BlueKey
A Bluetooth Secure Solution for Accessing Personal Computers

Aziz Barbar[1] and Anis Ismail[2]
[1]*American University of Science & Technology, Beirut, Lebanon*
[2]*University Institute of Technology, Lebanese University, Sidon, Lebanon*

Keywords: Security, Personal Computers, Computer Locking/Unlocking, Bluetooth, Mobile Application.

Abstract: A major realm of security breach for today's users is unprivileged access, modification or sometimes forgery of critical business, or user information. Existing computer locking/unoking methods serve as an intermediate barrier against unethical deeds. The proposed solution BlueKey is a software-based solution installed on Personal Computers (PC) that safely unlocks the PC by securing the Bluetooth communication channel between the user's mobile device and his/her PC. BlueKey helps end-users in not typing their passwords every time they need to access their PCs. At the same level, this solution includes a mobile application that allows the owner to fully control his/her PC via Bluetooth, and runs a breach detector module with safety measures to protect the PC when it is locked. At the technical level, BlueKey is a platform free application written using Java programming language, fulfilling the Write Once Run Anywhere (WORA) concept. This system is built using Java Development Kit (JDK) and compiled using Java Virtual Machine (JVM), and runs with Java Runtime Environment (JRE). Alongside, the mobile application is developed using Java 2 Micro Edition (J2ME), which is compatible with Android, Symbian, and BlackBerry operating systems.

1 INTRODUCTION

Security is the science of building a nearly perfect breach-proof shield by implementing cryptographic functions to encipher vital information. Security methods are not only a business of the modern world, yet it has roots that began around 2,000 B.C. in Egypt when hieroglyphics were used to decorate tombs to tell the story of life of the deceased. Just over 3,000 years later, and during World War II, security played an essential role in giving the upper hand to those parties which first implemented it. And the Germans were the first to deploy secure channels, and that was by inventing the "Enigma" machine that encoded communications among different squads in the army, the naval, ground forces, and air forces. But as time progressed, these methods evolved to be the corner stone that secures the digital world we live in today (Harris, 2011). Confidentiality, Integrity, Authenticity, and Availability are among the major aims of any security product that is built. Confidentiality (Bishop, 2004) is the act of keeping data secretes and unpublished. Integrity (Bishop, 2004) is the act of preserving the data transmitted, and ensures authorized modifications. Availability (Bishop, 2004) is the act of approving authorized access to resources. Authenticity (Bishop, 2004) is the act of ensuring that this action is traceable from that entity.

This paper targets computer-locking/unlocking methods for Personal Computers (PC) and laptops without having to enter manually the password to unlock the machine. These methods are found nowadays in all operating systems such as Windows, Mac OS, and Linux, where the major function of these methods is to prevent unethical users to gain access to a computer, and corrupt or misuse the data stored in them.

In this paper, section 2 will present the work done in this field, section 3 will show the proposed system architecture, section 4 will tackle the implementation and obtained results, and finally section 5 concludes the work.

2 RELATED WORK

In Windows OS, a user desktop may be locked for security reasons either by setting an automatic screen lock that is initiated with the screensaver after a set

Barbar A. and Ismail A..
BlueKey - A Bluetooth Secure Solution for Accessing Personal Computers.
DOI: 10.5220/0005470905090515
In *Proceedings of the 17th International Conference on Enterprise Information Systems* (ICEIS-2015), pages 509-515
ISBN: 978-989-758-097-0

period of inactivity, or by manually choosing lock the computer. Once the computer screen lock is invoked, access to the computer will only be allowed to the user whose account is currently logged on to the computer or by an authorized administrator (Microsoft, 2015).

The ability to easily lock the Linux desktop is useful in a wide range of situations (Spidle, 2015.). Whether users are just walking away from your computer for a few minutes or operate a public machine, it is important that the user configures the Linux computer to protect his/her private data and prevent unauthorized system changes. Linux includes some basic built-in features that allows user to initiate a lockdown on the system, but if user wants more control over the computer system locking features, he/she needs to install the lockdown manager packages freely available to most Linux distributions. There are two ways to lock the Linux desktop, Simple Desktop Lockdown and Complete System Lockdown. Initially the simple desktop lockdown, the user has to perform a series of steps; first he/she has to launch the screen-saver preferences panel. On the other hand, the second way to lock a Linux desktop is the complete system lockdown method.

