IJIRR

International Journal of Information Research and Review
Vol. 05, Issue, 02, pp.5200-5203, February, 2018

REVIEW ARTICLE

A MODEL FOR IMPLEMENTING DATABASE SECURITY USING RADIO FREQUENCY IDENTIFICATION (RFID) AND ROLE - BASED ACCESS CONTROL

***Nicholas Oluwole Ogini**

Department of Computer Science, Delta State University, Abraka

ARTICLE INFO

Article History:

Received 25th November, 2017
Received in revised form
10th December, 2017
Accepted 13th January, 2018
Published online 28th February, 2018

Keywords:

RFID,
Electormagnetic field,
TAG,
UHF,
LF.

ABSTRACT

To state that the computer has found its way into most fields of human interest is saying the obvious. This is because almost all corporate organizations now depend on computers for their day to day operations including the means of storing sensitive data and information vital to the organization. In this computer age, everyone needs a computer to remain relevant and up to date, and this has arguably made the computer to become the most sought after piece of electronic device (albeit for both legitimate and illegitimate use). Most organizations today are networking in order to share resources including databases thereby allowing several computers access the same database. Advantage of this is being taken by criminals as they have become aware of the enormous benefits of the illegal business of gaining access without authorization (hacking) database of organizations. One of the approaches of this is to device means of taking advantage of any idle computer in a remote area to access a common database. The security of remote computer systems from physical hackers is highly desired, in this paper therefore, the Radio frequency identification (RFID) is introduced into computers security using Tags and Readers. The general operations and applications of the RFID, its types and characteristics are discussed, and a framework for this is designed.

INTRODUCTION

Radio frequency identification (RFID) networks are an emerging type of network that is posed to play an important role in the Internet-of-Things. Responsible people work hard to legitimately make a living in order to support themselves and their families through life. However, some people sit in the comfort of their homes to device means of breaking into pockets of those who have worked so hard. A common crime is identity theft. This is the use of another person's identification documents or other identification in order to impersonate the real person. According to a 2003 survey by the United State Federal Trade Commission, an estimated 10 million people in the U.S found out that they are victims of identity theft. An approach to this theft is that of waiting for the computer owner to move away from the physical location of the computer, then an unauthorized person gain access to the computer in order to commit crime either by installing a spy ware, changing database contents, stealing sensitive data, deleting files, and so on, owing to the fact that the owner has left the system after logging in and failed to log-off or shut down before leaving. This is raising issues in corporate databases and networked environments as they are becoming more challenging by the day.

Corresponding author:* **Nicholas Oluwole Ogini
Department of Mathematics and Computer Science, Delta State University, Abraka

Hackers are on the prowl and it is advisable to always log off the computer as you physically leave such that on return, you have to log-on again using your password. If your office is an open suite or your system is mobile functionally, then you could be at risk, as some emergencies may demand that you leave your system unattended at some times, while already connected to a database of your organization, and leaving in such a hurry means a possibility of leaving without logging off, and with so much sensitive information to which your computer has access, the content of the whole corporate database is at risk.

The procedure to log off is implemented in some operating systems. For instance in Microsoft it is dealt with in two ways:

This implementation works because once you log off, your system is secure from that moment up to the time you return and enter your login password

- Click start
- User account
- Select the account you want to set password for
- Click create password
- Enter your password

Using a password protected screen saver.

The procedure for this set up is

- Click start
- Click control panel
- Click display
- On the tab click screen saver
- Chose the screen saver you need from the drop down menu
- Click the box labeled-on resume, password protect
- You can then select the duration you want the system to be idle. Before the screen saver automatically comes up, the problem with this is that it could keep popping up when you do not touch your system but you are present thereby becoming a nuisance as you will need to continuously login.

However, the very short time it may take before the screen saver comes up may be enough for the criminal to commit the crime he or she desires.We introduce the Radio Frequency Identification (RFID) technology that will provide a way around this problem. The RFID is a wireless non-contact use of radio frequency electromagnetic field to transfer data for the purpose of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by and read at short ranges through magnetic field. This concept emanated from the IFF transponder which was routinely used during the World War II.

