IPHV7I2049X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

RFID SECURITY AND PRIVACY DISTANCE-BOUNDING PROTOCOLS FOR LOCATION SENSING

[#1]P.ARUNA - M.Tech Student,
[#2] P.PREM KISHAN -Assistant.Professor,
Department of ECE,
MLR INSTITUTE OF TECHNOLOGY,DUNDIGAL,HYDERABAD, TELANAGANA,INDIA.

***Abstract*—** In this paper, we report on a new approach for enhancing security and privacy in certain RFID applications whereby location or location-related information (such as speed) can serve as a legitimate access context. Examples of these applications include access cards, toll cards, credit cards, and other payment tokens. We show that location awareness can be used by both tags and back-end servers for defending against unauthorized reading and relay attacks on RFID systems. On the tag side, we design a location-aware selective unlocking mechanism using which tags can selectively respond to reader interrogations rather than doing so promiscuously. On the server side, we design a location-aware secure transaction verification scheme that allows a bank server to decide whether to approve or deny a payment transaction and detect a specific type of relay attack involving malicious readers. The premise of our work is a current technological advancement that can enable RFID tags with low-cost location (GPS) sensing capabilities. Unlike prior research on this subject, our defenses do not rely on auxiliary devices or require any explicit user involvement.

Index terms: RFID, GPS, Location aware selective unlocking, malicious readers.

I.INTRODUCTION

The premise of the proposed work is based on a current technological advancement that enables many RFID tags with low-cost sensing capabilities.We report on a new approach for enhancing security and privacy in certain RFID applications where by location or location-related information (such as speed) can serve as a legitimate access context. Examples of these applications include access cards, toll cards, credit cards, and other payment tokens. We show that location awareness can be used by both tags and back-end servers for defending against unauthorized reading and relay attacks on RFID systems. On the tag side, we design a location-aware selective unlocking mechanism using which tags can selectively respond to reader interrogations rather than doing so promiscuously. On the server side, we design a location-aware secure transaction verification scheme that allows a bank server to decide whether to approve or deny a payment transaction and detect a specific type of relay attack involving malicious readers. We show that location transaction verification to defend against the reader-and-ghost attacks, a devastating relay attack against mobile payment systems involving malicious readers. This is based on a straightforward observation that, under normal scenarios, both the legitimate tag and legitimate reader are in close physical proximity, at roughly the same location. Thus, if the two devices indicate different physically disparate locations, a bank server could detect the presence of a reader-and-ghost attack. In Vibrate-to-Unlock, a user unlocks his/her RFID tags by authenticating to these tags through a vibrating phone. However, such an auxiliary device (required by above schemes) may not be available at the time of accessing RFID tags, and users may not be willing to always carry these devices. The payment card stores card details such as the credit card number, name of the owner, and expiration date. It also stores a symmetric key shared with its issuer bank.

II. LITERATURE SURVEY

A SURVEY OF CONTEXT-AWARE MOBILE COMPUTING RESEARCH

Two technologies allow users to move about with computing power and network resources at hand: portable computers and wireless communications. Computers are shrinking; allowing many to be held by hand despite impressive computing capabilities, while the bandwidth of wireless links keep increasing. These changes have increasingly enabled people to access their personal information, corporate data, and public resources “anytime, anywhere”. There are already many wireless handheld computers available, running different operating systems such as Palm OS, Microsoft Pocket PC (Windows CE).

Wireless cellular networks. For example, Palm VII automatically connects to the portal www.palm.net snap on to a device’s serial port or into an expansion port. Omnisky provides the cellular modem that outfits the Palm V. Qualcomm integrates the Palm device and cellular phone as a new product pd Smart Phone, while Handspring has a cellular module to make their Palm OS Visor a mobile phone too.

Wireless LAN networks. For example, the Symbol PPT 2700 has an embedded Spectrum24® antenna that supports the IEEE 802.11 airwave standard for wireless communications and the ITU H.323 standard for

multimedia communications. There are also various wireless LAN expansion modules supporting IEEE 802.11 and Open Air standards in the form of Compact Flash, PCMCIA and Springboard cards available on market.

Wireless PAN (Personal Area Network) or BAN(Body Area Network). Wireless PAN or BAN allow communication among devices within a personal operating space, with typical characteristics such as short range, low power, low cost, and small networks with 8 to 16 nodes. Bluetooth is one of the promising RF-based standards intended to replace the cable between devices. There are already Bluetooth enabled available, such as the Ericsson R520 mobile phone. The IEEE 802.15 working group is also developing Personal Area Network consensus standards for short distance wireless network (WPAN). Of course, the venerable IrDA standard allows line-of- sight short-range IR communications.

