed solution is that, no locking on windows commands is given. A attacker can easily kill the application programs by windows commands. Also, the time to encrypt and decrypt will be exponential to the amount of data in hard disk. This time factor can prove another drawback.

Another solution proposed was to monitor the screen saver activity and thereby lock the computer/laptop device when the screen saver is active. The activation of screen saver states that the computer device is inactive. But this is not feasible, as the user may be in proximity to the computer device but may happen to not use the device. In such cases also the computer device will get locked, creating an overhead.

2.3. BlueCove:

BlueCove is a Java library for Bluetooth (JSR-82 implementation) that currently interfaces with the Mac OS X, WIDCOMM, BlueSoleil and Microsoft Bluetooth stack found in Windows XP SP2 or Windows Vista and WIDCOMM and Microsoft Bluetooth stack on Windows Mobile. BlueCove-GPL is additional GPL licensed module to support BlueCove runtime on Linux BlueZ. BlueCove JSR-82 Emulator module is additional module for BlueCove to simulate Bluetooth stack.

BlueCove is a java library api, that helps in communication between Bluetooth enabled devices using Bluetooth. It provides functionalities and functions that can be used to search nearby devices and help in transmitting and receiving requests between devices.

2.4. Bluetooth Stack:

The Bluetooth Stack consists of layers that provide various functionalities to a user. Service Discovery Protocol(SDP) provides a means by which service applications running on different Bluetooth enabled devices may discover each other's existence, and exchange information to determine their characteristics. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used to determine which Bluetooth profiles are supported by the headset (headset profile, hands free profile, advanced audio distribution profile, etc.) and the protocol multiplexer settings needed to connect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128).

Object exchange (OBEX; also termed IrOBEX) is a communications protocol that facilitates the exchange of binary objects between devices. It is maintained by the Infrared Data Association but has also been adopted by the Bluetooth Special Interest Group and the SyncML wing of the Open Mobile Alliance (OMA). In Bluetooth, OBEX is used for many profiles that require simple data exchange (e.g., object push, file transfer, basic imaging, basic printing, phonebook access, etc.).

3. Proposed System:

User passwords are easy to crack as we have discussed above. Now, to have an added security for our systems, we need some more security parameters along with the normal windows authentication process.

One-time passwords can prove to be efficient in providing this extra security. Using OTP’s, intruders cannot penetrate the system as the password keep on changing on every login. But still generating a new OTP every time and remembering it becomes an issue.

For this, we will be using the Bluetooth Technology of our Mobile phones. The Bluetooth in our mobile phones connects with the Bluetooth of our computer device when in proximity. The OTP’s will now be sent to the mobile authenticated mobile device connected via Bluetooth. So, the users will now not have to remember the OTP’s and then can access it anytime with the help of the mobile device.

3.1. One –Time Passwords:

One-Time passwords give us an added security option along with the usual passwords. The OTP technology has been widely used by companies for authentication of users and also to provide them an added security. OTP’s are randomly generated characters or digits sent to the users mobile device usually via SMS.

3.2. Bluetooth Technology

Almost every mobile phone device now-a-days is equipped with the Bluetooth technology. Also, most of the computer devices are equipped with this. Bluetooth technology gives us the feature of communicating with the devices in proximity. Hence only devices near to each other can communicate with each other. The OTP’s sent to mobile phones will be sent to the users if and only if they are near to each other. Hence if the user is in proximity then only he/she can receive the OTP to unlock the computer.

4. Working

4.1. Overview

To use One-time passwords along with the regular windows authentication password, we need to send this one-time code to the authenticated user. For this, we use the Bluetooth Technology. Using the Bluetooth on Computer/laptop, we connect the user’s Mobile with Bluetooth enabled feature with the Laptop/Computer with Bluetooth feature. Once the user moves away from his/her computer device along with the mobile phone, the Bluetooth connection is lost between the computer and the mobile phone and the system gets locked automatically.

Once the user comes again to the proximity of the computer/laptop, the Bluetooth connection is set and the user receives an OTP on t\his/her mobile phone. The user enters this OTP. System permissions are given back once an authentic OTP is entered.

