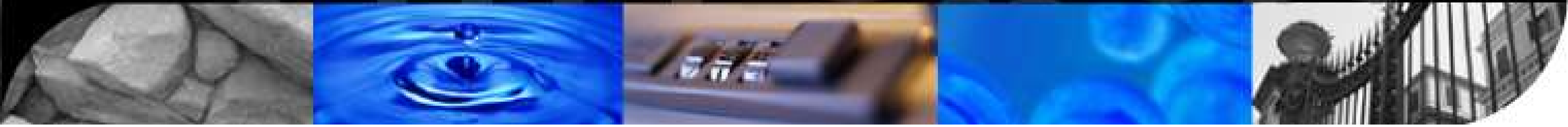
Comprehensive Network Security Solution



The Reality of RFID

Joan Ross, CISSP, NSA IAM, FCC Engineer
Founder & President, enCircle Corporation

2005 NEbraskaCERT Conference
10 August 2005

Electronic passports set to thwart forgers

- The U.S. passport is joining the digital age. After three years of research and discussion, the State Department has finalized most of the technical and logistical details of new, supposedly tamper-proof passports embedded with a "smart-card" chip.
- When swiped across an electronic reader, the chip in the passport wirelessly transmits data to a customs officer's computer screen. The e-passport relies on radio frequency identification technology (RFID).
- The e-passport has raised concerns among critics who say it lacks adequate privacy safeguards. Wireless transmission of data compromises security, and important personal data could fall into the wrong hands, they say. With proper equipment, someone could remotely intercept personal data, they say.

http://www.usatoday.com/tech/news/2005-08-08-electronic-passports_x.htm

The U.S. Department of Homeland Security has begun testing immigration documents laced with radio-frequency identification chips at five spots on the Mexican and Canadian borders.

- The goal of the technology is to speed up--if not automate--secure entry and exit of visitors at the nation's ports, according to a Homeland Security press release.
- The chips are embedded in Customs and Border Protection Form I-94A, which the government issues at all ports of entry to chart the departure and arrival of certain foreign visitors--typically those with nonimmigrant visas, such as students or guest workers.
- At the test sites, chip readers note the entry or exit of visitors who pass by and transmit that information to a government-maintained database. Each tag carries only a serial number, which cannot be changed, and holds no personal identifiers. Only U.S. government officials have the ability to link that number to the visitor's personal records, the press release said.

http://news.zdnet.com/2100-1009_22-5823958.html

- 02:00 AM Aug. 09, 2005 PT
- The British government is preparing to test new high-tech license plates containing microchips capable of transmitting unique vehicle identification numbers and other data to readers more than 300 feet away.
- Officials in the United States say they'll be closely watching the British trial as they contemplate initiating their own tests of the plates, which incorporate radio frequency identification, or RFID, tags to make vehicles electronically track-able.

http://www.wired.com/news/privacy/0,1848,68429,00.html?tw=rss.TOP

What is RFID?

RFID stands for radio frequency identification. It is a technology that has existed for decades. At a simple level, it is a technology that involves tags that emit radio signals and devices called readers that pick up the signal. RFID technology is a fundamental element of the EPCglobal Network.

http://www.epcglobalinc.org/about/faqs.html#6

- RFID is a highly reliable way to electronically control, detect and track a variety of items using FM transmission methods. A small tag, or transponder, affixed to or embedded into virtually any object (including livestock) individually identifies the object using a unique, factory-programmed, unalterable code.

http://www.aimglobal.org/technologies/rfid/resources/papers/applicationsofrfid.htm

- Included in a RFid system are a number of components including tags, handheld or stationary readers, antennas, and system software. A reader comprises of a transmitter, receiver, control module and communication functions, sometimes called a transceiver in radio terms for it to link to a controlling PC.

- The transponders or tags are used to identify objects, which can be uniquely programmed with information about the objects. Readers should have an attached antenna, which is used to transmit and receive the radio frequency signal. Each reader is accompanied with PC compatible software that allows the user to read and program tags.

http://www.ti.com/tiris/docs/customerService/faq.shtml#Gone

The RFID reader emits electro-magnetic, frequency modulated waves within a certain distance. The distance is generally determined by the size and power of the antenna

The corresponding passive transponder receives the energy waves, utilizes them (for charging as an example) and correspondingly responds to the data signal.

Active transponders utilize batteries for power, providing distance transmission, and more complex transmission and processing.

Semi-active/semi-passive utilize both battery and emission energy.

