INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 3, Issue 3 OCT 2014

SAFER CARDS ENHANCING RFID SECURITY AND PRIVACY VIA LOCATION SENSING

CHALUVADI.VENKATESWARLU [1], A.RAGHU RAM [2]

[1] Chaluvadi.Venkateswarlu, Dept Of Ece, Indira Institute Of Technology And Science's, Darimadugu, Markapur Mandal, Prakasam Dist, Ap, India

[2] Guide Details, A.Raghu Ram, M.Tech, Associate Professor, Indira Institute Of Technology And Science's, Darimadugu, Markapur Mandal, Prakasam Dist, Ap, 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 alocation-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:*Microcontroller,RFID,zigbee,Gps,Pc*

I. INTRODUCTION

Low cost, small size, and the ability of allowing computerized identification of objects make RadioFrequency IDentification (RFID) systems increasingly ubiquitous in both public and private domains. ProminentRFID applications supply chain management (inventorycontrol) e-passports credit cards , driver's licenses [60], [41], vehicle systems (toll collection or car key)access cards (building, parking or publictransport) and medical implants. NFC, or NearField Communication [26], is yet another upcoming RFIDtechnology that allows devices, such as smartphones, tohave 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 nextgeneration payment system and the latest buzz in thefinancial industry .A typical RFID system consists of tags, readers, and/orback-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 its owner [29]. Readers broadcast queries to tagsin their radio transmission ranges for information containedin tags and tags reply with such information. The queriedinformation is then sent to the server (which may coexist withthe reader) for further processing and the processing result isused 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 awide variety of security and privacy threats. A large number of these threats are due to the tag' promiscuous response to any reader requests. This renders sensitive taginformation easily subject to unauthorized reading .

II.

III. The Hardware System

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.

ARM7TDMI: ARM is the abbreviation of Advanced RISC Machines, it is the name of a class of processors, and is the name of a kind technology too. The RISC instruction set, and related decode mechanism are much simpler than those of Complex Instruction Set Computer (CISC) designs.

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.

