ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Review of RFID Technology

Vinay Kumar Bachu[*1],Sunil Saram[2], N.V.S.Shravan kumar Sharma[3]
[*1,2,3] Department of ECE, Vignana Bharathi Institute of Technology, Aushapur-501301, India
vinaykumarbachu@gmail.com

Abstract

This paper presents various approaches and analysis that describes the terminology for RFID malware. There are various approaches used for RFID malware analysis and still lot of work is going on in this direction. Our purpose this paper is to analyse the various basic terms and approaches that have been introduced in this particular domain.

Keywords: RFID, RFID Tag, Reader, Antenna.

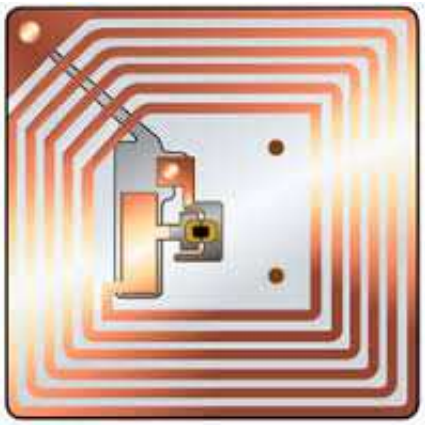
Introduction

Radio-frequency identification (RFID) is 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. The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or UHF radio waves (i.e.,electromagnetic radiation at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a bar code, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.Radio Frequency Identification (RFID) is the quintessential Pervasive Computing technology. Touted as the replacement for traditional barcodes,RFID's wireless identification capabilities promise to revolutionize our industrial, commercial, and medical experiences [1]. The heart of the utility is that RFID makes gathering information about physical objects easy. Information about RFID-tagged objects can be transmitted for multiple objects simultaneously, through physical barriers, and from a distance. In line with Mark Weiser's concept of "ubiquitous computing" RFID tags could turn our interactions with computing infrastructure into something subconscious and sublime. Some tags read via electromagnetic induction and require battery no battery. The tag contain electronically information that can be sensed from a distance of few meters . The tag does not need line of sight as required by barcodes.

RFID Tags: The basic RFID building blocks are miniature electronic devices known as Tags which talk to Readers. The RFID tags, also known as transponder, are usually small pieces of material, typically comprising three components: an antenna, a microchip unit containing memory storage an encapsulating material. Tag are embedded or attached to an item. The Tag has memory which stores information as either read only, write once or unlimited read/write. Tags typically range in size from a postage stamp to a book, depending on read distance and features. RFID tags come in a wide variety of shapes and sizes.RFID tags are categorized into active and passive. They are fundamentally distinct technologies with substantially different capabilities. Both of the technology use radio frequency energy to communicate between a tag and a reader, the method of powering the tags is different. Active RFID tags are powered by an internal battery or internal power source continuously power the tag and its RF communication circuitry and are typically read/write, i.e., tag data can be rewritten and/or modified.While passive RFID tags operate without a separate external power source and obtain operating power generated from the reader. The passive RFID relies on RF energy transferred from the reader to be tag to power the tag. Passive tags are consequently much lighter than active tags, less expensive, and offer a virtually unlimited operational lifetime

Design

ISSN: 2277-9655
Impact Factor: 1.852



RFID Readers:

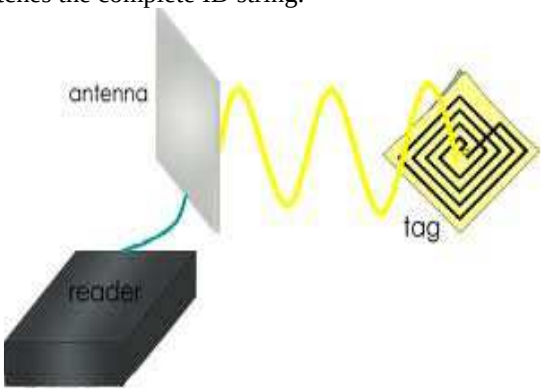
RFID systems can be classified by the type of tag and reader. A Passive Reader Active Tag (PRAT) system has a passive reader which only receives radio signals from active tags (battery operated, transmit only). The reception range of a PRAT system reader can be adjusted from 1–2,000 feet (0.30–610 m), allowing flexibility in applications such as asset protection and supervision.An Active Reader Passive Tag (ARPT) system has an active reader, which transmits interrogator signals and also receives authentication replies from passive tags. An Active Reader Active Tag (ARAT) system uses active tags awoken with an interrogator signal from the active reader. A variation of this system could also use a Battery-Assisted Passive (BAP) tag which acts like a passive tag but has a small battery to power the tag's return reporting signal.Fixed readers are set up to create a specific interrogation zone which can be tightly controlled. This allows a highly defined reading area for when tags go in and out of the interrogation zone. Mobile readers may be hand-held or mounted on carts or vehicles.

Signaling

Signaling between the reader and the tag is done in several different incompatible ways, depending on the frequency band used by the tag. Tags operating on LF and HF bands are, in terms of radio wavelength, very close to the reader antenna because they are only a small percentage of a wavelength away. In this near field region, the tag is closely coupled electrically with the transmitter in the reader. The tag can modulate the field produced by the reader by changing the electrical loading the tag represents. By switching between lower and higher relative loads, the tag produces a change that the reader can detect. At UHF and higher frequencies, the tag is more than one radio wavelength away from the reader, requiring a different approach. The tag canbackscatter a signal. Active tags may contain functionally separated transmitters and receivers, and the tag need not respond on a frequency related to the reader's interrogation signal.An Electronic Product Code (EPC) is one common type of data stored in a tag. When written into the tag by an RFID printer, the tag contains a 96-bit string of data. The first eight bits are a header which identifies the version of the protocol. The next 28 bits identify the organization that manages the data for this tag; the organization number is assigned by the EPCGlobal consortium. The next 24 bits are an object class, identifying the kind of product; the last 36 bits are a unique serial number for a particular tag. These last two fields are set by the organization that issued the tag. Rather like a URL, the total electronic product code number can be used as a key into a global database to uniquely identify a particular product.Often more than one tag will respond to a tag reader, for example, many individual products with tags may be shipped in a common box or on a common pallet. Collision detection is important to allow reading of data. Two different types of protocols are used to "singulate" a particular tag, allowing its data to be read in the midst of many similar tags. In a slotted Aloha system, the reader broadcasts an

ISSN: 2277-9655
Impact Factor: 1.852

initialization command and a parameter that the tags individually use to pseudo-randomly delay their responses. When using an "adaptive binary tree" protocol, the reader sends an initialization symbol and then transmits one bit of ID data at a time; only tags with matching bits respond, and eventually only one tag matches the complete ID string.



Conclusion

In this paper basic terminology related to RFID malware is explained. There are various issues related to designing get reviewed with prevention methods at last. This study will be helpful for basic idea in this domain and for further research .

References

[1] http://en.wikipedia.org/wiki/Radio-frequency_identification#Design
[2] http://www.intermec.com/learning/technologies/rfid/
[3] http://www.schreiner-logidata.com/3/about-schreiner-logidata/rfid-technology/
[4] www.csharpcorner.com. ,"Advance concepto prevent SQL injection"