4.2. Phases

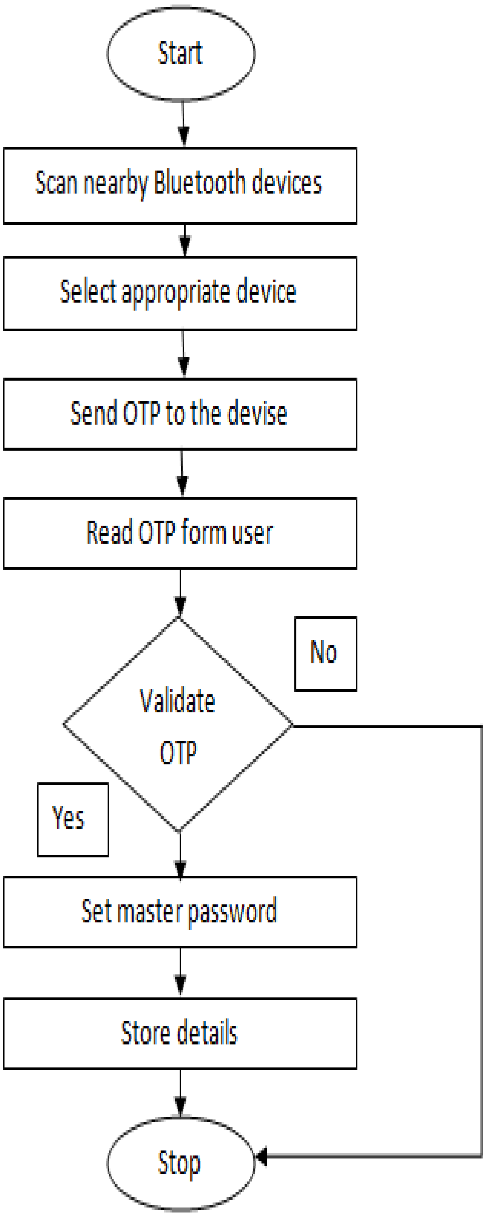
1. Registration / Configuration Phase:
2. Operational Phase

Registration / Configuration Phase:

In this phase, the user configures its Bluetooth device in order to be identified later in the operational phase. In this, the Software running on the Computer system (Desktop) searches for the nearby Bluetooth devices in the range. User selects the appropriate device from the list of the devices found. The token generation algorithm then generates a pseudo unique token; this is then sent to the selected device. Then user is asked to enter the token for the authentication. If token is valid the window prompts for setting a master password. Once master password is set, whole device and user details are stored into the database for further references in Operational phase.

Operational Phase:

After completion of the Registration phase, the software running on the computer system continuously scans the nearby Bluetooth device. If the Bluetooth device that is registered is available then the user is allowed to access all the features of the OS. If it does not find the registered Bluetooth device i.e. as soon as software detects that the connectivity has lost to the Bluetooth device, it locks the OS. In any other phase of Bluetooth device scanning if the software finds that the registered devices are in the range, the token generation algorithm generates pseudo unique token. This token is then sent to the device. The window pop-ups, that asks user to enter the token (One Time Password). If the token is valid then again it will ask for master password. If master password is valid then OS features are again accessible to user i.e. the OS gets Unlocked else the user will have to wait for the next round of scanning which will repeat the same procedure. In order to enhance the security, 2 Bluetooth devices are considered. The primary device will be the normal mobile phone Bluetooth which will receive OTP. And secondary Bluetooth device is the Bluetooth module which acts as passive authentication component.



