International Journal of Computer Applications Technology and Research
Volume 3– Issue 3, 146 - 149, 2014, ISSN: 2319–8656

Mobile Device Protection Using Sensors

Anna Rose Vembil
Department of Computer Science and Engineering
Jyothi Engineering College, Cheruthuruthy, Thrissur, India.

Shilna Latheef
Department of Computer Science and Engineering
Jyothi Engineering College, Cheruthuruthy, Thrissur, India

Swathy Ramadas
Department of Computer Science and Engineering
Jyothi Engineering College, Cheruthuruthy, Thrissur, India

Anil Antony
Department of Computer Science and Engineering
Jyothi Engineering College, Cheruthuruthy, Thrissur, India

Abstract: Mobile devices like laptops, iPhones and PDAs are highly susceptible to theft in public places like airport terminal, library and cafe. Moreover, the exposure of sensitive data stored in the mobile device could be more damaging than the loss of device itself. In this work, we propose and implement a mobile device protection system using sensors, based on sensing and wireless networking technologies. Comparing with existing solutions, it is unique in providing an integrated protection to both device and data. It is a context-aware system which adjusts the protection level to the mobile device dynamically according to the context information such as the user proximity to the mobile device, which is collected via the interactions between the sensors carried by the user, embedded with the mobile device and deployed in the surrounding environment.
Keywords: User Sensor (US), Mobile Device Sensor (MDS), Advanced Encryption Standard (AES), Central Server (CS)

1. INTRODUCTION

Mobile devices, such as laptops, smart phones and PDAs, have become an essential part of our daily life. They are small and easy to carry but also powerful in computational and storage capabilities. Unfortunately, these merits also put them at risk. For example, because mobile devices are small, they usually are highly susceptible to theft, especially at public places like airport terminal, library and cafe. As mobile devices get slimmer and more powerful, the number of mobile device thefts surges.

On the other hand, keeping data secure in a mobile device is a critical requirement. Unfortunately, a majority of the mobile device users do not take necessary actions to protect the data stored in their mobile devices. Therefore, the loss of a mobile device could mean the loss and exposure of sensitive information stored in the lost device, which may be much more valuable than the device itself. In this paper, we propose a mobile device protection system for sensors, with the help from sensing and wireless networking technologies. We deploy low-cost wireless devices at public places of our interest. Users and mobile devices carry special-purpose wireless sensing devices which provide protection to the mobile device and the data stored in it.

Specifically, this paper has the following unique features:

• Context Awareness: Sensors carried by the user and the mobile device interact with each other to collect context information (e.g., proximity of the user to the mobile device) and then the system adapts its behavior properly and promptly to the context change.

– Anti-theft Protection for Mobile Device: When the user is away from the mobile device, system monitors the mobile device. When a potential theft is detected, system quickly alerts the user.

– Data Protection: System adapts the protection level for data stored in the mobile device and incorporates a carefully-designed authentication mechanism to eliminate possible security attacks.

• Low-cost and Light-weight: System utilizes low-cost sensors and networking devices. The software implementation is light-weight and may be adapted for mobile devices of various kinds.

2. RELATED WORKS

a. Mobile Device Protection

Different models exist for the protection of the mobile device against theft In general, they can be classified into the following two categories: *recovery/tracking-oriented systems* and *prevention-oriented systems* .In *recovery/tracking –oriented* systems, a back-end software process runs on the device, which can send "help" messages across the Internet to the tracking service provider in case the device is lost or stolen. The service provider can pinpoint the location of the lost device based on the "help" messages. These systems are ineffective in preventing mobile device thefts since they aim at recovering the devices at theft.

In comparison, prevention-oriented systems aim at deterring the adversary from compromising the mobile device. When a potential theft is detected, the system raises an audible alarm to deter the adversary from completing the theft. Ka Yang, Nalin Subramanian, Daji Qiao, and Wensheng Zhang proposed a context-aware system which adjusts the protection level to the mobile device dynamically according to the context information such as the user proximity to the mobile device, which is collected via the interactions between the sensors carried by the user, embedded with the mobile device and deployed in the surrounding environment. When a potential theft is detected, an audible alarm will be triggered to deter the adversary from completing the theft. At the same time, alert messages will also be sent to the user. The MDS initiates the alert messages and sends them either directly to the user if the user is within direct communication range to the mobile device, or via the wireless network infrastructure. [1]