I. Design of Proposed Hardware System

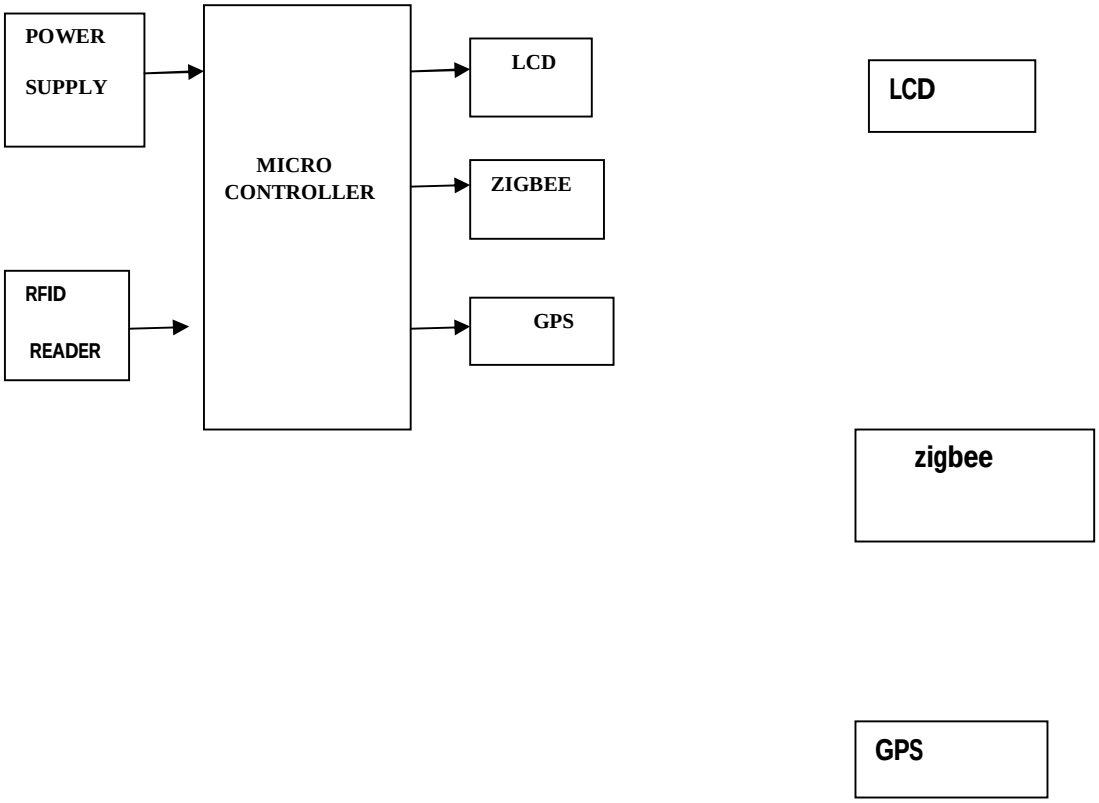

Fig.1.Block diagram

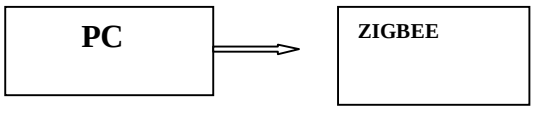

Fig.2.Block diagram

Fig.2.Block diagram

Now a day's energy product has some life time and that life time is going to decrease day by day for every product to check that life time we are going to spend a lot of money by checking the product life time. So by using the RFID and Zigbee Based Manufacturing system we can check the status of no of products manufactured in different nodes.

RFID monitoring devices can serve as the data collection system and the Zigbee wireless network can serve as the communication system to transmit the data to different levels of the enterprise management from the perspective of system automatic control.

The monitoring layer is the core of the RFID and Zigbee based manufacturing monitoring system. With the help of the readers placed in different locations, the information in the tags nearby will be collected, if gaining the permission, the readers can read the data on the tags and transfer the data to the end-user devices.

IV.Board Hardware Resources Features

Zigbee

Zigbee modules feature a UART interface, which allows any microcontroller or microprocessor to immediately use the services of the Zigbee protocol. All a Zigbee hardware designer has to do in this ase is ensure that the host's serial port logic levels are compatible with the XBee's 2.8- to 3.4-V logic levels. The logic level conversion can be performed using either a standard RS-232 IC or logic level translators such as the 74LVTH125 when the host is directly connected to the XBee UART. The below table gives the pin description of transceiver. Data is presented to the X-Bee module through its DIN pin, and it must be in the asynchronous serial format, which consists of a start bit, 8 data bits, and a stop bit. Because the input data goes directly into the input of a UART within the X-Bee module, no bit inversions are necessary within the asynchronous serial data stream. All of the required timing and parity checking is automatically taken care of by the X-Bee's UART

Rfid

Many types of RFID exist, but at the highest level, we can divide RFID devices into two classes:
active and **passive**.

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.

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 aware 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 thebar 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-232Interface,http://www.alibaba.com/productgs/435104168/GM_101_Cost_Effective_GPS_Module.html, 2011.

[4] GPSGlossory,http://www.gsmarena.com/glossary.php3?term=gps, 2011.

[5]NMEA0183Standard,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 TechniquesAdvances in Cryptology (EUROCRYPT),1993.

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

[8] M. Buckner, R. Crutcher, M.R. Moore, and S.F. Smith, "GPS andSensor-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$670Billionby2015,"http://www.mobiledia.com/news/96900.html, July 2011.

[11] G. Cropsey, "Designing a Distance and Speed Algorithm Usingthe Global Positioning System," http://www.egr.msu.edu/classes/ece480/capstone/spring08/group10/documents/ApplicationApplication%20Note-%20Gabe.pdf, Mar. 2008.

[12] A. Czeskis, K. Koscher, J. Smith, and T. Kohno., "RFIDs and SecretHandshakes: Defending against Ghost-and-Leech Attacks andUnauthorized Reads with Context-Aware Communications,"Proc. ACM Conf. Computer and Comm. Security,2008.MA ET AL.: LOCATION-AWARE AND SAFER CARDS: ENHANCING RFID SECURITY AND PRIVACY VIA LOCATION SENSING 67

[13] Y. Desmedt, C. Goutier, and S. Bengio, "Special Uses and Abusesof the Fiat-Shamir Passport Protocol," Proc. Conf. Theory andApplications of Cryptographic Techniques Advances in Cryptology(CRYPTO), 1988.

[14] S. Drimer and S.J. Murdoch, "Keep Your Enemies Close: DistanceBounding Against Smartcard Relay Attacks,"Proc. 16th USENIXSecurity Symp.,Aug. 2007.

[15]EMVCo,"AboutEMV,"http://www.emvco.com/about_emv.aspx, Nov. 2009.

[16] epic.org, "Wal-Mart Begins Tagging and TrackingMerchandisewithRFID,"http://epic.org/2010/07/wal-mart-begins-taggingand-tr.html, July 2010.

[17] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on PassiveKeyless Entry and Start Systems in Modern Cars,"Proc. 18th Ann.Network and Distributed System Security Symp. (NDSS),2011.

