A Pervasive Mobile Device Protection System

Ka Yang, Nalin Subramanian, Daji Qiao and Wensheng Zhang
Iowa State University, Ames, Iowa - 50011

I. 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. Recently, as mobile devices get slimmer and more powerful, the number of mobile device thefts surges. According to the FBI's National Crime Information Center, the number of reported laptop thefts in 2008 rose with a 48 percent increase over the previous two years, from 73,700 to almost 109,000.

On the other hand, keeping data secure in a mobile device is not just a daunting challenge, but 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. According to CNN, a laptop theft case in 2006 related to Veterans Affairs Department resulted in the exposure of millions of veterans' personally identifiable information and costed the department 20 million dollars to settle the lawsuit against it.

This demo implements a pervasive mobile device protection system with the help from sensing and wireless networking technologies. In the system, we deploy low-cost wireless devices at public places of our interest to form a wireless network infrastructure. Users and mobile devices carry special-purpose wireless sensing devices which work with the wireless network infrastructure to provide protection to the mobile device and the data stored in it. Specifically, the system has the following features:

- Context Awareness: sensors carried by users and mobile devices collect context information (e.g., proximity between users and mobile devices) and the system adapts its behavior properly and promptly to the context change.
  - Anti-theft Protection for Mobile Device: the system will alert the user (directly or multi-hop via the wireless network infrastructure) when it detects a potential theft (e.g., via proximity sensor and motion sensor).
  - Privacy Protection for User Data on Mobile Device: the system adapts the privacy protection level for user data on mobile device. For example, when a user is away from his/her mobile device, user data on mobile device shall be encrypted.
- Transparency: System adapts its behavior autonomously without requiring explicit user intervention or causing extra distractions to the user.

II. System Overview

In our prototype (see Fig. 1), each laptop and each user carries a wireless sensor which runs on battery power supply. Each building such as library, shopping center, hospital, and airport has several infrastructure sensors installed at different spots to form an infrastructure sensor network. For each building, one separate infrastructure sensor network is formed and one central server is installed.

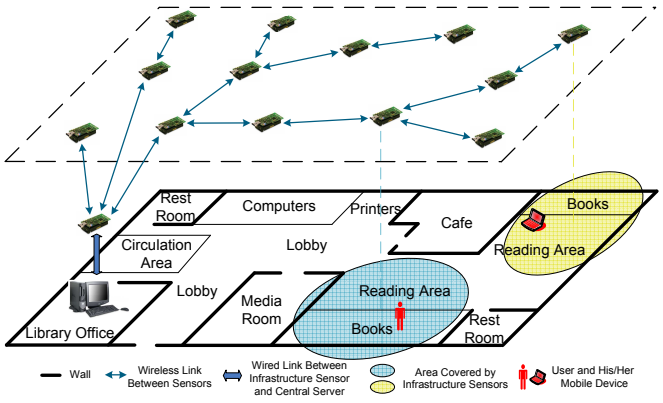

Fig. 1. System Architecture

Within an infrastructure sensor network, each laptop is monitored by its neighboring infrastructure sensors in the absence of its owner to detect suspicious activities. For example, suppose Alice enters a library. Alice's sensor and laptop's sensor join the infrastructure sensor network via an authenticated join message to neighboring infrastructure sensors. After joining the network, Alice's and her laptop's sensors periodically broadcast authenticated alive messages which can be heard by neighboring infrastructure sensors.

Suppose Alice wants to leave her laptop in a reading room for a while to get some coffee in the cafe. Commanded by safety modes based on Alice's proximity to her laptop, the laptop is locked automatically and sensitive information is protected by encryption. Further, the infrastructure sensors start to monitor her laptop. If moved by a thief, the laptop's sensor can detect the motion and trigger an alarm with alert messages sent to Alice (directly or via infrastructure). If the thief destroys the sensor in the laptop, the infrastructure sensors will not receive authenticated alive messages from the laptop sensors, thus detect the abnormal phenomenon. They will report the problem to the central server, which in turn automatically sends an alert message to Alice and the security authorities.

III. Demonstration Description

We demonstrate our pervasive 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 used in our prototype, b) demonstration setup, and c) scenarios to demonstrate the aforementioned features.

A. Hardware

We implement the pervasive mobile device protection system using various components. The user and infrastructure functionalities are implemented over TelosB motes. The property is composed of two parts, namely, a Dell Latitude laptop and a TelosB mote with SBT80 sensor board. SBT80 is a flexible sensor board with a variety of sensing modalities. The modality of SBT80 used for our prototype is a Dual-Axis Accelerometer (MMA6200). The central server is implemented in a Dell Latitude laptop connected to a TelosB mote. The transmission power level of motes for different components are adjusted to suit the demonstration circumstances and conditions.