The reader device receives the data response and can hold the data for later upload, or process the data through control lines and interface links to target systems.

- Read only transponder systems can be read up to relatively short distances and contain a unique programmed ID code of limited digits.

- Read-write transponder systems have programmable code capability to create customized data on the RFID tag. This customization facilitates integration with automation systems and other computerized data designs.

- Both types of RFID data transmissions can be sent to computer systems through standard or customized interfaces and stored in portable readers for later upload into data processing systems.

RFID Tags

The tag holds the data that the reader requests.

1. Integrated circuit (IC) with memory.
2. Chipless tags with no onboard IC.

Memory Capability

Read Only (RO)
Read-Write (RW)
Write Once-Read Many (WORM)

Frequencies

Operational function and frequency involves standards, regulations and corresponding applications.

LF: 135kHz or less

HF: 13.56MHz

UHF: 433MHz and up

MF: 2.45GHz and 5.8GHz

“Now you can find it!” is the advertising slogan for RF receiver discs that beep and flash to help locate missing objects. You attach the tag using an adhesive backing to items that have a tendency to be misplaced (TV remotes, toys, key chains, etc.). The receivers will both beep and flash when you’re within 40 feet when you use the transmitting device.

Frequently asked questions to research and consider:

2. **What are RF tags and how do passive and active tags differ?**
3. **What is the write distance of a tag?**
4. **How can I achieve the optimum read range?**
5. **What can cause a reduction in read distance?**
6. **What is a reading hole and what are possible causes?**
7. **What is the maximum Read-range?**
8. **What is the minimum separation between Tags?**
9. **How many tags can be identified?**
10. **What is the maximum antenna size?**
11. **What is the maximum allowed field strength?**
12. **How can I determine the inductance of an antenna?**
13. **How can I avoid coupling between antennas?**
14. **What are possible noise sources?**

http://www.ti.com/tiris/docs/customerService/faq.shtml#Gone

It’s all in your design and selection…

Mock Case Studies

#1: You are a retail organization that includes a pharmacy center. How are you intending to design your RFID for Phase I implementation?

#2: You manage an aeronautics manufacturing and maintenance division. How can RFID improve your organization?

http://www.packagingdigest.com/articles/200507/40.php enCircle

At the Metro Future Store in Rheinberg, Germany, technology partners are testing the use of RFID, wireless networks, Personal Shopping Assistants and other advanced electronics in a real, working store environment to set standards for the supermarket of the future.

Large RFID reader portals are placed at the store's dock door to track received goods, and in the corridor between the store's back room and the retail floor. Motion sensors determine whether the load of goods is moving to the retail floor or vice versa. Inventory levels are adjusted accordingly.

Electronic shelf labels display current prices of goods on the shelf. Unchanging information, such as the product name, is printed on a paper label affixed beneath the LCD display. From a computer in the back room or store headquarters, prices can be changed within seconds. In fact, all 40,000 SKUs in the Future Store can be changed in less than one hour.

RFID tags are attached by the store to each Pantene Pro-V product. Other products currently tagged include Kraft's Philadelphia cream cheese, Gillette Mach 3 razors and blades and all CDs and DVDs.

http://www.packagingdigest.com/articles/200507/40.php

Airplane mechanics utilize RFID to locate tools used for aircraft maintenance. After work is performed inside or outside of an aircraft a scan is performed to locate any tools set down.

- Airplane maintenance tools are very expensive and uniquely calibrated to ensure nuts and other mechanical devices are perfectly set. These tools are tagged to detail when the device has been certified and calibrated.

- Kanban just-in-time inventory for manufacturing and distribution is a popular methodology for keeping inventory costs low while delivering timely orders. When linked RDID it helps prevent obsolescence. RFID ensures that inventory supplies as part of a production “kit” is replenished to properly expedite an order.

Pharmaceutical companies have also been quick to see the benefits of RFID, primarily due to the track-and-trace and authentication tools the technology can provide to aid the industry in its fight against diversion, counterfeiting and management of expiration dates.

- Purdue Pharma of Stamford, Conn., for example, has an automated system to tag its OxyContin pain killer at the unit level. By the end of 2005, Pfizer Inc., … will tag cases and retail packages of Viagra, a product that has been a frequent victim of counterfeiting.
- GlaxoSmithKline…already tags product destined for METRO AG, an RFID-enabled retailer headquartered in Germany, as well as Wal-Mart's Texas distribution centers and will begin tagging at least one domestic product before mid-2006.
- Says David Pulman, president of global manufacturing and supply for GSK. “But this technology still requires development of industry-wide standards so that we can share information in a meaningful way.”

http://www.pmtdirect.com/website/article.asp?id=1276

Royal Canadian Mounted Police

The Canadian Mounted Police have structured an RFID implementation to readily track approximately 250 police cruisers and 800 deployed officers.