Desktop Lock (Desktop Lock, 2014) is a computer security protection and access control software product. Users can lock their computers to prevent people from accessing their private documents and resources. Users can lock their computers explicitly or automatically when system becomes idle. The user can customize the appearances of the locked desktop with the options provided by Desktop Lock. Desktop Lock also supports hotkey to lock the system.

PC Lockup (PC Lockup, 2014) is computer security software, which enables you to apply password protection to Windows and restrict others from being able to use your PC while you are away. It starts automatically with Windows and optionally locks your desktop upon loading. It hides your desktop at the same time and shows a picture, which you can change in the options. An allowed time schedule and duration can be defined for each user to restrict access to your PC in definite hours. PC Lockup also supports monitor power save options and has some additional useful features like built-in password protected screen saver and network user validation feature for Windows logon to increase your security. You will find the program interface very easy to negotiate.

3 SYSTEM ARCHITECTURE

The system architecture is composed of layers. We represent the system architecture as diagrams that illustrate the layers, topology, components, interactions, and stakeholders of the system. Layer architecture is a technique used in designing computer software, hardware, and communications in which system or network components are isolated in layers so that changes can be made in one layer without affecting the others.

3.1 Application Layer Architecture

The diagram shown in Figure 1 illustrates the different layers of the application. The application comprises of three architectural layers ordered as, Operating System, Application Core Structure, and Application Configuration Interface. The operating system layer forms the platform that accommodates the application and makes it operable on a computer. The operating system favors the application to functions and handles its requests and modules. The application core structure layer contains the application code structure that communicates with the operating system. In addition, it contains all the application major functions and defines the actual operations.

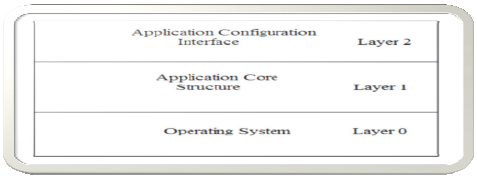

Figure 1: Application Layer.

This Application configuration interface layer contains a GUI (Graphical User Interface) interactive forms that interact with the application users. These GUI forms provide input data entered by the users and passed to the application core structure as parameters and operable data.

3.2 Mobile Application Layer Architecture

The mobile application comprises of three layers (Figure 2), Smart Phone Firmware, Mobile Application Core Structure, and Mobile Application Control Console (GUI). The Smart Phone Firmware layer is the software platform that controls the entire functions of a smart phone. It is pretty much as the operating system of a computer.

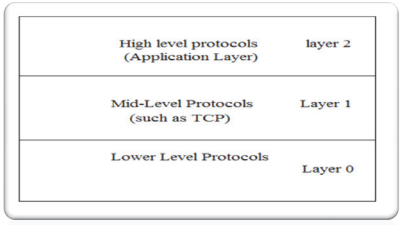

Figure 2: Mobile Application Layer.

The Mobile Application Core Structure is the layer which forms the communication between BlueKey application and the phone. This communication includes the basic computer control functions and the classes that handle the instructions that will travel via Bluetooth to predetermined MAC (the administrator computer) and forces the computer to execute these commands. The Mobile Application Control Console is the layer that communicates with the administrator, and receives his/her button presses.

3.3 Operational-logic Diagram (Reachable Device)

Figure 3 illustrates the procedure that takes place in the authentication process. Initially, the computer would scan for reachable devices, and enables the user to choose the trusted devices. In the first case, the mobile holder is within the Bluetooth range of the corresponding computer.

