Business Continuity Based on RFID

Waleed K. A . Abdulrahem[a] , Hebah H. O. Nasereddin[b],Said M. H. Fares [c]

[a] MEU — Middle East University, Amman, Jordan
wal1333@yahoo.com
[b] MEU — Middle East University, Amman, Jordan
hnasereddin@meu.edu.jo
[c] MEU — Middle East University, Amman, Jordan
smhf2004@yahoo.com

Abstract. In today's global age, business continuity has become one of the most important fields to protect any system. They aim to ensure that critical business will be available to stakeholders. Business continuity ensures that the organization will overcome common threats like: earthquake, fire, flood, cyber-attack, terrorism/piracy, war/civil disorder, and theft (insider or external threat, vital information or material). An organization is usually consisting of data, off-site, software, and hardware, which is our main concern. This paper describes how to protect organization's hardware from theft using Radio-frequency identification (RFID), which can be defined as the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects.

Keywords: Business continuity (BC), Radio-frequency identification (RFID), Tag.

1 INTRODUCTION

Business Continuity is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions, simply it means the ability to make the organization continue to operate even in worst case like earthquake, flood, fire, cyber-attack, terrorism, war, random failure of mission-critical systems, theft (insider or external threat, vital information or material). Organization parts that should be protected to ensure business continuity may include data, off-site, software, and hardware where this organization part is what we are focusing in this paper to protect using Radio-frequency identification (RFID).

2 RADIO FREQUENCY IDENTIFICATION (RFID)

Radio-frequency identification RFID is a technology that uses electronic tags placed on objects, people, or animals to relay identifying information to an electronic reader by means of radio waves. The components of RFID technology system are shown in figure (1).

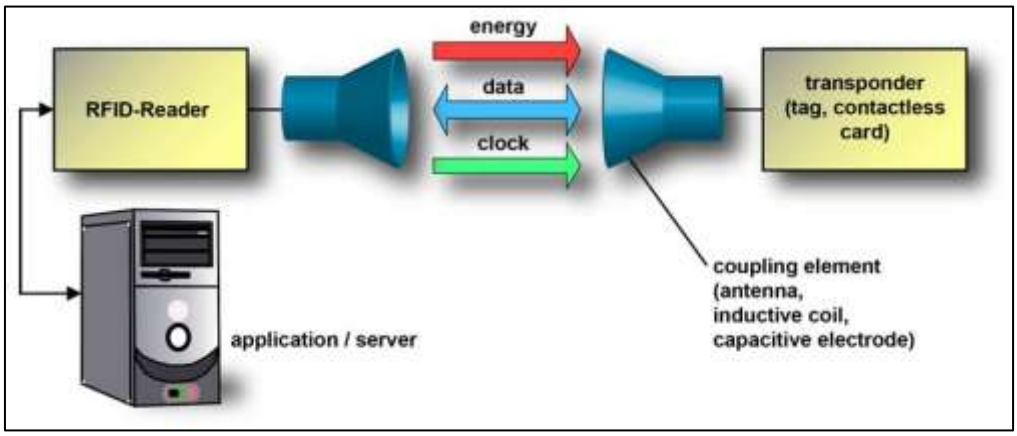

Figure (1) Components of RFID Technology System.

We can simply explain the RFID technology saying that a tag that is attached to the object intended to be tracked will send a response to the RFID reader upon request. That response will provide all details and data about the tracked object.

RFID tags has many characteristics, these characteristics are:

- Small chips that can be implanted anywhere even within people.
- The tag's information is stored electronically in a non-volatile memory.
- Have individual serial numbers.
- Includes a small RF transmitter and receiver.
- Size 0.05mm × 0.05mm up to several cms.
- Have a memory range from 128 bit up to 128 kb.
- Can be made of different materials like paper, metal, plastic …etc.
- Can be read-only, read/write, or write-once, read-multiple
- Have a cost range from .05 $ to 50 $.
- Contain at least two parts: a circuit for processing and storing data and an antenna for receiving and sending the signal.

There are two types of RFID tags: Passive and Active Tags. Passive tags have no battery, instead these tags make use of the radio energy transmitted by the reader as their energy source, and they are also very small in size.

Figure (2) Passive tag place on a thump.

Active Tags have on-board battery and periodically transmit their ID signal to the RFID reader and also have capability storage. RFID reader can be fixed or handled with different frequency bands. The table below explains RDIF frequency bands used and their characteristics.