[18] H. Gilbert, M. Robshaw, and Y. Seurin, "HB#: IncreasingtheSecurityandEfficiencyofHB+,"Proc.Int'l Conf. the Theory andApplications ofCryptographic Techniques Advances in Cryptology(EUROCRYPT),2008.

[19] Goldiron, "Numerex Unveils Hybrid Tag Includes Active RFID,

GPS,SatelliteanDSensors,"http://goldiron.wordpress.com/2009/02/25/numerex-unveils-hybrid-tag-includes-active-rfidgps-satellite-and-sensors/, Feb. 2009.

[20] T. Halevi, D. Ma, N. Saxena, and T. Xiang, "Secure ProximityDetection for NFC Devices Based on Ambient Sensor Data,"Proc.European Symp. Research in Computer Security (ESORICS),Sept.2012.

[21] G.P. Hancke and M.G. Kuhn, "An RFID Distance BoundingProtocol,"Proc. First Int'l Conf. Security and Privacy for EmergingAreas in Comm. Networks,2005.

[22]B.Hanlon,B.Ledvina,M.Psiaki,P.M.Kitner.,andT.E.Humphreys, "Assessing the GPS Spoofing Threat," GPSWorld,http://www.gpsworld.com/defense/security-surveillance/assessing-spoofin g-threat-3171?page_id=1, Jan. 2009.

[23] T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels, and T. O'Hare,"Vulnerabilities in First-Generation RFID-Enabled Credit Cards,"Proc. Int'l Conf. Financial Cryptography and Data Security,2007.

[24] J. Holleman, D. Yeager, R. Prasad, J. Smith, and B. Otis,"NeuralWISP: An Energy-Harvesting Wireless Neural Interfacewith 1-m Range,"Proc. Biomedical Circuits and Systems Conf.

(BioCAS), 2008.

[25] Infowars.com, "Texas Department of Transportation to InstateRFID TxTag," http://www.infowars.com/articles/bb/toll_roads_tx_tag.htm, Sept. 2005.

[26] ISO, "Near Field Communication Interface and Protocol (NFCIP-1)–ISO/IEC 18092:2004," http://www.iso.org/iso/catalogue_detail.htm?csnumber=38578, 2004.

[27] ITGlobal Consulting LTD, "RFID Toll Road Payment,"http://www.itglobalconsulting.com/rfidtollroadpayment.asp, 2013.

[28] A. Juels, "RFID Security and Privacy: A Research Survey,"IEEEJ. Selected Areas in Comm., vol. 24, no. 2, pp. 381-394, Feb. 2006.

[29] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issuesin E-Passports," Proc. First Int'l Conf. Security and Privacy forEmerging Areas in Comm. Networks (Securecomm),2005.

[30] A. Juels, R.L. Rivest, and M. Szydlo, "The Blocker Tag: SelectiveBlocking of RFID Tags for Consumer Privacy,"Proc. ACM Conf.Computer and Comm. Security (CCS),2003.

[31] A. Juels, P.F. Syverson, and D.V. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility,"Proc. Fifth Int'l Conf. Privacy Enhancing Technologies,2005.

[32] A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols,"Proc. Int'l Cryptology Conf. (CRYPTO),2005.

[33] J. Katz and J. Shin, "Parallel and Concurrent Security of the HB and HB+ Protocols,"Proc. Int'l Conf. Theory and Applications ofCryptographic Techniques Advances in Cryptology (EUROCRYPT),2006.

[34] Z. Kfir and A. Wool, "Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard,"Proc. Security and Privacy for EmergingAreas in Comm. Networks (Securecomm),2005.

[35] A. Kobsa, R. Nithyanand, G. Tsudik, and E. Uzun, "Usability ofDisplay-Equipped RFID Tags for Security Purposes,"Proc.European Symp. Research in Computer Security (ESORICS),2011.

[36] K. Koscher, A. Juels, V. Brajkovic, and T. Kohno, "EPC RFID Tag Security Weaknesses and Defenses: Passport Cards EnhancedDrivers Licenses and Beyond,"Proc. ACM Conf. Computer andComm. Security,2009.

[37] M. Kuhn, "An Asymmetric Security Mechanism for NavigationSignals,"Proc. Sixth Information Hiding Workshop,2004.

[38] Medical News Today, "VeriChip Corporation Announces Phase II Development of in Vivo Glucose-Sensing RFID Microchip with RECEPTORSLLC,"http://www.medicalnewstoday.com/articles/165894.php, Oct. 2009.

[39] N. Saxena, B. Uddin, J. Voris, and N. Asokan, "Vibrate-to-Unlock:Mobile Phone Assisted User Authentication to Multiple PersonalRFID Tags,"Proc. IEEE Int'l Conf. Pervasive Computing and Comm.(PerCom), 2011.