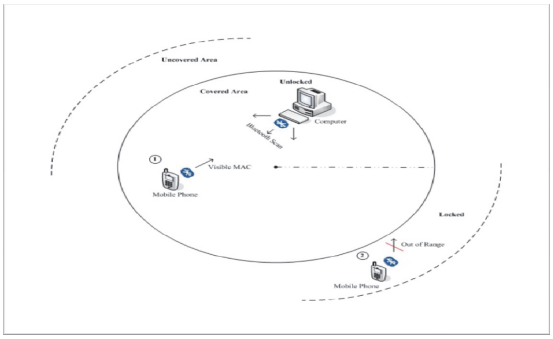

Figure 3: Operational Logic (Reachable Device).

At this point the computer is in unlocking mode. In the second case, the mobile holder is out of the Bluetooth range causing the corresponding computer to lock instantly. At the practical level, the Bluetooth receptor in the computer keeps track of the Bluetooth MAC address of the enabled devices and performs the suitable action.

3.4 Operational-logic Diagram (Unreachable Device)

Figure 4 justifies the operational logic of the application in case of the mobile phone is out of the computer Bluetooth range. At this stage, the computer would not define the MAC address as reachable, as a result the application orders the computer to lock, hence, the administrator is away from his/her machine.

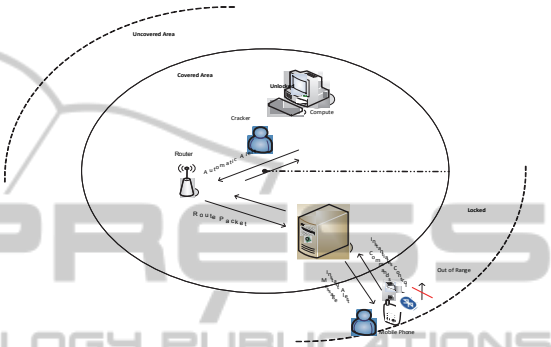

Figure 4: Operational Logic (Unreachable Device).

Figure 4 shows an intruder trying to run a password-cracking tool to break into a PC. One of the features of this system is the ability to inform the administrator of a possible crack. If a single key is pressed or any motion is detected on the mouse pad, the application triggers an alert message on the administrator's mobile via Bluetooth, notifying him/her of a possible intrusion.

3.5 Use-case Diagrams

Use-case (Whitte, 1986) is a diagram that shows the interactions between the system and external systems and users. It graphically describes who will use the system and in what ways the user expects to interact with the system. The use-case diagram is comprised of actors, and processes. The actors are the man-like characters, and they form all the actions initiators, meaning they initiate actions on the system, and the oval shaped components are the processes pertaining to the possible actions that are supported by the system. In the BlueKey use-case (Figure 5) the actors are administrator, trusted party, computer, and mobile application or the mobile phone itself. And the processes are add, drop, specify privilege, authenticate access application and access resources for actor administrator, moreover authenticate, access resources and exploit for the actor trusted party. For the actor mobile application the processes are request. The actor computer has processes executes

and sends message. Remark that process "configures" is not mentioned as administrator's processes since all the mentioned processes of administrator are configuration of the system, but the use-case rules state that between an actor and another there must exist a process, which in this case is "configure".

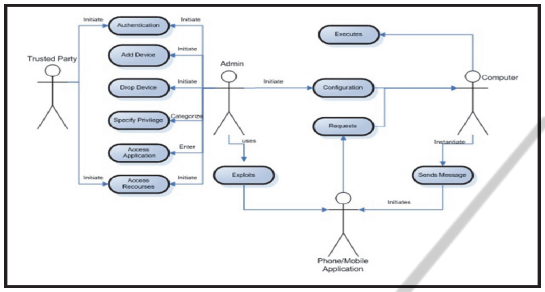

Figure 5: BlueKey Use-case.

3.6 System Sequence Diagram

System Sequence Diagram (SSD) (Choubey, 2012) is a diagram that depicts the interaction between an actor and the system for a use case scenario. Moreover it helps identify high-level messages that enter and exit the system.