Band	Regulations	Range	Data speed	Remarks	Approximate tag cost in volume (2006) US $
120–150 kHz (LF)	Unregulated	10 cm	Low	Animal identification, factory data collection	$1
13.56 MHz (HF)	ISM band worldwide	1 m	Low to moderate	Smart cards (MIFARE, ISO/IEC 14443)	$0.50
433 MHz (UHF)	Short Range Devices	1–100 m	Moderate	Defence applications, with active tags	$5
865-868 MHz (Europe) 902-928 MHz (North America) UHF	ISM band	1–2 m	Moderate to high	EAN, various standards	$0.15 (passive tags)
2450-5800 MHz (microwave)	ISM band	1–2 m	High	802.11 WLAN, Bluetooth standards	$25 (active tags)
3.1–10 GHz (microwave)	Ultra wide band	to 200 M	High	requires semi-active or active tags	$5 projected

Table (1) RFID frequency bands

RFID can be used in many different fields like access management, tracking of goods, people, animals, airport baggage …etc. and preventing of theft. The value of the RFID market in

2012 was $7.46 (USD) billion versus $6.37 (USD) billion in 2011. The RFID world market is estimated to surpass $20 billion (USD) by 2014.

3 LOCK-KEYS AND HARDWARE THEFT PROTECTION

Thieves usually does not look after the hardware itself, they usually look after the valuable data a hardware may contain like identities, credit cards …etc., but if a thief is capable of putting his hands on the hardware itself, this means that he could access your data. In Dec 2012, a Laptop from NASA were stolen, contain personally identifiable information of "at least" 10,000 NASA employees and contractors. That's why protecting hardware is becoming one of the main concerns in the world of technology today, companies spend millions of dollars to safe their hardware according to the saying "prevention is better than cure". Most hardware protection scenarios are based on locking the hardware itself or keeping it in a locked place protected with different technologies like finger or eye print. Most of these scenarios have weaknesses and have been hacked or overlapped.

Figure (3) PC locked with ordinary locker

Figure (4) Finger print protection systems.

4 RFID AND HARDWARE THEFT PROTECTION

By using proper RFID system on the Hardware, we add new safety factor to the organization which help business continuity. Adding RFID tag lock which can be read remotely by the manager will add value as the following states:

- Record can be implemented inside the tag which gives the manager a brief history about the hardware.
- Easy to be placed inside critical hardware.
- Inventory within seconds.
- Remotely from the manager room.
- Greater assurance of item identification (unique serial number).
- Not dependent on bin location accuracy.
- Manage very large number of items and a variety of sizes per unit.
- Easily added to existing storage areas and tool rooms.
- 24/7 self-service mode can reduce headcount.

A first scenario preventing hardware theft and in case of tag is still exists is based on RFID gates. The reader will read the tag at the gate and to make alarm, the gate contains magnetic and photo beam sensors combined with surveillance web cameras to offer security and accountability, and by Ethernet network it can be controlled by Client/Server software. An applied system that uses RFID gates is built by company called AutoCrib where a gate is a turnkey RFID system that is located at a choke point, in order to track material tagged with RFID labels in and out of a controlled area.

Figure (5) AutoCrib RFID gate.

A second scenario is based on thieve with good knowledge with RFID technology, here we suppose that a thief knows how RFID technology works, so he would just tear the tag placed

on hardware and when he passes the gate no alarm will be initiated. The solution to this scenario is based on RFID continuous circle between RFID reader and tags placed on hardware. RFID reader continuously connects to obtain a signal from an RFID tag placed on hardware that is within its field of communication, this make a circle. In some RFID system, if the tag were breakdown, the circle will turn-off which give alarm sign.

A third scenario can take place in case of protecting valuable hardware by adding a second tag hidden within the hardware itself, this tag must be a one of large field of communications so that it can be tracked if the some failure happened to first shown tag.

5 CONCLUSION

This paper concerns with business continuity based on RFID technology to protect organization's hardware components against theft. Three scenarios discussed, the first scenario based on RFID gates which has been applied, the second scenario based on RFID continuous circle between RFID reader and tags placed on hardware, last scenario adds second tag hidden within the hardware itself, this tag must be a one of large field of communications so that it can be tracked if the some failure happened to first shown tag. Second and third scenarios have not been applied yet (as far as we know).

REFERENCES

E. Bottani and A. Rizzi(2008). Economical assessment of the impact of RFID technology and EPC system on the fast-moving consumer goods supply chain. International Journal of Production Economics, 112:548; 569.

H. Baars, H.G. Kemper, H. Lasi, and M. Siegel(2008). Combining RFID technology and business intelligence for supply chain optimization scenarios for retail logistics. Proceedings of the 41st Hawaii International Conference on System Sciences. ISBN ISSN:1530-1605 , 0-7695-3075-8.

G. Gaukler, O. Ozer, and W. Hausman(2005). RFID and product progress information: Improved emergency ordering policies. Technical report, Dept. of Management Science and Engineering, Stanford University, Stanford, CA.

http://www.autocrib.com/PressRelease.asp?ref=21

http://en.wikipedia.org/wiki/Radio-frequency_identification

RFID Journal http://www.rfidjournal.com/