International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Enhancing and providing security via RFID and Location sensing

[1]Burra Manojkumar; [2]G. Purna Chandra Rao & [3]M. Shyam sundar
1. M.Tech, SVS Institute of Technology, Warangal, Hasanparthy, Bheemaram, Hanamkonda, Telangana 506015.
2. Associate Prof,, SVS Institute of Technology, Warangal, Hasanparthy, Bheemaram, Hanamkonda, Telangana 506015.
3. Associate Prof, SVS Institute of Technology, Warangal, Hasanparthy, Bheemaram, Hanamkonda, Telangana 506015.

ABSTRACT:

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 Although a variety of security solutions exist, many of them do not meet the constraints and requirements of the underlying RFID applications in terms of (one or more of) efficiency, security, and usability. In an attempt to address these drawbacks, this system proposes a general research direction one that utilizes sensing technologies to address unauthorized reading and relay attacks in RFID systems without necessitating any changes to the traditional RFID usage model. The proposed work is based on a current technological advancement that enables many RFID tags with low-cost sensing capabilities. Various types of sensors have been incorporated with many RFID tag. Intel's Wireless Identification and Sensing Platform (WISP) is a representative example of a sensor-enabled tag, which extends RFID beyond simple identification to in-depth sensing. This new generation of RFID devices can facilitate numerous promising applications for ubiquitous sensing and computation. They also suggest new ways of providing security and privacy services by leveraging the unique properties of the physical environment or physical status of the tag (or its owner). In this system, we specifically focus on the design of context aware security primitives and protocols by utilizing sensing technologies so as to provide improved protection against unauthorized reading and relay attacks.

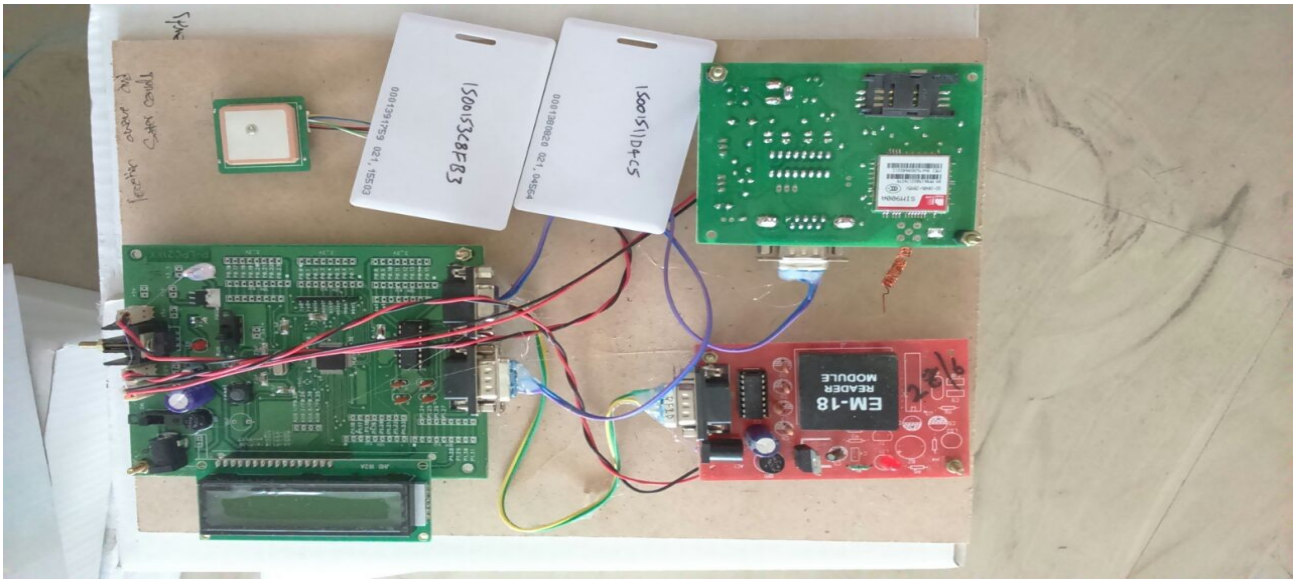
INTRODUCTION:

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 its owner [29]. Readers broadcast queries to tags in

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

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]. Promiscuous responses also incite different types of relay attacks. One class of these attacks is referred to as "ghost and-leech" [34]. In this attack, an adversary, called a "leech," relays the information surreptitiously read from a legitimate RFID tag to a colluding entity known as a "ghost." The ghost can then relay the received information to a corresponding legitimate reader and vice versa in the other direction. This way a ghost and leech pair can succeed in impersonating a legitimate RFID tag without actually possessing the device. A more severe form of relay attacks, usually against payment cards, is called "reader-and-ghost"; it involves a malicious reader and an unsuspecting owner intending to make a transaction [14].1 In this attack, the malicious reader, serving the role of a leech and colluding with the ghost, can fool the owner of the card into approving a transaction which she did not intend to make (e.g., paying for a diamond purchase made by the adversary while the owner only intending to pay for food). We note that addressing this problem requires secure transaction verification, i.e., validation that the tag is indeed authorizing the intended payment amount.

