INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

LOCATION-AWARE AND SAFER CARDS: ENHANCING RFID SECURITY AND PRIVACY VIA LOCATION SENSING USING GSM AND GPS

PURUSHOTHAM K[1], VASU GT[2]

1. M.Tech, Embedded System, 2nd year, SIDDHARTH INSTITUTE OF ENGG &TECHNOLOGY, Puttur, Chittoor Dist., ANDHRA PRADESH, India.
2. M.Tech, (Ph.D),. Assistant professor, SIDDHARTH INSTITUTE OF ENGG &TECHNOLOGY, Puttur, Chitoor Dist., ANDHRA PRADESH, India.

Accepted Date: 24/10/2014; Published Date: 01/11/2014

Abstract: In this paper, 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. 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.

Keywords: RFID, mobile payment system, relay attacks, context recognition, location sensing

Corresponding Author: MR. K. PURSHOTHAM

Access Online On:

www.ijpret.com

How to Cite This Article:

Purushotham K, Vasu GT; IJPRET, 2014; Volume 3 (3):63-72

PAPER-QR CODE

INTRODUCTION

LOW cost, small size, and the ability of allowing computerized identification of objects make Radio Frequency IDentification (RFID) systems increasingly ubiquitous in both public and private domains. Prominent RFID applications supply chain management (inventory control) [16], e-passports [57], credit cards [15], driver's licenses [60], [41], vehicle systems (toll collection or car key) [17], [27], [25], access cards (building, parking or public transport) [46], and medical implants [38]. NFC, or Near Field Communication [26], is yet another upcoming RFID technology that allows devices, such as smart phones, to have both RFID tag and reader functionality. In particular, the use of NFC-equipped mobile devices as payment tokens (such as Google Wallet) is considered to be the next generation payment system and the latest buzz in the financial industry [10]. A typical RFID system consists of tags, readers, and/or back-end servers. Tags are miniaturized wireless radio devices that store information about their corresponding subject. Such information is usually sensitive and personally identifiable. For example, a US e-passport stores the name, nationality, date of birth, digital photograph, and (optionally) fingerprint of itsowner [29]. Readers broadcast queries to tags in their radio transmission ranges for information contained in tags and tags reply with such information. The queried information is then sent to the server (which may coexist with the reader) for further processing and the processing result is used to perform proper actions (such as updating inventory, opening gate, charging toll or approving payment). Due to the inherent weaknesses of underlying wireless radio communication, RFID systems are plagued with a wide variety of security and privacy threats [28]. A large number of these threats are due to the tag's promiscuous response to any reader requests. This renders sensitive tag information easily subject to unauthorized reading [23].Information (might simply be a plain identifier) gleaned from a RFID tag can be used to track the owner of the tag, or be utilized to clone the tag so that an adversary can impersonate the tag's owner [28].**:** RFID, Microcontroller and GPS.

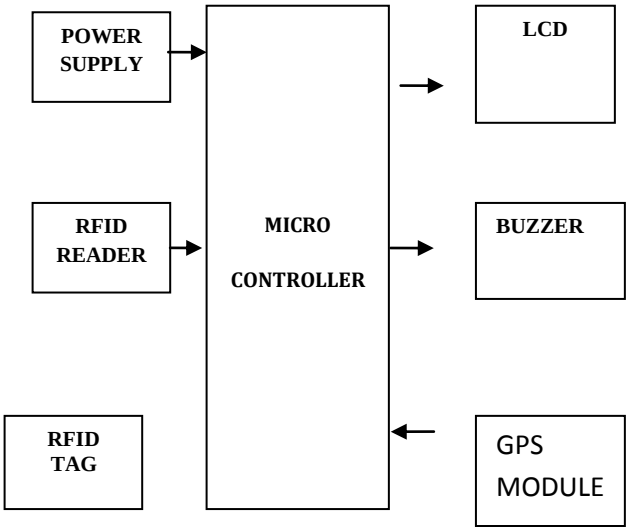

Fig 1: Block diagram for proposed method

Micro controller: This section forms the control unit of the whole project. This section basically consists of a Microcontroller with its associated circuitry like Crystal with capacitors, Reset circuitry, Pull up resistors (if needed) and so on. The Microcontroller forms the heart of the project because it controls the devices being interfaced and communicates with the devices according to the program being written.