[40] R. Nithyanand, G. Tsudik, and E. Uzun, "Readers BehavingBadly: Reader Revocation in PKI-Based RFID Systems,"Proc.European Symp. Research in Computer Security (ESORICS),2010.

[41] NYS DMV, "Enhanced Driver Licenses and Non-Driver IdentificationCards,"http://www.nydmv.state.ny.us/broch/C158.pdf,July 2010.

[42] Y. Oren and A. Wool, "Relay Attacks on RFID-Based ElectronicVoting Systems," Cryptology ePrint Archive,Report2009/422,http://eprint.iacr.org/2009/422, 2009.

[43] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning:Attacks and Countermeasures,"Proc. IEEE Military Comm. Conf.(MILCOM), pp. 1-7, Nov. 2008.

[44] P. Papadimitratos and A. Jovanovic, "Protection and FundamentalVulnerability of Global Navigation Satellite Systems (GNSS),"Proc. Int'l Workshop Satellite and Space Comm. (IWSSC),2008.

[45] K.B. Rasmussen and S.Capkun, "Realization of RF DistanceBounding,"Proc. USENIX Security Symp.,2010.

[46] RFID Asia, "New Ez-Link Contactless Smart Cards ConvergeTransit and Payment Applications," http://journal.rfid-asia.info/2008/12/new-ez-link-contactless-smart-cards.htm, Dec. 2008.

[47] M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "RFID Guardian: ABattery-Powered Mobile Device for RFID Privacy Management,"Proc. Australasian Conf. Information Security and Privacy (ACISP),2005.

[48] A. Ruhanen et al., "Sensor-Enabled RFID Tag Handbook," http://www.bridge project.eu/data/File/BRIDGE_WP01_RFID_tag_handbook.pdf, Jan. 2008.

[49] A. Sample, D. Yeager, and J.R. Smith, "A Capacitive TouchInterface for Passive RFID Tags,"Proc. IEEE Int'l Conf. RFID,2009.

[50] A. Sample, D. Yeager, P. Powledge, and J. Smith, "Design of aPassively-Powered Programmable Sensing Platform for UHFRFID Systems,"Proc. IEEE Int'l Conf. RFID,2007.

[51] N. Saxena and J. Voris, "Still and Silent: Motion Detection forEnhanced RFID Security and Privacy without Changing the UsageModel,"Proc. Workshop RFID Security (RFIDSec),June 2010.

[52] D. Schon, H. Lemelson, and W. Effelsberg, "Situation-AwareChoice of the Most Accurate Positioning System,"Proc. IEEE Int'lConf. Pervasive Computing Comm. Workshops (PerCom '12),2012.

[53] L. Scott, "Anti-Spoofing and Authenticated Signal Architecturesfor Civil Navigation Signals," Proc. 16th Int'l Technical Meeting ofthe Satellite Division of the Inst. of Navigation (ION GPS/GNSS),pp. 1543-1552, 2003.

[54]J.R.Smith,P.S.Powledge,S.Roy,andA.Mamishev,"AWirelessly-Powered Platform for Sensing and Computation,"Proc. Eighth Int'l Conf. Ubiquitous Computing (UbiComp),2006.

[55] sparkfun, "32 Channel San Jose Navigation GPS 5HzReceiverwithAntennahttp://www.sparkfun.com/products/8266, 2011.

[56] N.O. Tippenhauer, C. Popper, K.B. Rasmussen, and S. Capkun,"On the Requirements for Successful GPS Spoofing Attacks,"Proc.ACM Conf. Computer and Comm. Security (CCS '11),Oct. 2011.

[57] U.S. Dept. of State, "The U.S. Electronic Passport,"http://travel.state.gov/passport/passport_2498.html, 2013.

[58] D. Wagner, "Privacy in Pervasive Computing: What CanTechnologists Do?"Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. (SecureComm '05),2005.

[59] J.S. Warner and R.G. Johnston, "Think GPS Cargo Tracking =High Security?" technical report, Los Alamos Nat'l Laboratory,2003.

[60] Washington State Dept. of Licensing, "Enhanced Driver License/ ID Card," http://www.dol.wa.gov/about/news/priorities/edl.html, 2013..

GUIDE DETAILS:

NAME: A.RAGHU RAM
Qualification: M.Tech
Designation: Senior Profecesor
Mail Id: raghuram223344@gmail.com
Ph No: 9966753056

STUDENT DETAILS:

NAME: CHALUVADI.VENKATESWARLU

Qualification: M.TECH

Mail Id: venkatesha0455@gmail.com

Phone: 9705940383