Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

RFID an Effective Authentication and Attendance System

Rupak Kumar
Lecturer (Computer Science Deptt)
Al-Falah School of Engg & Tech
Dhauj Haryana, India

Harshi Solanki
M. tech Scholar(Computer Science)
Al-Falah School of Engg & Tech
Dhauj Haryana, India

Abstract: In every sphere of life we find that identification is becoming very crucial. Whether it is finding objects in a busy shop or it is about the attendance of employees in an organization. RFID has become a very prominent system. This study proposes a general RFID based authentication system which can be used anywhere where authentication of persons or objects is required. The proposed RFID system is also accompanied with PC interfacing and database logging software which is used to display the output of the system and notifies about the validity of the RFID tag and it also logs the authentication details that is RFID tag number along with date and time when the tag was authenticated in a Microsoft Access database. This is a web based system that using a VB.net script that will process the data and translate the data. For the system design, process and software architecture, components, modules, interfaces, and data for a computer system to satisfy specified requirements are studied and design for the system are made..

Keywords: Identification; Authentication; Database logging software; Software architecture; Modules

I. INTRODUCTION

Airports, railway stations, cinemas, etc are some places where identification is necessary. Identification can be made automatic using Auto-identification. There are various methods for auto-identification; some of them are bar-code systems, optical character recognition, biometrics, smart cards and RFIDs.
All RFID systems are comprised of three main components:
– The RFID tag, or *transponder*, which is located on the object to be identified and is the data carrier in the RFID system,
– The RFID reader, or *transceiver*, which may be able to both read data from and write data to a transponder, and
– The *data processing subsystem* which utilizes the data obtained from the transceiver in some useful manner.
Typical *transponders* (*trans*mitters/re*sponders*) consist of a microchip that stores data and a coupling element, such as a coiled antenna, used to communicate via radio frequency communication. Transponders may be either active or passive[1]. Active transponders have an on-tag power supply (such as a battery) and actively send an RF signal for communication while passive transponders obtain all of their power from the interrogation signal of the transceiver and either reflect or load modulate the transceiver's signal for communication. Most transponders, both passive and active, communicate only when they are interrogated by a transceiver. Typical *transceivers* (*trans*mitter/re*ceivers*), or RFID readers, consist of a radio frequency module, a control unit, and a coupling element to interrogate electronic tags via radio frequency communication. In addition, many transceivers are fitted with an interface that enables them to communicate their received data to a data processing subsystem, e.g., a database running on a personal computer. The use of radio frequencies for communication with transponders allows RFID readers to read passive RFID tags at small to medium distances and active RFID tags at small to large distances even when the tags are located in a hostile environment and are obscured from view.

II. THE BASIC SYSTEM

Components of an RFID system combine in essentially the same manner for all applications and variations of RFID systems. All objects to be identified are physically tagged with transponders. The type of tag used and the data stored on the tag varies from application to application. Transceivers are strategically placed to interrogate tags where their data is required. For example, an RFID-based access control system locates its readers at the entry points to the secure area. A sports timing system, meanwhile, locates its readers at both the starting line and the finish line of the event. The readers continuously emit an interrogation signal. The interrogation signal forms an interrogation zone within which the tags may be read[1]. The actual size of the interrogation zone is a function of the transceiver and transponder characteristics. In general, the greater the interrogation signal power and the higher the interrogation signal frequency, the larger the interrogation zone. Sending power to the transponders via the reader-to-tag communication signal is the bottleneck in achieving large read range with passive tags. Active tags do not suffer from this drawback; thus, they typically have larger communication ranges than an otherwise equivalent passive tag. The transceivers and transponders simply provide the mechanism for obtaining data (and storing data in the case of writable tags) associated with physical objects. Passive RFID systems are the most promising to provide low-cost ubiquitous tagging capability with adequate performance for most supply chain management applications. These low-cost RFID systems are, of necessity, very resource limited, and the extreme cost pressures make the design of RFID systems a highly coupled problem with sensitive trade-offs[2]. Unlike other computation systems where it is possible to abstract functionality and think modularly, almost every aspect of an RFID system affects every other aspect. We present a brief overview of the critical components of RFID technology and summarize some of these trade-offs in passive RFID design.