Application first time Login For the first time login, the application would force the administrator to enter a password to be considered by the application a login password. The application would request from the administrator through requestappinfo() method with no parameter usually it's a GUI (graphical user interface window), afterwards the administrator would provide the specific password by provides() method with a string parameter. Consequently, the application would inform the administrator that the information entered has been saved in a file. Application nth time Login After the password is requested and saved in corresponding file, every login would require the administrator to provide this exact password to gain permission to enter to the application configuration options and settings (Figure 6).

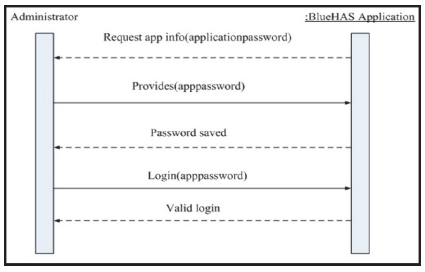

Figure 6: Login SSD.

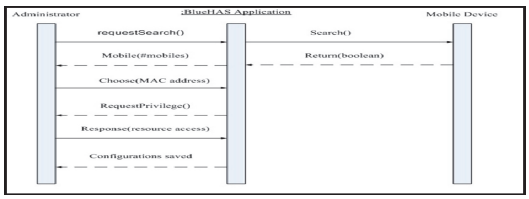

Figure 7: Scanning SSD.

Scanning Settings (Figure 7) after login the administrator would start configuring his/her mobile device and other desired trusted mobile devices. The administrator presses the configuration button; this would initiate a Bluetooth scan facility to trace any mobile device within the computer Bluetooth range. The administrator would then select the MAC addresses of the desired mobile devices, then the administrator is meant to set the parameters of his/her mobile device for locking and unlocking the PC, and then save these configurations in a respective file (repository file). Authentication this part of the application procedure is formulated when the administrator's mobile is usually publishing it MAC address. A condition is implemented within the application at the level of coding to control the distance-locking combination. If the distance of the mobile device within the range, the application would authenticate this mobile device instantly, on the other hand, if the mobile device is out of the range the application would lock instantly. In case, a cracker is trying to attack the PC, the method Scanner () would detect any change in data input, and initiate a read action from the default message file and send an alert message to the administrator's mobile device. At this point, the Administrator would send a Bluetooth control command to shutdown, or restart the PC under attack.

4 SYSTEM IMPLEMENTATION AND TESTING

BlueKey System is written in Java programming language, since Java technology is a high-level programming, a platform independent language, and has GUI features that provide friendly user interface. Java is a WORA (Write Once Run Anywhere), furthermore, Java is used to create standalone applications which may run on a single computer or in distributed network.

4.1 BlueKey Graphical User Interface

The mobile phone acts as a wireless "key" to the

administrator desktop. This system requires the use of Bluetooth on the device and the PC to pair the two. The Bluetooth signal includes a crude "distance" between the two devices. When the device goes out of range, the system will automatically trigger the screensaver and can also lock the screen of the computer with a password. The BlueKey system keeps monitoring the distance, and when the device comes back within range, the computer automatically wakes up without ever having to enter a password. Before the administrator runs the BlueKey System for the first time, he/she should make sure that the Bluetooth is set up on his/her computer, and he/she has paired his/her Bluetooth device with respective computer. The system will run in the background, and display a small icon in the taskbar to show its status. So the administrator will be able to click on the icon to configure its settings. When running the BlueKey System to configure a device, a GUI interface will be displayed. This interface contains several tabs, among them, a tab to configure the Bluetooth device, another to specify the proximity Details, and another to lock the PC.

4.1.1 Bluetooth Device Configuration

The initial GUI screen (Figure 11) would be displayed containing several buttons and text fields. When the administrator clicks on the "Scan for devices" button, a list of MAC addresses along with the Names of all devices within the range of the computers Bluetooth receiver would be displayed in the text field named "Bluetooth Device". When the administrator chooses a device to configure, he/she would then select the button "Use selected device", the MAC address will be displayed in the text Field "MAC Address". Moreover, the administrator could click on the "Delete" button to remove a configured device, or click on "Rename" button to rename the selected one.