b. Data Protection

There are systems which give importance to the protection of the data. Mark D Corner and Brian D. Noble, proposed a system, where the user wears a small authentication token that communicates with a laptop over a short-range, wireless link.Whenever the laptop needs decryption authority, it acquires it from the token. The token will continuously authenticate to the laptop by means of a short-range, wireless link. Each on-disk object is encrypted by some symmetric key, Ke. File decryption takes place on the laptop, not the token. The file system stores each Ke, encrypted by some key-encrypting key, Kk. Only tokens know key-encrypting keys. A token with the appropriate Kk can decrypt Ke, and hence able to read files encrypted by Ke[2]. Carl E. Landwehr proposed a system where the user is given a token called wireless identification agent. It consists of a key unique to that WIA to each user. Once per *Tre-ident*or when prompted by the WIA, the user enters the PIN, becoming an

identified user. The detector attached to the workstation verifies the user. If the Detector fails to get a valid response from the current user's WIA within specified period *Td*, the Detector blanks the screen and disables the keyboard. Thus prevents the thief from accessing the data[4].Eagle vision protects the data the file system on the mobile device by encryption using a symmetric key *K*enc , which allows lower encryption and decryption latency. *K*enc is protected with a PKI public key *K*pub and the encrypted symmetric key *{K*enc*}K*pub is stored on the mobile device [1].

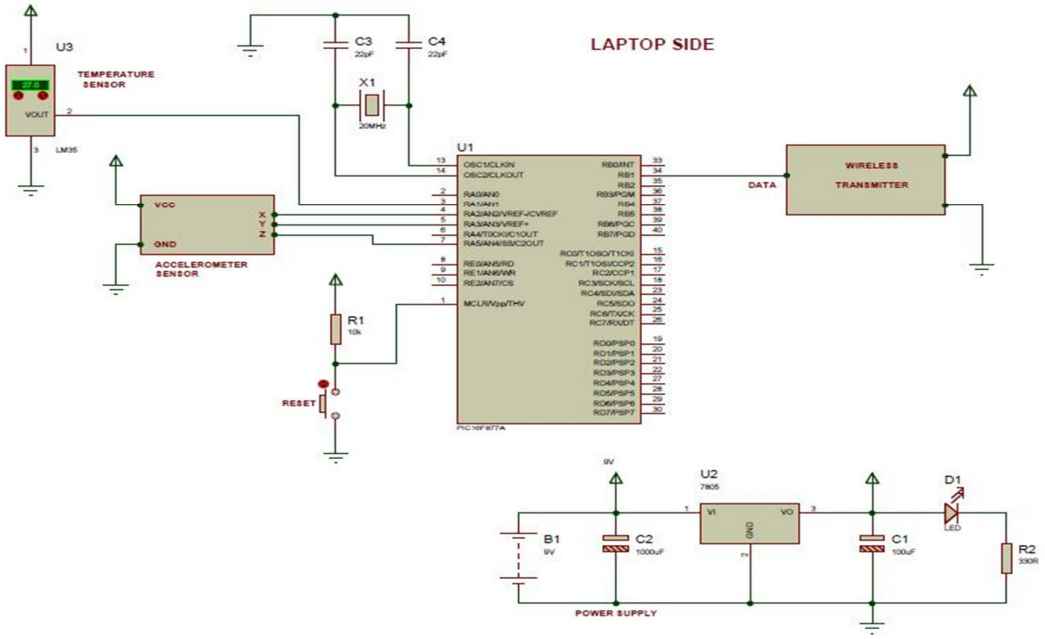

Figure 1 Mobile Sensor Circuit Diagram

3. PROPOSED SYSTEM

In this section we discuss about our proposed system. The proposed scheme enhances the security level in our mobile device by providing various features.

A. *Temperature Detection*

When the temperature of the surrounding environment increases it can cause damage to the mobile devices. Here we set a certain threshold value of temperature for the mobile device. When the value of the temperature exceeds this threshold value, an alert is send to the user by setting an alarm and the important data that is selected by the user is stored as a backup. The temperature sensor we used here is LM35.

B. *Low Cost*

In other papers a two way communication is maintained which involves the use of ZigBee which is very costly. But in this paper we implement a one way communication between the US and the MDS which does not involve the use of such expensive sensors and thus makes it a cost effective system.