III. COUPLING AND COMMUNICATION

Passive RFID tags obtain their operating power by harvesting energy from the electromagnetic field of the reader's communication signal[3]. The limited resources of a passive tag require it to both harvest its energy and communicate with a reader within a narrow frequency band as permitted by regulatory agencies. We denote the center of this frequency band by f, and we refer to RFID systems operating at frequency f with the understanding that this is the center frequency of the band within which it operates. Passive tags typically obtain their power from the communication signal either through inductive coupling or far field energy harvesting. Inductive coupling uses the magnetic field generated by the communication signal to induce a current in its coupling element (usually a coiled antenna and a capacitor). The current induced in the coupling element charges the on-tag capacitor that provides the operating voltage, and power, for the tag. In this way, inductively coupled systems behave much like loosely coupled transformers. Consequently, inductive coupling works only in the near-field of the communication signal. The near field for a frequency f extends up to $1/(2\pi f)$ meters from the signal source. Generally in communication and information processing, a transmitter is any object (source) which sends information to an observer (receiver). When used in this more general sense, vocal cords may also be considered an example of a transmitter. In radio electronics and broadcasting, a transmitter usually has a power supply, an oscillator, a modulator, and amplifiers for audio frequency (AF) and radio frequency (RF)[5]. The modulator is the device which piggybacks (or modulates) the signal information onto the carrier frequency, which is then broadcast. In broadcasting, and telecommunication, the part which contains the oscillator, modulator, and sometimes audio processor, is called the exciter. Confusingly, the high-power amplifier which the exciter then feeds into is often called the "transmitter" by broadcast engineers. The final output is given as transmitter power output (TPO), although this is not what most stations are rated by. Effective radiated power (ERP) is used when calculating station coverage, even for most non-broadcast stations. It is the TPO, minus any attenuation or radiated loss in the line to the antenna, multiplied by the gain (magnification) which the antenna provides toward the horizon. This is important, because the electric utility bill for the transmitter would be enormous otherwise, as would the cost of a transmitter. For most large stations in the VHF- and UHF-range, the transmitter power is no more than 20% of the ERP. For VLF, LF, MF and HF the ERP is typically not determined separately. In most cases the transmission power found in lists of transmitters is the value for the output of the transmitter. This is only correct for omnidirectional aerials with a length of a quarter wavelength or shorter. For other aerial types there are gain factors, which can reach values until 50 for shortwave directional beams in the direction of maximum beam intensity.

Since some authors take account of gain factors of aerials of transmitters for frequencies below 30 MHz and others not, there are often discrepancies of the values of transmitted powers.

IV Micro Controller

A micro controller (also MCU or µC) is a functional computer system-on-a-chip. It contains a processor core, memory, and programmable input/output peripherals[11]. Microcontrollers include an integrated CPU, memory (a small amount of RAM, program memory, or both) and peripherals capable of input and output. It emphasizes high integration, in contrast to a microprocessor which only contains a CPU (the kind used in a PC). In addition to the usual arithmetic and logic elements of a general purpose microprocessor, the microcontroller integrates additional elements such as read-write memory for data storage, read-only memory for program storage, Flash memory for permanent data storage, peripherals, and input/output interfaces. At clock speeds of as little as 32KHz, microcontrollers often operate at very low speed compared to microprocessors, but this is adequate for typical applications. They consume relatively little power (milliwatts or even microwatts), and will generally have the ability to retain functionality while waiting for an event such as a button press or interrupt. Power consumption while sleeping (CPU clock and peripherals disabled) may be just nanowatts, making them ideal for low power and long lasting battery applications. Microcontrollers are used in automatically controlled products and devices, such as automobile engine control systems, remote controls, office machines, appliances, power tools, and toys. By reducing the size, cost, and power consumption compared to a design using a separate microprocessor, memory, and input/output devices, microcontrollers make it economical to electronically control many more processes

V. Conclusion

1. No "line of sight" requirements: Bar code reads can sometimes be limited or problematic due to the need to have a direct "line of sight" between a scanner and a bar code. RFID tags can be read through materials without line of sight.
2. More automated reading: RFID tags can be read automatically when a tagged product comes past or near a reader, reducing the labor required to scan product and allowing more proactive, real-time tracking.
3. Improved read rates: RFID tags ultimately offer the promise of higher read rates than bar codes, especially in high-speed operations such as carton sortation.
4. Greater data capacity: RFID tags can be easily encoded with item details such as lot and batch, weight, etc.

5. Write" capabilities: Because RFID tags can be rewritten with new data as supply chain activities are completed, tagged products carry updated information as they move throughout the supply chain.

References

[1]. M. Abadi, M. Burrows, C. Kaufman, and B. W. Lampson. Authentication and delegation with smart-cards, In *Theoretical Aspects of Computer Software*, pages 326–345, 1991.

[2]. R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In *IWSP: International Workshop on Security Protocols, LNCS*, 1997.

[3]. B. Bing. *Broadband Wireless Access,* Boston, Kluwer Academic Publishers, 2000.

[4]. D. Boneh, R.A. DeMillo, and R.J. Lipton. On the importance of checking cryptographic protocols for faults. In *EUROCRYPT'97*, volume 1233, pages 37–51. Lecture Notes in Computer Science, Advances in Cryptology, 1997.

[5]. S. Chari, C. Jutla, J.R. Rao, and P. Rohatgi. A cautionary note regarding evaluation of AES candidates on smart-cards. In *Second Advanced Encryption Standard (AES) Candidate Conference*, Rome, Italy, 1999.

[6]. EAN International and the Uniform Code Council, Note to Editors, http://www.ean-int.org/index800.html

[7]. D. Engels. The Reader Collision Problem. Technical Report.MIT-AUTOID-WH-007,2001. http://www.autoidcenter.org/research/MIT-AUTOID-WH-007.pdf.

[8]. K. Finkenzeller. *RFID Handbook,* John Wiley & Sons. 1999.

[9]. H. Gobioff, S. Smith, J.D. Tygar, and B. Yee. Smart cards in hostile environments. In *2nd USENIX Workshop on Elec. Commerce*, 1996.

[10]. J. Hoffstein, J. Pipher, and J.H. Silverman. NTRU: A ring-based public key cryptosystem. *Lecture Notes in Computer Science,* volume 1423, 1998.

[11]. International Telecommunications Union. Radio Regulations, Vol. 1, 1998.

[12]. B.S. Kaliski Jr. and M.J.B. Robshaw. Comments on some new attacks on cryptographic devices. RSA Laboratories' Bulletin No. 5, July 14, 1997. Available from http://www.rsasecurity.com/rsalabs/bulletins/.