DRAWBACKS

People want to access information anytime and anywhere with the personal devices they carry all the time. Traditional distributed systems that assume a stationary execution environment are no longer suitable for such extremely mobile scenarios. In light of this, many mobile computing researchers have tried to shield the mobility and make frequent disconnection transparent to end users.

LOCATION AWARENESS: EXPLORING SOCIAL COORDINATION

Mobile devices such as cellular telephones and handheld computers are becoming increasingly pervasive in our culture and society. For many, these mobile devices are essential technologies that help facilitate their social interactions. The size and form of mobile devices allow them to accompany us throughout our daily activities where our, as well as the environment and people around us, change frequently. Cellular telephones and handheld computers, once separate devices, are merging into a single platform as can be seen with today's current iteration of smart phones (e.g., Blackberry, and Audiovox SMT5600). These smart phones integrate mobile communication with lightweight computation and provide wireless connectivity using 802.11 and Bluetooth. Bluetooth and 802.11 enable a smart phone to connect with wireless networks and other independent technologies (e.g., a global positioning system (GPS) receiver, a desktop computer, and other smart phones). Harnessing information from many sources and combining it creates exciting new opportunities for applications and expands the usefulness of our independent mobile devices by combining their benefits. For example, combining GPS and wireless connectivity using a smart phone opens opportunities for smart phone applications to facilitate social coordination. GPS can provide location information to the smart phone that can be annotated on a virtual map and displayed on the screen for the user. The location of this smart phone can then be communicated wirelessly to other smart phone users within the user's social group, providing everyone within the social group an awareness of each others' locations. The location information can then be used to facilitate coordinating activities, such as meeting up at the bar later in the evening for a drink. The use of location awareness information on mobile devices has been shown to be useful for social engagement. Using Active Campus and with the popularity of Dodgeball.com (acommercial mobile socialapplication). Depending on usage, availability of input techniques, and the task to be completed, location information can be presented, interpreted, and used in a variety of ways. Colbert showed that mobile telephones were the preferred communication medium for people during a rendezvous. However, the exchange of contextual information such as location can be difficult to convey accurately through dialog. The verbal exchange of location, instructions, and intentions between coordinating people can be ambiguous, misinterpreted, and misunderstood. As mobile telephony hardware evolves, location-aware applications can be developed to augment verbal communication to facilitate the exchange and understanding of location.

DRAWBACKS

Mobile devices are extremely constrained in terms of how much information they can display and the complexity of the presentation. It is critical that effective use is made of the available display space, showing only relevant information, appropriately presented, and filtering out information irrelevant to the current task. Equally constrained by device size and mobility is interaction with the mobile device. A small screen has small input widgets that can be difficult to select, particularly given a high level of mobility. For example, imagine rushing across campus to a meeting for which you are late and that is located in an unfamiliar location. It would be difficult to interact with your mobile telephone, selecting widgets and navigating menus and still be aware of your surroundings.

SIMULTANEOUS PLAN RECOGNITION AND MONITORING (SPRAM) FOR ROBOT ASSISTANTS

Service robots that work in human environments should carry out tasks that their human supervisors are not able to do or do not want to do and assist the human with tasks that cannot be done alone. While a useful service robot will probably very often receive explicit instructions by the human, an efficient

IPHV7I2049X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

robot will also sometimes have to make decisions on its own while being aware of the current state of the human. Consider for example a cleaning robot that is supposed to clean the apartment. This is why we propose the idea of Simultaneous Plan Recognition and Monitoring (SPRAM) that enables us to use (partial) observations of the human to maintain a probabilistic model about several human activities and their state of execution. This has the advantage that even if we are not sure about which activity we are observing, we can still draw conclusions about the human intentions and reacts adequately. Imagine, for example, a household robot that is observing a human in a kitchen during his daily morning routine. Even if the robot is not sure if the human is preparing

Cereals, curd-cheese or bread for breakfast, it could still infer that the human is preparing a meal, which has the consequence that the table has to be cleaned afterwards.

DRAWBACKS

Thus, the knowledge about human task performance becomes an inevitable part of a robotic system that is aimed to work together with humans in human centered environments like a household. But high uncertainties within the robots sensors as well as unpredictable behavior of humans and partial occlusions usually make it hard to achieve certainty about human task execution.