ARM7-2148: The Lpc2141/42/44/46/48 microcontrollers are focused about a 16-bit/32-bit Arm7tdmi-S CPU with advancing assuming and amid chase help, that accompany microcontroller with built-in accelerated bonfire anamnesis active from 32kb to 512kb. A 128-bit advanced anamnesis interface and a atypical dispatch abettor structural engineering empower 32-bit cipher beheading at the a lot of acute alarm rate. For acute cipher admeasurements applications, the advantage 16-bit Thumb approach diminishes cipher by added than 30 % with bush beheading punishment. Because of their accessory admeasurements and low ability utilization, Lpc2141/42/44/46/48 are absolute for applications area ascent down is a key prerequisite, for example, admission ascendancy and purpose of-offer. Serial correspondences interfaces extending from a USB 2.0 Full-speed gadget, abundant Uarts, SPI, SSP to I2c-transport and on-chip SRAM of 8kb up to 40kb, accomplish these accessories acutely adapted for accord entryways and assemblage converters, aerial modems, articulation distinguishment and low end imaging, giving both abundant abutment admeasurements and top advancing force. Different 32-bit clocks, individual or bifold 10-bit Adc(s), 10-bit DAC, PWM channels and 45 quick GPIO curve with up to nine bend or akin aerial

alfresco intrude on pins accomplish these microcontrollers acceptable for automated ascendancy and alleviative frameworks.

Liquid-crystal display (**LCD**)**:** is a flat panel display, electronic visual display that uses the light modulation properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images or fixed images which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements.

GPS: The Global Positioning System (GPS) is a satellite based navigation system that sends and receives radio signals. A GPS receiver acquires these signals and provides the user with information. Using GPS technology, one can determine location, velocity and time, 24 hours a day, in any weather conditions anywhere in the world for free.

GPS was formally known as the NAVSTAR (Navigation Satellite Timing and Ranging). Global Positioning System was originally developed for military. Because of its popular navigation capabilities and because GPS technology can be accessed using small, inexpensive equipment, the government made the system available for civilian use. The USA owns GPS technology and the Department of Defence (DOD) maintains it.

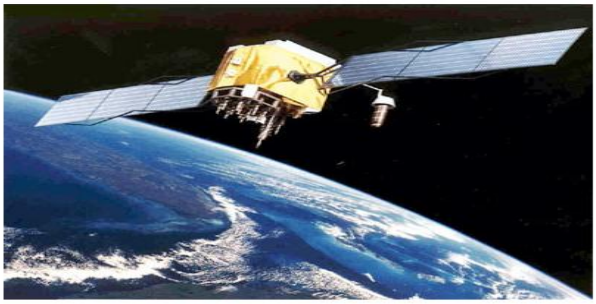

Fig 2: A GPS Satellite

1. The architectural components of GPS are typically referred to as the control segment (ground stations), the space segment (satellites) and the user segment (receivers). The goal of the Global Positioning System (GPS) is to determine the position of a person or any object on Earth in three dimensions: east-west, north-south and vertical (longitude, latitude and altitude). Signals from three overhead satellites provide this information. Each satellite sends a signal that codes where the satellite is and the time of emission of the signal. The

receiver clock times the reception of each signal, then subtracts the emission time to determine the time lapse and hence how far the signal has traveled (at the speed of light).

The accuracy of GPS depends on a number of factors, number of channels on the receiver, number of satellites in view, and signal interference caused by buildings, mountains and ionosphere disturbances. Accuracy should be within 15 meters (without SA) provided the receiver has a clear shot at a minimum of four satellites.
There are several methods that can improve GPS accuracy. Two commonly discussed are Differential GPS (DGPS) and Wide Area Augmentations System (WAAS). These improve accuracy to within 1 to 3 meters. DGPS uses fixed, mounted GPS receivers to calculate the difference between their actual known position and the calculated GPS position. This difference is then broadcast over a local FM signal. GPS units within range of the local FM signal can improve their position accuracy to within 1cm over short distances (but more typically 3-5 meters).