This RFID implementation is integrated into the prevention of unauthorized access to their facilities.

Design requirements include the technological ability to accurately transpond through extreme weather conditions such as dirt, grime, snow and also to process security access data promptly and precisely.

“RFID technology gives Kraft a level of flexibility and reliability that bar coding alone can not provide. The introduction of hands-off, ‘invisible’ scanning means no human intervention and 100 percent scanning compliance and accuracy,” said TrenStar’s Manager of Food Solutions Jim Krigbaum. “Food manufacturers can benefit immensely when RFID is used to capture data on location, dwell times and turn frequency on the IBC, thereby providing the necessary data to allow for improvement in production and inventory management within their supply chains.”

As part of the extended contract TrenStar will supplement existing bar codes with radio frequency identification (RFID) tags to track 800-liter stainless steel IBCs in use by Kraft suppliers.

TrenStarCM provides a precise level of data on each container and is fully Web-enabled to allow Kraft and its suppliers to view data that was previously uncollected and unanalyzed.

http://www.logisticstoday.com/sNO/5056/LT/displayStory.asp

Why RFID?

❑Business Efficiency
❑Business Intelligence
❑Supply chain management
❑Inventory replenishment
❑Decrease shrinkage
❑Compliance considerations
❑Systematic Processes
❑Direct integration to ERP systems
❑Precise tracking
❑Accurate identification
❑Identity management
❑Find your keys

What could possibly go wrong?!

- RFID Vendors to Launch Patent Pool **Some 20 providers of RFID technology have announced plans to create a patent pool, which could end confusion and contention over patent royalties.**

  By Mark Roberti

  Aug. 9, 2005—In what could be a major step toward resolving the ongoing confusion over radio frequency identification patents, nearly 20 providers of RFID technology have announced plans to form an intellectual property (IP) licensing consortium-essentially a patent pool-to make it easier for vendors to license patents, reduce risks for end users and provide a convenient way for patent holders to manage their IP.

  The consortium will be similar to those set up to manage patents for MPEG-2 and DVD technologies. The plan is to license intellectual property on a reasonable and nondiscriminatory (RAND) basis. Source say the consortium will likely charge one royalty fee on all RFID products based on EPCglobal's Gen 2 standard for the Electronic Product Code air interface protocol, as well as on International Organization for Standardization (ISO) protocols, and divide the revenue among the patent holders, based on the importance of their patents. The companies proposing the formation of the pool believe this will keep the cost of RFID equipment down, fostering adoption, and provide a way for companies to be compensated for their IP.

http://www.rfidjournal.com/article/articleview/1786/1/1/

Although the January 2005 deadline related to radio frequency identification (RFID) mandated by Wal-Mart Stores of Bentonville, Ark., has come and gone, packaging industry experts say that most suppliers are still relatively low on the technology curve and have yet to widely apply the tags in an automated fashion.

The degree of automation has, in many cases, lagged behind expectations.

“Most suppliers are manually applying labels in a slap-and-ship operations, but over time we anticipate much more strategic use of the technology,” Bauly says. A handful of packagers have taken the next step and automated the application of smart labels, but only a couple have announced they have integrated RFID to such a degree that the data generated can be used by other systems. Still, there are exceptions.

http://www.pmtdirect.com/website/article.asp?id=1276

Readability of tags

I am currently doing some testing of RFID products in our warehouse. I have been tagging cardboard boxes that have a PCB inside(the box dimensions are approx. 8x12x2 inches). I am currently testing the Symbol MC9000-G RFID handheld reader with passive Gen1 Class 1 tags from <vendor> that are packaged on a Zebra 4x6 inch label. I have been placing the boxes on shelves in the warehouse. I have not been able to read the tags on the boxes that are stacked directly behind the first row.

Has anyone had any success reading passive tags in a second row of boxes with a handheld reader?

Is there any inexpensive solutions to reading the tags that are buried in a stack of boxes?

Any help or advice you can offer will be greatly appreciated.

Real Time Location Systems

The technical material available does not help much.

It seems that <vendor> uses a TDOA triangulation technique over a dedicated channel.