Implementation:



International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

ARM7

The ARM7 family includes the ARM7TDMI, ARM7TDMI-S, ARM720T, and ARM7EJ-S processors. The ARM7TDMI core is the industry's most widely used 32-bit embedded RISC microprocessor solution. Optimized for cost and power-sensitive applications, the ARM7TDMI solution provides the low power consumption, small size, and high performance needed in portable, embedded applications.

The ARM7EJ-S processor is a synthesizable core that provides all the benefits of the ARM7TDMI low power consumption, small size, and the thumb instruction set while also incorporating ARM's latest DSP extensions and enabling acceleration of java-based applications. Compatible with the ARM9™, ARM9E™, and ARM10™ families, and Strong-Arm® architecture software written for the ARM7TDMI processor is 100% binary-compatible with other members of the ARM7 family and forwards-compatible with the ARM9, ARM9E, and ARM10 families, as well as products in Intel's Strong ARM and x scale architectures. This gives designers a choice of software-compatible processors with strong price-performance points. Support for the ARM architecture today includes:

- Operating systems such as Windows CE, Linux, palm and SYMBIAN OS.
- More than 40 real-time operating systems, including qnx, Wind River's vxworks and mentor graphics' vrtx.
- Co simulation tools from leading eda vendors
- A variety of software development tools.

GSM Module

GSM (Global System for Mobile communications) is an open, digital cellular technology used for transmitting mobile voice and data services. It is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of Time Division Multiple Access (TDMA)and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA. It operates at either the 900 MHz or 1,800 MHz frequency band. It supports voice calls and data transfer speeds of up to 9.6 kbps, together with the transmission of SMS (Short Message Service) [9].The message sending module is SIM900, it is a complete Quad-band GSM/GPRS module designed by SIM Com. SIM900 delivers GSM/GPRS850/900/1800/1900MHz performance for voice, SMS, Data and Fax in a small form factor and with low power consumption. SIM900 is designed as a DCE (Data Communication Equipment). It provides a full modem serial port, which is used for data transmission and for sending AT commands. The SIM900 is integrated with the TCP/IP protocol; extended TCP/IP AT commands are developed for customers to use the TCP/IP protocol easily, which is very useful for those data transfer applications. Both GPS and GSM are interfaced to the control unit using serial communication protocol [9].

GPS Module

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 [7].There is a set of 24 satellites that are continuously orbiting the earth. These satellites are equipped with atomic clocks and send out radio signals as to the exact time and their location. These radio signals from the satellites are picked up by the GPS receiver. Once the GPS receiver locks on to four or more of these satellites, it can triangulate its location from the known positions of the satellites [7]. It is a high performance, low power satellite based model. It is a cost effective and portable system which accurately detects the location. A software standard for commercial GPS receiversis NMEA 0183. This is a serial protocol using ASCII sentences to convey information from the GPS receiver. According to NMEA-0183 protocol standard specifications, GPS receiver transmits the position and speed information to the PC and PDA etc. via the serial port. It is the most widely GPS receiver used protocol currently. The receiver sends multiple types of statements, only a few of letters in certain statements is valid, so it needs to parse the received data, separating out the required information.

RFID READER:

An RFID reader's function is to interrogate RFID tags. The means of interrogation is wireless and because the distance is relatively short; line of sight between the reader and tags is not necessary. A reader contains an RF module, which acts as both a transmitter and receiver of radio frequency signals. The transmitter consists of an oscillator to create the carrier frequency; a modulator to impinge data commands upon this carrier signal and an amplifier to boost the signal enough to awaken the tag. The receiver has a demodulator to extract the returned data and also contains an amplifier to strengthen the signal for processing. A microprocessor forms the control unit, which employs an operating system and memory to filter and store the data. The data is now ready to be sent to the network.

Conclusion:

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] Varsha Goud, V. Padmaja, “Vehicle Accident AutomaticDetection and Remote Alarm Device”, IJRES, Vol. 1, No. 2,July 2012.

[2] Wang Wei, Fan Hanbo, “Traffic Accident AutomaticDetection and Remote Alarm Device”, IEEE 2011.

[3] Rajesh Kannan Megalingam, Ramesh Nammily Nair,Sai Manoj Prakhya, Amrita Vishwa Vidyapeetham,Amritapuri, Clappana, “Wireless Vehicular AccidentDetection and Reporting System”, IEEE 2010.

[4] Kumar Chaturvedula, “RFID Based Embedded Systemfor Vehicle Tracking and Prevention of Road Accidents”,IJERT, Vol. 1, Issue 6, August – 2012.

[5] Rubini, Uma Makeswari, “Over Speed ViolationManagement of a Vehicle through Zigbee”, IJET, Vol. 5, No.1, Feb-Mar 2013.