C. *Encryption and File Transfer*

When a threat is detected the files in the mobile device are encrypted and sent to the central server. The files are selected according to their importance by the user. The files are transferred to the server through socket programming.

D. *Alert*

The mobile device sensor consists of an accelerometer having x, y and z coordinates. A certain threshold value for these coordinates is defined. When the value of these coordinates exceeds this threshold value it gives an alert to the user by setting an alarm.

4. IMPLEMENTATION

We demonstrate our mobile device protection system for the following features: anti-theft protection, privacy protection,

alerts dispatch and context awareness. In the following, we present a) details of hardware b) system model, c) trust and threat model and d) an example scenario.

a. Hardware Components

We implement the mobile device protection system using various components. We have a mobile device sensor as well as user sensor.. Mobile device sensor and user sensor communicate with each other using RF module. Mobile device sensor consists of RF transmitter and user sensor consists of RF receiver. As the laptop moves the accelerometer detects the motion. We use PIC16F877A here. The change in y, z coordinate and the temperature is noted. The temperature sensor used here is LM35. We use an encoder HT12E in mobile device sensor which encodes the value and passes it to the transmitter.

Transmitter sends this value to the receiver. We use a decoder HT12D at user sensor which decodes the value received from receiver. We use RS232 in mobile device sensor. RS232 is the traditional name for a series of standards for serial binary single ended data and control signals connecting between DTE (data terminal equipment) and DCE (data circuit-terminating equipment). It is commonly used in computer serial ports. We also use MAX232

that converts signals from an RS-232 serial port to signals suitable for use in TTL compatible digital logic circuits.

We also use 7805 regulator in mobile device sensor. 7805 is a voltage regulator integrated circuit. The voltage source in a circuit may have fluctuations and could not give the fixed voltage output. The voltage regulator maintains the output voltage at a constant value. Capacitors of suitable values can be connected at input and output pins depending upon the respective voltage levels. An accelerometer is a device that measures proper acceleration. Here we use MMA7260 sensor. 3-Axis accelerometer with selectable range and low-power sleep mode. The MMA7260Q from Free scale is a very nice sensor with easy analog interface. Runs at 3.3V with 3 analog output channels for the three axes. An accelerometer is a sensor that measures the physical acceleration experienced by an object due to inertial forces or due to mechanical excitation. Acceleration is defined as rate of change of velocity with respect to time. It is a measure of how fast speed changes. It is a vector quantity having both magnitude and direction. As a speedometer is a meter to measures speed, an accelerometer is a meter to measure acceleration. An ability of an accelerometer to sense acceleration can be put to use to measure a variety of things like tilt, vibration, rotation, collision, gravity, etc.

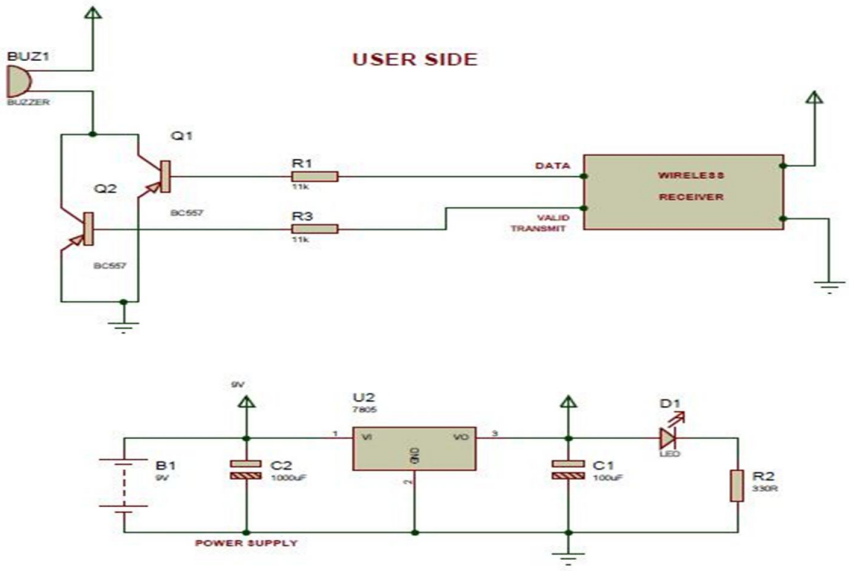

Figure 2 User Sensor Circuit Diagram

b. *System Model*

The Mobile Device protection System using Sensors consists of three components: *Mobile Device Sensor (MDS)*, *User Sensor (US)* and *Central Server (CS)*. Each mobile device carries an MDS which has several embedded sensors like an accelerometer and a temperature sensor. The MDS can communicate wirelessly with other system components. User of the mobile device carries a US, which interacts with other system components.