B. Demo Setup

We will set up the demonstration as what follows:

- The infrastructure sensors (3∼5 TelosB motes) and a central server (a laptop) are set on a table to emulate the infrastructure in a building.
- Each user (emulated by a TelosB mote) enters the demonstration area with a laptop attached with a Telosb mote. During this step, the user and the laptop are registered with the infrastructure. The registration information is displayed on the central server screen.
- For demo purpose we use two users (say, X and Y), each carrying a laptop.
- As the user and laptop moves, their latest location information (room ID) is updated and displayed on the central server screen.

C. Demo Scenarios

We plan to demonstrate our system through six typical scenarios as shown in Fig. 2.

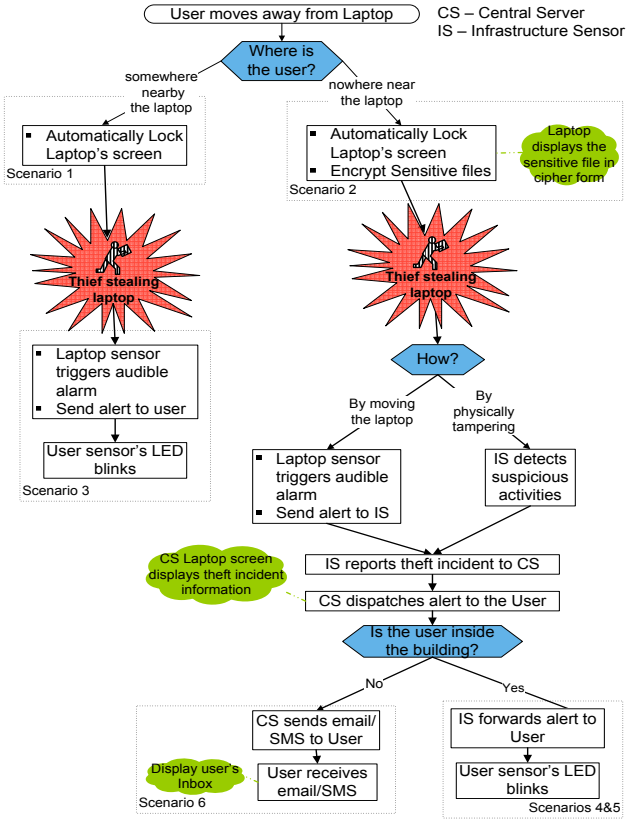

Fig. 2. Demonstration Scenarios

- *Scenario 1*: User X leaves the laptop and starts to move away; his/her laptop will *automatically lock the screen* thus restricts any unauthorized access.
- *Scenario 2*: User Y leaves the laptop and starts to move away; upon user Y *moving far away*, say to another room, his/her laptop will *automatically encrypt* the user predefined sensitive files. We will display a separate window on the screen of user laptop showing transition of a sensitive file from plain text to encrypted form as the encryption is performed. Note: for demonstration purpose we will disable screen lock feature for the laptop of user Y.
- *Scenario 3*: User X leaves the laptop and *moves to a nearby location* in the building. A *theft* event is emulated by *moving the laptop*. Our system demonstrates the response to this incident by means of (a) sounding an audible alarm, and (b) sending an alert message to the user directly (reception of the alert message is demonstrated via blinking user sensor's LED).
- *Scenario 4*: User X leaves the laptop and *moves far away* from the laptop in the building. A *theft* event is emulated by *moving the laptop*. Our system demonstrates the response to this incident by means of (a) sounding an audible alarm, (b) immediately reporting theft incident information to the central server (reception of theft incident is demonstrated via displaying on the screen of central server), and (c) quickly dispatching an alert message to the user based on last known user location information via wireless network infrastructure (reception of the alert message is demonstrated via blinking user sensor's LED).
- *Scenario 5*: User X leaves the laptop and moves far away from the laptop in the building. A *theft* event is emulated by physically *tampering the laptop* (say for instance, forcibly shutting down laptop and its associated sensor). Our system demonstrates the response to this incident by means of (a) quickly identifying theft incident by infrastructure, (b) reporting theft incident information to the central server, and (c) quickly dispatching an alert message to the user based on last known user location information via wireless network infrastructure (reception of the alert message is demonstrated via blinking user sensor's LED).
- *Scenario 6*: User X leaves the laptop and *moves out of the building*. A theft event is emulated by either moving the laptop or by physically tampering the laptop. Our system demonstrates the response to this incident by means of (a) sounding an audible alarm (in case of no physical tampering), (b) quickly identifying theft incident by infrastructure (in case of physical tampering), (c) reporting theft incident information to the central server, and (d) quickly dispatching an alert message to the user via instant messaging, for instance, e-mail (reception of the e-mail is demonstrated via displaying user's inbox messages in a separate window on the screen of central server).