II. BLOCK DIAGRAM

Transmitting Section

In the transmitting section fig 2.1, first we take an RFID card and place it before the RFID reader then a password is generated and transmitted to the smart phone so that we can access the system. The password received at the receiver section fig 2.2 is used to access the atm system.

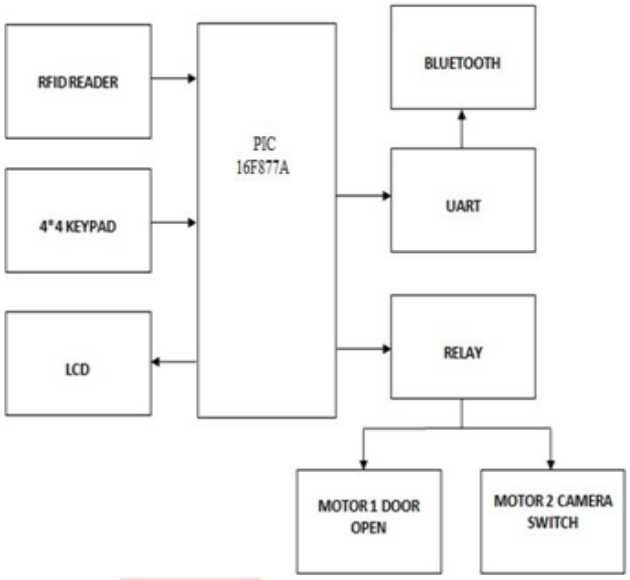

Fig:2.1 Transmitting section Receiving Section

III. DESCRIPTION AND WORKING PRINCIPLE

A board of PIC16F877A is taken, which consists of slots for interfacing an LCD display, UART module consisting MAX232 IC. An RFID reader is taken and connected to the board as an external peripheral. RFID reader is used to detect the card which is operated at 125Khz frequency. It contain a password which can be used to access the card. If we take an ATM application and we take the card as ATM card, then we can access the card and take out the money.

A. Pic Controller

The name PIC initially referred to "Peripheral Interface Controller". PIC mc's (Programmable Interface Controllers), are electronic circuits that can be programmed to carry out a vast range of tasks. They can be programmed to be timers or to control a production line and much more. They are found in most electronic devices such as alarm systems, computer control systems, phones, in fact almost any electronic device.

Features:

- Only 35 single-word instructions
- Operating speed: DC – 20 MHz clock input DC – 200 ns instruction cycle
- Up to 8K x 14 words of Flash Program Memory, Up to 368
- Timer0: 8-bit timer/counter with 8-bit pre scalar
- Timer1:16-bit timer/counter with pre scalar, can be incremented during Sleep via external crystal/clock •
- Timer2:8-bit timer/counter with 8-bit period register, pre scalar and post scalar
- Synchronous Serial Port (SSP) with SPI™ (Master mode) and I2C™ (Master/Slave)

B. UART

A universal asynchronous receiver/transmitter is a type of "asynchronous receiver/transmitter", a piece of computer hardware that translates data between parallel and serial forms.

The UART takes bytes of data and transmits the individual bits in a sequential fashion. At the destination, a second UART re-assembles the bits into complete bytes. A UART is used to convert the transmitted information between its sequential and parallel form at each end of the link. Each UART contains a shift register which is the fundamental method of conversion between serial and parallel forms.

MAX232

The MAX232 is an integrated circuit that converts signals from an RS-232 serial port to signals suitable for

use in TTL compatible digital logic circuits.

The drivers provide RS-232 voltage level outputs (approx. ± 7.5 V) from a single + 5 V supply via on-chip charge pumps and external capacitors. The receivers reduce RS-232 inputs (which may be as high as ± 25 V), to standard 5 V TTL levels.

C. RFID

Radio frequency identification (RFID) is a generic term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an object or person wirelessly, using radio waves. . RFID data can be read through the human body, clothing and non-metallic materials. The basic components of an RFID system are an antenna or coil, a tranceiver (decoder) and a transponder (RF tag) electronically programmed with unique information.

A typical reader is a device that has one or more antennas that emit radio waves and receive signals back from the tag. The reader then passes the information in digital form to a computer system. The first access control systems used low-frequency RFID tags. Recently, vendors have introduced 13.56 MHz systems that offer longer read range. Most countries have assigned the 125 kHz or 134 kHz area of the radio spectrum for low-frequency systems, and 13.56 MHz is used around the world for high-frequency systems.