The accelerometer in the MDS detects the motion of the device and the temperature sensor present detects the temperature of the surrounding atmosphere. The MDS constantly interacts with the US using RF transmitter and receiver. This has a unique ID which helps in identifying the User Sensor the CS keeps the information about users and their mobile devices.

c. *Trust and Threat Model*

In our project the CS is considered to be trustable. A US is assumed to be secure as long as it is in the user's possession. An MDS is assumed to be secure when the user is nearby but may be tampered by the adversary if the user is away.

d. *An Example Scenario*

The following example scenario explains how our project works. Suppose Alice enters a library reading room with her laptop. Alice sets priority to certain files and Alice leaves the reading room to get some coffee from the café. Laptop's MDS starts to sample its accelerometer to detect any movement of the laptop and the temperature sensor checks the surrounding temperature for fluctuations. If a sudden movement is detected or the temperature rises, the laptop's MDS triggers an alarm in the US and the prioritized files are sent to the Central Server. Also the monitor locks itself. Alice can then decrypt files from the Central Server. The working is as given in figure 3.

5. CONCLUSION

In this paper, we propose a mobile device protection system. It is a context-aware system and protects the data stored in the mobile device in an adaptive manner .We implements this system using a mobile device, which consist of an accelerometer and a temperature sensor. It detects the motion as well as temperature. As motion is detected, the files are encrypted and transferred to the server. This system responds promptly to the context change and provides adequate protection to data, while not requiring explicit user intervention or causing extra distractions to the user. Future work includes further improvement of the system responsiveness.

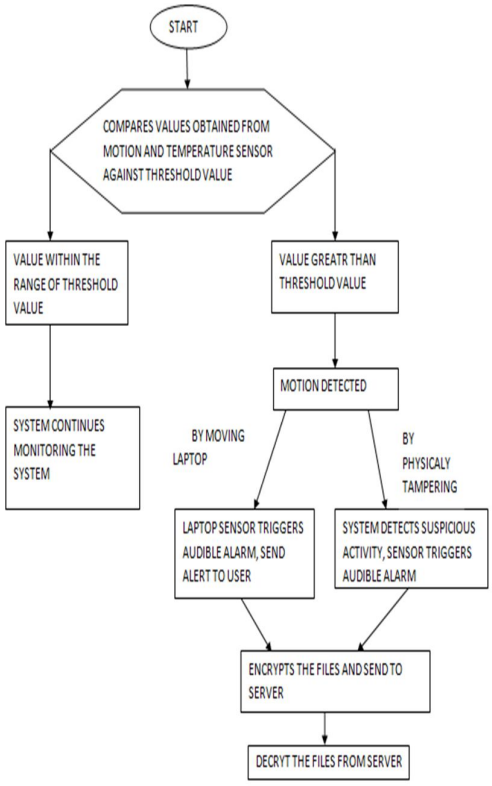

Figure 3 An Example Scenario

6. REFERENCES

[1] Eagle Vision: A Pervasive Mobile Device Protection System Ka Yang, Nalin Subramanian, DajiQiao, and Wensheng Zhang Iowa State University, Ames, Iowa – 50011

[2] M. D. Corner and B. D. Noble, "Zero-interaction authentication," in Proceedings of the 8th annual international conference on Mobile computing And networking, 2002.

[3] Mobile Device Security Using Transient Authentication, Anthony J. Nicholson, Mark D. Corner, and Brian D. Noble.

[4] Protecting Unattended Computers without Software, Carl E. Landwehr Naval Research Laboratory Code 5542Washington DC 20375-5337.

[5] Self Encryption Scheme for Data Protection in Mobile Devices, Yu Chen and Wei-Shinn Ku, Dept. of Electrical and Computer Engineering, SUNY Binghamton, Binghamton, NY 13902, Dept. of Computer Science and Software Engineering Aubum University, Aubum, Aubum AL 36849.

[6] A Hardware Implementation of Advanced Encryption Standard (AES) Algorithm using System Verilog. Bahram Hakhamaneshi, B. S. Islamic Azad University, Iran, 2004.

Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park