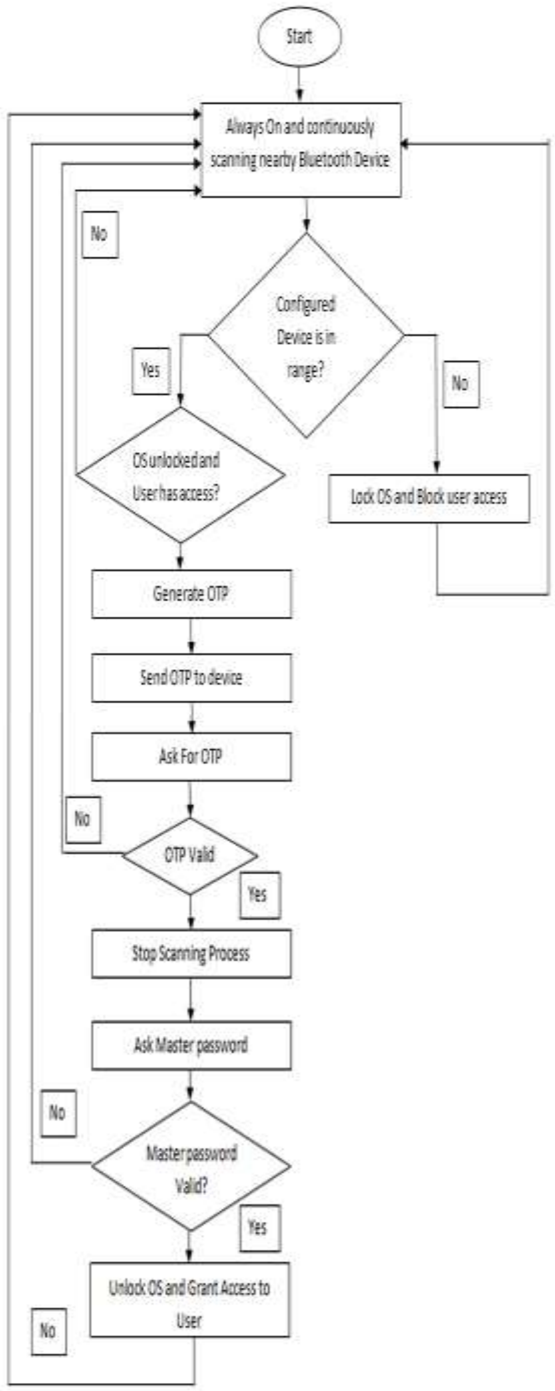
4.3. Hardware Requirements of the System:

- Mobile phone with Bluetooth:
  The phone should be enabled with a working Bluetooth. OS specifications are not an issue. The Bluetooth MAC address is taken by the computer application and store it in the database for future communications.
- Bluetooth dongle Plug n Play:
  Required for the computer or laptop devices that do not have an in-built Bluetooth feature.
- PC or a Laptop.

System Design

5.1 Registration Phase Flowchart

5.2 Operational Phase Flowchart:


Start
Always On and continuously scanning nearby Bluetooth Device
No
Configured Device is in range?
Yes
No
OS unlocked and User has access?
Lock OS and Block user access
Generate OTP
Send OTP to device
Ask For OTP
No
OTP Valid
Yes
Stop Scanning Process
Ask Master password
No
Master password Valid?
Yes
Unlock OS and Grant Access to User
No

6. Results

This proposed system will add another security layer to the default security layer of the windows operating system. The proposed system is easy to use, just requires one time registration and the OTP ensures access to only authenticated users.

The default windows security policies are easy to break involving only passwords to protect you. The proposed system makes it difficult for an attacker to get into the system. The OTP is sent only to an authenticated and registered mobile device, which ensures that no one other gets it.

A drawback with the proposed system is that, the process is a little time consuming. Also, time is involved in setting up a connection and sending the OTP to the user.

Here, a trade-off between time and security takes place. The windows authentication policies require less time but are insecure. While the proposed system is a little time consuming, but ensure user security.

7. Future Scope

- Decreasing the execution time of programs.
- Installing Bluetooth module in a wearable technology and using it as a reference check for connectivity.
- This technology can be extended for securing other computing devices such as computerized locks in cars, house, offices, etc.

8. Conclusion

By using this method of OTP along with Bluetooth technology, we can secure our computer devices and our vital data from being exposed easily. This can be additional security mechanism to our normal windows authentication process. Using this technology also does not cost any extra cost to the user. Also this proposed solution overcomes the disadvantages of other solutions proposed by others till now. Also, almost all computing devices running Bluetooth can be secured using just a single authentication device, where user need not remember any passwords for them.

9. References:

1. Pharaoh Chaka, Hilton Chikwiriro, Clive Nyasondo, Improving the windows password policies using the mobile Bluetooth and rijndael encryption, IJCSMC vol.3 issue 3, 2014.
2. http://bluecove.org/
3. https://Microsoft.com
4. www.airccj.org/cscp/volume2/csit2417.pdf