My immediate questions are:

1. Can I mix-n-match 802.11b/g?
2. They claim outside reading range up to 1,000ft and 2mW power consumption. How about the data rate? How realistic is 1,000ft?
3. How do they deal with interference on the single channel they use? I am thinking to critical installation such that for Homeland Security

Can you or some one provide me some info on tags to use… if i put a tag at 902-928 MHz on item , how it will be read in europe at 865 - 867 and vice versa .., is'nt the tags also need to be compatible.

Do we have such tag label printer as well.

Also Asian countries are opening up different frequencies for RFID , in INDIA its 865 – 867 MHz with max 1 W TP, 4 W ERP and 200 kHz carrier bandwidth.

Good question! I don't know the answer, but maybe I can conjecture some of the answer...

<vendor> web site says their dual frequency support is "configurable"; I interpret that as meaning it operates in one mode or the other but not both at the same time. It is probably setable within program software, so that the application program within the reader could switch frequencies if a tag was sensed but it did not respond to a default frequency.

A survey of tags reveals that only one tag, a <vendor> designed for Metro (Euro), responds to both 869 & 915 Mhz frequencies. I interpret this as meaning the market has not yet demanded dual frequency tags, so you will need a separate tag for each frequency on a single carton/pallet, if the item is expected to handle dual standards. I don't know of any other reader that supports US/Euro standards than <vendor>, but they do make a short range reader for printers. I don't know if any printer company is incorporating this reader in their printer.

I suspect that a company like <company> in China may use 950MHz internally (and for Pacific Rim) and then add a 86X or 915 MHz tag depending on where the item is to be shipped.

Q: Is it possible to store significant amount of data on an RFID tag by using compression or some other means? I am looking store 500-1000 characters on the RFID tag which will give me critical inormation about the object which is being tagged.

A: You can have tag where you can store even 2kbits...

It really depends on the amount of data you wanted to store..
But the tag is more expensive is you have a huge memory space..

So it really depends on which type of tags, on which prices you wanted to work on (or even which frequency used) .

Dear RFID Mate,

Q: Can anyone share knowledge how to measure 125KHz and 13.56 MHz RFID Tags, such as resonant frequency, bandwidth and Q factor?

And what sort of measuring equipments should we have?

A: For that kind of measurement you need a rlc bridge or even a device which is called a LCZ meter, with which you can test the Q factor, the dissipation .... but only for your antenna..

Car key RFID chips cracked
Researchers successfully crack and emulate RFID tags designed to protect automobiles from thieves. *posted 11:00am EST Mon Jan 31*

- A funded team of graduate students at Johns Hopkins University reported this weekend that they successfully cracked the security in Digital Signature Transponders (DST) used in automobile ignition systems' "immobolizer" chips and the ExxonMobil SpeedPass system. The team developed a system made up of commercially-available components to break the 40-bit proprietary encryption utilized in 5 of these DSTs in under two hours.

  The team then developed software that could be implemented on a laptop computer to interact with DSTs in close proximity and extract the product code utilized by the device. With that information, the group was able to successfully purchase gasoline from ExxonMobil gas stations on a cracked SpeedPass account, as well as start an automobile that utilizes an immobilzer chip using a key that contains no chip.

http://www.geek.com/news/geeknews/2005Jan/gee20050131028905.htm

Counter Espionage and Current Investigations

“Security in search of the problem”

Obtaining tag data: reading fast moving inventory in your competitors RFID implementation, one can stock their business with that inventory

The ability to break code and obtain sensitive data

Spoof RFID attacks to obtain sensitive data

Good Source Material

3. Understanding Radio Frequency IDentification (RFID), R. Muroz, Ltd, http://www.rmoroz.com/rfid.html
4. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Klaus Finkenzeller
5. RFID Field Guide: Deploying Radio Frequency Identification Systems, Manish Buptani, Shahram Moradpour
6. RFID Radio Frequency Identification, Steven Sheppard
7. RFID Labeling: Smart Labeling Concepts & Applications for the Consumer Packaged Goods Supply Chain, Robert A. Kleist, Theodore A. Chapman, David A. Sakai, Brad S. Jarvis
8. Ready, willing and labeled? WalMart, Target, Metro and Albertsons are rolling with their RFID initiatives. But where does that leave the rest of the industry?, Food Logistics by John Karolefski

enCircle

Joan Ross, CISSP, NSA IAM, FCC Engineer

joanross@encirclecorp.com

206.605.3100

msi
systems integrators

RSM McGladrey

About Us | Services | Resources | Media | Careers | Events | Contact Us |