RFID: Radio frequency identification (RFID) is a general term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an object wirelessly using radio waves. RFID technologies are grouped under the more generic Automatic Identification (Auto ID) technologies.

In recent years, radio frequency identification technology has moved from obscurity into mainstream applications that help speed the handling of manufactured goods and materials. RFID enables identification from a distance and unlike earlier bar-code technology; it does so without requiring a line of sight. RFID tags support a larger set of unique IDs than bar codes and can incorporate additional data such as manufacturer, product type and even measure environmental factors such as temperature. Furthermore, RFID systems can discern many different tags located in the same general area without human assistance.

Many types of RFID exist, but at the highest level, we can divide RFID devices into two classes:

Active and **passive**.

Fig 3: Types of Tags

Active tags require a power source i.e., they are either connected to a powered infrastructure or use energy stored in an integrated battery. In the latter case, a tag's lifetime is limited by the stored energy, balanced against the number of read operations the device must undergo. However, batteries make the cost, size, and lifetime of active tags impractical for the retail trade.

Passive RFID is of interest because the tags don't require batteries or maintenance. The tags also have an indefinite operational life and are small enough to fit into a practical adhesive label. A passive tag consists of three parts: an antenna, a semiconductor chip attached to the antenna and some form of encapsulation. The tag reader is responsible for powering and communicating with a tag. The tag antenna captures energy and transfers the tag's ID (the tag's chip coordinates this process). The encapsulation maintains the tag's integrity and protects the antenna and chip from environmental conditions or reagents.

RF (Radio Frequency) communication occurs by the transference of data over electromagnetic waves. By generating a specific electromagnetic wave at the source, its effect can be noticed at the receiver far from the source, which then identifies it and thus the information

In an RFID system, the RFID tag which contains the tagged data of the object generates a signal containing the respective information which is read by the RFID reader, which then may pass this information to a processor for processing the obtained information for that particular application.

Thus, an RFID System can be visualized as the sum of the following three components:

1. RFID tag or transponder
2. RFID reader or transceiver
3. Data processing subsystem

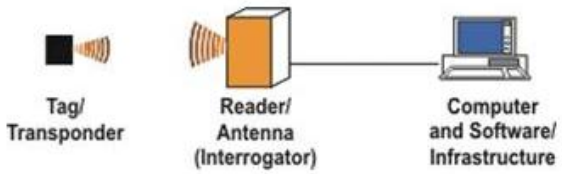

Fig 4: Architecture of RFID system

An RFID tag is composed of an antenna, a wireless transducer and an encapsulating material. These tags can be either active or passive. While the active tags have on-chip power, passive tags use the power induced by the magnetic field of the RFID reader. Thus passive tags are cheaper but with lower range (<10mts) and more sensitive to regulatory and environmental constraints, as compared to active tags.

An RFID reader consists of an antenna, transceiver and decoder, which sends periodic signals to inquire about any tag in vicinity. On receiving any signal from a tag it passes on that information to the data processor. The data processing subsystem provides the means of processing and storing the data.

Much like tuning in to the favourite radio station, RFID tags and readers must be tuned into the same frequency to enable communications. RFID systems can use a variety of frequencies to communicate, but because radio waves work and act differently at different frequencies, a frequency for a specific RFID system is often dependant on its application. High frequency RFID systems (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) offer transmission ranges of more than 90 feet, although wavelengths in the 2.4 GHz range are absorbed by water, which includes the human body and therefore has limitations.

Two fundamentally different RFID design approaches exist for transferring power from the reader to the tag: magnetic induction and electromagnetic (EM) wave capture. These two designs take advantage of the EM properties associated with an RF antenna—the *near field* and the *far field*. Both can transfer enough power to a remote tag to sustain its

Operation—typically between 10W and 1 mW, depending on the tag type.