4.1.2 System Details

In the System Details tab, locking and unlocking details will be displayed. The administrator can set the distance and times to lock and unlock the computer. The distance is a numeric value between 0-255 which is a rough range of how far the Bluetooth device is from the computer. At the bottom of the tab, "Measure atm" displays the current distance, as well as the minimum and maximum distances that have (Figure 8) been detected.

The duration corresponds to the number of seconds the Bluetooth device needs to be outside of the distance before the computer locks. The administrator may need to use some trial and error to find the right value. The "Unlocking" options are similar to those of "Locking" options, but have exactly opposite functions. When the Bluetooth device is detected within the specified distance for the complete duration, the computer unlocks.

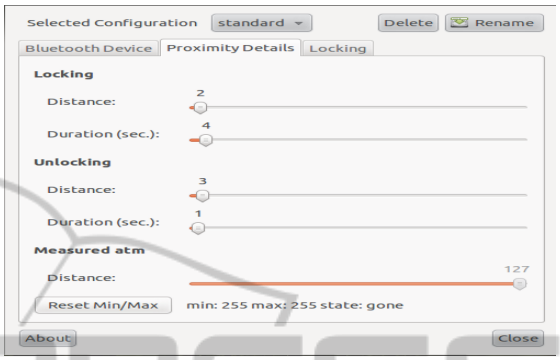

Figure 8: Computer application configuration windows.

4.1.3 System Features

The final preferences tab, "Locking" (Figure 9), controls how the system locks and unlocks the computer. In the "Locking Command/Unlocking command" text fields, the application developer would previously embed the specific command to lock and unlock the computer in correspondence to the existing computer platform. Basically, BlueKey System will call screensaver-command to control the screensaver–turning functions appropriately. Consequently, the administrator would also need to set up a screensaver.

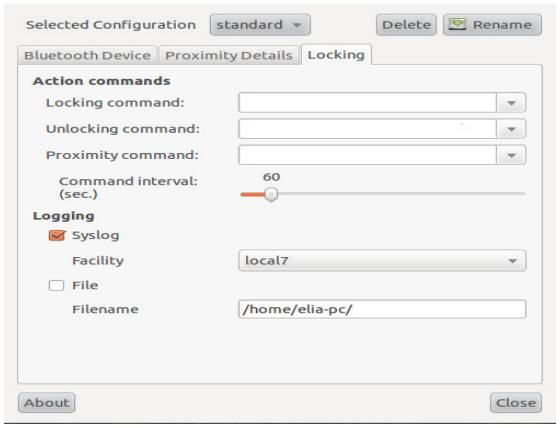

Figure 9: Computer Application Locking/Unlocking Window.

4.2 Desktop Application Testing

BlueKey application consists of several components.

The components are majorly divided into a login process, cryptography process, scan process, plug-in detection process, messaging process, file sender process, and a mobile application server process. The login page is the first page to appear when the user launches the application. The login page is sort of a welcome screen that debriefs the first time user on the application. In the Login page a password should be provided and then saved in a file in a specific directory.

BlueKey application consists of several components. The components are majorly divided into a login process, cryptography process, scan process, plug-in detection process, messaging process, file sender process, and a mobile application server process. The login page is the first page to appear when the user launches the application. The login page is sort of a welcome screen that debriefs the first time user on the application. In the Login page a password should be provided and stored in a file under a specific directory. A message box appears for first time users giving the indications for the following step and a little note about the Operating System identity.

4.2.1 Cryptography and Password Testing

Cryptography process ensures that some cryptographic algorithm secures confidential data related to the system. In BlueKey, the DES algorithm is applied and tested to ensure that the password is still the same after the encryption and the decryption processes.

4.2.2 File Testing

Every time the user runs the BlueKey Application, all files are inspected for their existence. If not, the creation of a new file should be proved. Then, two testing phases are conducted. One of them ensures the creation of new file after being deleted, and the other ensures the creation of the whole folder that holds the file to be created. Another testing criterion is applied on the hidden file, when the user enters the password, the directory that holds the file that's containing the password is checked to make certain that the file is hidden. If the user wishes to change the admin password, the file containing the password should be checked if changed that's to say overridden. As for the trusted MAC addresses should be appended to the previously saved MAC addresses. Even if the user deletes any of these files (AdminMac, TrustedMac) the application will generate it again.