Current Applications

Most common uses for radio frequency identification technologies included transportation, materials management, and security. Today, there are a variety of other applications for RFID. One of the leading users of RFID technology is the transportation industry. RFID applications in transportation include railroad car management, traffic management, tolls and fees, fare collection, equipment identification, fleet management, solid waste hauling, and fuel dispensing (CII, 2001). In developed societies, when an indigene driver passes through an express toll lane an RFID tag alerts the tag reader that someone has passed through the toll and the reader then identifies that driver and communicates the charge to an account setup in a networked computer system. Many hotel businesses use RFID to control access to facilities by attaching a tag to an employee's room card or ID badge. Such technology ensures that only authorized persons are allowed access to particular rooms or entrances. This is also becoming more common in nursing homes and hospitals where there is the need to track individuals. RFID chips have been embedded into automobile keys that enable the car only to start if the key has the proper chip embedded into it. Law enforcement officers are now able to track credit cards, jewelry, vehicles and artwork by radio frequency tags embedded in these objects. Tracking goods through the manufacturing process, is also possible. A use for RFID tags in international athletics is found in almost all major track and field events. Road races, running races or marathons in the streets, use shoelace RFID tags to get race results of runners as they cross the start and finish lines where there time is officially kept regardless of when the runner begins the race. These technologies are also being used to track athletes to verify that the path travelled is the same as the course defined by the race officials. Global Positioning Systems (GPS) have revolutionized the means to accurately locate and identify objects on the earth's surface using a system of satellites in space and transmitters and receivers on earth. The combination of GPS and RFID identification tags has made real-time tracking a reality. Materials and assets can be identified and tracked as they are installed or transported. RFID tags could be used to track and identify airline luggage and passengers increasing national security, speeding up luggage sorting and transfer, and decreasing expenditures resulting from heightened security measures. The International Air Transport Association (IATA) believes this technology has countless potential benefits for simplifying passenger travel for airports and airlines. The major advantages of RF technology in baggage handling are an increased journey speed of luggage as a result of faster read rates and elimination of human intervention in misdirected bags and security procedures. Access and tracking of patients and guests with authorized wristbands through hospitals, is an electronic tagging and monitoring system for controlling the movement of new-born babies in a hospital environment. The system comprises active transponders attached to the baby, monitoring receivers at doorways and a computer networking system to reduce the risk of abduction and to ensure mother and child identification.

MATERIALS AND METHODS

For a System to make use of RFID technology there must be typically three key elements:

- An RFID tag, or transponder, that carries object-identifying data.
- An RFID tag reader, or transceiver, that reads and writes tag data.
- A back-end database, that stores records associated with tag contents.