D. RELAY

A relay is an electrically operated switch. Relays allow one circuit to switch a second circuit which can be completely separate from the first.

There is no electrical connection inside the relay between the two circuits; the link is magnetic and mechanical. Relays can switch AC and DC, transistors can only switch DC. Relays can switch many contacts at once. Relays cannot switch rapidly (except reed relays), transistors can switch many times per second.

Relays use more power due to the current flowing through their coil.

E. KEYPAD

A 4*4 keypad is used for loading numerics into the microcontroller. It consists of 16 buttons arranged in a form of an array containing four lines and four columns.

F. LIQUID CRYSTAL DISPLAY (LCD)

LCDs are most commonly used because of their advantages over other display technologies. They are thin and flat and consume very small amount of power compared to LED displays and cathode ray tubes (CRTs).

LCDs have become very popular over recent years for information display in many „smart" appliances. They are usually controlled by microcontrollers.

If RS=0 Instruction command Code register is selected, allowing user to send command RS=1 Data register is selected allowing to send data that has to be displayed.

G. DC MOTOR

A direct-current motor is a shunt-wound motor in which the field windings and the armature may be connected in parallel across a constant-voltage supply. A 12V DC motor consists of two magnets facing the same direction, that surround two coils of wire that reside in the middle of the 12V DC motor around a rotor.

The coils are positioned to face the magnets, causing electricity to flow to them. This generates a magnetic field, which ultimately pushes the coils away from the magnets they are facing, and causes the rotor to turn. The current shuts off at the rotor makes a 180 turn, causing each rotor to face the opposite magnet.

As the current turns on again, the electricity flows oppositely, sending another pulse that causes the rotor to turn once again. The brushes that are located within the 12V DC motor transfer the electricity from the rotor, controlling the motors timing; turning it on and off when instructed.

Here we are using blue tooth technology for sending the password to a smart phone. The smart phone holder can only access the card because the password is sent to the smart phone which is paired up to the blue tooth device in our board.

After that, when the password is typed on the keypad, it is displayed on LCD. If the password is right, relay in our cicuit activates one of the motor which shows us the person is authorised and the atm can be accessed. If it shows the password is wrong, then the person is unauthorised and the camera switch is switched on and the person cannot access the card.

Thus if any third person who doesn't get the password cannot access the card. Likewise the privacy of the user can be enhanced.

IV. RESULT

As mentioned above the circuit and the result is as shown below. When the card is shown to the rfid reader, the password is generated. The password is sent to the smart phone, then it is typed on keypad. Then LCD displays whether the is password is right or wrong. According to the display relay comes in to the action.

When LCD displays right, relay switches ON and motor 1 will be ON. When LCD displays wrong, relay switches OFF and motor 2 will be ON that is to show that the user is unauthorized and he cannot access the card. Thus this paper shows the enhancement of the security of the cards not to be accessed by the malicious users. It also provides security for the users if the is misplaced.

Fig 4.1: Result of the circuit

V. CONCLUSION AND FUTURE WORK

In this paper, we reported a new approach to defend against unauthorized reading. When any unauthorised user commits to access the card, he would not have the actual user's smart phone. So he cannot know the password and he cannot type the password and can't access the money. And also instead of a motor, if we connect a camera and write certain code for it, the camera takes the photograph of the person.

The extension for this paper would be, GPS can be used to track the malicious readers. Instead of blue tooth GPS can be used so as to send the password to smart phone from long distances.

REFERENCES

[1] RFID Toll Collection Systems, http://www.securitysa.com/news.aspx?pklnewsid=2591, 2007
[2] M. Buettner, R. Prasad, M. Philipose, and D. Wetherall, "Recognizing Daily Activities with RFID-Based Sensors," Proc. Int"l Conf. Ubiquitous Computing (UbiComp), 2009.
[3].http://www.datasheetarchive.com/pic%20microcontroller%2016F877A-datasheet.html
[4].http://www.maximintegrated.com/products/interface/controllers-expanders/uart.cfm
[5].http://www.engineersgarage.com/electroniccomponents/16x2-lcd-module-datasheet
[6].http://ww1.microchip.com/downloads/jp/DeviceDoc/39582b
[7].*www.microchip.com/wwwproducts/Devices.aspx?dDocName=en010242*