GSM:

Global Positioning System (GPS) technology is dynamical the approach we've a bent to figure and play. You will be able to use GPS technology when you area unit driving, flying, fishing, sailing, hiking, running, biking, working, or exploring. With a GPS receiver, you have an improbable amount of knowledge at your fingertips. Here a unit merely several samples of but you will be able to use GPS technology

The world Positioning System (GPS) may be a satellite-based navigation system that sends and receives radio signals. A GPS receiver acquires these signals and provides you with information. exploitation GPS technology, you will be able to make sure location, velocity, and time, twenty four hours day by day, in any climate anywhere at intervals the world—for free.GPS, formally mentioned because the NAVSTAR (Navigation Satellite temporal property and Ranging). World

Positioning System originally was developed for the military. Owing to its well-liked navigation capabilities and since you will be able to access GPS technology exploitation little, low cost instrumentality, the govt. created the system out there for civilian use. The USA owns GPS technology and additionally the Department of Defense maintains it.At least twenty four GPS satellites orbit the globe doubly day by day terribly} very specific pattern. These satellites area unit spaced so as that a GPS receiver anywhere at intervals the globe can receive signals from a minimum of 4 of them.

The signals can stand up to clouds, glass, and plastic. Most solid objects like buildings attenuate (decrease the ability of) the signals. The signals cannot stand up to objects that contain a lot of metal or objects that contain water (such as underwater locations). The GPS satellites area unit high-powered by alternative energy. If alternative energy is out of stock, for example, figure 5.1 shows GSM modem, once the satellite is at intervals the earth's shadow, satellites use backup batteries to continue running. Each GPS satellite is made to last regarding 10 years. The Department of Defense monitors and additionally the satellites to form positive that GPS technology continues to run smoothly for years to come back.The Department of Defense monitors and also the satellites to confirm that GPS technology continues to run swimmingly for years to return.

CONCLUSION

In this paper, we reported a new approach to defend against unauthorized reading and relay attacks in some RFID applications whereby location can be used as a valid context. We argued

the feasibility of our approach in terms of both technical and economical aspects. Using location and derived speed information, we designed location aware selective unlocking mechanisms and a location ware transaction verification mechanism. For collecting this information, we made use of the GPS infrastructure. To demonstrate the feasibility of our location-aware defense mechanisms, we integrated a low-cost GPS receiver with a RFID tag (the Intel's WISP) and conducted relevant experiments to acquire location and speed information from GPS readings. Our results show that it is possible to measure location and speed with high accuracies even on a constrained GPS-enabled platform, and that our location aware defenses are quite useful in significantly raising the bar against the reader-and-leech attacks. As an immediate avenue for further work, we intend to further optimize and fine-tune our location detection algorithms for better efficiency on resource-constrained RFID platforms and improved tolerance to errors whenever applicable. Additionally, we are exploring the use of ambient sensors to determine proximity based on location-specific sensor information for the second security primitive secure transaction verification. We will also evaluate the promising of proposed techniques by means of usability studies.

REFERENCES

1. RFID Toll Collection Systems, http://www.securitysa.com/news.aspx?pklnewsid=25591, 2007.

2. 66-Channel LS20031 GPS Receiver Module, http://www.megachip.ru/pdf/POLOLU/66_CHANNEL.pdf, 2011.

3. GM-101 Cost Effective GPS Module with Ttl Rs-232 Interface, http://www.alibaba.com/product-gs/435104168/GM_101_Cost_Effective_GPS_Module.html, 2011.

4. GPS Glossory, http://www.gsmarena.com/glossary.php3?term=gps, 2011.

5. NMEA 0183 Standard, http://www.nmea.org/content/nmea_standards/nmea_083_v_400.asp, 2011.

6. S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques Advances in Cryptology (EUROCRYPT), 1993.

7. J. Bringer, H. Chabanne, and E. Dottax, "HB++: A Lightweight Authentication Protocol Secure against Some Attacks," Proc. Second Int'l Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006.

8. M. Buckner, R. Crutcher, M.R. Moore, and S.F. Smith, "GPS and Sensor-Enabled RFID Tags," http://www.ornl.gov/webworks/cppr/y2001/pres/118169.pdf, 2013.

9. M. Buettner, R. Prasad, M. Philipose, and D. Wetherall, "Recognizing Daily Activities with RFID-Based Sensors," Proc. Int'l Conf. Ubiquitous Computing (UbiComp), 2009.

10. M. Calamia, "Mobile Payments to Surge to $670 Billion by 2015," http://www.mobiledia.com/news/96900.html, July 2011.