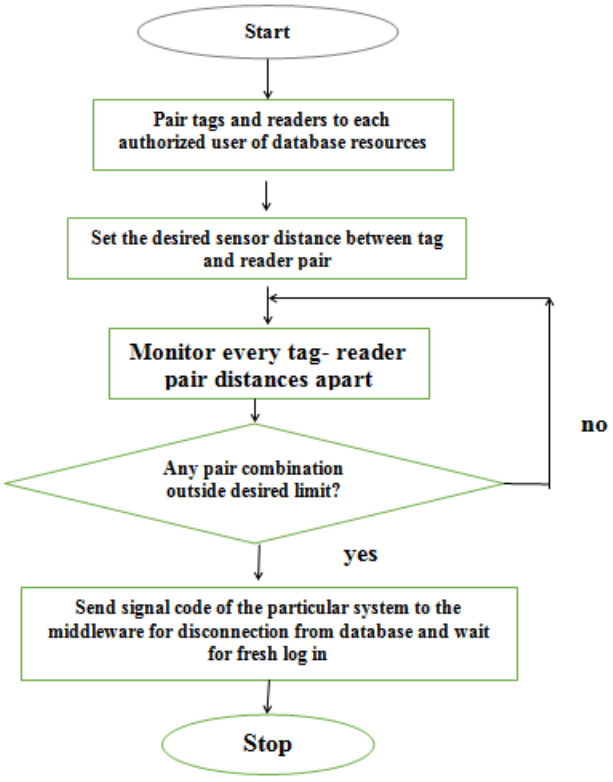

Fig. 1. A flowchart of the system

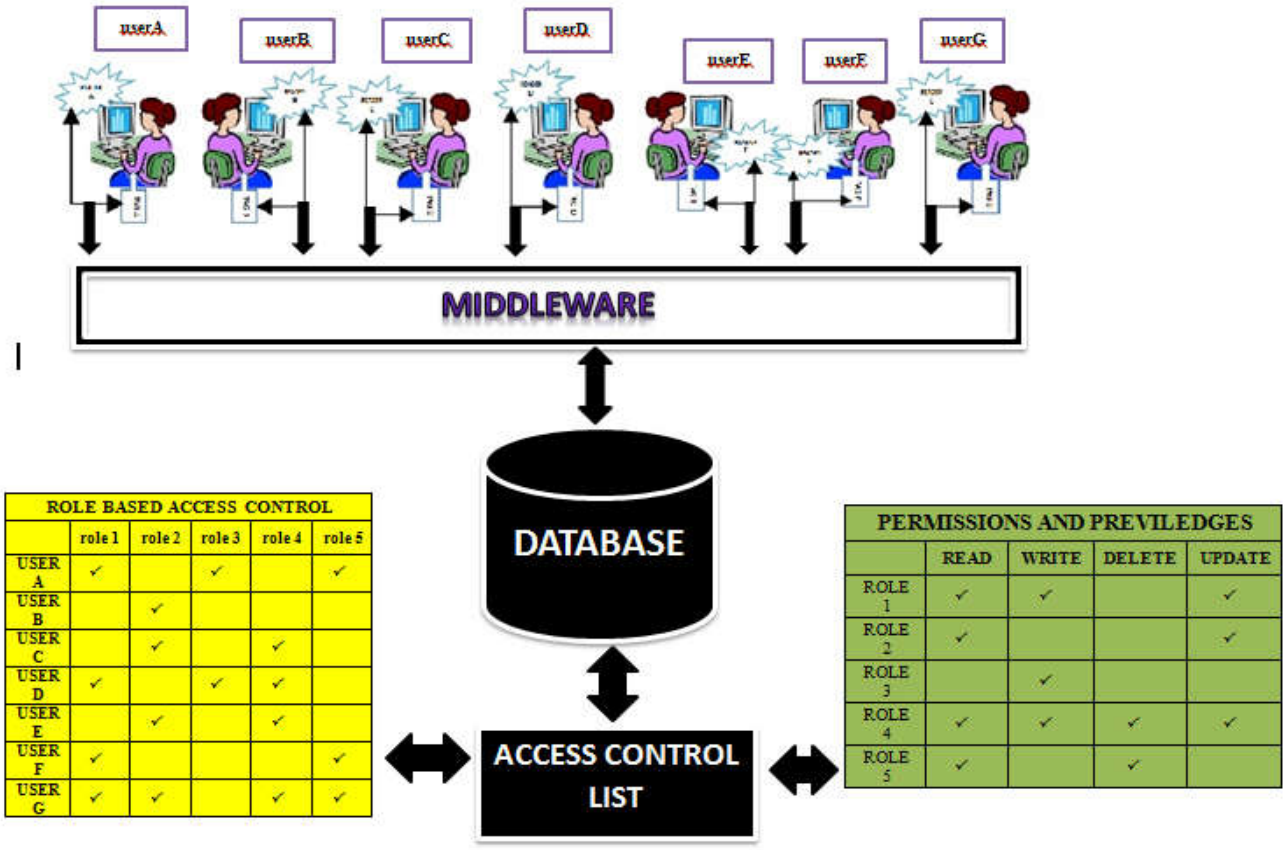

Fig. 2. A model for implementing database security using RFID and ROLE - BASED access control

Types of tags and readers

Table 1. Classification of RFID Tags Types

Passive	Semi-passive	Active
The reader sends electromagnetic waves that induce current in the tag's antenna, the tag reflects the RF signal transmitted and adds information by modulating the reflected signal. It obtains operating power from the reader this is also called 'pure passive', 'reflective' or 'beam powered'	uses a battery to maintain memory in the tag or power the electronics that enable the tag to modulate the reflected signal communicates in the same method, as the other passive tags	This is powered by an internal battery, used to run the microchip's circuitry and to broadcast a signal to the reader. It generally ensures a longer read range than passive tags. It is more expensive and the batteries must be replaced periodically.