4.2.3 Scan Testing

Scanning is a major part of the workflow within the application itself. The testing of this component is briefed out as activating the Bluetooth hardware device, and simply pressing "SCAN" (Figure 10). This triggers an embedded Bluetooth scan class that does Bluetooth explorations of all devices that are within the range of a specific PC. Tests are applied to check if all the inbound devices are listed on the configuration console. The types of devices that are included within the list are the BB, Sony Ericsson, Samsung, iPhone, Nokia except for the HTC. In addition to that, out-of-bound devices are tested for their removal from the list.

Figure 10: BlueKey Scan Window.

An additional feature that alarms against hackers attacks is the Pre-Alarm system. User should set his account settings, provide his username and password and enter his mobile phone number to enable the trigger automatic warning messages. The administrator has the privilege of changing the application password, can send files via Bluetooth through the application to his/her own mobile phone, and can launch the mobile application from within the Desktop Application.

4.2.4 Activation Testing

After activating the pinging process, the application is checked to ensure that the MAC addresses in the AdminMac and TrustedMac files are being pinged simultaneously. All the trusted devices including the admin device should be out of range for the system to lock. Ping should stop only when deactivated. Pushing the lock process to take place by moving the device out of the Bluetooth range proves this and then moving it within range, hence when unlocked, ping is verified. The unlock process of the application may face some defects that may lead the system to crash.

4.2.5 Operating System Detection Testing

The application is tested on both platforms, Windows and Linux. The detection of OS holding the application is perfectly done and suitable code is automatically launched corresponding to the platform being boot.

4.3 Mobile Application Testing

The mobile application enables the user to have full control over the desktop holding the application. The application is verified to be able to allow the admin to browse, access all resources, and have full control over the PC hosting the application. The mobile server that enables the full control over the PC, works on both internet and Bluetooth technologies. A password should be provided for authentication for the connection to take place. The mobile application takes some time after connecting to stream the PC screen and consequently click events trigger the execution process. Integrating the application increments all together, system should be tested as a whole to ensure reduced errors, acceptable performance and tolerable errors.

5 CONCLUSIONS AND FUTURE WORK

BlueKey provides the user an ease of use during the authentication process, and an ease of mind for knowing that the personal resources are safe, and a full control from a 24/24 companion, which is the user's mobile phone. The authentication process is no longer manual; the PC knows the user and authenticates him/her without even providing a password. Moreover, the application changes the PC into a smarter one since it enables it to lock itself whenever the user is out of the desktop Bluetooth range; it becomes automatically safe even if the user leaves it unlocked. It provides efficiency of time and minimization of effort, through the remote desktop control that can be done in all times anywhere, from the mobile screen via Bluetooth or Internet. Future plans include finalizing the development of the Pre-alarm messaging system and adding more features to it, such as allowing the warning messages to be sent via the Web for free.

REFERENCES

Harris S., 2011. *textbook*, 200075, Available: www.cccure.org/Documents/Cryptography/cisspallinone.pdf

Bishop M., 2004. Introduction to Computer Security, Addison-Wesley.

Whitte J. L., 1986. Bentley-Whitten. *Systems Analysis and Design for Global Enterprise* 7th, McGraw-Hill International Edition, pp 31-32.

Choubey M. K., 2012. *IT Infrastructure and Management* (For the GBTU and MMTU). p. 53.

Microsoft, 2015. *Locking and Unlocking a User Desktop*, http://technet.microsoft.com/en-us/library/dd277426.aspx.

Spidle J., 2015. *How to Lock Down the Desktop in Linux*, http://www.ehow.com/how_5887726_lock-down-desktop-linux.html.

Desktop Lock, 2014, http://www.toplang.com/desktoplock.htm.

PC Lockup, 2014, http://www.softheap.com/wlock.html.