Table 2. Classification by the tag's memory type

Read-only	Read-write
The memory is factory programmed, and cannot be modified after its manufacture. Its data is static and has a very limited quantity of data can be stored, usually 96 bits of information. It can be easily integrated with data collection systems typically they are cheaper than read-write tags	It can be read as well as written into hence its data can be dynamically altered and can store a larger amount of data, typically ranging from 32kBytes to 128kbBytes. being more expensive than read-only chips, is impractical for tracking inexpensive items

Table 3. Classification By the method of wireless signal used for communication between the tag and reader

Induction	Propagation
Generally use. LF and HF frequency bands Close proximity electromagnetic, or inductive coupling—near field	Operate in the UHF and microwaves frequency bands Propagating electromagnetic waves—far field

Table 4. Classification of readers by design and technology used

Read	Read/write
only reads data from the tag usually a micro-controller-based unit with a wound output coil, peak detector hardware, comparators, and firmware designed to transmit energy to a tag and read information back from it by detecting the backscatter modulation different types for different protocols, frequencies and standards exist	reads and writes data from/to the tag

The RFID has two major components; they are the tag and the reader. The components on the tag have two parts: Microprocessor to store and process information, and a receiver and transmitter to receive and transmit signal. In this design, other requirements include

- Authorized computer users
- Access control list
- Computer systems
- A role-based access control structure

RESULTS AND DISCUSSION

Every user of the database is first authorized this implies that the user can access the database and use its resources. However, the database is created to take care of the different job description in the organization, called views. Roles are then created and are assigned permissions and privileges. For instance, in this model, the role 1 has the privilege of reading from the database, writing into the database, and updating the database. Role 3 for instance has a permission and privilege of only writing into that database. The function of each user then determines which group of roles can be assigned to a user as shown in the ROLE BASED ACCESS CONTROL table. The access control list (ACL) actually contains every user's permissions records in the database.

Therefore, it is linked to the middleware which is in constant check of the link between the tag and reader. Once the user wearing the tag walks away from the computer system beyond an allowable distance, for instance the passive low frequency band type of distance of less than 3 meters range, the reader alerts the middleware which in turn communicate with the ACL to switch off access to the given user's access to the database, thereby providing the desired security.

Conclusion

In conclusion, this study has revealed that there is the need to inhibit or eliminate hackers from computer systems or database resources. The computer science community is being stretched to its limit by the actions of these hoodlums as it is being reported daily. However it is mostly the careless nature of the authorized user and not only the smartness of the hacker that breaks the systems. The several models implemented has provided little cover so far, this model therefore provide an RFID approach that depends on technology to provide the desired security.

REFERENCES

Avoine, G. 2011, RFID Security & Privacy Lounge. http://www.avoine.net/ rfid/. Accessed 14 march, 2015.

Batina, L. Guajardo J.. Kerins T. Mentens N. Tuyls P and.Verbauwhede I, 2011, 'Public-Key Cryptography for RFID-Tags' URL: https://www.cosic.esat.kuleuven.be/ publications/article-821.pdf

Juels, A. 2004. "Yoking-Proofs" for RFID Tags. International Workshop on Pervasive Computing and communication Security.

Koscher, K., Juels, A., Kohno, T. and Brajkovic, V. 2009. EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. In Proceedings of the 2009 ACM Conference on Computer and Communications Security (CCS'09), pp. 33–42.

Moskowitz, P. A., Lauris, A. and Morris, S. 2007. A Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag. In Proceedings of the 2007 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom'07, pp. 348–351.

RFID SECURITY FEBRUARY, 2008, http://www.infosec. gov.hk/english/technical/files/rfid.pdf

Tan, C.C.; Bo Sheng and Qun Li, 2010. Efficient techniques for monitoring missing RFID tags, Wireless Communications, IEEE Transactions on Volume: 9, Issue: 6 , pp 1882-1889.

Clark, D.D. and Wilson. D.R. 1987. A Comparison of Commercial and Military Computer Security Policies. In *IEEE Symposium on Computer Security and Privacy*, April.

John Barkley, "Implementing Role-Based Access Control using Object Technology," *First ACM Workshop on Role-Based Access Control*, Gaithersburg, Maryland, November 30-December 1, 1995.

David F. F., Janet A. C., and Kuhn D. R., "Role-Based Access Control (RBAC): Features and Motivations," *11th Annual Computer Security Applications Proceedings,* 1995.

****